

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

FINJAN, INC., a Delaware Corporation)	
)	
Plaintiff,)	Redacted: Public Version
)	
v.)	C.A. No. 20-371-LPS
)	
TRUSTWAVE HOLDINGS, INC., a)	DEMAND FOR JURY TRIAL
Delaware Corporation and SINGAPORE)	
TELECOMMUNICATIONS LIMITED, a)	
Singapore Corporation,)	
)	
Defendants.)	

**FIRST AMENDED COMPLAINT FOR PATENT INFRINGEMENT
AGAINST DEFENDANTS AND BREACH OF CONTRACT AGAINST SINGTEL**

OF COUNSEL:
Bijal Vakil
WHITE & CASE LLP
3000 El Camino Real
2 Palo Alto Square, Suite 900
Palo Alto, CA 94306
(650) 213-0300

Dated: August 19, 2020

Karen E. Keller (No. 4489)
Jeff Castellano (No. 4837)
SHAW KELLER LLP
I.M. Pei Building
1105 North Market Street, 12th Floor
Wilmington, DE 19801
(302) 298-0700
kkeller@shawkeller.com
jcastellano@shawkeller.com
Attorneys for Plaintiff Finjan, Inc.

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

FINJAN, INC., a Delaware Corporation)	
)	
Plaintiff,)	Redacted: Public Version
)	
v.)	C.A. No. 20-371-LPS
)	
TRUSTWAVE HOLDINGS, INC., a)	DEMAND FOR JURY TRIAL
Delaware Corporation and SINGAPORE)	
TELECOMMUNICATIONS LIMITED, a)	
Singapore Corporation,)	
)	
Defendants.)	

**FIRST AMENDED COMPLAINT FOR PATENT INFRINGEMENT AGAINST
DEFENDANTS AND BREACH OF CONTRACT AGAINST SINGTEL**

1. Plaintiff Finjan, Inc. (“Finjan”), by and through its undersigned counsel, files this Complaint for Patent Infringement and Jury Demand against Trustwave Holdings, Inc. (“Trustwave”) and its parent entity, Singapore Telecommunications Limited (“Singtel”) (collectively, “Defendants”), and alleges as follows:

NATURE OF THE ACTION

2. This is a civil action for patent infringement arising under the patent laws of the United States, 35 U.S.C. § 100 *et seq.*, and for breach of contract under Delaware law.

3. Singtel and Trustwave have infringed literally or under the doctrine of equivalents, and continue to infringe, have contributed to, and continue to contribute to the infringement of, and have induced, and continue to induce the infringement of U.S. Patent No. 8,141,154 (“the ’154 Patent”) at least by making, using, selling, offering for sale and/or importing into the United States cybersecurity products and services that infringe one or more claims of the ’154 Patent. A true and correct copy of the ’154 Patent is attached as **Exhibit A**.

4. Finjan is the legal owner by assignment of the '154 Patent, which was duly and legally issued by the United States Patent and Trademark Office ("USPTO"). Finjan seeks monetary damages and injunctive relief to address ongoing and willful infringement by Defendants of the '154 Patent.

5. Finjan, Trustwave, and Singtel are parties to the Amended and Restated Patent License Agreement (the "Contract"), which was signed between Finjan and Trustwave in 2012, attached as **Exhibit B**. Finjan is the licensor of certain patents, not including the '154 Patent, pursuant to the Contract. Finjan licensed these patents to Trustwave, with express provisions that operate if Trustwave is acquired. Singtel acquired Trustwave (as defined by the Contract) on August 31, 2015, which now governs obligations by Singtel in addition to Trustwave.

6. Trustwave and Singtel owe patent royalties to Finjan pursuant to the Contract for certain Licensed Patents as identified in the Contract, not including the '154 Patent. As a result of Singtel's "Acquisition" of Trustwave on August 31, 2015, pursuant to Section 1.1 of the Contract, Singtel became an "Acquirer" under Section 1.1 of the Contract, while Trustwave became an "Affiliate" of the "Acquirer" (Singtel) under Section 1.3 of the Contract.

PARTIES

7. Finjan is a Delaware corporation with a principal place of business at 2000 University Avenue, Suite 600, East Palo Alto, California 94303.

8. Upon information and belief, Defendant Trustwave Holdings, Inc., is a Delaware corporation with a principal place of business at 70 W. Madison St., Suite 600, Chicago, Illinois 60602.

9. Upon information and belief, Defendant Singapore Telecommunications Limited is a corporation existing under the laws of Singapore with a principal place of business at 31 Exeter Road, Comcentre, Singapore, 239732.

JURISDICTION AND VENUE

10. This is a civil action for patent infringement arising under the Patent Act, 35 U.S.C. § 100 *et seq.* This Court has subject matter jurisdiction over this controversy pursuant to 28 U.S.C. §§ 1331 and 1338.

11. This Court has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) over the breach of contract claim against Singtel in this Complaint that arises under state law because the state law claim is so related to the exclusively federal patent claims that it forms part of the same case or controversy and derives from a common nucleus of operative facts. In fact, Trustwave has asserted in its breach of contract Counterclaim that Trustwave and Singtel are not liable for infringement of the '154 Patent based on the Contract, a federal patent defense.

12. This Court has personal jurisdiction over Defendants. This Court has personal jurisdiction over Trustwave because it is incorporated in the State of Delaware.

13. This Court also has personal jurisdiction over Trustwave and Singtel because they are parties to the Contract, which includes an express consent to jurisdiction in Delaware courts. Trustwave consented to jurisdiction when it signed the Contract in 2012. Singtel voluntarily became a party to the Contract as of its acquisition of Trustwave pursuant to Section 2.5 of the Contract, which states:

[REDACTED]

Therefore, both Trustwave and Singtel consented to personal jurisdiction in Section 6.4 of the Contract, which states:

[REDACTED]

[REDACTED]

This dispute arises out of and relates to the Contract by virtue of breach of various provisions, described above and detailed further below. Therefore, both Trustwave and Singtel consented to personal jurisdiction in this Court.

14. This Court also has personal jurisdiction over Singtel because it has established minimum contacts with the State of Delaware and the exercise of personal jurisdiction over Singtel would not offend traditional notions of fair play and substantial justice. Singtel is not only a party to the Contract that is the subject of this dispute, it purposefully availed itself of the laws of Delaware by acquiring Trustwave, a Delaware corporation. Singtel's acquisition of Trustwave at issue in this dispute has resulted in Singtel's integration of its cybersecurity capabilities, technologies, and resources under the Trustwave brand, a wholly owned Delaware subsidiary that sells the products at issue in this litigation, including in this District. For example, Trustwave's December 4, 2018 News Release states: "Singtel . . . has pooled the cybersecurity capabilities, technologies and resources of Singtel, Optus, Trustwave and NCS into a single global corporate identity operating under the Trustwave brand." *See Exhibit C* (<https://www.trustwave.com/en-us/company/newsroom/news/singtel-integrates-global-cybersecurity-capabilities-under-trustwave-to-create-an-industry-powerhouse/>).

15. Further, this Court also has personal jurisdiction over Singtel because it has purposefully availed itself of the privilege of conducting business activities in the State of Delaware through a number of subsidiaries besides Trustwave, including, but not limited to, Singtel USA, Inc. (registered agent at Corporation Trust Center, 1209 Orange Street, Wilmington, Delaware 19801), Singtel Enterprise Security (US), Inc. (registered agent at 251 Little Falls Drive, Wilmington, Delaware 19808), Singtel Communications LLC (registered agent at 108 West 13th Street, Wilmington, Delaware 19801), Singtel

Innov8 Ventures LLC (registered agent at Corporation Trust Center, 1209 Orange Street, Wilmington, Delaware 19801), Singtel Mobile Marketing, Inc. (registered agent at 251 Little Falls Drive, Wilmington, Delaware 19808), Amobee Inc. (registered agent at 850 New Burton Road Suite 201), Lucid Media Networks, Inc. (registered agent at Corporation Trust Center, 1209 Orange Street, Wilmington, Delaware 19801), and Pixable Inc. (registered agent at Corporation Trust Center, 1209 Orange Street, Wilmington, Delaware 19801).

16. Further, this Court also has personal jurisdiction over Singtel because it places its products into the stream of U.S. commerce through its subsidiaries (including Trustwave, a wholly owned Delaware subsidiary) that are incorporated in this District, including the products at issue in this case.

17. Also, this Court has personal jurisdiction over Singtel because Trustwave, Singtel's wholly owned subsidiary, acted as Singtel's agent in negotiating about amending the Contract and both Singtel's and Trustwave's obligations under the Contract. Even now, the same counsel represent both Trustwave and Singtel in this litigation.

18. Venue is proper in this Court pursuant to 28 U.S.C. §§ 1391(b)-(c) and 1400(b).

FINJAN'S INVENTIONS

19. Finjan was founded in 1997 as a wholly owned subsidiary of Finjan Software Ltd., an Israeli corporation. In 1998, Finjan moved its headquarters to San Jose, California. Finjan was, and has been recognized as, a pioneer in developing proactive security technologies capable of detecting previously unknown and emerging cybersecurity threats, recognized today under the umbrella term "malware." These technologies protect, among other things, networks and endpoints by identifying suspicious patterns and behaviors of content delivered over the Internet. Finjan has been granted numerous patents covering inventions in the United States and around the world

resulting directly from Finjan's more than decades-long research and development efforts, supported by a dozen inventors and more than US\$65 million in R&D investments.

20. Finjan built and sold software, including application program interfaces ("APIs") and appliances for network security, using these patented technologies. These products and related customers continue to be supported by Finjan's licensing partners. At its height, Finjan employed nearly 150 employees around the world building and selling security products and operating the Malicious Code Research Center, through which it frequently published research regarding network security and current threats on the Internet. Finjan's pioneering approach to cybersecurity drew equity investments from two major software and technology companies—the first in 2005, followed by the second in 2006. Finjan has generated millions of dollars in product sales and related services and support revenues. Additionally, Finjan has generated more than US\$350 million in revenue from over 25 patent licenses covering Finjan's patented inventions to date.

21. In 2015, Finjan formed Finjan Mobile, Inc. ("Finjan Mobile") to focus on cybersecurity in the mobile space. Finjan Mobile's first product, released in June 2015, was the Finjan Mobile Secure Browser. Featuring Finjan's patented inventions, including those from the '154 Patent, the Finjan Mobile Secure Browser is a simple-to-use, secure browser that protects users from potentially malicious Uniform Resource Locators ("URLs").

22. In October 2016, Finjan Mobile released the next version of its product—namely, the Gen3 VitalSecurity™ Browser. Finjan Mobile's Gen3 VitalSecurity™ Browser offered complete browser functionality while guarding users' privacy by not collecting any personal data. It also provided detailed analyses of virus and malware threats aggregated from more than 60 top virus companies. It also featured biometric and passcode security to further protect the users' experience. Finjan Mobile continued to update its VitalSecurity™ Browser product, releasing, for example, Gen 3.5 in April

2017, Gen 3.7 in June 2017, and Gen 4.0 in September 2017. Each upgrade to Finjan Mobile's VitalSecurity™ Browser product continued to embody Finjan's patented inventions, including the '154 Patent.

23. In addition to developing secure browser products, Finjan Mobile has also developed and released Virtual Private Network ("VPN") products. Finjan Mobile's first VPN product was incorporated into the VitalSecurity™ Gen 4.0 Secure Mobile Browser (also known as VitalSecurity™ VPN), which was the first fully functional browser with an integrated VPN for use on mobile platforms. In September 2018, Finjan Mobile released InvinciBull™, a stand-alone VPN mobile app that keeps global consumer data safe by encrypting all Internet traffic when using public Wi-Fi, such as in a coffee shop, a hotel, or an airport.

IMPACT OF FINJAN'S TECHNOLOGY ON TRUSTWAVE'S SUCCESS

24. One of the many companies that recognized the value of Finjan's products and technology was M86 Security, Inc. ("M86 Security"). In 2009, M86 Security entered into an agreement with Finjan whereby M86 Security would share revenues generated through the use of Finjan's technology, along with a nonexclusive license to practice certain Finjan patents ("Licensed Patents") to offer products and services. The Licensed Patents do not include the '154 Patent. Through this agreement, M86 Security continued Finjan's success through the use of the Licensed Patents in the cybersecurity marketplace.

25. Trustwave struggled to compete in the increasingly crowded cybersecurity marketplace. In 2010, Trustwave posted US\$4.6 million in losses despite recording US \$115 million in revenues and had to abandon its plans for an Initial Public Offering ("IPO"). See **Exhibit D** (<https://www.chicagobusiness.com/article/20110811/NEWS01/110819976/trustwave-postpones-ipo>).

26. In 2012, Trustwave acquired M86 Security. See **Exhibit E** (<https://www.trustwave.com/en-us/company/newsroom/news/trustwave-completes->

acquisition-of-m86-security/). With the acquisition, Trustwave gained access to M86 Security's valuable limited license to practice the Licensed Patents to offer products and services, including "Web and email security products," "[a]dvanced malware detection technology," and "[b]roader threat intelligence and security research," and gaining access to "M86 Security's more than 25,000 customers with 26 million users." *See Exhibit F* (<https://www.trustwave.com/en-us/company/newsroom/news/trustwave-to-acquire-m86-security/>).

27. Recognizing the important role of Finjan's patents to Trustwave's post-acquisition success, in 2012, Trustwave and Finjan voluntarily amended the 2009 M86 Security-Finjan license agreement, resulting in the Contract. The Contract does not include the '154 Patent.

28. The acquisition of M86 Security's products and services that practice Finjan's Licensed Patents catapulted Trustwave's presence in the cybersecurity marketplace. Upon information and belief, Trustwave's revenues in 2010 were US\$115 million. *See Exhibit D*. Within two years of the 2012 Contract, Trustwave's revenue nearly doubled to US \$216 million in 2014. *See Exhibit G* (<https://www.reuters.com/article/us-singtel-m-a-trustwave/singtel-buying-u-s-cyber-security-firm-trustwave-for-810-million-idUSKBN0MY2C820150408>).

SINGTEL'S ACQUISITION AND INTEGRATION OF TRUSTWAVE

29. The cybersecurity industry began to recognize Trustwave's success following its acquisition of M86 Security's products and services that practice Finjan's Licensed Patents. On or about August 31, 2015, Singtel purchased Trustwave for more than US\$810 million (nearly four times Trustwave's 2014 revenues) in order to enter the cybersecurity and, upon information and belief, Internet-of-Things ("IoT") markets on a global basis. *See Exhibit G*. Singtel's purchase included the Contract.

30. In fact, Trustwave's products and services were so successful that Singtel decided in or about 2018 to integrate all of its cybersecurity products and services under

the brand name “Trustwave,” recognizing the value of the Trustwave brand and Finjan’s patented inventions. *See Exhibit C* (“Singtel today announced that it has pooled the cybersecurity capabilities, technologies and resources of Singtel, Trustwave and NCS into a single global corporate identity operating under the Trustwave brand.”). Today, Trustwave operates as “the global cybersecurity arm of Singtel.” *Id.* Thus, Trustwave and Singtel have realized and enjoyed the value of Finjan’s Licensed Patents.

31. Singtel’s publicly available financial information includes Trustwave revenues as part of Singtel’s enterprise revenues. *See Exhibit H*, Singtel 2020 Fourth Quarter Financial Summary (<https://www.singtel.com/content/dam/singtel/investorRelations/financialResults/2020/Q4FY20-Hist-Summary.xlsx>). For example, Singtel recognized US\$112 million in revenue from Trustwave as part of Singtel’s enterprise revenues for the fourth quarter of 2020. *Id.* (“Group Enterprise” and “Group P&L by business” tabs).

ACTS GIVING RISE TO BREACH OF CONTRACT

32. The Contract is a binding contract for a worldwide, limited patent license supported by offer, acceptance and mutual consideration. Among other things, under Section 2.1.1 of the Contract, Finjan [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Parties to license agreements in high technology industries, such as cybersecurity, often negotiate for worldwide licenses in order to avoid the type of dispute before this Court.

33. Under the Contract, the parties pre-negotiated an acquisition provision. The parties agreed that [REDACTED]

[REDACTED]

[REDACTED] Specifically, Section 2.5 of the Contract

states:

[REDACTED]

34. Singtel performed due diligence prior to acquiring Trustwave sufficient to discover that Singtel would assume Trustwave's [REDACTED]

[REDACTED]

35. The only exception to the royalty obligations for the Licensee post-acquisition are [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Finjan does not seek royalties from the Licensee: either (1) Singtel for the "Existing Business," since, by definition, Singtel did not actually offer or distribute any Licensed Products or Services prior to the Acquisition, or (2) Trustwave, for the "Existing Business" for its Licensed Products and Services actually offered or distributed as of August 31, 2015, or modifications or updates to those Licensed Products or Services.

36. The royalty rate owed by the Licensee post-acquisition (both Singtel and its affiliate, Trustwave) is expressly defined by the Contract. Section 3.2.1 of the Contract, [REDACTED]

[REDACTED]

[REDACTED]

Pursuant to Sections 2.5 and 3.2.1 of the Contract, royalties of Net Sales would be due on

[REDACTED]

[REDACTED]

[REDACTED]

37. Further, in addition to the royalty due by the Licensee (both Singtel and its affiliate, Trustwave) under Section 3.3 of the Contract, [REDACTED]

[REDACTED]

38. The Contract also provides for [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] See Contract § 3.2.1.

39. The parties' course of conduct supports that royalties are owed post-acquisition. In May 2015, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

40. Finjan's points of contact with Trustwave during negotiations were Annabel Lewis, Trustwave's General Counsel (and eventual Singtel employee), and James Kunkel, Trustwave's Executive Vice President of Business Development and Strategy.

41. Annabel Lewis [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

42. Upon information and belief, Singtel was apprised of and involved with the license negotiations between Finjan and Trustwave through its agent, Trustwave, who was negotiating to become an Affiliate of Singtel pursuant to the Contract.

43. In a July 22, 2015 email, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

44. After extensive discussions of different licensing options, Annabel Lewis

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

45. Upon information belief, on August 31, 2015, Singtel completed its acquisition of Trustwave. At no time prior, during or after the acquisition did Singtel or Trustwave reject any of the numerous provisions of the Contract that applied to Singtel and its affiliate, Trustwave, such as Sections 1.1, 1.3, 1.8, 2.5, 3.2, 3.2.1, or the right to an audit under Section 3.4.

46. After Singtel completed its acquisition of Trustwave, even though Trustwave and Finjan had already substantially reached agreement regarding additional royalties, Trustwave suddenly, and without explanation, stopped responding in good faith to Finjan's emails and phone calls and repudiated its obligations under the Contract, further incurring additional costs and fees owed to Finjan for their failure to pay.

47. On September 15, 2015, [REDACTED]

[REDACTED]

[REDACTED]

48. Upon information and belief, Annabel Lewis transitioned from being Trustwave's General Counsel to being employed by Singtel as General Counsel in September, 2015 since Singtel had acquired Trustwave as an affiliate. *See Exhibit O*, Annabel Lewis LinkedIn profile (<https://www.linkedin.com/in/annabel-lewis-0b676a2/>). Annabel Lewis continued to represent both Trustwave and Singtel in negotiations with Finjan for an amendment to the Contract.

49. Similarly, Singtel's 2016 and 2017 Annual Reports listed Trustwave Chief Executive Officer, Robert J. McCullen as a member of Singtel's senior management team. *See Exhibit P*, Singtel 2016 Annual Report at 22 (<https://www.singtel.com/>

content/dam/singtel/investorRelations/annualReports/2016/Singtel_AR2016.pdf);
Exhibit Q Singtel 2017 Annual Report at 28 (<https://www.singtel.com/content/dam/singtel/investorRelations/annualReports/2017/singtelar17-full-AR.pdf>).

50. Annabel Lewis continued to represent both Trustwave and Singtel in negotiations with Finjan; however, subsequent to Singtel's acquisition of Trustwave, [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

51. In December, [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

52. Upon information and belief, James Kunkel informed Finjan that [REDACTED]

[REDACTED]
[REDACTED].

53. Upon information and belief, Singtel exerted its control over Trustwave to force its subsidiary to not to enter an amended Limited License. Instead, Singtel ordered Trustwave to repudiate Singtel's and Trustwave's contractual obligations to Finjan after Singtel acquired Trustwave.

54. On June 22, 2016, after radio silence from Trustwave and Singtel for months, Finjan requested an audit pursuant to Section 3.4 of the Contract for an accounting of the royalties resulting from Singtel's acquisition of Trustwave. Section 3.4 of the Contract states:

[REDACTED]

Finjan, Trustwave, and Singtel mutually agreed to retain KPMG as the independent accounting firm to perform the audit. Under the Agreement, Finjan initially paid for the audit; however, under Section 3.4, [REDACTED]

[REDACTED]

[REDACTED].

55. KPMG attempted to perform its established intellectual property audit, but Trustwave denied KPMG access to various, necessary, and customary information about Singtel and Trustwave, in violation of Section 3.4 of the Contract. Trustwave and Singtel—who on information and belief arranged to have personnel from its Singapore accounting office participate in overseeing KPMG’s audit—unilaterally dictated the scope of KPMG’s audit in violation of the Contract by, among other things, interfering with KPMG’s ability to conduct an independent audit and refusing KPMG access to pertinent sales and technical information on Trustwave’s security products. Trustwave insisted on postponing KPMG’s audit until Singtel personnel were present to supervise.

56. KPMG repeatedly asked Trustwave for access to sales and technical information on Singtel’s products; however, Trustwave steadfastly refused to provide any requested information on Singtel. Annabel Lewis continued to represent both Trustwave and Singtel throughout the audit process and was directly involved in preventing KPMG from conducting its independent inspection. *See* [REDACTED]

[REDACTED]

[REDACTED].

57. During the audit process, Mark Henrikson, then Senior Counsel to Trustwave, represented to the auditors at KPMG that [REDACTED]

58. KPMG determined that at least an additional US\$1,526,445.95 was due under the Agreement, even based solely on Net Sales by Singtel's affiliate, Trustwave. Even though KPMG was denied complete access to the books and records of the Licensee (Singtel and its affiliate, Trustwave), Finjan sought at least the amounts owed under Section 3.4 at that time. Due to the amount by which Trustwave was in underpayment, it was also required to pay for the audit, in the amount of US\$50,654.67. On October 1, 2017, Finjan requested payment of those fees and the cost of the audit, and asked that Trustwave advise whether it would pay by October 18, 2017. Trustwave first ignored and then refused to pay the royalty amounts or costs owed in accordance with the Contract.

60. Upon information and belief, Singtel acquired Trustwave in order to leverage and expand Trustwave’s products and services through Singtel’s global sales network. *See Exhibit P*, Singtel 2016 Annual Report at 4 (“Our acquisition of Trustwave last September brings with it a global customer base that we intend to build on and expand.”); page 7 (“A key priority for us this year is to leverage this Trustwave acquisition to create a global platform that can provide managed security services – 24/7.”); *see also* https://www.singtel.com/content/dam/singtel/investorRelations/annualReports/2016/Singtel_AR2016.pdf (2016 Annual Report).

61. Upon information and belief, Singtel immediately integrated and consolidated Trustwave's operations, sales, and marketing into that of Singtel and its other subsidiaries. *See Exhibit P*, Singtel 2016 Annual Report at 40 (including advertisement for "Singtel Managed Security Services, powered by Trustwave").

Singtel

**AN INFECTED COMPUTER
CAN SERIOUSLY HURT YOUR BUSINESS.**

Protect your business with Singtel Managed Security Services, powered by Trustwave. Beyond just anti-virus, we deliver email protection for your business. With Singtel Managed Security Services, you are protected before and during cyber attacks.

ONLY \$6.42/mth per user
Managed Security Services for computer and email protection

Defend
24/7 monitoring against all cyber threats for your office email and computers.

Inform
Daily summary of viruses and malware attacks that have been blocked.

Investigate
24/7 helpdesk and breach reporting to recover from attacks.

Get protection from cyber attacks now, call us at 1800-763-1111 or visit www.singtel.com/SecuritySolutionsSTA

Trustwave helps businesses fight cybercrime, protect data and reduce security risk. With cloud and managed security services, integrated technologies and a team of security experts, ethical hackers and researchers, Trustwave enables businesses to transform the way they manage their information security and compliance programs. More than three million businesses are enrolled in the Trustwave TrustKeeper® cloud platform, through which Trustwave delivers automated, efficient and cost-effective threat, vulnerability and compliance management.

A Singtel Company
Trustwave
Smart security on demand

1800-SM-S 1111 (1800-763-1111) Singtel Shop Concierge business.singtelshop.com

Terms and Conditions apply
Copyright © 2015 Singtel Telecommunications Ltd (STN). TM0070243. All rights reserved.

62. Singtel's 2016 Annual Report explicitly states that Trustwave was "consolidated" into Singtel on acquisition. *See Exhibit P*, Singtel 2016 Annual Report at 104.

63. Singtel's 2016 Annual Report lists Trustwave as a subsidiary of Singtel at page 218. Singtel defines a subsidiary as an entity "controlled by the Group . . . through

existing rights that give the Group the ability to direct activities that significantly affect the entity's returns." See **Exhibit P**, Singtel 2016 Annual Report at 138. "Subsidiaries are **consolidated** from the date that control commences until the date that control ceases. *All significant inter-company balances and transactions are eliminated on consolidation.*" *Id.* at 138 (emphasis added). This confirms Trustwave's representations during the first KPMG audit that "no Trustwave product is sold to SingTel." See **Exhibit U**, Email from R. Ballow to J. Mar-Spinola (Jan. 27, 2017).

64. Singtel continues to list Trustwave as a subsidiary in its reports using substantially the same definition of subsidiary. See **Exhibit V**, Singtel 2019 Annual Report at 151, 246 (<https://www.singtel.com/content/dam/singtel/investorRelations/annualReports/2019/singtel-annual-report-2019.pdf>). Under this definition, Trustwave is an "Affiliate" of Singtel under Section 1.3 of the Contract. Trustwave's status as an "Affiliate" has not changed since the August 31, 2015 Acquisition under Section 1.1 of the Contract.

65. Upon information and belief, Singtel has exerted its control over Trustwave to, for example, partner with other companies "to provide Trustwave's cyber security services in Japan to help businesses build cyber resilience and protect critical infrastructure." **Exhibit Q**, Singtel 2017 Annual Report at 3. Singtel's leveraging of Trustwave and its brand to create a global platform for cybersecurity products and services without paying any additional royalties to Finjan directly contravenes the intent of the Contract. See *id.* at 6 ("Cyber security is a high-growth sector where we have established a global platform by leveraging our acquisition of Trustwave, a U.S.-based leading managed security services provider. We are building out a global cyber security business which we expect to become a key growth driver in our future.") and at 47 ("Trustwave, our cyber security arm, provides managed security services, including comprehensive threat intelligence, threat data analytics, and advanced security automation for incident response, backed by its elite SpiderLabs team.").

66. Over time, Singtel has continued to consolidate Trustwave with itself and its subsidiaries. For example, “[i]n April 2018, the Group consolidated its cyber security operations across Singtel, Trustwave, Optus, and NCS into a single global unit to strengthen and scale the cyber business to accelerate growth.” See **Exhibit W**, Singtel 2018 Annual Report at 120 (<https://www.singtel.com/content/dam/singtel/investorRelations/annualReports/2018/singtel-annual-report-2018.pdf>). Singtel “[c]onsolidated cyber assets globally under the Trustwave brand to form one of the industry’s most comprehensive cyber security companies.” See **Exhibit V** Singtel 2019 Annual Report at 3, 5. Singtel has also integrated its cybersecurity operations with its subsidiaries, including Trustwave. See *id.* at 44 (“Our global network of Advanced Security Operations Centres is now supported by the new Trustwave SpiderLabs Fusion Centre in Chicago, a cutting-edge cyber security command centre providing unprecedented threat hunting capabilities through pioneering threat intelligence.”).

67. Singtel shares supervisory personnel between its cybersecurity subsidiaries, including with Trustwave. For example, Kevin Kilraine was Vice President at Singtel’s subsidiary, Optus, from August 2011 to April 2016. Then Mr. Kilraine served as Trustwave’s Chief Financial Officer from April 2016 to June 2018. Mr. Kilraine transferred back to Optus as Vice President of Finance and Transformation from June 2018 to the present. See **Exhibit X**, Kevin Kilraine LinkedIn profile (<https://www.linkedin.com/in/kevinkilraine>) (last accessed Aug. 15, 2020). Mr. Kilraine is currently featured on Trustwave’s website as its Chief Financial Officer. See Kevin Kilraine biography, <https://www.trustwave.com/en-us/resources/authors/kevin-kilraine> (last accessed Aug. 15, 2020).

68. Singtel’s subsidiaries market Trustwave products and services in set geographical areas using Singtel and its subsidiaries pooled resources and technology. For example, in Australia, “Optus Cybersecurity is now known as Trustwave, an Optus company.” See Optus Security, <https://www.optus.com.au/enterprise/security> (last

accessed Aug. 19, 2020). “[Singtel and its subsidiaries] have **pooled the resources** of Singtel, Optus, Trustwave and NCS, to create one of the industry’s most comprehensive global cybersecurity companies. *See* Optus Security, <https://www.optus.com.au/enterprise/security#trustwave> (last accessed Aug. 19, 2020) (emphasis added).

69. Upon information and belief, Singtel shares common procedures and controls to report financial data and prepare financial statements with its subsidiaries, including Trustwave. Singtel considers all its cybersecurity subsidiaries, including Trustwave, to constitute one consolidated cash generating unit for the purposes of audit controls and financial reporting. *See Exhibit V* at 133.

70. Finjan maintains that Trustwave and Singtel, including its subsidiaries, comprise one entity for the purposes of sales of cybersecurity products and services-related business decisions because:

- i. Singtel owns all or most of the stock of Trustwave;
- ii. Singtel consolidates its subsidiaries, including Trustwave, and all significant inter-company balances and transactions are eliminated on consolidation;
- iii. Singtel and Trustwave share common officers and directors; for example, Trustwave’s General Counsel, Annabel Lewis, was employed by Singtel starting in September 2015 and continued to act as Finjan’s main point of contact for negotiations of an amended Contract;
- iv. Singtel has integrated its own and its subsidiaries’ cybersecurity products and services under the Trustwave brand;
- v. Singtel and its subsidiaries share common use of the Trustwave trademark or logo;
- vi. Singtel and its subsidiaries share common use of employees, including as with Trustwave;

- vii. Singtel and its subsidiaries, including Trustwave, share an integrated sales system;
- viii. Singtel and its subsidiaries, including Trustwave, share supervisory personnel;
- ix. Singtel performs business functions through its subsidiaries, including Trustwave, which Finjan expected that a company like Singtel would conduct through its own agents; for example, negotiating an amended license agreement with Finjan that would cover Singtel and its subsidiaries other than Trustwave or asserting Singtel's rights under the Contract, Sections 1.1 and 1.3;
- x. Singtel and its subsidiaries conduct marketing on behalf of Trustwave and Trustwave's brand;
- xi. Singtel and its subsidiaries, including Trustwave, distribute Trustwave branded products and services in set geographical regions;
- xii. Singtel and its subsidiaries, including Trustwave, share security technology, methods, and processes, as well as Finjan's patented technology covered by the Contract;
- xiii. Singtel's subsidiaries, including Trustwave, receive instructions and form (or reject) contracts based on Singtel's instruction; for example, Trustwave's decision to reject its contractual obligations to Finjan based on Singtel's instruction; and
- xiv. Singtel shares common procedures and controls to report financial data and prepare financial statements with its subsidiaries, including Trustwave.

71. On information and belief, Singtel retains significant financial benefits from its total control over its subsidiaries. In 2019 alone, Singtel recorded at least

\$548.7 million in operating revenue from cybersecurity products and services sold by its subsidiaries, including Trustwave. On information and belief, some of this money may have come directly from sales of products and services that are royalty-bearing under the Contract.

72. Finjan and Trustwave have been involved in separate litigation regarding Trustwave's alleged breach of the Contract for the specific licensed patents. Finjan only brought suit against Trustwave to recover presently unpaid amounts under Section 3.4, since the KPMG audits only covered Trustwave's Net Sales, not Singtel's. *Finjan, Inc. v. Trustwave Holdings, Inc.*, C.A. No. N18C-04-006 WCC CCLD (Sup. Ct. Del.) ("*Finjan v. Trustwave*").

FINJAN'S U.S. PATENT NO. 8,141,154

73. On March 20, 2012, the USPTO issued to David Gruzman and Yuval Ben-Itzhak U.S. Patent No. 8,141,154, titled "SYSTEM AND METHOD FOR INSPECTING DYNAMICALLY GENERATED EXECUTABLE CODE." See **Exhibit A**.

74. All rights, title, and interest in the '154 Patent have been assigned to Finjan, who is the sole owner of the '154 Patent. Finjan has been the sole owner of the '154 Patent since its issuance. The '154 Patent has been posted on Finjan's website since as early as December 1, 2013.

75. The '154 Patent is generally directed towards a gateway computer protecting a client computer, such as a laptop, from dynamically generated malicious content. One of the ways this is accomplished is by using a content processor to process a first function and invoke a second function if a security computer indicates that it is safe to invoke the second function. The '154 Patent discloses and specifically claims inventive concepts that represent significant improvements over conventional network security technology that was available at the time of filing of the '154 Patent and are more than just generic software components performing conventional activities.

76. The '154 Patent has successfully withstood multiple invalidity challenges

over a number of years. To date, Finjan has successfully defended against seven petitions for *Inter Partes* Review (“IPR”) filed before the USPTO’s Patent Trial and Appeal Board (“PTAB”) challenging various claims of the ’154 Patent. Of those seven IPR petitions, four had all challenged claims upheld by the PTAB, and in some cases, by the Federal Circuit (IPR2015-01979, IPR2016-00151, IPR2016-01071, IPR2016-00919); two were denied institution (IPR2015-01547 and IPR2019-00031); and one was terminated due to settlement prior to institution (IPR2016-00937).

77. The ’154 Patent has also withstood validity challenges in another District Court. *See e.g., Finjan, Inc. v. Sophos Inc.*, Case No. 14-cv-1197-WHO, ECF No. 407 (N.D. Cal. Oct. 31, 2016) (finding claim 1 of the ’154 Patent not invalid and directly infringed).

78. The ’154 Patent is also being litigated before the Honorable Maryellen Noreika. Judge Noreika recently issued a Claim Construction Order construing certain terms of the ’154 Patent. *Finjan, Inc. v. Rapid7, Inc. et al.*, Case No. 18-cv-1519-MN, ECF No. 123 (D. Del. Feb. 5, 2020).

ACTS GIVING RISE TO PATENT INFRINGEMENT

79. As detailed below, Singtel and Trustwave have infringed literally or under the doctrine of equivalents, and continue to infringe, have contributed to, and continue to contribute to the infringement of, and have induced, and continue to induce the infringement of the ’154 Patent at least by making, using, selling, offering for sale and/or importing into the United States cybersecurity products and services that infringe one or more claims of the ’154 Patent. Defendants’ cybersecurity products and services sold under the Trustwave brand include, but are not limited to, Trustwave Secure Web Gateway and Trustwave Secure Email Gateway (“Accused Products”). Discovery may reveal additional Singtel or Trustwave products and services that practice the ’154 Patent, and Finjan hereby reserves the right to assert its patent infringement claims against such Singtel or Trustwave products and services.

80. Singtel and Trustwave received additional actual notice of the '154 Patent on or around November 1, 2015. On November 1, 2015, Finjan provided Trustwave a list of Finjan's patents for potential further licensing, which specifically identified the '154 Patent, as well as the Trustwave products that practiced such patents. Despite having knowledge that their products and services infringed unlicensed Finjan patents, Singtel and Trustwave have ignored, among others, Finjan's '154 Patent rights since that time.

81. On or around December 13, 2019, Finjan again communicated to Trustwave and Singtel that their products and services infringed and continue to infringe Finjan's '154 Patent. In a letter dated December 23, 2019, Finjan enclosed a proof chart setting forth in reasonable detail how the Accused Products infringed the '154 Patent. To date, neither Singtel nor Trustwave has responded to Finjan's letters or emails substantively.

COUNT I: DIRECT INFRINGEMENT OF U.S. PATENT NO. 8,141,154

82. Finjan re-alleges and incorporates by reference the allegations of the preceding paragraphs of this Complaint as if fully set forth herein.

83. Defendants infringed, and continue to infringe, at least Claim 1 of the '154 Patent in violation of 35 U.S.C. § 271(a).

84. Defendants' infringement is based upon literal infringement or, in the alternative, infringement under the doctrine of equivalents.

85. Defendants' acts of making, using, importing, selling and offering for sale infringing products and services were without the permission, consent, authorization, or license of Finjan.

86. Defendants' infringement includes the manufacture, use, offer for sale, sale, and importation of Defendants' Accused Products.

87. As shown below, the Accused Products practice the patented invention of the '154 Patent and infringed, and continue to infringe, at least Claim 1 of the '154 Patent

because they comprise, include or utilize a system for protecting a computer from dynamically generated malicious content, comprising (1) a content processor for processing content received over a network, the content including a call to a first function, and the call including an input, and for invoking a second function with the input, only if a security computer indicates that such invocation is safe; (2) a transmitter for transmitting the input to the security computer for inspection, when the first function is invoked; and (3) a receiver for receiving an indicator from the security computer whether it is safe to invoke the second function with the input.

88. For example, as shown below, the Trustwave Secure Email Gateway includes or utilizes a system for protecting a computer from dynamically generated malicious content.

<p style="text-align: center;">Make Email Safer</p> <p>Protecting your email environment against spam, malware, phishing attacks, business email compromise, account takeover, ransomware and more is one of your top priorities. Trustwave Secure Email Gateway multi-layered intelligence and detection engine performs deep analysis of your inbound email traffic, in real-time, to protect your users from cyber threats, enables you to integrate the workflow of your email content into business processes , while scrutinizing outbound email traffic to prevent your proprietary data, intellectual property, confidential documents and financial records from electronically leaving the building.</p>

Exhibit Y

(<https://www.trustwave.com/en-us/services/technology/secure-email-gateway/>)

<p>The Trustwave SEG Blended Threat Module uses a number of validation methods, including real-time behavioral analysis and content inspection as well as information from a number of industry standard sources, to identify and block sites that serve suspicious or malicious code.</p> <p>Because validation is performed in real time by a cloud service when a link is clicked, it provides superior effectiveness in catching and neutralizing new exploits for all users on any device from any location.</p>

Exhibit Y

89. The Trustwave Secure Email Gateway includes or utilizes a content processor (i) for processing content received over a network, the content including a call to a first function and the call including an input; and (ii) for invoking a second function with the input, only if a security computer indicates that such invocation is safe.

3 How Does the BTM Work?

The BTM functions as follows:

1. SEG scans email messages and rewrites URL links before delivering the email.
2. Clicking a link invokes the Trustwave Link Validator cloud service.
3. The Link Validator passes the URL to one or more validation services.
4. Depending on the results of validation, the Link Validator redirects the request to the original site, or blocks the request, as described below.

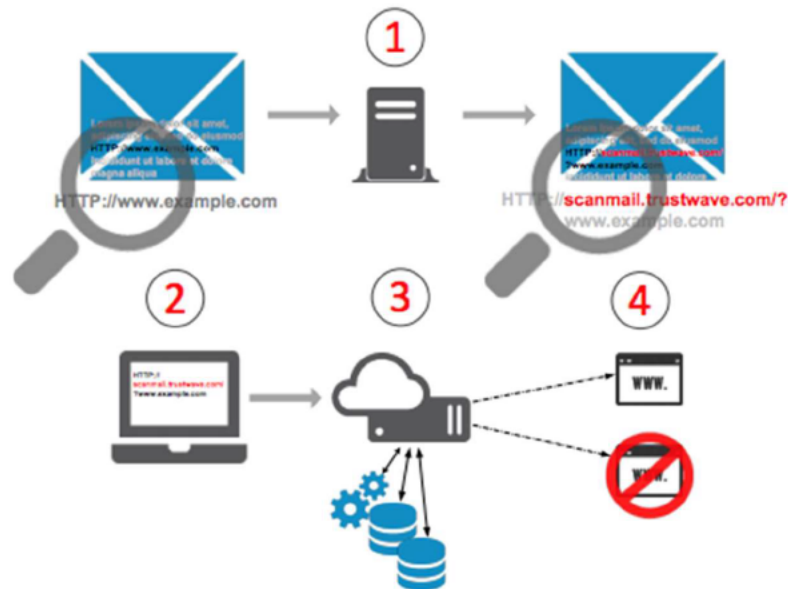


Exhibit Z

(https://www3.trustwave.com/software/MailMarshal SMTP/SEG_BT M_FAQ.pdf)

90. The Trustwave Secure Email Gateway includes or utilizes a transmitter for transmitting the input to the security computer for inspection when the first function is invoked.

When a user opens a message, if the message is displayed in plain text all links will be visibly altered. HTML messages will not be visibly altered, but hovering over a link shows the rewritten URL.

The URL of the Link Validator cloud service accessed by the email clients is:
<http://scanmail.trustwave.com/>

When the user clicks a link, the URL is passed to the Trustwave Link Validator for evaluation. An information page displays briefly.

Exhibit Z

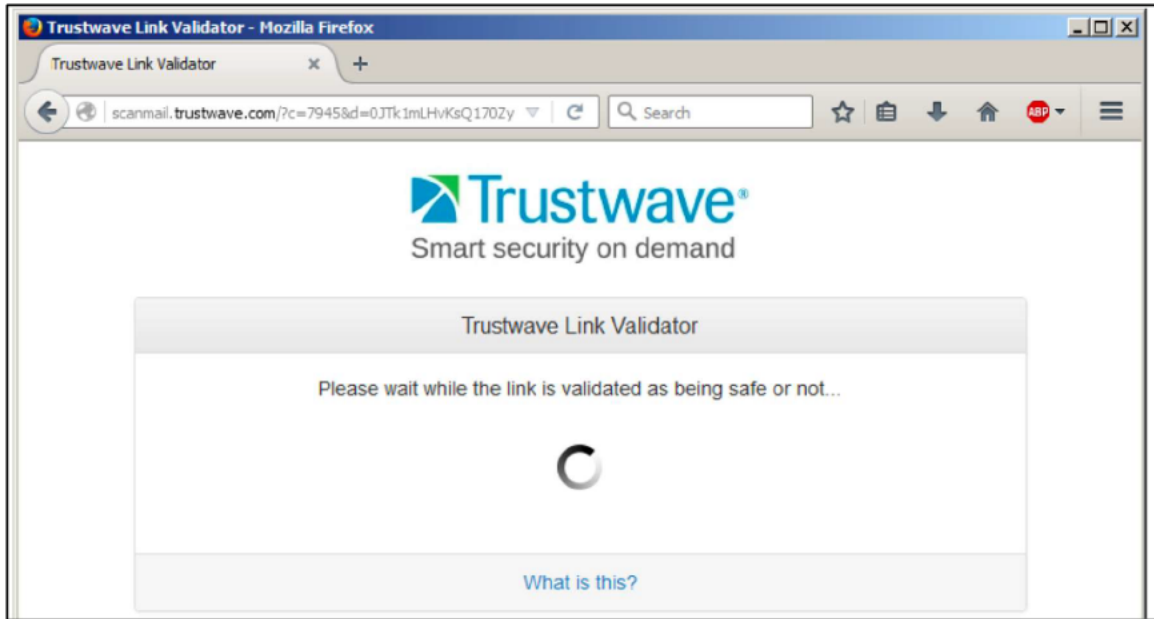


Exhibit Z

91. The Trustwave Secure Email Gateway includes or utilizes a receiver for receiving an indicator from the security computer whether it is safe to invoke the second function with the input.

If the result is "safe", the user is automatically redirected to the original URL.

If the result is "unsafe", a block page displays. In some cases a link with more specific information about the block source is included.

Exhibit Z

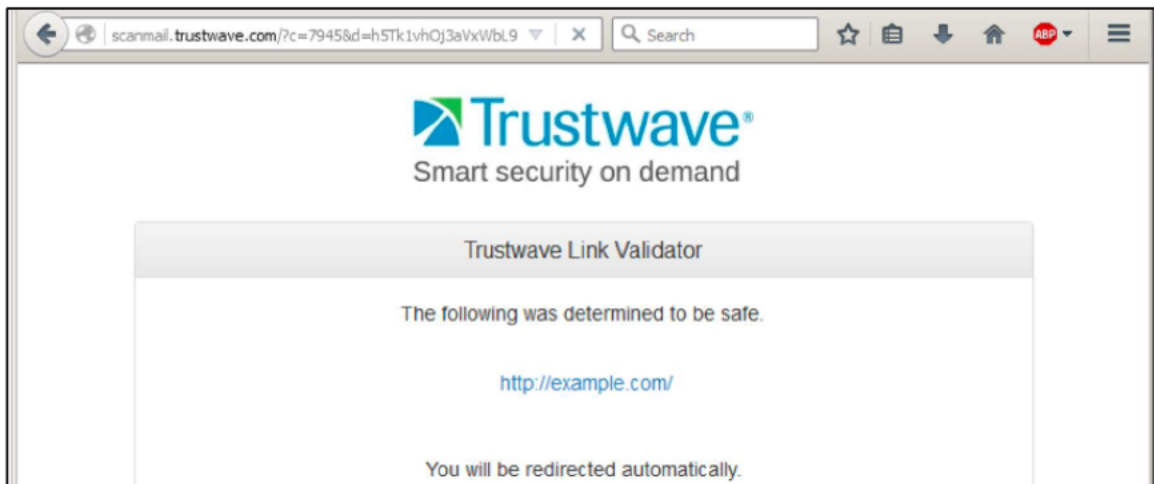


Exhibit HZ

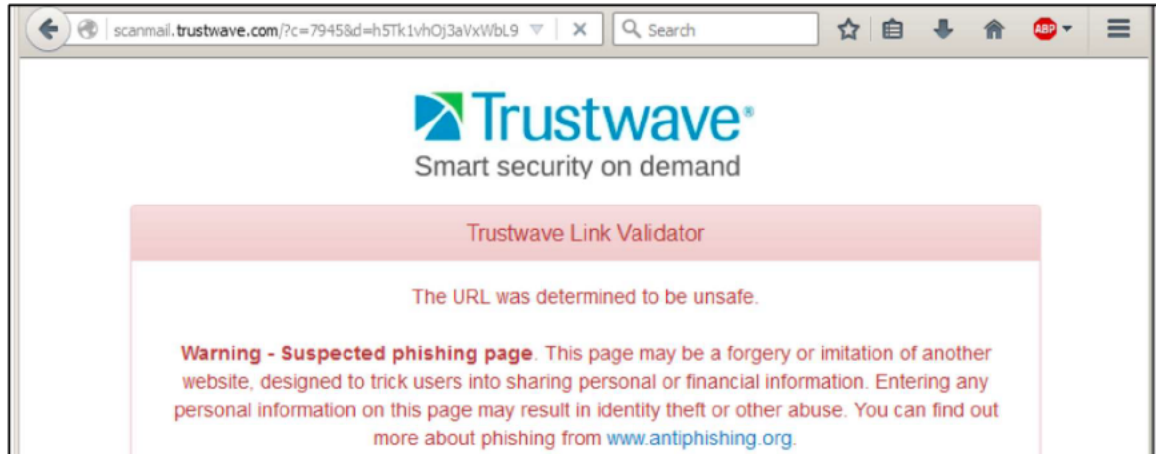


Exhibit Z

92. To the extent the Accused Products used and/or use a system that includes modules, components or software owned by third parties, the Accused Products still infringe the '154 Patent because Defendants are vicariously liable for the use of the patented system by controlling the entire system and deriving a benefit from the use of every element of the entire system.

93. Defendants' infringement has damaged and continues to damage Finjan in an amount yet to be determined, of at least a reasonable royalty. Further, Defendants' infringement also caused and continues to cause irreparable harm for which there is no adequate remedy at law. Finjan, Finjan's licensees, and Defendants all compete in the cybersecurity marketplace. Defendants' continued infringement is severely impeding Finjan's efforts to develop and provide competitive products and services in the cybersecurity marketplace. Defendants' continued infringement is also eroding the value of the patent licenses Finjan has conferred to its licensees.

94. Defendants have been aware of Finjan's patents, including the '154 Patent, for years and continued their unauthorized infringing activity despite this knowledge. As discussed above, Finjan notified Trustwave and Singtel regarding Defendants' infringement of the '154 Patent as early as November 2015. Even after being shown that their products infringe the '154 Patent, on information and belief, Defendants made no effort to avoid infringement. Instead, Defendants continued to incorporate their

infringing technology into their products and services, such as those identified in this Complaint. All of these actions demonstrate the Defendants' disregard for Finjan's patent rights. As such, Defendants acted recklessly, willfully, wantonly and deliberately engaged in acts of infringement of the '154 Patent, justifying an award to Finjan of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

COUNT II: INDIRECT INFRINGEMENT OF U.S. PATENT NO. 8,141,154

95. Finjan realleges and incorporates by reference the allegations of the preceding paragraphs of this Complaint as if fully set forth herein.

96. Defendants have indirectly infringed and continue to indirectly infringe—either by having induced or contributed to, and continuing to induce or contributing to the infringement of—at least Claim 1 of the '154 Patent in violation of 35 U.S.C. § 271(b) for inducement of infringement and 271(c) for contributory infringement.

97. Defendants indirectly infringe the '154 Patent by instructing, directing and/or requiring others, including, but not limited to, its customers, users and developers to use or include some of the components of the system claims, either literally or under the doctrine of equivalents, of the '154 Patent, where all components are included or utilized by Defendants or their customers, users or developers, or some combination thereof.

98. Defendants knew or were willfully blind to the fact that they were inducing others, including customers, users, and developers, to infringe by practicing, either themselves or in conjunction with Defendants, one or more claims of the '154 Patent.

99. Defendants knowingly and actively aided and abetted the direct infringement of the '154 Patent by instructing and encouraging its customers, users and developers to use the Accused Products, including the Trustwave Secure Email Gateway. Such instructions and encouragement include, but are not limited to, advising third parties

to use the Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the '154 Patent (*e.g.*, through the use of the Trustwave Secure Email Gateway), advertising and promoting the use of the Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the Accused Products in an infringing manner.

100. For example, Defendants provide customers, users and developers with case studies, e-books, datasheets, whitepapers, overviews, perspectives, tips and tricks, and other instructions advertising, promoting and encouraging the use of the Accused Products on its websites at trustwave.com and singtel.com (which redirects to trustwave.com). *See e.g.*, **Exhibit AA** (https://trustwave.azureedge.net/media/16574/secure-email-gateway-spe_letter-final.pdf?rnd=132260111910000000), **Exhibit AB** (<https://trustwave.azureedge.net/media/16425/secure-email-gateway-cloud.pdf?rnd=132180474070000000>).

COUNT III: BREACH OF CONTRACT AGAINST SINGTEL

101. Finjan realleges and incorporates by reference the allegations of the preceding paragraphs of this Complaint as if fully set forth herein.

102. Singtel is directly liable for royalties for all sales of products or services that would infringe on the licensed patents included in the Contract.

103. Singtel is liable for the non-payment of royalties pursuant to Section 3 of the Contract.

104. Both Singtel and its affiliate Trustwave are the Licensee under Sections 1, 2, and 3 of the Contract.

105. Both Singtel and its affiliate Trustwave are jointly and severally liable for the royalties owed under the Contract.

106. Both Singtel and its affiliate Trustwave have express payment obligations pursuant to Section 2.5 of the Contract, based on the August 31, 2015 Acquisition of Trustwave by Singtel that qualifies as an “Acquisition” under Section 1.1 and 1.3 of the

Contract.

107. Furthermore, Singtel is also liable for Trustwave's unpaid royalties on the licensed patents, because Trustwave acted as Singtel's agent during negotiations to amend the Contract.

108. Upon information and belief, Singtel directly oversaw the renegotiation process between Finjan and Trustwave and exerted its control over Trustwave during the negotiations.

109. Trustwave acted as Singtel's agent throughout the renegotiation process and subsequent breach of the Contract.

110. Singtel and its affiliate, Trustwave, breached the Contract by refusing to pay any royalties under the Contract in responses to third-party audits identifying payments owed by Trustwave. Following the October 18, 2017 KPMG audit, as well as subsequent audits and reviews, Singtel and Trustwave have refused to pay any royalties owed, or any of the audit costs as required under the Contract.

111. Singtel breached the Contract by refusing to provide Singtel's books and records in order to enable an audit under the Contract.

112. Singtel breached the Contract by refusing to pay any royalties under the Contract following a proper examination of its books and records in order to enable an audit under the Contract.

113. Since the prior audits of Singtel's affiliate, Trustwave, already determined that the royalty amounts were underpaid by at least US\$50,000, Singtel and its affiliate, Trustwave, owe for the payments for the audits made to KPMG.

114. Following the prior KPMG audit, as well as subsequent audits and reviews, Singtel and Trustwave have refused to pay any royalties owed, or any of the audit costs as required under the Contract.

115. Singtel's breach of the Contract has harmed Finjan, at least in the form of damages related to unpaid royalties and audit costs.

PRAYER FOR RELIEF

WHEREFORE, Finjan respectfully requests entry of judgment as follows:

- A. Declaring that Singtel has breached the Contract and is responsible for royalties under the licensed patents therein;
- B. Declaring that all amounts due under the Contract are owed by the Licensee post-acquisition by Singtel, from August 31, 2015 through the expiration of the Contract, which is the last day prior to expiration of any of the patents in Exhibit A to the Contract;
- C. Declaring that Defendants have infringed U.S. Patent No. 8,141,154, directly and indirectly, by way of inducement or contributory infringement, literally or under the doctrine of equivalents;
- D. Declaring that Defendants and all affiliates, employees, agents, officers, directors, attorneys, successors and assigns and all those acting on behalf of or in active concert or participation with any of them, be enjoined from infringing U.S. Patent No. 8,141,154 and from inducing the infringement of U.S. Patent No. 8,141,154, and for all further and proper injunctive relief pursuant to 35 U.S.C. § 283;
- E. An award of such past damages, not less than a reasonable royalty, that is sufficient to fully compensate Finjan for Defendants' infringement under 35 U.S.C. § 284;
- F. A finding that Defendants' infringement has been willful, wanton and deliberate, and that the damages against Defendants be increased up to treble on this basis or for any other basis in accordance with the law;
- G. A finding that this case is "exceptional" and an award to Finjan of its costs and reasonable attorneys' fees, as provided by 35 U.S.C. § 285;
- H. An accounting of all infringing sales and revenues, together with prejudgment and post-judgment interest from the first date of infringement of U.S. Patent No. 8,141,154; and

I. Such further and other relief as the Court may deem proper and just.

DEMAND FOR JURY TRIAL

Finjan hereby demands a jury trial on all issues so triable.

OF COUNSEL:

Bijal Vakil
WHITE & CASE LLP
3000 El Camino Real
2 Palo Alto Square, Suite 900
Palo Alto, CA 94306
(650) 213-0300

Dated: August 19, 2020

/s/ Jeff Castellano
Karen E. Keller (No. 4489)
Jeff Castellano (No. 4837)
SHAW KELLER LLP
I.M. Pei Building
1105 North Market Street, 12th Floor
Wilmington, DE 19801
(302) 298-0700
kkeller@shawkeller.com
jcastellano@shawkeller.com
Attorneys for Plaintiff Finjan, Inc.

CERTIFICATE OF SERVICE

I, Jeff Castellano, hereby certify that on August 19, 2020, this document was served on the persons listed below in the manner indicated:

BY EMAIL

Jack B. Blumenfeld
Alexandra M. Cumings
MORRIS, NICHOLS, ARSHT
& TUNNELL LLP
1201 North Market Street
P.O. Box 1347
Wilmington, DE 19899
(302) 658-9200
jblumenfeld@mnat.com
acumings@mnat.com

Jared A. Brandyberry
BAKER & HOSTETLER LLP
1801 California Street
Suite 4400
Denver, CO 80202
(303) 861-0600
jbrandyberry@bakerlaw.com

John S. Letchinger
Matthew J. Caccamo
BAKER & HOSTETLER LLP
One North Wacker Drive
Suite 4500
Chicago, IL 60606
(312) 416-6200
jletchinger@bakerlaw.com
mcaccamo@bakerlaw.com

/s/ Jeff Castellano
Karen E. Keller (No. 4489)
Jeff Castellano (No. 4837)
SHAW KELLER LLP
I.M. Pei Building
1105 North Market Street, 12th Floor
Wilmington, DE 19801
(302) 298-0700
kkeller@shawkeller.com
jcastellano@shawkeller.com
Attorneys for Plaintiff Finjan, Inc.

EXHIBIT A



US008141154B2

(12) **United States Patent**
Gruzman et al.

(10) **Patent No.:** **US 8,141,154 B2**
(45) **Date of Patent:** **Mar. 20, 2012**

(54) **SYSTEM AND METHOD FOR INSPECTING
DYNAMICALLY GENERATED EXECUTABLE
CODE**

(75) Inventors: **David Gruzman**, Ramat Gan (IL);
Yuval Ben-Itzhak, Tel Aviv (IL)

(73) Assignee: **Finjan, Inc.** (IL)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **12/814,584**

(22) Filed: **Jun. 14, 2010**

(65) **Prior Publication Data**

US 2010/0251373 A1 Sep. 30, 2010

(51) **Int. Cl.**
G06F 11/00 (2006.01)

(52) **U.S. Cl.** **726/22; 726/23; 726/24; 713/188**

(58) **Field of Classification Search** None
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,359,659	A	10/1994	Rosenthal	726/24
5,974,549	A	10/1999	Golan	726/23
5,983,348	A	11/1999	Ji	726/13
6,092,194	A	7/2000	Touboul	726/24
6,167,520	A	12/2000	Touboul	726/23
6,272,641	B1	8/2001	Ji	726/24
6,934,857	B1	8/2005	Bartleson et al.	726/5
6,965,968	B1	11/2005	Touboul	711/118
7,203,934	B2	4/2007	Souloglou et al.	717/146
7,287,279	B2	10/2007	Bertman et al.	726/23
7,313,822	B2	12/2007	Ben-Itzhak	726/24
7,739,682	B1 *	6/2010	Badenell	717/174
7,836,504	B2 *	11/2010	Ray et al.	726/24

2001/0005889	A1 *	6/2001	Albrecht	713/201
2002/0116635	A1	8/2002	Sheymov	726/24
2004/0133796	A1	7/2004	Cohen et al.	726/24
2004/0153644	A1	8/2004	McCorkendale et al.	713/156
2004/0158729	A1	8/2004	Szor	713/190
2005/0108562	A1	5/2005	Khazan et al.	726/23
2005/0149749	A1 *	7/2005	Van Brabant	713/200
2006/0015940	A1	1/2006	Zamir et al.	726/22
2006/0161981	A1	7/2006	Sheth et al.	726/22
2007/0016948	A1	1/2007	Dubrovsky et al.	726/22

* cited by examiner

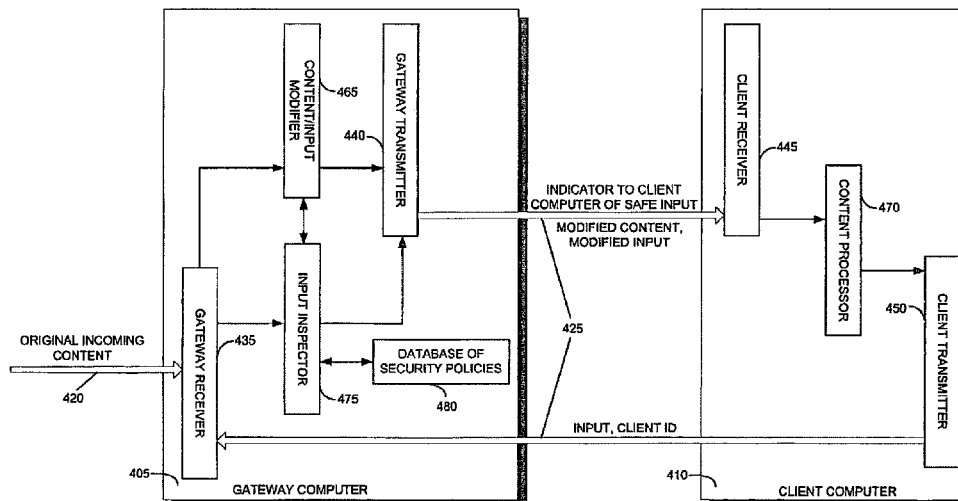
Primary Examiner — Ponnoreay Pich

(74) *Attorney, Agent, or Firm* — Dawn-Marie Bey; King & Spalding LLP

(57) **ABSTRACT**

A method for protecting a client computer from dynamically generated malicious content, including receiving at a gateway computer content being sent to a client computer for processing, the content including a call to an original function, and the call including an input, modifying the content at the gateway computer, including replacing the call to the original function with a corresponding call to a substitute function, the substitute function being operational to send the input to a security computer for inspection, transmitting the modified content from the gateway computer to the client computer, processing the modified content at the client computer, transmitting the input to the security computer for inspection when the substitute function is invoked, determining at the security computer whether it is safe for the client computer to invoke the original function with the input, transmitting an indicator of whether it is safe for the client computer to invoke the original function with the input, from the security computer to the client computer, and invoking the original function at the client computer with the input, only if the indicator received from the security computer indicates that such invocation is safe. A system and a computer-readable storage medium are also described and claimed.

12 Claims, 5 Drawing Sheets



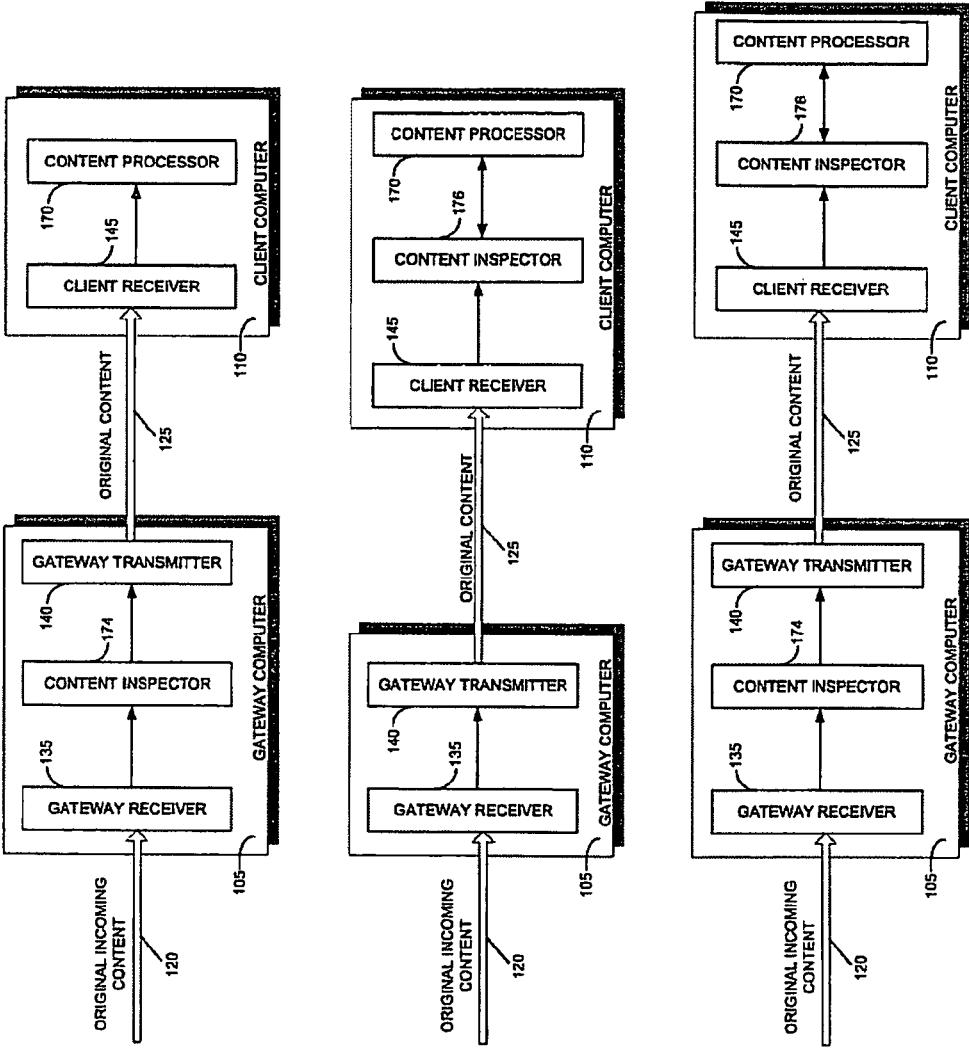


FIG. 1
(PRIOR ART)

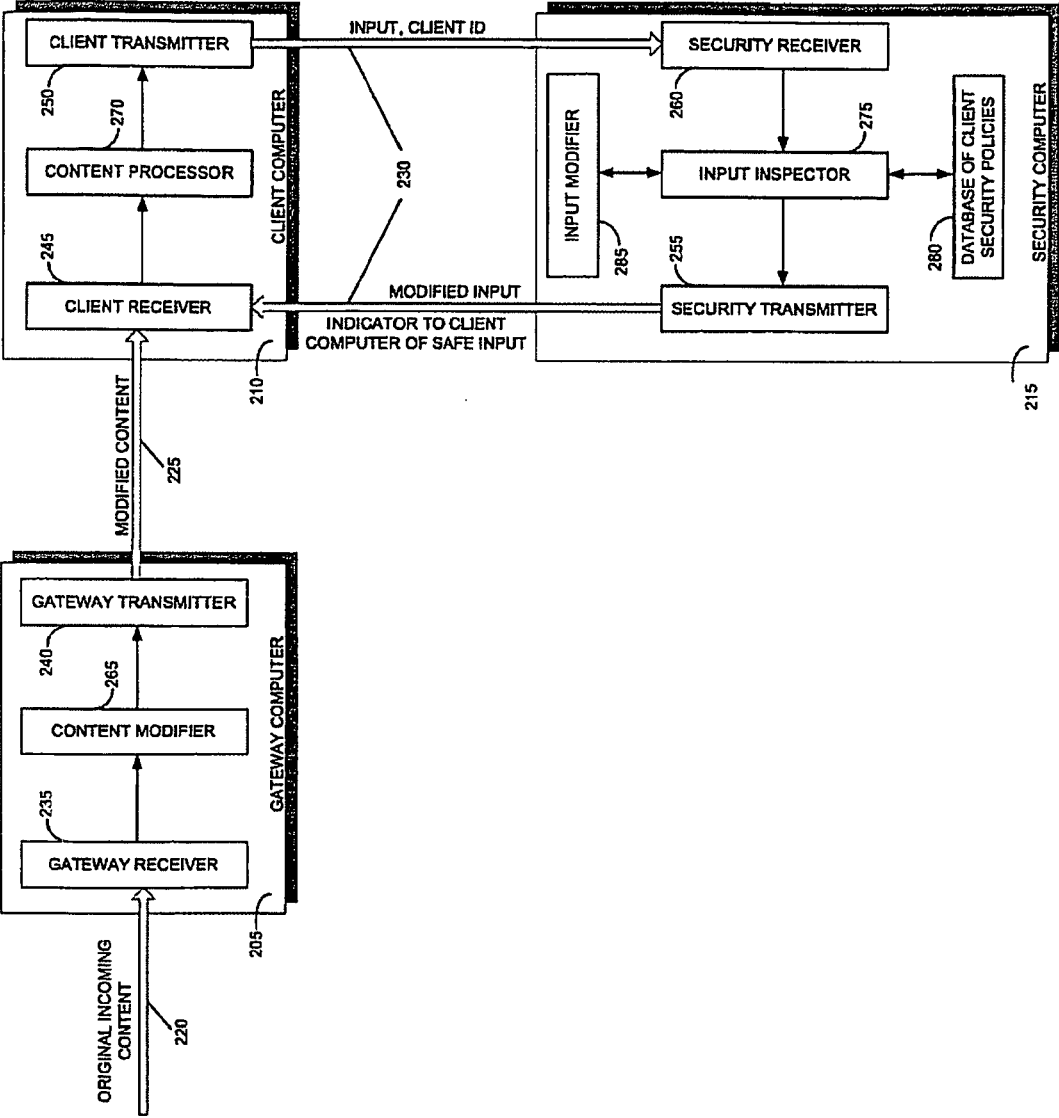


FIG. 2

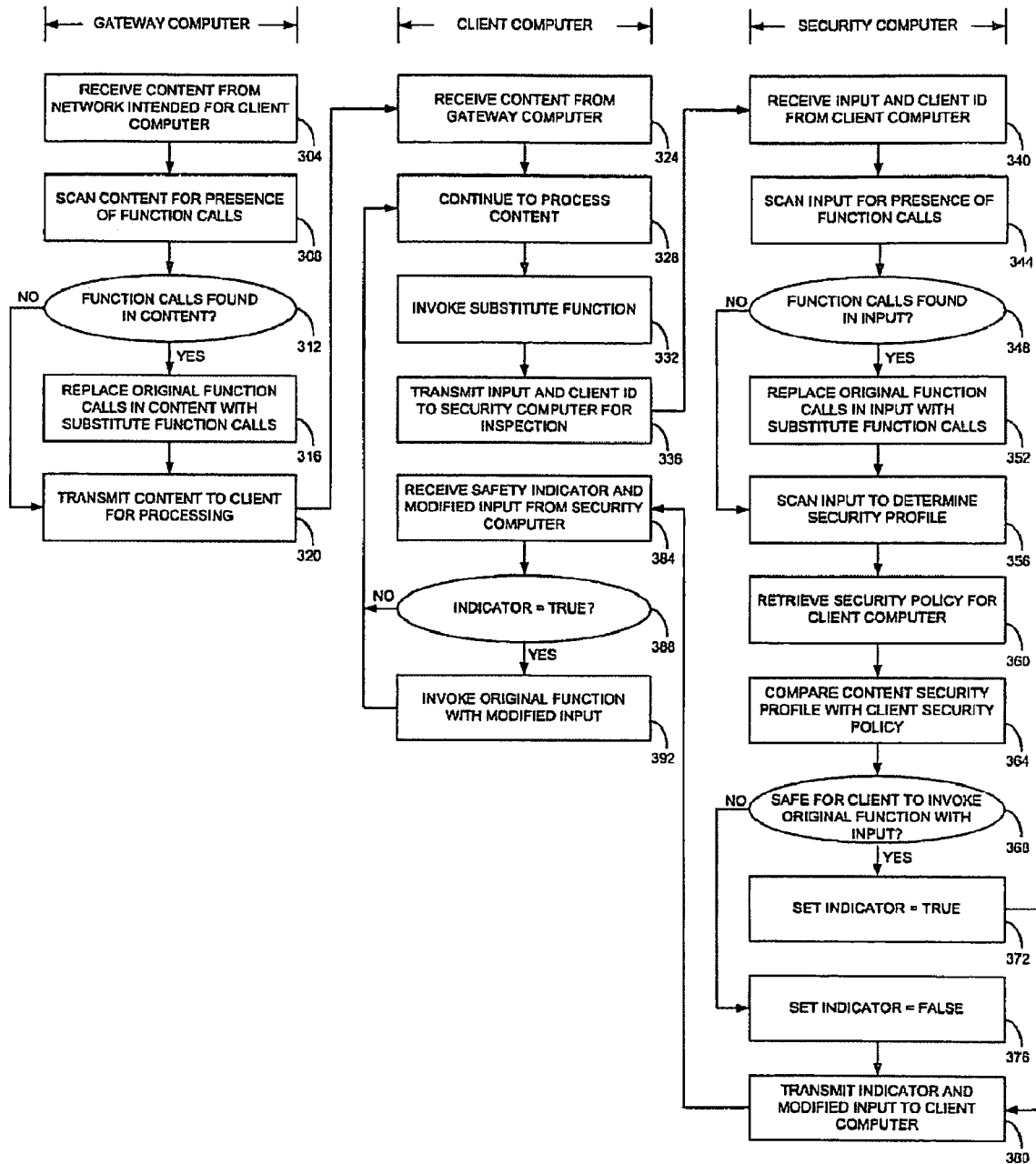


FIG. 3

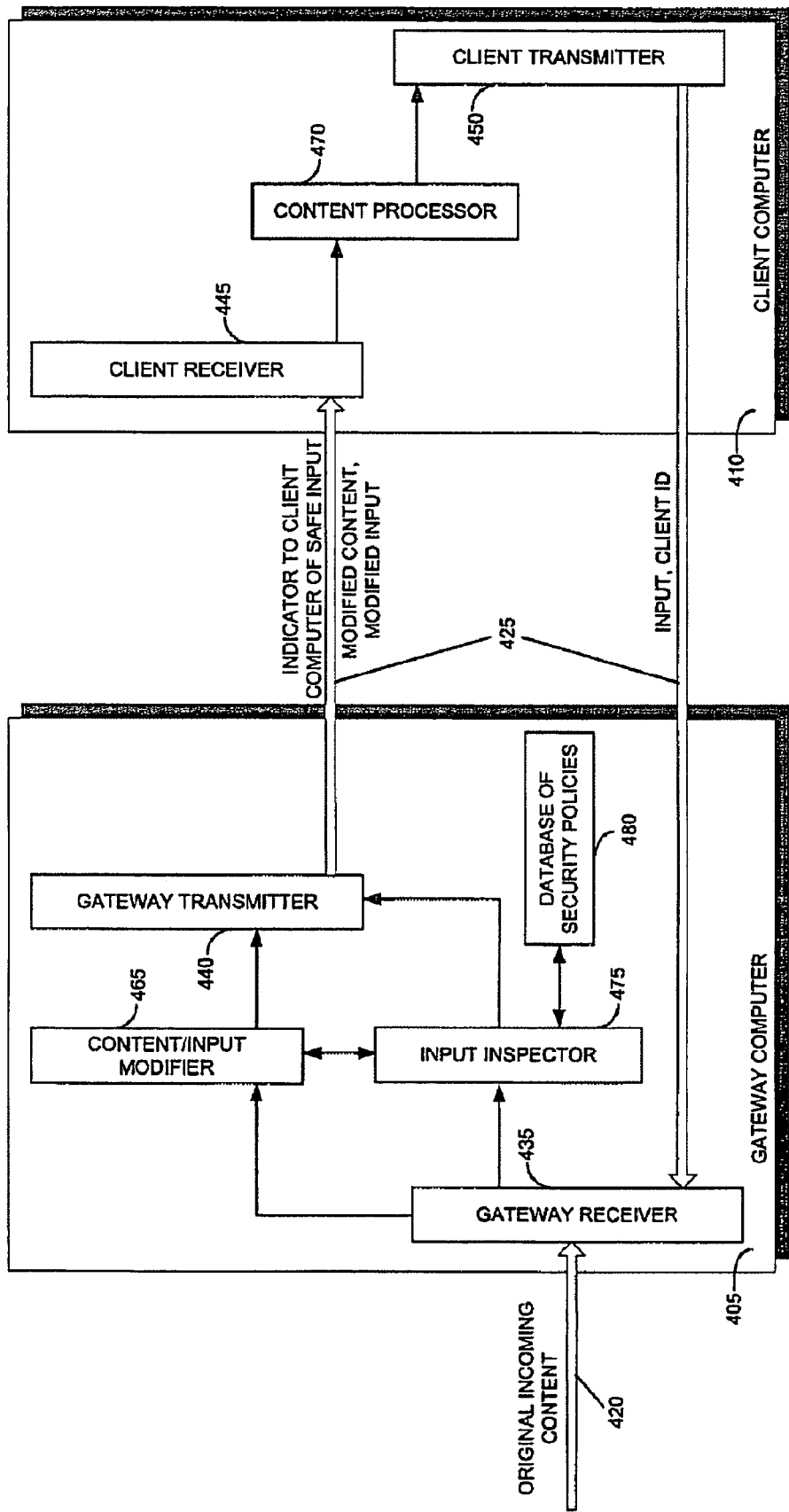


FIG. 4

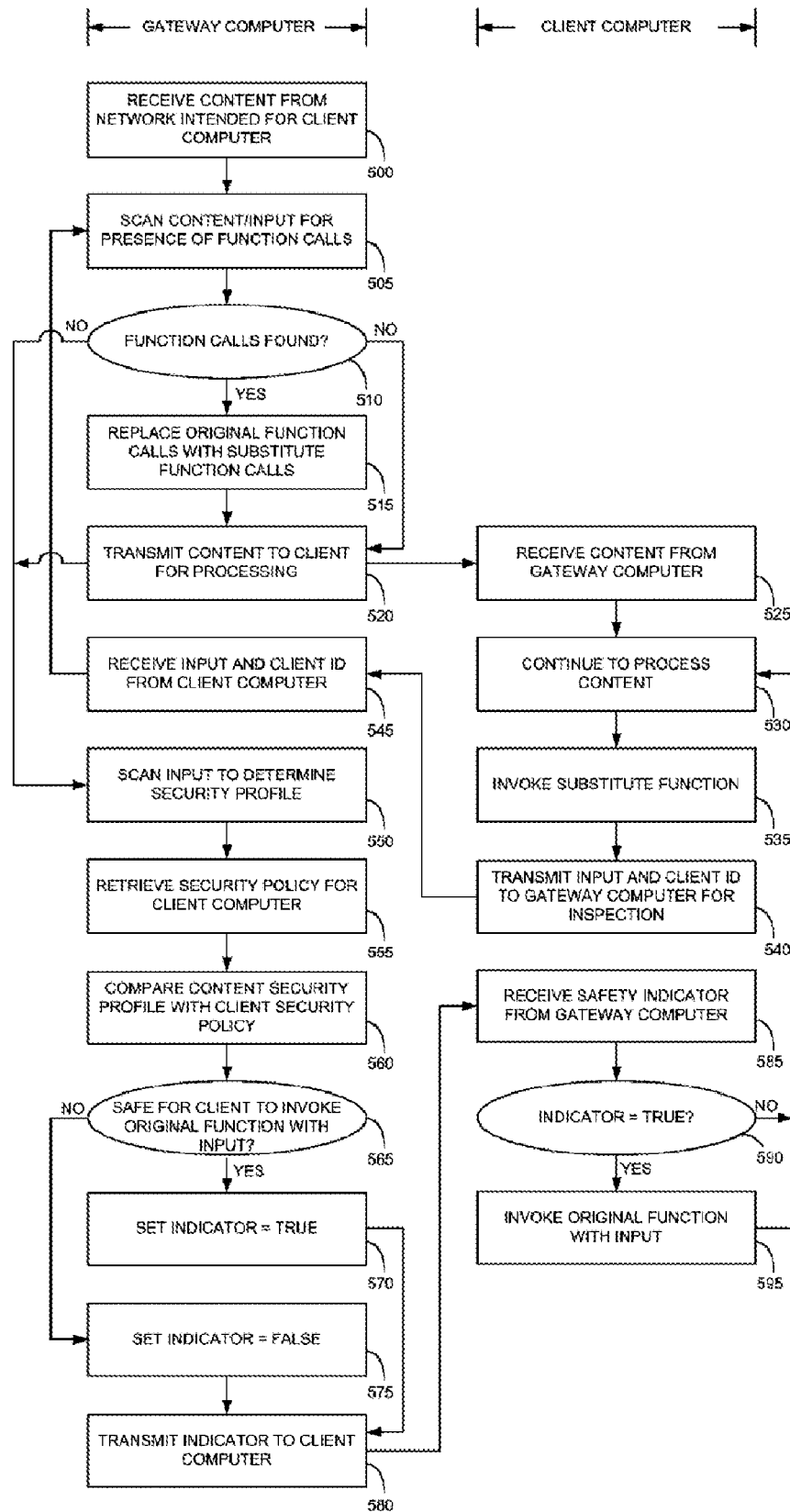


FIG. 5

US 8,141,154 B2

1

SYSTEM AND METHOD FOR INSPECTING DYNAMICALLY GENERATED EXECUTABLE CODE

FIELD OF THE INVENTION

The present invention relates to computer security, and more particularly to protection against malicious code such as computer viruses.

BACKGROUND OF THE INVENTION

Computer viruses have been rampant for over two decades now. Computer viruses generally come in the form of executable code that performs adverse operations, such as modifying a computer's operating system or file system, damaging a computer's hardware or hardware interfaces, or automatically transmitting data from one computer to another. Generally, computer viruses are generated by hackers willfully, in order to exploit computer vulnerabilities. However, viruses can also arise by accident due to bugs in software applications.

Originally computer viruses were transmitted as executable code inserted into files. As each new virus was discovered, a signature of the virus was collected by anti-virus companies and used from then on to detect the virus and protect computers against it. Users began routinely scanning their file systems using anti-virus software, which regularly updated its signature database as each new virus was discovered.

Such anti-virus protection is referred to as "reactive", since it can only protect in reaction to viruses that have already been discovered.

With the advent of the Internet and the ability to run executable code such as scripts within Internet browsers, a new type of virus formed; namely, a virus that enters a computer over the Internet and not through the computer's file system. Such Internet viruses can be embedded within web pages and other web content, and begin executing within an Internet browser as soon as they enter a computer. Routine file scans are not able to detect such viruses, and as a result more sophisticated anti-virus tools had to be developed.

Two generic types of anti-virus applications that are currently available to protect against such Internet viruses are (i) gateway security applications, and (ii) desktop security applications. Gateway security applications shield web content before the content is delivered to its intended destination computer. Gateway security applications scan web content, and block the content from reaching the destination computer if the content is deemed by the security application to be potentially malicious. In distinction, desktop security applications shield against web content after the content reaches its intended destination computer.

Moreover, in addition to reactive anti-virus applications, that are based on databases of known virus signatures, recently "proactive" antivirus applications have been developed. Proactive anti-virus protection uses a methodology known as "behavioral analysis" to analyze computer content for the presence of viruses. Behavior analysis is used to automatically scan and parse executable content, in order to detect which computer operations the content may perform. As such, behavioral analysis can block viruses that have not been previously detected and which do not have a signature on record, hence the name "proactive".

Assignee's U.S. Pat. No. 6,092,194 entitled SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES, the

2

contents of which are hereby incorporated by reference, describes gateway level behavioral analysis. Such behavioral analysis scans and parses content received at a gateway and generates a security profile for the content. A security profile is a general list or delineation of suspicious, or potentially malicious, operations that executable content may perform. The derived security profile is then compared with a security policy for the computer being protected, to determine whether or not the content's security profile violates the computer's security policy. A security policy is a general set of simple or complex rules, that may be applied logically in series or in parallel, which determine whether or not a specific operation is permitted or forbidden to be performed by the content on the computer being protected. Security policies are generally configurable, and set by an administrator of the computer that is being protected.

Assignee's U.S. Pat. No. 6,167,520 entitled SYSTEM AND METHOD FOR PROTECTING A CLIENT DURING RUNTIME FROM HOSTILE DOWNLOADABLES, the contents of which are hereby incorporated by reference, describes desktop level behavioral analysis. Desktop level behavioral analysis is generally implemented during runtime, while a computer's web browser is processing web content received over the Internet. As the content is being processed, desktop security applications monitor calls made to critical systems of the computer, such as the operating system, the file system and the network system. Desktop security applications use hooks to intercept calls made to operating system functions, and allow or block the calls as appropriate, based on the computer's security policy.

Each of the various anti-virus technologies, gateway vs. desktop, reactive vs. proactive, has its pros and cons. Reactive anti-virus protection is computationally simple and fast; proactive virus protection is computationally intensive and slower. Reactive anti-virus protection cannot protect against new "first-time" viruses, and cannot protect a user if his signature file is out of date; proactive anti-virus protection can protect against new "first-time" viruses and do not require regular downloading of updated signature files. Gateway level protection keeps computer viruses at a greater distance from a local network of computers; desktop level protection is more accurate. Desktop level protection is generally available in the consumer market for hackers to obtain, and is susceptible to reverse engineering; gateway level protection is not generally available to hackers.

Reference is now made to FIG. 1, which is a simplified block diagram of prior art systems for blocking malicious content, as described hereinabove. The topmost system shown in FIG. 1 illustrates a gateway level security application. The middle system shown in FIG. 1 illustrates a desktop level security application, and the bottom system shown in FIG. 1 illustrates a combined gateway+desktop level security application.

The topmost system shown in FIG. 1 includes a gateway computer 105 that receives content from the Internet, the content intended for delivery to a client computer 110. Gateway computer 105 receives the content over a communication channel 120, and gateway computer communicates with client computer 110 over a communication channel 125. Gateway computer 105 includes a gateway receiver 135 and a gateway transmitter 140. Client computer 110 includes a client receiver 145. Client computer generally also has a client transmitter, which is not shown.

Client computer 110 includes a content processor 170, such as a conventional web browser, which processes Internet content and renders it for interactive viewing on a display monitor. Such Internet content may be in the form of execut-

able code, JavaScript, VBScript, Java applets, ActiveX controls, which are supported by web browsers.

Gateway computer 105 includes a content inspector 174 which may be reactive or proactive, or a combination of reactive and proactive. Incoming content is analyzed by content inspector 174 before being transmitted to client computer 110. If incoming content is deemed to be malicious, then gateway computer 105 preferably prevents the content from reaching client computer 110. Alternatively, gateway computer 105 may modify the content so as to render it harmless, and subsequently transmit the modified content to client computer 110.

Content inspector 174 can be used to inspect incoming content, on its way to client computer 110 as its destination, and also to inspect outgoing content, being sent from client computer 110 as its origin.

The middle system shown in FIG. 1 includes a gateway computer 105 and a client computer 110, the client computer 110 including a content inspector 176. Content inspector 176 may be a conventional Signature-based anti-virus application, or a run-time behavioral based application that monitors run-time calls invoked by content processor 170 to operating system, file system and network system functions.

The bottom system shown in FIG. 1 includes both a content inspector 174 at gateway computer 105, and a content inspector 176 at client computer 110. Such a system can support conventional gateway level protection, desktop level protection, reactive anti-virus protection and proactive anti-virus protection.

As the hacker vs. anti-virus protection battle continues to wage, a newer type of virus has sprung forward; namely, dynamically generated viruses. These viruses are themselves generated only at run-time, thus thwarting conventional reactive analysis and conventional gateway level proactive behavioral analysis. These viruses take advantage of features of dynamic HTML generation, such as executable code or scripts that are embedded within HTML pages, to generate themselves on the fly at runtime.

For example, consider the following portion of a standard HTML page:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0  
Transitional//EN">  
<HTML>  
  <SCRIPT LANGUAGE="JavaScript">  
    document.write("<h1>text that is generated at run-time</h1>");  
  </SCRIPT>  
<BODY>  
</BODY>  
</HTML>
```

The text within the <SCRIPT> tags is JavaScript, and includes a call to the standard function document.write(), which generates dynamic HTML. In the example above, the function document.write() is used to generate HTML header text, with a text string that is generated at run-time. If the text string generated at run-time is of the form <SCRIPT>malicious JavaScript</SCRIPT> then the document.write() function will insert malicious JavaScript into the HTML page that is currently being rendered by a web browser. In turn, when the web browser processes the inserted text, it will perform malicious operations to the client computer.

Such dynamically generated malicious code cannot be detected by conventional reactive content inspection and conventional gateway level behavioral analysis content inspection,

since the malicious JavaScript is not present in the content prior to run-time. A content inspector will only detect the presence of a call to Document.write() with input text that is yet unknown. If such a content inspector were to block all calls to Document.write() indiscriminately, then many harmless scripts will be blocked, since most of the time calls to Document.write() are made for dynamic display purposes only.

U.S. Pat. Nos. 5,983,348 and 6,272,641, both to Ji, describe reactive client level content inspection, that modifies downloaded executable code within a desktop level anti-virus application. However, such inspection can only protect against static malicious content, and cannot protect against dynamically generated malicious content.

Desktop level run-time behavioral analysis has a chance of shielding a client computer against dynamically generated malicious code, since such code will ultimately make a call to an operating system function. However, desktop anti-virus protection has a disadvantage of being widely available to the hacker community, which is always eager to find vulnerabilities. In addition, desktop anti-virus protection has a disadvantage of requiring installation of client software.

As such, there is a need for a new form of behavioral analysis, which can shield computers from dynamically generated malicious code without running on the computer itself that is being shielded.

SUMMARY OF THE DESCRIPTION

The present invention concerns systems and methods for implementing new behavioral analysis technology. The new behavioral analysis technology affords protection against dynamically generated malicious code, in addition to conventional computer viruses that are statically generated.

The present invention operates through a security computer that is preferably remote from a client computer that is being shielded while processing network content. During run-time, while processing the network content, but before the client computer invokes a function call that may potentially dynamically generate malicious code, the client computer passes the input to the function to the security computer for inspection, and suspends processing the network content pending a reply back from the security computer. Since the input to the function is being passed at run-time, it has already been dynamically generated and is thus readily inspected by a content inspector. Referring to the example above, were the input to be passed to the security computer prior to run-time, it would take the form of indeterminate text; whereas the input passed during run-time takes the determinate form <SCRIPT>malicious JavaScript</SCRIPT>, which can readily be inspected. Upon receipt of a reply from the security computer, the client computer resumes processing the network content, and knows whether to by-pass the function call invocation.

To enable the client computer to pass function inputs to the security computer and suspend processing of content pending replies from the security computer, the present invention operates by replacing original function calls with substitute function calls within the content, at a gateway computer, prior to the content being received at the client computer.

The present invention also provides protection against arbitrarily many recursive levels of dynamic generation of malicious code, whereby such code is generated via a series of successive function calls, one within the next.

By operating through the medium of a security computer, the present invention overcomes the disadvantages of desktop anti-virus applications, which are available to the hacker

US 8,141,154 B2

5

community for exploit. Security applications embodying the present invention are concealed securely within managed computers.

There is thus provided in accordance with a preferred embodiment of the present invention a method for protecting a client computer from dynamically generated malicious content, including receiving at a gateway computer content being sent to a client computer for processing, the content including a call to an original function, and the call including an input, modifying the content at the gateway computer, including replacing the call to the original function with a corresponding call to a substitute function, the substitute function being operational to send the input to a security computer for inspection, transmitting the modified content from the gateway computer to the client computer, processing the modified content at the client computer, transmitting the input to the security computer for inspection when the substitute function is invoked, determining at the security computer whether it is safe for the client computer to invoke the original function with the input, transmitting an indicator of whether it is safe for the client computer to invoke the original function with the input, from the security computer to the client computer, and invoking the original function at the client computer with the input, only if the indicator received from the security computer indicates that such invocation is safe.

There is further provided in accordance with a preferred embodiment of the present invention a system for protecting a client computer from dynamically generated malicious content, including a gateway computer, including a gateway receiver for receiving content being sent to a client computer for processing, the content including a call to an original function, and the call including an input, a content modifier for modifying the received content by replacing the call to the original function with a corresponding call to a substitute function, the substitute function being operational to send the input to a security computer for inspection, and a gateway transmitter for transmitting the modified content from the gateway computer to the client computer, a security computer, including a security receiver for receiving the input from the client computer, an input inspector for determining whether it is safe for the client computer to invoke the original function with the input, and a security transmitter for transmitting an indicator of the determining to the client computer, and a client computer communicating with the gateway computer and with the security computer, including a client receiver for receiving the modified content from the gateway computer, and for receiving the indicator from the security computer, a content processor for processing the modified content, and for invoking the original function only if the indicator indicates that such invocation is safe; and a client transmitter for transmitting the input to the security computer for inspection, when the substitute function is invoked.

There is yet further provided in accordance with a preferred embodiment of the present invention a computer-readable storage medium storing program code for causing at least one computing device to receive content including a call to an original function, and the call including an input, replace the call to the original function with a corresponding call to a substitute function, the substitute function being operational to send the input for inspection, thereby generating modified content, process the modified content, transmit the input for inspection, when the substitute function is invoked while processing the modified content, and suspend processing of the modified content, determine whether it is safe to invoke the original function with the input, transmit an indicator of whether it is safe for a computer to invoke the original function with the input, and resume processing of the modified

6

content after receiving the indicator, and invoke the original function with the input only if the indicator indicates that such invocation is safe.

There is additionally provided in accordance with a preferred embodiment of the present invention a method for protecting a client computer from dynamically generated malicious content, including receiving content being sent to a client computer for processing, the content including a call to an original function, and the call including an input, modifying the content, including replacing the call to the original function with a corresponding call to a substitute function, the substitute function being operational to send the input to a security computer for inspection, and transmitting the modified content to the client computer for processing.

There is moreover provided in accordance with a preferred embodiment of the present invention a system for protecting a client computer from dynamically generated malicious content, including a receiver for receiving content being sent to a client computer for processing, the content including a call to an original function, and the call including an input, a content modifier for modifying the received content by replacing the call to the original function with a corresponding call to a substitute function, the substitute function being operational to send the input to a security computer for inspection, and a transmitter for transmitting the modified content to the client computer.

There is further provided in accordance with a preferred embodiment of the present invention a computer-readable storage medium storing program code for causing a computing device to receive content including a call to an original function, and the call including an input, and replace the call to the original function with a corresponding call to a substitute function, the substitute function being operational to send the input for inspection.

There is yet further provided in accordance with a preferred embodiment of the present invention a method for protecting a client computer from dynamically generated malicious content, including receiving content being sent to a client computer for processing, the content including a call to an original function, and the call including an input, modifying the content, including replacing the call to the original function with a corresponding call to a substitute function, the substitute function being operational to send the input for inspection, transmitting the modified content to the client computer for processing, receiving the input from the client computer, determining whether it is safe for the client computer to invoke the original function with the input, and transmitting to the client computer an indicator of whether it is safe for the client computer to invoke the original function with the input.

There is additionally provided in accordance with a preferred embodiment of the present invention a system for protecting a client computer from dynamically generated malicious content, including a receiver (i) for receiving content being sent to a client computer for processing, the content including a call to an original function, and the call including an input, and (ii) for receiving the input from the client computer, a content modifier for modifying the received content by replacing the call to the original function with a corresponding call to a substitute function, the substitute function being operational to send the input for inspection, an input inspector for determining whether it is safe for the client computer to invoke the original function with the input, and a transmitter (i) for transmitting the modified content to the client computer, and (ii) for transmitting an indicator of the determining to the client computer.

There is moreover provided in accordance with a preferred embodiment of the present invention a computer-readable

US 8,141,154 B2

7

storage medium storing program code for causing a computing device to receive content including a call to an original function, and the call including an input, replace the call to the original function with a corresponding call to a substitute function, the substitute function being operational to send the input for inspection, and determine whether it is safe for a computer to invoke the original function with the input.

There is further provided in accordance with a preferred embodiment of the present invention a method for protecting a computer from dynamically generated malicious content, including processing content received over a network, the content including a call to a first function, and the call including an input, transmitting the input to a security computer for inspection, when the first function is invoked, receiving from the security computer an indicator of whether it is safe to invoke a second function with the input, and invoking the second function with the input, only if the indicator indicates that such invocation is safe.

There is yet further provided in accordance with a preferred embodiment of the present invention a system for protecting a computer from dynamically generated malicious content, including a content processor (i) for processing content received over a network, the content including a call to a first function, and the call including an input, and (ii) for invoking a second function with the input, only if a security computer indicates that such invocation is safe, a transmitter for transmitting the input to the security computer for inspection, when the first function is invoked, and a receiver for receiving an indicator from the security computer whether it is safe to invoke the second function with the input.

There is additionally provided in accordance with a preferred embodiment of the present invention a computer-readable storage medium storing program code for causing a computing device to process content received over a network, the content including a call to a first function, and the call including an input, transmit the input for inspection, when the first function is invoked, and suspend processing of the content, receive an indicator of whether it is safe to invoke a second function with the input, and resume processing of the content after receiving the indicator, and invoke the second function with the input only if the indicator indicates that such invocation is safe.

There is moreover provided in accordance with a preferred embodiment of the present invention a method for protecting a client computer from dynamically generated malicious content, including receiving an input from a client computer, determining whether it is safe for the client computer to invoke a function with the input, and transmitting an indicator of the determining to the client computer.

There is further provided in accordance with a preferred embodiment of the present invention a system for protecting a client computer from dynamically generated malicious content, including a receiver for receiving an input from a client computer, an input inspector for determining whether it is safe for the client computer to invoke a function with the input, and a transmitter for transmitting an indicator of the determining to the client computer.

There is further provided in accordance with a preferred embodiment of the present invention a computer-readable storage medium storing program code for causing a computing device to receive an input from a computer, determine whether it is safe for the computer to invoke a function with the input, and transmit an indicator of the determination to the computer.

The following definitions are employed throughout the specification and claims.

8

SECURITY POLICY—a set of one or more rules that determine whether or not a requested operation is permitted. A security policy may be explicitly configurable by a computer system administrator, or may be implicitly determined by application defaults.

SECURITY PROFILE—information describing one or more suspicious operations performed by executable software.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be more fully understood and appreciated from the following detailed description, taken in conjunction with the drawings in which:

FIG. 1 is a simplified block diagram of prior art systems for blocking malicious content;

FIG. 2 is a simplified block diagram of a system for protecting a computer from dynamically generated malicious executable code, in accordance with a preferred embodiment of the present invention;

FIG. 3 is a simplified flowchart of a method for protecting a computer from dynamically generated malicious executable code, in accordance with a preferred embodiment of the present invention;

FIG. 4 is a simplified block diagram of a system for protecting a computer from dynamically generated malicious executable code, in which the gateway computer itself performs the code inspection, in accordance with a preferred embodiment of the present invention; and

FIG. 5 is a simplified flowchart of a method for protecting a computer from dynamically generated malicious executable code, whereby the gateway computer itself performs the code inspection, in accordance with a preferred embodiment of the present invention.

DETAILED DESCRIPTION

The present invention concerns systems and methods for protecting computers against dynamically generated malicious code.

Reference is now made to FIG. 2, which is a simplified block diagram of a system for protecting a computer from dynamically generated malicious executable code, in accordance with a preferred embodiment of the present invention. Three major components of the system are a gateway computer 205, a client computer 210, and a security computer 215. Gateway computer 205 receives content from a network, such as the Internet, over a communication channel 220. Such content may be in the form of HTML pages, XML documents, Java applets and other such web content that is generally rendered by a web browser. Client computer 210 communicates with gateway computer 205 over a communication channel 225, and communicates with security computer 215 over a communication channel 230. Gateway computer 205 receives data at gateway receiver 235, and transmits data at gateway transmitter 240. Similarly, client computer 210 receives data at client receiver 245, and transmits data at client transmitter 250; and security computer 215 receives data at security receiver 260 and transmits data at security transmitter 265.

It will be appreciated by those skilled in the art that the network topology of FIG. 2 is shown as a simple topology, for purposes of clarity of exposition. However, the present invention applies to general architectures including a plurality of client computers 210 that are serviced by one or more gateway computers 205, and by one or more security computers 215. Similarly, communication channels 220, 225 and 230

may each be multiple channels using standard communication protocols such as TCP/IP.

Moreover, the functionality of security computer 215 may be included within gateway computer 205. Such a topology is illustrated in FIG. 4.

The computers shown in FIG. 2 also include additional processing modules, each of which is described in detail hereinbelow. Gateway computer 205 includes a content modifier 265, client computer 210 includes a content processor 270, and security computer 215 includes an inspector 275, a database of client security policies 280, and an input modifier 285.

Content modifier 265 preferably modifies original content received by gateway computer 205, and produces modified content, which includes a layer of protection to combat dynamically generated malicious code. Specifically, content modifier 265 scans the original content and identifies function calls of the form

Function(input), (1)
Content modifier 265 further modifies selected ones of the function calls (1) to corresponding function calls

Substitute_function(input,*), (2)
whereby the call to Function() has been replaced with a call to Substitute_junction(). It is noted that the input intended for the original function is also passed to the substitute function, along with possible additional input denoted by “*”.

It will be appreciated by those skilled in the art that content modifier 265 may modify all detected function calls, or only a portion of the detected function calls. Functions that are known to be safe, regardless of their inputs, need not be modified by content modifier 265. Similarly, functions that are not passed any inputs when invoked and are known to be safe, also need not be modified by content modifier 265.

Preferably, when call (2) is made, the substitute function sends the input to security computer 215 for inspection. Preferably, content modifier 265 also inserts program code for the substitute function into the content, or a link to the substitute function. Such a substitute function may be of the following general form shown in TABLE I.

TABLE I	
Generic substitute function	
Function Substitute_function(input)	
{	
inspection_result = Call_security_computer_to_inspect (
input, ID_of_client_computer);	
if (inspection_result)	
Original_function(input)	
else	
//do nothing	
}	

Preferably, the above function call_security_computer_to_inspect() passes the input intended for the original function to security computer 215 for inspection by inspector 275. In addition, an ID of client computer 210 is also passed to security computer 215. For example, the ID may correspond to a network address of client computer 210. When security computer 215 services many such client computers 210 at once, it uses the IDs to determine where to return each of its many results.

Optionally, the substitute function may pass additional parameters to security computer 215, such as the name of the original function, or security policy information as described hereinbelow with reference to database 280.

The function call_security_computer_to_inspect() preferably returns an indicator, inspection_result, of whether it is safe for client computer 210 to invoke the original function call (1). The indicator may be a Boolean variable, or a variable with more than two settings that can carry additional safety inspection information. In addition, as described hereinbelow with reference to input modifier 285, the function call_security_computer_to_inspect() may modify the input, and return to client computer 210 modified input to be used when invoking the original function call (1), instead of the original input. Use of input modifier 285 protects client computer 210 against recursively generated malicious code whereby the input itself to a first function generates a call to a second function.

For example, suppose a portion of the original content is of the form shown in TABLE II.

TABLE II	
Example original content	
<!DOCTYPE HTML PUBLIC "-//w3c//DTD HTML 4.0 Transitional//EN">	
<HTML>	
<SCRIPT LANGUAGE="JavaScript">	
<!	
Document.write("<h1>hello</h1>");	
</SCRIPT>	
<BODY>	
</BODY>	
</HTML>	

Preferably, content modifier 265 alters the original content in TABLE II to the modified form shown in TABLE III. Specifically, content modifier 265 substitutes the call to the standard function Document.write(), with a call to the substitute function Substitute_document.write(), and inserts the function definition for the substitute function into the content. The standard function Document.write() generally writes lines of HTML and inserts them into the HTML page currently being processed by a client web browser.

TABLE III	
Example modified content	
<!DOCTYPE HTML PUBLIC "-//w3c//DTD HTML 4.0 Transitional//EN">	
<HTML>	
<SCRIPT LANGUAGE="JavaScript">	
<!	
Function Substitute_document.write(text)	
{	
inspection_result = Call_security_computer_to_inspect(text);	
if inspection_result	
Document.write(text)	
Else	
//do nothing	
}	
Substitute_document.write("<h1>hello</h1>");	
</SCRIPT>	
<BODY>	
</BODY>	
</HTML>	

Content processor 270 processes the modified content generated by content modifier 265. Content processor may be a web browser running on client computer 210. When content processor invokes the substitute function call (2), the input is passed to security computer 215 for inspection. Processing of the modified content is then suspended until security computer 215 returns its inspection results to client computer 210. Upon receiving the inspection results, client computer 210

US 8,141,154 B2

11

resumes processing the modified content. If inspection_result is true, then client computer 210 invokes the original function call (1); otherwise, client computer 210 does not invoke the original function call (1).

Security computer 215 may also modify the input that is passed to it by the substitute function. In such case, client computer 210 invokes the original function with such modified input, instead of the original input, after receiving the inspection results.

Input inspector 275 analyzes the input passed to security computer 215 by client computer 210; specifically, the input passed when client computer 210 invokes the function call (2). Generally, input inspector 275 scans the input to determine the potentially malicious operations that it may perform, referred to as the input's "security profile". Such potentially malicious operations can include inter alia operating system level commands, file system level commands, network level commands, application level commands, certain URLs with hyperlinks, and applets already known to be malicious. Security profiles are described in assignee's U.S. Pat. No. 6,092,194 entitled SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES, the contents of which are hereby incorporated by reference. Security profiles encompass access control lists, trusted/un-trusted certificates, trusted/un-trusted URLs, and trusted/un-trusted content.

After determining a security profile for the input, inspector 275 preferably retrieves information about permission settings for client computer 210, referred to as client computer's "security policy". Such permission settings determine which commands are permitted to be performed by content processor 270 while processing content, and which commands are not permitted. Security policies are also described in assignee's U.S. Pat. No. 6,092,194. Security policies are flexible, and are generally set by an administrator of client computer 210. Preferably, security computer 215 has accesses to a database 280 of security profile information for a plurality of client computers. Database 280 may reside on security computer 215, or on a different computer.

By comparing the input's security profile to client computer 210's security policy, input inspector 275 determines whether it is safe for client computer 210 to make the function call (1). Security computer 215 sends back to client computer 210 an indicator, inspection_result, of the inspector's determination. Comparison of a security profile to a security policy is also described in assignee's U.S. Pat. No. 6,092,194. Security policies may include simple or complex logical tests for making a determination of whether or not an input is safe.

For example, suppose the content is an HTML page, and the function call (1) is the following JavaScript:

```
Document.write("<h1><SCRIPT>Some
JavaScript</SCRIPT></h1>")
```

(3)

Such a function call serves to instruct content processor 270 to insert the text between the <h1> header tags into the HTML pages; namely the text <SCRIPT>JavaScript</SCRIPT> which itself invokes the JavaScript between the <SCRIPT> tags. It is noted that the function call (1) uses a function Document.write() that is normally considered to be safe. Indeed, the function Document.write() does not access client computer 210's operating system or file system and does not send or receive data outside of client computer 210. Moreover, the input in the call (3) to Document.write() may itself be dynamically generated, and not available for inspection prior to processing the HTML page. That is, the call may be of the form

12

Document.write("content that is dynamically generated at run-time"),

where input to Document.write() may be in the form of a text string that itself is dynamically generated at run-time. Generally, such a function call cannot be analyzed successfully by behavioral based anti-virus software prior to run-time.

However, when input inspector 275 receives the input from client computer during run-time, after client computer has invoked the substitute call (2), the input has already been dynamically generated by content processor 270 and can thus be readily analyzed. Referring to the example above, when client computer 210 invokes the substitute call (2), it passes the input string

```
"<h1><SCRIPT>JavaScript</SCRIPT></h1>"
```

(4)

to security computer 215. This string is then analyzed by input inspector 275, which recognizes the JavaScript and scans the JavaScript to determine any potentially malicious operations it includes. If potentially malicious operations are detected, and if they violate client computer 210's security policy, then inspector 275 preferably sets inspection_result to false. Otherwise, inspector 275 preferably sets inspection_result to true.

It may thus be appreciated by those skilled in the art that input inspector 275 is able to detect malicious code that is generated at runtime.

Malicious code may be generated within further recursive levels of function calls. For example, instead of the function call (3), which invokes a single function to dynamically generate JavaScript, two levels of function calls may be used. Consider, for example, the recursive function call

```
Document.write("<h1>Document.write
("<h1><SCRIPT>Some JavaScript</SCRIPT>
</h1>")</h1>")
```

(5)

Such a function call first calls Document.write() to generate the function call (3), and then calls Document.write() again to generate the JavaScript. If the inputs to each of the Document.write() invocations in (5) are themselves dynamically generated at run-time, then one pass through input inspector may not detect the JavaScript.

To this end, input inspector 275 preferably passes inputs it receives to input modifier 285, prior to scanning the input. Input modifier preferably operates similar to content modifier 265, and replaces function calls detected in the input with corresponding substitute function calls. Referring to the example above, when client computer 210 invokes the outer call to Document.write() in (5), the input text string

```
"<h1>Document.write("<h1><SCRIPT>Some
JavaScript</SCRIPT></h1>")</h1>"
```

(6)

is passed to security computer 215. Input modifier 285 detects the inner function call to Document.write() and replaces it with a corresponding substitute function call of the form (2). Input inspector 275 then inspects the modified input. At this stage, if the input to the inner call to Document.write() has not yet been dynamically generated, input inspector 275 may not detect the presence of the JavaScript, and thus may not set inspection_result to false if the JavaScript is malicious. However, security computer 215 returns the modified input to client computer 210. As such, when content processor 270 resumes processing, it adds the modified input into the HTML page. This guarantees that when content processor 270 begins to process the modified input, it will again invoke the substitute function for Document.write(), which in turn passes the input of the inner Document.write() call of (5) to security

US 8,141,154 B2

13

computer **215** for inspection. This time around input inspector **275** is able to detect the presence of the JavaScript, and can analyze it accordingly.

It may thus be appreciated by those skilled in the art that when input modifier **285** supplements input inspector **275**, inspector **275** has sufficient logic to be able to detect malicious code that is generated recursively at run-time.

In addition to inspecting inputs, security computer **215** preferably maintains an event log of potential security breaches. When input inspector **275** determines that an input is not safe, security computer **215** enters information about the input and client computer **210** into a log that is available for review by an administrator of client computer **210**.

In accordance with a preferred embodiment of the present invention, it is anticipated that many client computers **210** use the same security computer **215** for protection. Each client computer may independently send inputs to security computer **215** for inspection. Security computer **215** may use cache memory to save results of inspection, so as to obviate the need to analyze the same input more than once. Use of cache memory when working with a plurality of security policies is described in assignee's U.S. Pat. No. 6,965,968 entitled POLICY-BASED CACHING.

Similarly, it is anticipated that gateway computer **205** services many client computers **210**. Gateway computer may include its own content inspector, which is useful for detecting malicious content that is not dynamically generated, as described in assignee's U.S. Pat. No. 6,092,194.

It may be appreciated that substitute functions as in TABLE I may also pass the name of the original function to the security computer. That is, the call to `Call_security_computer_to_inspect()` may also pass a variable, say `name_of_function`, so that input inspector **275** can determine whether it is safe to invoke the specific original function with the input. In this way, input inspector **275** can distinguish between different functions with the same input.

Reference is now made to FIG. 3, which is a simplified flowchart of a method for protecting a computer from dynamically generated malicious executable code, in accordance with a preferred embodiment of the present invention. The leftmost column of FIG. 3 shows steps performed by a gateway computer, such as gateway computer **205**. The middle column of FIG. 3 shows steps performed by a client computer, such as client computer **210**. The rightmost column of FIG. 3 shows steps performed by a security computer, such as security computer **215**.

At step **304**, the gateway computer receives content from a network, the content on its way for delivery to the client computer. Such content may be in the form of an HTML web page, an XML document, a Java applet, an EXE file, JavaScript, VBScript, an ActiveX Control, or any such data container that can be rendered by a client web browser. At step **308**, the gateway computer scans the content it received, for the presence of function calls. At step **312**, the gateway computer branches, depending on whether or not function calls were detected at step **308**. If function calls were detected, then at step **316** the gateway computer replaces original function calls with substitute function calls within the content, thereby modifying the content. If function calls were not detected, then the gateway computer skips step **316**. At step **320**, the gateway computer sends the content, which may have been modified at step **316**, to the client computer.

At step **324** the client computer receives the content, as modified by the gateway computer. At step **328** the client computer begins to continuously process the modified content; i.e., the client computer runs an application, such as a web browser or a Java virtual machine, that processes the

14

modified content. At step **332**, while processing the modified content, the client computer encounters a call (2) to a substitute function, such as the substitute function listed in TABLE I. Client computer then transmits the input to the substitute function and an identity of the client computer, to the security computer for inspection, at step **336**. The identity of the client computer serves to inform the security computer where to return its inspection result. Since one security computer typically services many client computers, passing client computer identities is a way to direct the security computer where to send back its results. At this point, client computer suspends processing the modified content pending receipt of the inspection results from the security computer. As mentioned hereinabove, the client computer may also send the name of the original function to the security computer, for consideration in the inspection analysis.

At step **340** the security computer receives the input and client computer identifier. At step **344** the security computer scans the input for the presence of function calls. At step **348** the security computer branches, depending on whether or not function calls were detected at step **344**. If function calls were detected, then the security computer replaces original function calls with substitute function calls at step **352**, thereby modifying the input. The security computer may insert definitions of the substitute functions into the input, as indicated in TABLE III, or may insert links to such definitions. Otherwise, the security computer skips step **352**. Steps **344**, **348** and **352** are similar to respective steps **308**, **312** and **316** performed by the gateway computer.

At step **356** the security computer scans the input, which may have been modified at step **352**, for the presence of potentially malicious operations. Preferably, the security computer determines a security profile for the input, which corresponds to a list of the potentially malicious operations that are detected.

At step **360** the security computer retrieves a security policy that governs the client computer. The security policy may be retrieved from a database that stores a plurality of security policies, each policy configurable by an administrator of client computers. Security policies may be set at a fine granularity of a policy for each client computer, or at a coarser granularity of a policy that applies to an entire department or workgroup.

At step **364** the security computer compares the security profile of the input under inspection with the security policy of the client computer, to determine if it is permissible for the client computer to invoke an original function with the input. Such determination may involve one or more simple or complex logical tests, structured in series or in parallel, or both, as described in assignee's U.S. Pat. No. 6,092,194.

At step **368** the security computer branches depending on the result of the comparison step **364**. If the comparison step determines that the input is safe; i.e., that the input's security profile does not violate the client computer's security policy, then at step **372** the security computer sets an indicator of inspection results to true. Otherwise, at step **376** the security computer sets the indicator to false. At step **380** the security computer returns the indicator to the client computer. In addition, if the security computer modified the input at step **352**, then it also returns the modified input to the client computer.

At step **384** the client computer receives the indicator and the modified input from the security computer and resumes processing the modified content, which had been suspended after step **336** as described hereinabove. At step **388** the client computer branches depending on the value of the indicator it received from the security computer. If the indicator is true, indicating that it is safe for the client computer to invoke the

US 8,141,154 B2

15

original function call (1), then the client computer invokes the original function using the modified input it received from the security computer, at step 392. Otherwise, the client computer does not invoke the original function, since the indicator indicates that such invocation may be malicious to the client computer. The client computer then loops back to step 328 to continue processing the modified content.

As described hereinabove, steps 344, 348 and 352, which modify the input, are useful in protecting against malicious code that is dynamically generated in a recursive manner, as in function call (5). The security computer may require multiple passes to detect such malicious code, and steps 344, 348 and 352 provide the mechanism for this to happen.

Reference is now made to FIG. 4, which is a simplified block diagram of a system for protecting a computer from dynamically generated malicious executable code, in which the gateway computer itself performs the code inspection, in accordance with a preferred embodiment of the present invention. The system illustrated in FIG. 4 is similar to the system of FIG. 2, where the functionality of the security computer has been incorporated into the gateway computer. The elements in FIG. 4 are thus similar in functionality to the elements in FIG. 2.

Two major components of the system, gateway computer 405 and client computer 410 communicate back and forth over communication channel 425. Gateway computer 405 includes a gateway receiver 435 and a gateway transmitter 440; and client computer 410 includes a client receiver 445 and a client transmitter 450. Although FIG. 4 includes only one client computer, this is solely for the purpose of clarity of exposition, and it is anticipated that gateway computer 405 serves many client computers 410.

Gateway computer 405 receives content, such as web content, from a network, over communication channel 420. Client computer 410 includes a content processor 470, such as a web browser, which processes content received from the network.

In accordance with a preferred embodiment of the present invention, gateway computer 405 includes an input inspector 475, and a content modifier 465 which also serves as an input modifier. That is, content modifier 465 incorporates the functionalities of content modifier 265 and input modifier 285 from FIG. 2. In addition, gateway computer 405 includes a database 480 of security policies, or else has access to such a database. The operations of input inspector 475 and content/input modifier 465 are similar to the operations of the corresponding elements in FIG. 2, as described hereinabove.

Incoming content received at gateway computer 405 passes through content modifier 465, which replaces function calls of the form (1) with substitute function calls of the form (2), and the modified content is transmitted to client computer 410. Content processor 470 processes the modified content and, while processing the modified content, if it encounters a substitute function call it sends the function's input to inspector 475 for inspection, and suspends processing of the modified content. The input passes through input modifier 465, and input inspector 475 analyzes the modified input for the presence of potentially malicious operations. Gateway computer 405 returns the input inspection results to client computer 410. Gateway computer 405 may also return the modified input to client computer 410. After receiving the inspection results, client computer 410 resumes processing the modified content and invokes or does not invoke the original function call, based on the inspection results.

Reference is now made to FIG. 5, which is a simplified flowchart of a method for protecting a computer from dynamically generated malicious executable code, whereby

16

the gateway computer itself performs the code inspection, in accordance with a preferred embodiment of the present invention. The leftmost column indicates steps performed by a gateway computer, such as gateway computer 405; and the rightmost column indicates steps performed by a client computer, such as client computer 410.

The method illustrated in FIG. 5 is similar to that of FIG. 3, where steps 340-380 performed by the security computer in FIG. 3 are performed by the gateway computer in FIG. 5. At step 500 the gateway computer receives content from a network, the content intended for delivery to the client computer. At step 505 the gateway computer scans the content for the presence of function calls. At step 510 the gateway computer branches. If function calls within the content were detected at step 505, then at step 515 the gateway computer modifies the content by replacing original function calls of the form (1) with corresponding substitute function calls of the form (2). Otherwise, if function calls were not detected at step 505, then the gateway computer skips step 515. At step 520 the gateway computer transmits the content, which may have been modified at step 515, to the client computer.

At step 525 the client computer receives the content from the gateway computer, and at step 530 the client computer begins processing the content. While processing the content, the client computer invokes a substitute function call of the form (2) at step 535. The substitute function, being of the form listed on TABLE I, instructs the client computer to transmit the function input and a client computer identifier to the gateway computer for inspection. At step 540 the client computer transmits the input and the identifier to the gateway computer, and suspends processing of the content pending a reply from the gateway computer.

At step 545 the gateway computer receives the input and the client identifier from the client computer, and loops back to step 505 to scan the input for the presence of function calls. At step 510 the gateway computer branches. If function calls within the input were detected at step 505, then the gateway computer modifies the input at step 515, by replacing function calls of the form (1) with corresponding function calls of the form (2). Otherwise, if function calls were not detected at step 505, then the gateway computer skips step 515.

The gateway computer then proceeds to step 550, and scans the input, which may have been modified at step 515, to identify potentially malicious operations within the input. The potentially malicious operations identified form a security profile for the input.

At step 555 the gateway computer retrieves a security policy for the client computer from a database of security policies. At step 560 the gateway computer compares the input's security profile with the client computer's security policy to determine whether or not the security profile violates the security policy. At step 565 the gateway computer branches. If the results of step 560 indicate that the input security profile does not violate the client computer security policy, then it is safe for the client to invoke the original function call, and an indicator of the inspection results is set to true at step 570. Otherwise, the indicator is set to false at step 575. At step 580 the gateway computer returns the indicator to the client computer. The gateway computer may also return the modified input, as modified at step 515, to the client computer.

At step 585 the client computer receives the reply back from the gateway computer and resumes processing of the content, which processing had been suspended after step 540. At step 590 the client computer branches. If the indicator was set to true by the gateway computer at step 570, then the client computer invokes the original function call (1). If the gateway

US 8,141,154 B2

17

computer had modified the input at step 515, then preferably the client computer uses the modified input instead of the original input when invoking the original function call. Otherwise, if the indicator was set to false by the gateway computer at step 575, then the client computer skips step 595. The client computer then loops back to step 530 to continue processing of the content.

Having read the above disclosure, it will be appreciated by those skilled in the art that the present invention can be used to provide protection to computers against both statically and dynamically generated malicious code. Moreover, such protection may be afforded by a security computer that is remote from the computers being protected, thus adding another layer of security to methods and systems that embody the present invention.

In reading the above description, persons skilled in the art will realize that there are many apparent variations that can be applied to the methods and systems described. Thus it may be appreciated that the present invention applies to a variety of computing devices, including mobile devices with wireless Internet connections such as laptops, PDAs and cell phones.

In the foregoing specification, the invention has been described with reference to specific exemplary embodiments thereof. It will, however, be evident that various modifications and changes may be made to the specific exemplary embodiments without departing from the broader spirit and scope of the invention as set forth in the appended claims. Accordingly, the specification and drawings are to be regarded in an illustrative rather than a restrictive sense.

What is claimed is:

1. A system for protecting a computer from dynamically generated malicious content, comprising:

a content processor (i) for processing content received over a network, the content including a call to a first function, and the call including an input, and (ii) for invoking a second function with the input, only if a security computer indicates that such invocation is safe;

a transmitter for transmitting the input to the security computer for inspection, when the first function is invoked; and

a receiver for receiving an indicator from the security computer whether it is safe to invoke the second function with the input.

2. The system of claim 1 wherein said content processor (i) suspends processing of the content after said transmitter transmits the input to the security computer, and (ii) resumes processing of the content after said receiver receives the indicator from the security computer.

3. The system of claim 1 wherein the input is dynamically generated by said content processor prior to being transmitted by said transmitter.

4. A non-transitory computer-readable storage medium storing program code for causing a computing device to:

process content received over a network, the content including a call to a first function, and the call including an input;

transmit the input for inspection, when the first function is invoked, and suspend processing of the content;

receive an indicator of whether it is safe to invoke a second function with the input; and

18

resume processing of the content after receiving the indicator, and invoke the second function with the input only if the indicator indicates that such invocation is safe.

5. The non-transitory computer-readable storage medium of claim 4 wherein the program code causes the computer device to dynamically generate the input prior to transmitting the input for inspection.

6. A system for protecting a computer from dynamically generated malicious content, comprising:

a content processor (i) for processing content received over a network, the content including a call to a first function, and the first function including an input variable, and (ii) for calling a second function with a modified input variable;

a transmitter for transmitting the input variable to a security computer for inspection, when the first function is called; and

a receiver for receiving the modified input variable from the security computer,

wherein the modified input variable is obtained by modifying the input variable if the security computer determines that calling a function with the input variable may not be safe.

7. The system of claim 6 wherein said content processor (i) suspends processing of the content after said transmitter transmits the input variable to the security computer, and (ii) resumes processing of the content after said receiver receives the modified input variable from the security computer.

8. The system of claim 6 wherein the input variable is dynamically generated by said content processor prior to being transmitted by said transmitter.

9. The system of claim 6 wherein the input variable includes a call to an additional function, and wherein the modified input variable includes a call to a modified additional function instead of the call to the additional function.

10. A non-transitory computer-readable storage medium storing program code for causing a computing device to:

process content received over a network, the content including a call to a first function, and the first function including an input variable;

transmit the input variable for inspection, when the first function is called, and suspend processing of the content;

receive a modified input variable; and

resume processing of the content after receiving the modified input variable, and calling a second function with the modified input variable,

wherein the modified input variable is obtained by modifying the input variable if the inspection of the input variable indicates that calling a function with the input variable may not be safe.

11. The non-transitory computer-readable storage medium of claim 10 wherein the program code causes the computer device to dynamically generate the input variable prior to transmitting the input variable for inspection.

12. The non-transitory computer-readable storage medium of claim 10 wherein the input variable includes a call to an additional function, and wherein the modified input variable includes a call to a modified additional function instead of the call to the additional function.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 8,141,154 B2
APPLICATION NO. : 12/814584
DATED : March 20, 2012
INVENTOR(S) : David Gruzman et al.

Page 1 of 1

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

On the Title Page, insert Item (63):

-- Related U.S. Application Data --

-- (63) Divisional of application no. 11/298,475, filed on Dec. 12, 2005, Now Pat. No. 7,757,289. --

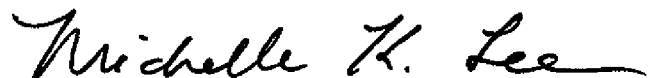
In the Specification

In Column 1, add the following heading and paragraph directly below the title of the invention:

-- CROSS-REFERENCE TO RELATED APPLICATIONS --

-- This application is a divisional of and claims priority to U.S. Patent Application Serial No. 11/298,475, filed December 12, 2005, entitled "System and Method For Inspecting Dynamically Generated Executable Code," now U.S. Patent No. 7,757,289. --

Signed and Sealed this
Twenty-fifth Day of February, 2014



Michelle K. Lee
Deputy Director of the United States Patent and Trademark Office

EXHIBIT B

Redacted In Its Entirety

EXHIBIT C



(/en-us/)



NEWSROOM

Trustwave News Releases document our latest announcements, including corporate news, product and service launches and industry accolades.

🕒 December 04, 2018



Trustwave Becomes One of the Industry's Most Comprehensive Security Companies Poised to Confront Growing Cyber Threats Head On

CHICAGO, SINGAPORE and SYDNEY – December 4, 2018 – Singtel today announced it has pooled the cybersecurity capabilities, technologies and resources of Singtel, Optus, Trustwave and NCS, into a single global corporate identity operating under the Trustwave brand. The strategic measure forms one of the industry's most comprehensive global cybersecurity companies offering a complete range of managed security services (</en-us/services/managed-security/>), consulting, education and leading-edge technologies to help organizations worldwide contend with rapidly evolving external and internal threats.

Through the integration, the new Trustwave can harness the synergies and strengths of Singtel's global cybersecurity business, revenue, capabilities and teams across the Americas, Europe and Asia Pacific. Trustwave's global cyber business now has about 2,000 security employees, a global network of ten connected Advanced Security Operations Centers (</en-us/company/about-us/advanced-security-operations-centers/>) (ASOCs) supported by its elite Trustwave SpiderLabs (</en-us/company/about-us/spiderlabs/>) security team, millions of businesses enrolled in its cloud-based security platform, more than 10,000 managed security services customers, and nearly 1,000 channel partners and numerous technology partners worldwide. The Trustwave portfolio includes many services and technologies recognized as industry-leading by analysts.

"Uniting the security assets and deep expertise of Singtel, Optus, Trustwave and NCS under one brand and single vision – what we call the new Trustwave – is a pivotal milestone for our customers, partners, employees and company," said Arthur Wong, Chief Executive Officer at Trustwave. "Trustwave is well-positioned to further its role as a recognized leader in cybersecurity and managed security services, areas vital for effective security programs as enterprises accelerate their digital transformation. Customers benefit by having a trusted security partner with true global reach and intelligence, offering around-the-clock monitoring, detection and eradication of threats in addition to deep regional security expertise necessary for successfully addressing global threats and localized attack campaigns."

As part of the integration, Trustwave has re-designed its logo, giving it a bold modern look with new brand identity and color scheme, and launched a new corporate website at www.trustwave.com (<http://www.trustwave.com/en-us/>). The website serves as the digital hub showcasing all Trustwave offerings, including those from Singtel, Optus and NCS.

Benefits of the integration include:

- **Broader security services portfolio** – The new Trustwave portfolio includes managed security services, security testing, consulting, technology solutions and cybersecurity education. The integration provides Trustwave with additional managed security services, third-party technology solutions and cybersecurity education and training services like the Cyber Security Institute in Singapore.
- **Increased focus on industry-leading technologies** – Trustwave will continue to offer both its own technologies and those from third parties. Trustwave has added and will continue to add more industry-leading third-party technologies that are integrated or wrapped with its managed security and consulting services to offer even more compelling solutions that solve cybersecurity problems and challenges.
- **More cybersecurity resources and talent** – Through the integration of Singtel's global cybersecurity assets under Trustwave, the company has added more resources, employees and services to help customers protect their data and reduce risk. At a time when there is a world-wide security skills shortage, the company has about 2,000 security professionals worldwide delivering, selling, marketing and supporting Trustwave cybersecurity solutions and managed security services. The added personnel complements ten interlinked Advanced Security Operations Centers responsible for delivering continuous threat monitoring, detection and threat elimination along with threat intelligence to ensure organizations are continuously protected regardless of location.
- **Advanced security training and continued education** – Trustwave has combined the training and continued education assets from Singtel's cybersecurity businesses including Trustwave Academy and the Cyber Security Institute into a comprehensive program delivered on-premises and remotely. Cybersecurity education has become paramount to addressing the threat landscape through knowledge and best practices. Customers, partners and employees can learn the latest techniques for detecting threats, defending networks, protecting data and optimizing technologies from many of the world's top minds in cybersecurity. Options for earning industry recognized certifications and accreditation in penetration testing, data forensics, incident response and other fields are offered.
- **Separate business unit focused on compliance** – Trustwave has created a separate global Payment Card Industry (PCI) compliance and risk management arm (<https://www.trustwavecompliance.com/>) to help organizations achieve and maintain regulatory compliance. The division represents a continued commitment to focus on compliance, risk and data privacy customer challenges while building upon Trustwave's foundation as a payment card industry data security standard (PCI DSS) pioneer.

Industry Recognition Demonstrates Trustwave Momentum and Leadership

In 2018, renowned industry analysts worldwide recognized Trustwave for its leadership in cybersecurity and managed security services.

Gartner, Inc., a leading information and technology and advisory company, placed Trustwave in the Leaders quadrant in the 2018 Gartner Magic Quadrant for Managed Security Services, Worldwide.ⁱ

International Data Corporation (IDC) named Trustwave a Leader in the IDC MarketScape U.S. Incident Readiness, Response, and Resiliency Services 2018 Vendor Assessment - Beyond the Big 5 Consultancies.ⁱⁱ IDC also named Trustwave a Leader in the IDC MarketScape: Asia/Pacific Managed Security Services 2018.ⁱⁱⁱ Additionally, IDC named Trustwave a Leader in the IDC MarketScape: Canadian Security Services Providers, 2018 Vendor Assessment.^{iv}

Most recently, Frost & Sullivan presented Trustwave with the prestigious 2018 Singapore and Southeast Asia Managed Security Service Provider of the Year award. (/en-us/)



About Trustwave

Trustwave is a leading cybersecurity and managed security services provider that helps businesses fight cybercrime, protect data and reduce security risk. Offering a comprehensive portfolio of managed security services, security testing, consulting, technology solutions and cybersecurity education, Trustwave helps businesses embrace digital transformation securely. Trustwave is a Singtel company and the global security arm of Singtel, Optus and NCS, with customers in 96 countries. For more information about Trustwave, visit <https://www.trustwave.com> (<https://www.trustwave.com>).

About Singtel

Singtel is Asia's leading communications technology group, providing a portfolio of services from next-generation communication, technology services to infotainment to both consumers and businesses. For consumers, Singtel delivers a complete and integrated suite of services, including mobile, broadband and TV. For businesses, Singtel offers a complementary array of workforce mobility solutions, data hosting, cloud, network infrastructure, analytics and cyber-security capabilities. The Group has presence in Asia, Australia and Africa and reaches over 700 million mobile customers in 21 countries. Its infrastructure and technology services for businesses span 21 countries, with more than 428 direct points of presence in 362 cities. For more information, visit www.singtel.com (<http://www.singtel.com>). Follow us on Twitter at www.twitter.com/SingtelNews (<http://www.twitter.com/SingtelNews>).

ⁱ Source: Gartner, "Magic Quadrant for Managed Security Services, Worldwide" by Toby Bussa, Kelly M. Kavanagh, Pete Shoard, Sid Deshpande, February 27, 2018.

ⁱⁱ Source: IDC MarketScape: IDC MarketScape U.S. Incident Readiness, Response, and Resiliency Services 2018 Vendor Assessment - Beyond the Big 5 Consultancies, (IDC# US44257117, October 2018).

ⁱⁱⁱ Source: IDC MarketScape: Asia/Pacific Managed Security Services 2018, (IDC# AP42609818, June 2018).

^{iv} Source: IDC MarketScape: Canadian Security Services Providers, 2018 Vendor Assessment (IDC# CA3005218, March 2018).

(<https://www.linkedin.com/company/trustwave>) (<https://www.facebook.com/Trustwave>) (<https://www.youtube.com/channel/UCv83N0djhqA>)
SERVICES (/EN-US/SERVICES/) **CAPABILITIES (/EN-US/CAPABILITIES/)**
 Managed Security (/en-us/services/managed-security/) By Topic (/en-us/capabilities/by-topic/)

[Security Testing \(/en-us/services/security-testing/\)](/en-us/services/security-testing/)

[Technology \(/en-us/services/technology/\)](/en-us/services/technology/)

[Consulting \(/en-us/services/consulting/\)](/en-us/services/consulting/)

[Education \(/en-us/services/education/\)](/en-us/services/education/)

RESOURCES (/EN-US/RESOURCES/)

[Blogs & Stories \(/en-us/resources/blogs/\)](/en-us/resources/blogs/)

[Resource Library \(/en-us/resources/library/\)](/en-us/resources/library/)

[Security Resources \(/en-us/resources/security-resources/\)](/en-us/resources/security-resources/)

[Events & Webinars \(/en-us/resources/upcoming/\)](/en-us/resources/upcoming/)

[By Industry \(/en-us/capabilities/by-industry/\)](/en-us/capabilities/by-industry/)

[By Mandate \(/en-us/capabilities/by-mandate/\)](/en-us/capabilities/by-mandate/)

[By Mandate \(/en-us/capabilities/by-mandate/\)](/en-us/capabilities/by-mandate/)

COMPANY (/EN-US/COMPANY/)

[About Trustwave \(/en-us/company/about-us/\)](/en-us/company/about-us/)

[Careers \(https://jobs.jobvite.com/trustwave\)](https://jobs.jobvite.com/trustwave)

[Newsroom \(/en-us/company/newsroom/\)](/en-us/company/newsroom/)

[Contact \(/en-us/company/contact/\)](/en-us/company/contact/)

[Support \(/en-us/company/support/\)](/en-us/company/support/)



STAY INFORMED

Sign up to receive the latest security news and trends from Trustwave.

SUBSCRIBE

No spam, unsubscribe at any time.

LEGAL (/EN-US/LEGAL-DOCUMENTS/)

[TERMS OF USE \(/EN-US/LEGAL-DOCUMENTS/TERMS-OF-USE/\)](/EN-US/LEGAL-DOCUMENTS/TERMS-OF-USE/)

[PRIVACY POLICY \(/EN-US/LEGAL-DOCUMENTS/PRIVACY-POLICY/\)](/EN-US/LEGAL-DOCUMENTS/PRIVACY-POLICY/)

UNITED STATES - ENGLISH



Copyright © 2020 Trustwave Holdings, Inc.

All rights reserved.

EXHIBIT D



MENU

Home > Finance & Banking

August 11, 2011 07:00 AM

Trustwave postpones IPO

Staff

TWEET

SHARE

SHARE

EMAIL

REPRINTS

(Crain's) — Trustwave Holdings Inc. is postponing its initial public offering because of "market conditions."

Chicago-based Trustwave, which makes security-compliance software for the credit card industry, planned to raise \$100 million in an offering this week.

U.S. and other stock markets have swung wildly this week, with the Dow Jones industrial average falling 4.6% Wednesday.

Trustwave's revenue soared 52% last year to \$115 million, nearly double its 2008 sales, but it remained unprofitable, posting a \$4.6-million loss. The company launched nine years ago.

RECOMMENDED FOR YOU



Banks exiting or closing branches in hyper-competitive Evanston



Chicago spared Northern Trust's ax



For Citadel, it's full speed ahead in China



Sponsored Content: Chicago's Meeting and Event Planning Guide

SIGN UP FOR NEWSLETTERS

- ☐ Morning 10 - *Need-to-know stories from Crain's and around the web. Monday-Friday at 7 a.m.*
- ☐ Today's Crain's - *A roundup of the day's important business news. Monday-Friday around 3 p.m.*
- ☐ Breaking News Alerts - *Up-to-the-minute info on what's happening in Chicago business right now.*
- ☐ Health Pulse Chicago - *Your source for actionable, exclusive and inside news and data on the health care industry. Monday, Wednesday and Friday at 5:30 a.m.*
- ☐ People on the Move - *Highlights prominent personalities, job changes and executive appointments. Thursday.*
- ☐ Chicago Real Estate Report - *The best source in Chicago for exclusive commercial real estate news. Monday-Thursday.*
- ☐ Chicago Residential Real Estate Report - *Scoops on Chicago's residential real estate industry. Tuesday-Thursday.*

EMAIL ADDRESS

SUBMIT

GET OUR NEWSLETTERS

Staying current is easy with Crain's news delivered straight to your inbox, free of charge.

Email Address

SIGN UP NOW

SUBSCRIBE TODAY

Get the best business coverage in Chicago, from breaking news to razor-sharp analysis, in print and online.

SUBSCRIBE NOW

CONNECT WITH US



CRAIN'S CHICAGO BUSINESS

CONTACT US

150 N. Michigan Ave.
Chicago, IL 60601
E-mail our editor
(312) 649-5200

[More contacts](#)[Customer service](#)

RESOURCES

[About Us](#)[Classified Advertising](#)[Crain's Chicago jobs](#)[Staff](#)[Advertise with Us](#)[Reprints](#)[Media Kit](#)[Ad Choices](#)[Sitemap](#)

AWARDS

[Special reports](#)

LEGAL

[Terms and Conditions](#)[Privacy Policy](#)[Privacy Request](#)

CRAIN

Copyright © 1996-2020. Crain Communications, Inc. All Rights Reserved.

Some U.S. state privacy laws offer their residents specific consumer privacy rights, which we respect as described in our [privacy statement](#). To opt-out of our making available to third parties information relating to cookies and similar technologies for advertising purposes, select "Opt-Out". To exercise other rights you may have related to cookies, select "More Info" or see this "[Privacy Request](#)" link.

[Accept](#)[Opt-Out](#)[More Info](#)

EXHIBIT E



(/en-us/)



NEWSROOM

Trustwave News Releases document our latest announcements, including corporate news, product and service launches and industry accolades.

🕒 March 19, 2012



Acquisition Strengthens Trustwave's Cloud and Managed Security Services with M86 Security's Advanced Anti-Malware Technology

CHICAGO - March 19, 2012 - Trustwave, a leading provider of cloud-based compliance and information security solutions, today announced it has completed its acquisition of M86 Security (<https://www.trustwave.com/acquisition>), a global leader in Web security solutions and advanced anti-malware technology.

"By acquiring M86 Security, Trustwave has added Web security and enhanced email security to one of the industry's most comprehensive security portfolios," said Robert J. McCullen, Chairman, Chief Executive Officer and President, Trustwave. "We now offer compliance, application, network, data and Web security solutions. We've entered the large, growing multi-billion dollar Web security market with a powerful set of M86 content security products that we'll continue to offer as software and appliances and begin to offer as managed security services. M86 Security also brings to Trustwave advanced anti-malware technology that we'll make available to customers through our cloud-based TrustKeeper portal."

As a combined company, Trustwave is approaching 1,000 employees worldwide. Trustwave announced plans to acquire privately-held M86 Security (<https://www.trustwave.com/acquisition>) on March 6, 2012.

About Trustwave

Trustwave is a leading provider of compliance, Web, application, network and data security solutions delivered through the cloud, managed security services, software and appliances. For organizations faced with today's challenging data security and compliance environment, Trustwave provides a unique approach with comprehensive solutions that include its TrustKeeper® portal and other proprietary security solutions. Trustwave has helped hundreds of thousands of organizations--ranging from Fortune 500 businesses and large financial institutions to small and medium-sized retailers--manage compliance and secure their network infrastructures, data communications and critical information assets. Trustwave is headquartered in Chicago with offices worldwide. For more information, visit <https://www.trustwave.com> (<https://www.trustwave.com/>) .



<https://www.linkedin.com/company/trustwave>
SERVICES (/EN-US/SERVICES/)

<https://www.facebook.com/Trustwave>
CAPABILITIES (/EN-US/CAPABILITIES/)

<https://www.youtube.com/channel/UC83W0djhqA>

- [Managed Security \(/en-us/services/managed-security/\)](/en-us/services/managed-security/)
[Security Testing \(/en-us/services/security-testing/\)](/en-us/services/security-testing/)
[Technology \(/en-us/services/technology/\)](/en-us/services/technology/)
[Consulting \(/en-us/services/consulting/\)](/en-us/services/consulting/)
[Education \(/en-us/services/education/\)](/en-us/services/education/)
- [By Topic \(/en-us/capabilities/by-topic/\)](/en-us/capabilities/by-topic/)
[By Industry \(/en-us/capabilities/by-industry/\)](/en-us/capabilities/by-industry/)
[By Mandate \(/en-us/capabilities/by-mandate/\)](/en-us/capabilities/by-mandate/)

- RESOURCES (/EN-US/RESOURCES/)**
[Blogs & Stories \(/en-us/resources/blogs/\)](/en-us/resources/blogs/)
[Resource Library \(/en-us/resources/library/\)](/en-us/resources/library/)
[Security Resources \(/en-us/resources/security-resources/\)](/en-us/resources/security-resources/)
[Events & Webinars \(/en-us/resources/upcoming/\)](/en-us/resources/upcoming/)
- COMPANY (/EN-US/COMPANY/)**
[About Trustwave \(/en-us/company/about-us/\)](/en-us/company/about-us/)
[Careers \(https://jobs.jobvite.com/trustwave\)](https://jobs.jobvite.com/trustwave)
[Newsroom \(/en-us/company/newsroom/\)](/en-us/company/newsroom/)
[Contact \(/en-us/company/contact/\)](/en-us/company/contact/)
[Support \(/en-us/company/support/\)](/en-us/company/support/)

STAY INFORMED

Sign up to receive the latest security news and trends from Trustwave.

SUBSCRIBE

No spam, unsubscribe at any time.

- LEGAL (/EN-US/LEGAL-DOCUMENTS/)**
TERMS OF USE (/EN-US/LEGAL-DOCUMENTS/TERMS-OF-USE/)
PRIVACY POLICY (/EN-US/LEGAL-DOCUMENTS/PRIVACY-POLICY/)

UNITED STATES - ENGLISH ☐

Copyright © 2020 Trustwave Holdings, Inc.
All rights reserved.

EXHIBIT F



(/en-us/)



NEWSROOM

Trustwave News Releases document our latest announcements, including corporate news, product and service launches and industry accolades.

🕒 March 06, 2012



- *Acquisition strengthens Trustwave's cloud and managed security services*
- *Products and advanced anti-malware technology prevent targeted, Web-based security threats*
- *Trustwave enters multi-billion dollar Web security market*

CHICAGO - March 6, 2012 - Trustwave, a leading provider of cloud-based compliance and information security (<https://www.trustwave.com/>) solutions, today announced it has signed a definitive agreement to acquire M86 Security, a global leader in Web security solutions and advanced anti-malware technology. The acquisition is expected to close within the next few weeks, and financial terms were not disclosed.

"By acquiring M86 Security, Trustwave is adding Web security to one of the industry's most comprehensive security (<https://www.trustwave.com/>) product portfolios - including our compliance, application, network and data security solutions," Robert J. McCullen, Chairman, Chief Executive Officer and President, Trustwave. "Customers and partners will benefit from our simplified approach to delivering advanced anti-malware technology through the cloud and our managed services."

With the acquisition, Trustwave aims to protect its customers from the more than 90 percent of all malware that is delivered through the Web. Even "good" websites, including social networks and news sites, can serve up malware designed to compromise users' computers and steal data: a staggering 80-85 percent of all infected websites are legitimate ones. Additionally, the majority of email threats now come from links to malicious websites rather than through attachments. Combating these threats requires the right products, anti-malware technology and threat intelligence - all areas that will be augmented by Trustwave's acquisition of M86 Security.

With the acquisition of M86 Security, Trustwave is gaining:

- **Web and email security products** - With the acquisition, Trustwave gains M86 Secure Web Gateway, M86 WebMarshal and M86 Web Filtering and Reporting Suite products. Trustwave also enhances its position in email security with the addition



of M86 MailMarshal. In 2011 Gartner, Inc. positioned M86 Security as Visionary in both the Magic Quadrant for Secure Web Gateways and the Magic Quadrant for Secure Email Gateways. (/en-us/)

- **Advanced malware detection technology** - Trustwave also gains advanced anti-malware technologies, including a new cloud-based technology that M86 Security is developing to protect organizations from targeted attacks in emails. Trustwave plans to add these technologies to its existing products, including its cloud-based TrustKeeper portal (<https://www.trustwave.com/trustKeeper.php>).
- **Broader threat intelligence and security research** (<https://www.trustwave.com/spiderlabs/threat-intelligence>) - M86 Security Labs will become part of Trustwave SpiderLabs, the advanced security team within Trustwave focused on penetration testing, incident response, application security and security research. The M86 Security Labs team is a global team of specialized security experts and researchers who provide proactive updates to M86 Security products, enabling customers to detect and defend against new and emerging exploits and malware threats.
- **New Managed Secure Web Gateway based on Trustwave Managed Security Services** -- Trustwave will add the M86 Secure Web Gateway to the broad portfolio of Trustwave Managed Security Services (<https://www.trustwave.com/managed-security-services/>). The company also plans to integrate M86 Security products into Trustwave's cloud-based TrustKeeper portal.
- **Customers and channel partners** - Trustwave gains M86 Security's more than 25,000 customers with 26 million users in more than 96 countries. M86 Security's strong channel and service provider partners also complement Trustwave's existing robust partner network, and Trustwave plans to adopt and expand M86 Security's award-winning partner program, Partner Focus. The acquisition also bolsters Trustwave's international presence particularly in the Europe, Middle East and Africa (EMEA) and Asia Pacific regions.

"Trustwave has a tremendously successful track record of not only finding, acquiring and integrating security companies but also continuing to innovate their products and technologies," said John Vigouroux, Chief Executive Officer, M86 Security.

"Customers and partners have a lot to look forward to as the combination of Trustwave and M86 Security gives them access to a broader, unified security portfolio powered by the industry's most advanced threat technology intelligence."

M86 Security is a privately-held company headquartered in Irvine, Calif. with approximately 300 employees worldwide.

About Trustwave

Trustwave is a leading provider of compliance, Web, application, network and data security solutions delivered through the cloud, managed security services, software and appliances. For organizations faced with today's challenging data security and compliance environment, Trustwave provides a unique approach with comprehensive solutions that include its TrustKeeper® portal and other proprietary security solutions. Trustwave has helped hundreds of thousands of organizations--ranging from Fortune 500 businesses and large financial institutions to small and medium-sized retailers--manage compliance and secure their network infrastructures, data communications and critical information assets. Trustwave is headquartered in Chicago with offices worldwide. For more information, visit <https://www.trustwave.com> (<https://www.trustwave.com/>) .

<https://www.linkedin.com/company/trustwave>
SERVICES (/EN-US/SERVICES/)

<https://www.facebook.com/Trustwave>
CAPABILITIES (/EN-US/CAPABILITIES/)

<https://www.youtube.com/channel/UC83W0djhqA>

- [Managed Security \(/en-us/services/managed-security/\)](/en-us/services/managed-security/)
[Security Testing \(/en-us/services/security-testing/\)](/en-us/services/security-testing/)
[Technology \(/en-us/services/technology/\)](/en-us/services/technology/)
[Consulting \(/en-us/services/consulting/\)](/en-us/services/consulting/)
[Education \(/en-us/services/education/\)](/en-us/services/education/)
- [By Topic \(/en-us/capabilities/by-topic/\)](/en-us/capabilities/by-topic/)
[By Industry \(/en-us/capabilities/by-industry/\)](/en-us/capabilities/by-industry/)
[By Mandate \(/en-us/capabilities/by-mandate/\)](/en-us/capabilities/by-mandate/)

- RESOURCES (/EN-US/RESOURCES/)**
[Blogs & Stories \(/en-us/resources/blogs/\)](/en-us/resources/blogs/)
[Resource Library \(/en-us/resources/library/\)](/en-us/resources/library/)
[Security Resources \(/en-us/resources/security-resources/\)](/en-us/resources/security-resources/)
[Events & Webinars \(/en-us/resources/upcoming/\)](/en-us/resources/upcoming/)
- COMPANY (/EN-US/COMPANY/)**
[About Trustwave \(/en-us/company/about-us/\)](/en-us/company/about-us/)
[Careers \(https://jobs.jobvite.com/trustwave\)](https://jobs.jobvite.com/trustwave)
[Newsroom \(/en-us/company/newsroom/\)](/en-us/company/newsroom/)
[Contact \(/en-us/company/contact/\)](/en-us/company/contact/)
[Support \(/en-us/company/support/\)](/en-us/company/support/)

STAY INFORMED
Sign up to receive the latest security news and trends from Trustwave.

SUBSCRIBE

No spam, unsubscribe at any time.

- LEGAL (/EN-US/LEGAL-DOCUMENTS/)**
TERMS OF USE (/EN-US/LEGAL-DOCUMENTS/TERMS-OF-USE/)
PRIVACY POLICY (/EN-US/LEGAL-DOCUMENTS/PRIVACY-POLICY/)

UNITED STATES - ENGLISH ☐

Copyright © 2020 Trustwave Holdings, Inc.
All rights reserved.

EXHIBIT G

interim PM amid political uncertainty

7 MINUTES AGO



coronavirus vaccine as pandemic...

29 MINUTES AGO



DEFORESTATION RISK PART ONE – **FREE MAGAZINE**

A deep-dive into the supply chains for palm oil, forest and timber products.

Download the 60-page magazine issue now

[Download today >](#)



TECHNOLOGY NEWS

APRIL 7, 2015 / 9:00 PM / 5 YEARS AGO

Singtel buying U.S. cyber security firm Trustwave for \$810 million

Aradhana Aravindan



SINGAPORE (Reuters) - Singapore Telecommunications, Southeast Asia's largest telecommunications operator by revenue, is buying U.S.-based cyber-security firm Trustwave for \$810 million, marking its biggest acquisition outside the main telecoms sector.



NOW READING Singtel buying U.S. cyber security firm Trustwave for \$810 million

Malaysia's Mahathir returns as interim PM amid political uncertainty

7 MINUTES AGO



Washington pledges \$1 billion for coronavirus vaccine as pandemic...

29 MINUTES AGO



A man walks past a Singtel pay phone booth at their head office in Singapore February 12, 2015. REUTERS/Edgar Su

The deal comes as Singtel is moving away from being a pure-play telecoms company and pursues expansion in areas such as “digital life”, which includes mobile video and digital advertising, and cyber security through partnerships with FireEye Inc and Akamai, among others.

It also comes as the managed security services industry - which refers to the management of an IT system by a third party - is forecast to grow 15 percent annually from 2014 to reach \$24 billion in 2018, according to IT consultancy Gartner.

That growth potential has already stoked other acquisitions in the cyber-security business, including BAE Systems’s \$232.5 million deal to buy SilverSky and FireEye’s \$1 billion takeover of Mandiant Corp, both in 2014.

“Today’s acquisition of Trustwave is a critical step to capturing global opportunities in the cyber security market,” Singtel CEO Chua Sock Koong told reporters at a briefing.

Before Wednesday’s deal, Singtel spent about S\$900 million (\$663 million) on acquisitions since 2012, mainly to build its digital life business.

Singtel, which owns stakes in regional operators including India’s Bharti Airtel and Thailand’s Advanced Info Service PCL, will buy a 98 percent equity stake in the company from a group of investors assembled by Trustwave’s chairman and chief executive officer, Robert McCullen. He will hold the remaining 2 percent.

NOW READING Singtel buying U.S. cyber security firm Trustwave for \$810 million

Malaysia's Mahathir returns as interim PM amid political uncertainty

7 MINUTES AGO



Washington pledges \$1 billion for coronavirus vaccine as pandemic...

29 MINUTES AGO



names of specific clients.

Trustwave reported revenue of \$216 million in 2014, with the North American market contributing 75 percent.

Last year, Trustwave withdrew its application with the U.S. Securities and Exchange Commission to sell shares in an initial public offering, citing unfavorable market conditions.

Singtel expects the deal, which will be funded through debt and cash, to be completed in three to six months. It forecast the transaction to add to earnings from the third year.

ADVERTISEMENT



PAID FOR AND POSTED BY FISHER INVESTMENTS

2020 Election Analysis

Is it possible to draw conclusions from current polls?

[Read to Learn More >](#)

The Asian unit of U.S. investment bank Evercore advised Singtel on the deal.

Singtel shares were trading down 0.9 percent on Wednesday morning in a broader Singapore market that was down 0.3 percent.

(\$1 = 1.3582 Singapore dollars)

Editing by Muralikumar Anantharaman

NOW READING Singtel buying U.S. cyber security firm Trustwave for \$810 million

Malaysia's Mahathir returns as interim PM amid political uncertainty

7 MINUTES AGO



Washington pledges \$1 billion for coronavirus vaccine as pandemic...

29 MINUTES AGO



NOW READING Singtel buying U.S. cyber security firm Trustwave for \$810 million

Malaysia's Mahathir returns as interim PM amid political uncertainty

7 MINUTES AGO



Washington pledges \$1 billion for coronavirus vaccine as pandemic...

29 MINUTES AGO



Taking root. How can investors protect the world's plants and forests?

UBS



New Year, new decade, new Brexit?

Nomura



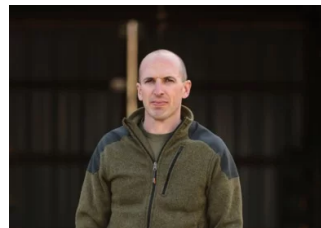
Motley Fool Issues Rare "All In" Buy Alert

The Motley Fool



Compare The Top Travel Credit Cards

NerdWallet



Gold Will Have Its Day Again... soon

The Manward Letter

Sponsored Video by



Turn your stay into another vacay

Learn more

The IHG® Rewards Club Premier Credit Card



NOW READING **Singtel buying U.S. cyber security firm Trustwave for \$810 million**

Malaysia's Mahathir returns as interim PM amid political uncertainty

7 MINUTES AGO



Washington pledges \$1 billion for coronavirus vaccine as pandemic...

29 MINUTES AGO



Video Ad by [dianomi](#)

MORE FROM REUTERS



Weinstein found guilty of sexual assault, rape, in victory for...

25 Feb



Battle against coronavirus turns to Italy; Wall Street falls on...

25 Feb



Virus can still be beaten, too early to declare pandemic: WHO

24 Feb



Stocks tumble, oil falls, gold spikes as virus fears grip markets

24 Feb



Coronavirus clampdown spreads fear and doubt in northern Italy

24 Feb

NOW READING Singtel buying U.S. cyber security firm Trustwave for \$810 million

Malaysia's Mahathir returns as interim PM amid political uncertainty

7 MINUTES AGO



Washington pledges \$1 billion for coronavirus vaccine as pandemic...

29 MINUTES AGO



NOW READING Singtel buying U.S. cyber security firm Trustwave for \$810 million

Malaysia's Mahathir returns as interim PM amid political uncertainty

7 MINUTES AGO



Washington pledges \$1 billion for coronavirus vaccine as pandemic...

29 MINUTES AGO



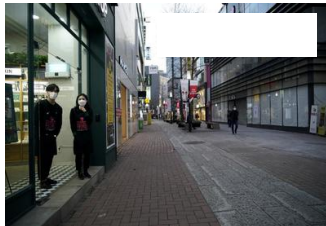
Cargill to challenge Beyond Meat, Impossible Foods with new plant-...

24 Feb



U.S. prepares for coronavirus pandemic, school and business...

21 Feb



South Korea coronavirus cases surge, two more die

24 Feb



Dozens hurt as car plows into German carnival parade

25 Feb



Health insurer shares pummeled by Sanders surge, virus worries

24 Feb

NOW READING Singtel buying U.S. cyber security firm Trustwave for \$810 million

Malaysia's Mahathir returns as interim PM amid political uncertainty

7 MINUTES AGO



Washington pledges \$1 billion for coronavirus vaccine as pandemic...

29 MINUTES AGO



[Apps](#) [Newsletters](#) [Advertise with Us](#) [Advertising Guidelines](#) [Cookies](#) [Terms of Use](#) [Privacy](#)



All quotes delayed a minimum of 15 minutes. See [here](#) for a complete list of exchanges and delays.

NOW READING Singtel buying U.S. cyber security firm Trustwave for \$810 million

Malaysia's Mahathir returns as interim PM amid political uncertainty

7 MINUTES AGO



Washington pledges \$1 billion for coronavirus vaccine as pandemic...

29 MINUTES AGO



EXHIBIT H

Singapore Telecommunications Ltd

GROUP

S\$ Million	Quarterly FY2018/19				Quarterly FY2019/20 ⁽¹⁾				FY2018/19 Total	FY2019/20 Total
	1Q Total	2Q Total	3Q Total	4Q Total	1Q Total	2Q Total	3Q Total	4Q Total		
Income Statement										
Operating revenue	4,134	4,270	4,626	4,342	4,113	4,152	4,378	3,899	17,372	16,542
Operating expenses	(2,992)	(3,191)	(3,483)	(3,238)	(2,978)	(3,040)	(3,255)	2,906	(12,905)	(12,180)
Other income	1,142 65	1,079 50	1,143 47	1,104 63	1,135 49	1,112 50	1,123 41	993 40	4,467 225	4,363 179
EBITDA	1,207	1,129	1,190	1,166	1,184	1,162	1,164	1,032	4,692	4,541
EBITDA margin (%)	29.2%	26.4%	25.7%	26.9%	28.8%	28.0%	26.6%	26.5%	27.0%	27.5%
Share of associates' pre-tax profits	416	330	371	419	359	442	420	521	1,536	1,743
EBITDA & share of associates' pretax profits	1,623	1,459	1,561	1,586	1,543	1,604	1,584	1,554	6,228	6,284
Depreciation	(477)	(472)	(473)	(474)	(561)	(550)	(557)	(561)	(1,896)	(2,229)
Amortisation of intangibles	(77)	(82)	(80)	(88)	(84)	(91)	(76)	(100)	(326)	(352)
Depreciation & amortisation	(554)	(554)	(553)	(561)	(644)	(641)	(633)	(662)	(2,222)	(2,580)
EBIT	1,069	905	1,007	1,025	898	963	951	892	4,006	3,704
Net finance expense	(70)	(94)	(98)	(93)	(51)	18	(156)	(93)	(355)	(282)
Profit before EI and tax	999	811	909	932	847	981	794	799	3,651	3,422
Taxation	(271)	(102)	(235)	(241)	(279)	(250)	(250)	(209)	(850)	(988)
Profit after tax	728	709	674	691	569	731	544	591	2,801	2,434
Minority interests	5	6	6	6	6	6	7	3	23	22
Underlying net profit	733	715	680	697	575	737	551	594	2,825	2,457
Exceptional items (post-tax)	98	(48)	143	76	(34)	(1,405)	76	(19)	270	(1,382)
Net profit	832	667	823	773	541	(668)	627	574	3,095	1,075
Group Operating Revenue Composition										
Mobile service	1,392	1,353	1,338	1,312	1,245	1,231	1,226	1,153	5,396	4,855
Sale of equipment	579	649	929	708	682	614	768	504	2,865	2,568
Leasing	17	25	54	45	50	54	50	46	141	200
Mobile service	1,988	2,027	2,322	2,064	1,976	1,899	2,044	1,703	8,401	7,623
Data and Internet	827	824	831	871	859	944	983	871	3,353	3,052
Infocomm Technology ("ICT")	679	745.0	771.0	839.0	682	731	769	826	3,034	3,612
Digital Businesses	271	313	383	278	307	297	326	239	1,245	1,169
Fixed voice	246	242	219	192	194	183	165	164	899	705
Pay television	104	103	85	81	80	79	77	78	373	314
Others	18	16	16	18	16	19	13	20	67	68
	4,134	4,270	4,626	4,342	4,113	4,152	4,378	3,899	17,372	16,542
Group Operating Expenses Composition										
Selling and administrative	622	645	621	603	497	524	527	539	2,490	2,087
Traffic expenses	392	399	397	387	383	406	407	397	1,573	1,593
Staff costs	677	666	626	622	628	649	616	534	2,590	2,426
Cost of sales	1,234	1,380	1,726	1,520	1,371	1,366	1,599	1,318	5,860	5,654
Repair and maintenance	86	96	105	101	98	89	92	111	388	390
Others	(17)	6	9	6	1	6	15	8	3	29
	2,992	3,191	3,483	3,238	2,978	3,040	3,255	2,906	12,905	12,180

Notes:

(1): With effect from 1 April 2019, the Group has adopted SFRS(l) 16, *Leases*, on prospective basis with no restatement to the comparatives.

Q4FY20	SINGTEL EX OPTUS (\$ million)					OPTUS (A\$ million)		Associates	Total	SUPPLEMENTARY INFORMATION	
	Singapore Consumer	Singapore Enterprise ⁽¹⁾	Group Digital Life	International Group	Corporate	Australia Consumer	Australia Enterprise ⁽³⁾			NCS ⁽²⁾	Trustwave ⁽²⁾ (US\$)
Operating Revenue	465	1,282	234	2	-	1,801	303		3,899	637	112
Operating expenses	(286)	(916)	(240)	(23)	(18)	(1,278)	(285)		(2,906)	(540)	(106)
Other income	3	11	3	(1)	4	21	3		40	1	1
EBITDA	181	377	(4)	(21)	(15)	543	21		1,032	98	7
EBITDA margin (%)	38.9%	29.4%				30.2%	6.9%		26.5%	15.5%	29.9%
Share of associates' pre-tax profits	-	-	-	-	-	-	-	521	521		
EBITDA & share of associates' pretax profits	181	377	(4)	(21)	(15)	543	21		1,554	98	7
Depreciation & amortisation	(65)	(148)	(28)	(1)	(1)	(402)	(56)		(662)	(24)	(19)
EBIT	116	229	(32)	(23)	(16)	141	(35)		892	74	(12)
Net finance expense									(93)		
Profit before EI and tax									799		
Taxation									(209)		
Profit after tax									591		
Minority interests									3		
Underlying net profit									594		
Exceptional items (post-tax)									(19)		
Net profit									574		

(1): Singapore enterprise revenues includes Trustwave and NCS.

(2): Pre-elim basis.

(3): Australia enterprise revenues includes Hivint.

FY20	SINGTEL EX OPTUS (\$ million)					OPTUS (A\$ million)		Associates	Total	SUPPLEMENTARY INFORMATION	
	Singapore Consumer	Singapore Enterprise ⁽¹⁾	Group Digital Life	International Group	Corporate	Australia Consumer	Australia Enterprise ⁽³⁾			NCS ⁽²⁾	Trustwave ⁽²⁾ (US\$)
Operating Revenue	2,110	4,899	1,145	10	-	7,753	1,205		16,542	2,142	391
Operating expenses	(1,381)	(3,444)	(1,196)	(67)	(91)	(5,300)	(1,118)		(12,180)	(1,863)	(424)
Other income	28	41	2	2	4	100	9		179	13	1
EBITDA	757	1,496	(48)	(55)	(87)	2,553	96		4,541	293	(32)
EBITDA margin (%)	35.9%	30.5%				32.9%	8.0%		27.5%	15.3%	33.1%
Share of associates' pre-tax profits	-	-	-	-	-	-	-	1,743	1,743		
EBITDA & share of associates' pretax profits	757	1,496	(48)	(55)	(87)	2,553	96		6,284	293	(32)
Depreciation & amortisation	(260)	(520)	(92)	(5)	(5)	(1,593)	(223)		(2,580)	(83)	(46)
EBIT	497	976	(140)	(60)	(92)	960	(128)		3,704	210	(78)
Net finance expense									(282)		
Profit before EI and tax									3,422		
Taxation									(988)		
Profit after tax									2,434		
Minority interests									22		
Underlying net profit									2,457		
Exceptional items (post-tax)									(1,382)		
Net profit									1,075		

(1): Singapore enterprise revenues includes Trustwave and NCS.

(2): Pre-elim basis.

(3): Australia enterprise revenues includes Hivint.

Singapore Telecommunications Ltd

SINGAPORE CONSUMER

S\$ Million	Quarterly FY2018/19				Quarterly FY2019/20 ⁽¹⁾					
	1Q Total	2Q Total	3Q Total	4Q Total	1Q Total	2Q Total	3Q Total	4Q Total	FY2018/19 Total	FY2019/20 Total
Income Statement										
Operating revenue	545	554	596	539	518	563	565	465	2,234	2,110
Operating expenses	(356)	(375)	(407)	(373)	(336)	(382)	(376)	(286)	(1,510)	(1,381)
Other income	6	4	8	6	7	11	8	3	25	28
EBITDA	196	183	197	172	188	191	197	181	748	757
EBITDA Margin (%)	35.9%	33.1%	33.1%	31.9%	36.3%	34.0%	34.9%	38.9%	33.5%	35.9%
Depreciation & amortisation	(61)	(62)	(61)	(63)	(65)	(65)	(65)	(65)	(247)	(260)
EBIT	135	121	136	109	123	126	132	116	501	497
Singapore Consumer Operating Revenue Composition										
Total Mobile Revenue	368	388	447	390	365	408	414	313	1,591	1,500
Mobile service	265	257	261	248	248	244	243	218	1,031	954
Equipment	103	131	185	140	115	162	168	92	558	537
Leasing	-	*	1	1	2	2	2	3	2	9
Fixed broadband	62	61	61	62	63	64	64	64	246	254
Residential Pay TV	65	66	49	49	48	49	50	50	230	197
Fixed voice	33	32	29	28	29	28	28	28	122	113
Others	18	7	10	11	12	14	10	10	45	47
	545	554	596	539	518	563	565	465	2,234	2,110
Singapore Consumer Operating Expenses Composition										
Selling and administrative	72	73	73	80	69	72	69	73	298	283
Traffic expenses	52	50	48	45	44	43	43	41	194	172
Staff costs	56	59	53	53	50	54	48	33	221	185
Cost of sales	170	187	227	187	165	205	210	136	771	716
Repair and maintenance	12	13	12	13	12	15	11	12	51	50
Others	(6)	(6)	(6)	(5)	(5)	(6)	(6)	(8)	(24)	(24)
	356	375	407	373	336	382	376	286	1,510	1,381

Notes:

(1): With effect from 1 April 2019, the Group has adopted SFRS(I) 16, *Leases*, on prospective basis with no restatement to the comparatives.

Singapore Telecommunications Ltd

AUSTRALIA CONSUMER

A\$ Million	Quarterly FY2018/19				Quarterly FY2019/20 ⁽¹⁾				FY2018/19 Total	FY2019/20 Total
	1Q Total	2Q Total	3Q Total	4Q Total	1Q Total	2Q Total	3Q Total	4Q Total		
Income Statement										
Operating revenue	1,792	1,830	2,072	1,964	1,938	1,918	2,096	1,800	7,659	7,753
Operating expenses	1,227	1,292	1,484	1,296	1,315	1,262	1,445	1,278	5,299	5,300
Other income	32	36	27	28	26	28	25	21	123	100
EBITDA	597	574	615	697	649	684	677	543	2,483	2,553
EBITDA Margin (%)	33.3%	31.3%	29.7%	35.5%	33.5%	35.7%	32.3%	30.20%	32.4%	32.9%
Depreciation & amortisation	325	325	327	328	411	388	391	402	1,304	1,593
EBIT	272	249	288	369	238	296	285	141	1,178	960

Australia Consumer Operating Revenue Composition

Total Mobile Revenue	1,313	1,355	1,585	1,444	1,406	1,305	1,449	1,288	5,697	5,448
Mobile service	916	898	897	912	855	866	869	863	3,623	3,452
Equipment	380	433	634	486	501	384	528	378	1,933	1,791
Leasing	17	24	54	45	50	55	52	48	141	205
Total Retail Fixed ² (previously Mass Market Fixed)	323	320	341	376	386	462	498	350	1,361	1,695
Total Wholesale Fixed ³	156	155	146	145	146	152	150	162	601	610
NBN migration and site preparation revenues	24	23	44	93	98	187	233	90	184	607

Australia Consumer Operating Expenses Composition

Selling and administrative	361	369	355	329	276	294	318	303	1,424	1,191
Traffic expenses	211	225	226	229	238	263	268	273	891	1,041
Staff costs	177	154	145	130	144	146	133	106	597	529
Cost of sales	447	488	697	563	599	514	665	537	2,195	2,315
Repair and maintenance	29	40	45	39	45	29	41	43	153	157
Others	1	16	16	6	13	16	21	16	40	67
	1,227	1,292	1,484	1,296	1,315	1,262	1,445	1,278	5,299	5,300

Notes:

(1): With effect from 1 April 2019, the Group has adopted SFRS(I) 16, Leases, on prospective basis with no restatement to the comparatives.

(2) Include small-sized businesses

(3) Include medium-sized businesses

Singapore Telecommunications Ltd

GROUP ENTERPRISE

S\$ Million	Quarterly FY2018/19				Quarterly FY2019/20 ⁽¹⁾					
	1Q Total	2Q Total	3Q Total	4Q Total	1Q Total	2Q Total	3Q Total	4Q Total	FY2018/19 Total	FY2019/20 Total
Income Statement										
Operating revenue	1,519	1,573	1,606	1,632	1,442	1,489	1,536	1,559	6,329	6,026
Singapore enterprise revenue	1,129	1,204	1,263	1,303	1,142	1,216	1,259	1,282	4,899	4,899
Australia enterprise revenue (A\$ million)	386	369	347	341	315	290	298	303	1,444	1,205
Operating expenses	(1,095)	(1,143)	(1,188)	(1,276)	(1,041)	(1,113)	(1,160)	(1,175)	(4,702)	(4,489)
Other income	24	10	11	23	16	13	7	13	68	49
EBITDA	449	440	428	379	417	389	383	397	1,695	1,587
Singapore enterprise EBITDA	389	383	380	329	380	376	362	377	1,481	1,496
Australia enterprise EBITDA (A\$ million)	60	57	49	51	39	14	22	21	217	96
EBITDA Margin (%)	29.5%	28.0%	26.7%	23.2%	28.9%	26.1%	25.0%	25.5%	26.8%	26.3%
Depreciation & amortisaion	(150)	(151)	(152)	(162)	(164)	(186)	(179)	(199)	(615)	(729)
EBIT	299	289	276	216	253	203	204	198	1,080	858
Group Enterprise Operating Revenue Composition										
Managed Services	426	457	488	510	403	426	447	501	1,881	1,777
Business Application Services	120	121	114	130	131	140	138	156	485	564
Cyber Security	114	138	137	160	120	136	147	163	549	566
Communications Engineering	20	29	31	39	27	29	38	51	119	145
ICT	679	745	771	839	682	731	769	871	3,034	3,052
Mobile	293	284	311	280	267	260	280	216	1,168	1,022
Mobile service	202	197	192	182	179	168	171	146	773	663
Sale of equipment	91	86	119	98	88	93	109	70	395	359
Data & Internet	405	410	398	392	378	384	384	363	1,605	1,510
Fixed voice	124	120	112	106	103	98	92	91	462	384
Others	18	14	14	15	13	16	11	18	62	57
Carriage	840	828	835	793	761	758	767	688	3,296	2,974
	1,519	1,573	1,606	1,632	1,442	1,489	1,536	1,559	6,329	6,026
Group Enterprise Operating Expenses Composition										
Selling and administrative	155	160	158	165	133	143	138	171	638	585
Traffic expenses	127	124	125	120	112	115	114	108	496	448
Staff costs	370	373	351	361	357	376	369	334	1,454	1,435
Cost of sales	410	454	515	583	408	443	505	510	1,962	1,866
Repair and maintenance	41	38	41	44	36	41	37	55	165	170
Others	(7)	(6)	(2)	2	(5)	(4)	(3)	(3)	(12)	(15)
	1,095	1,143	1,188	1,276	1,041	1,113	1,160	1,175	4,702	4,489

Notes:

(1): With effect from 1 April 2019, the Group has adopted SFRS(I) 16, *Leases*, on prospective basis with no restatement to the comparatives.

Singapore Telecommunications Ltd

GROUP DIGITAL LIFE

S\$ Million	Quarterly FY2018/19				Quarterly FY2019/20 ⁽¹⁾					
	1Q Total	2Q Total	3Q Total	4Q Total	1Q Total	2Q Total	3Q Total	4Q Total	FY2018/19 Total	FY2019/20 Total
Income Statement										
Operating revenue	259	313	379	274	301	289	321	234	1,224	1,145
Digital marketing	269	322	385	274	305	293	324	237	1,250	1,159
Others	7	7	9	16	11	11	12	13	40	47
Intercompany eliminations	(18)	(16)	(15)	(16)	(14)	(15)	(15)	(16)	(66)	(61)
Operating expenses	(283)	(347)	(394)	(291)	(313)	(313)	(330)	(240)	(1,315)	(1,196)
Other gain/(loss)	1	-	(1)	*	*	*	*	3	(0)	2
EBITDA	(23)	(34)	(16)	(18)	(12)	(25)	(8)	(4)	(92)	(48)
Depreciation & amortisation	(13)	(15)	(15)	(17)	(20)	(21)	(22)	(28)	(60)	(92)
EBIT	(36)	(49)	(32)	(35)	(32)	(46)	(30)	(32)	(152)	(140)
Group Digital Life Operating Expense Composition										
Cost of sales	203	251	298	206	227	233	262	183	957	904
Staff costs	55	65	64	55	62	55	52	54	239	223
Selling & administrative	22	26	25	25	18	19	10	(1)	98	45
Others	4	5	7	6	6	6	7	6	22	24
	283	347	394	291	313	313	330	240	1,315	1,196

Notes:

(1): With effect from 1 April 2019, the Group has adopted SFRS(I) 16, *Leases*, on prospective basis with no restatement to the comparatives.

Singapore Telecommunications Ltd

ASSOCIATES

	Quarterly FY2018/19				Quarterly FY2019/20				FY2018/19	FY2019/20
	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q		
<u>Associates PBT before EI (\$\$ million)</u>										
Telkomsel	237	291	305	296	280	290	289	310	1,128	1,169
AIS	94	79	80	91	94	103	84	84	343	365
Bharti	(63)	(176)	(129)	(143)	(162)	(112)	(87)	(42)	(511)	(403)
Globe	95	88	65	120	98	104	85	123	368	410
Intouch	28	22	21	25	26	29	22	24	96	101
Regional associates subtotal	391	303	342	389	335	414	393	500	1,424	1,642
Others	25	27	29	31	24	29	27	23	112	103
Total	416	330	371	419	359	442	420	523	1,536	1,744
<u>Associates PAT after EI (\$\$ million)</u>										
Telkomsel	177	216	227	223	207	215	217	247	843	885
AIS	78	66	67	76	78	86	72	70	286	305
Bharti	19	(6)	(86)	(98)	(119)	(107)	(93)	(41)	(171)	(359)
Globe	65	60	42	82	66	70	58	84	251	278
Intouch	23	18	17	21	21	24	18	20	79	83
Regional associates subtotal	363	354	268	304	253	287	271	380	1,287	1,191
Others	21	23	24	28	20	25	23	18	95	85
Total	384	377	291	331	273	313	294	398	1,383	1,277
<u>Associates Dividends (\$\$ million)</u>										
Telkomsel	954	-	-	-	802	-	104	-	954	906
AIS	102	109	-	-	98	114	-	-	211	212
Bharti	-	30	29	-	-	-	-	-	59	-
Globe	36	36	36	36	37	37	37	44	144	154
Intouch	41	38	-	-	34	40	-	-	79	73
Regional associates subtotal	1,133	213	65	36	970	191	141	44	1,447	1,346
Others	49	14	34	5	39	19	33	3	102	94
Total	1,182	227	99	41	1,009	210	174	46	1,549	1,439
<u>Associates mobile subs ('000)</u>										
Telkomsel	177,888	167,809	162,988	168,642	167,792	170,928	171,105	162,567	168,642	162,567
AIS	40,095	40,647	41,169	41,491	41,464	41,558	42,014	41,156	41,491	41,156
Bharti	438,040	429,287	384,656	384,078	383,375	386,151	393,109	397,200	384,078	397,200
- India	344,564	332,764	284,224	282,640	281,132	279,430	283,036	283,667	282,640	283,667
- Africa	91,193	94,096	97,922	98,851	99,670	103,881	107,140	110,604	98,851	110,604
- South Asia	2,283	2,427	2,510	2,587	2,573	2,840	2,933	2,929	2,587	2,929
Globe	65,142	65,360	74,094	83,490	92,942	97,358	94,204	89,320	83,490	89,320
Intouch's share of AIS	NM	NM	NM	NM	NM	NM	NM	NM	NM	NM
Total	721,165	703,103	662,907	677,701	685,573	695,995	700,432	690,243	677,701	690,243

Singapore Telecommunications Ltd And Subsidiary Companies

SINGAPORE PRODUCT INFORMATION

	Quarterly FY2018/19				Quarterly FY2019/20				FY2018/19	FY2019/20
	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q		
International telephone										
IDD outgoing mins (mil)	527	483	429	434	368	333	312	308	1,874	1,322
IDD ave collection rate (S\$/ min)	0.086	0.087	0.088	0.086	0.097	0.096	0.092	0.089	0.087	0.094
National telephone										
Res Fixed Working Lines ('000s)	764	758	751	747	742	739	736	734	747	734
Biz Fixed Working Lines ('000s)	632	621	609	594	576	558	541	523	594	523
Total Fixed Working Lines ('000s) ⁽²⁾	1,396	1,379	1,360	1,341	1,318	1,297	1,277	1,257	1,341	1,257
Mobile Revenue ⁽³⁾ (S\$m)	588	606	693	611	576	617	637	476	2,499	2,306
Mobile Service Revenue ⁽⁴⁾	421	411	410	390	390	378	376	329	1,632	1,473
mobile subscribers ('000s)										
- Prepaid	1,616	1,620	1,641	1,621	1,607	1,615	1,592	1,578	1,621	1,578
- Postpaid	2,465	2,506	2,542	2,574	2,609	2,639	2,673	2,704	2,574	2,704
- Total	4,081	4,126	4,183	4,195	4,216	4,254	4,265	4,282	4,195	4,282
mobile ARPU (S\$)										
- Prepaid	18	18	18	17	17	17	16	14	18	16
- Postpaid	46	43	43	41	40	39	39	33	43	38
- Blended	35	33	33	32	31	30	30	26	33	30
Data as % ARPU	64%	62%	64%	65%	65%	66%	67%	66%	64%	66%
Data and internet										
Total Fixed Broadband lines ('000)	621	624	628	630	632	637	640	642	630	642
Fibre Broadband lines ('000)	609	616	624	629	632	636	640	642	629	642
Singtel TV										
Total Singtel TV customers ('000)	387	383	381	381	382	383	383	382	381	382
On-the-go service customers ('000)	109	114	116	118	130	162	193	215	118	215
Number of households on triple/quad play services ('000)	507	513	515	517	518	520	520	518	517	518

Note

(1): With effect from 1 April 2019, the Group has adopted SFRS(I) 16, *Leases*, on prospective basis with no restatement to the comparatives.

(2): Fixed working lines refer to Direct Exchange Lines (DEL) and Home Digital Lines.

(3): This comprises revenues from mobile service, sale of mobile equipment and handset leasing.

(4): This is determined net of bill rebates and prepaid sales discount, and includes mobile revenue earned from international telephone calls and broadband bundles.

Singapore Telecommunications Ltd
OPTUS PRODUCT INFORMATION

	FY2018/19 (A\$)					FY2019/20 (A\$) ⁽¹⁾				
Product Information for Total Optus	Q1	Q2	Q3	Q4	YTD	Q1	Q2	Q3	Q4	YTD
Optus Mobile Revenue (A\$m)	1,386	1,422	1,652	1,506	5,966	1,467	1,360	1,511	1,348	5,687
Optus Mobile Service Revenue (A\$m)	963	943	942	956	3,803	897	903	912	903	3,614
Mobile										
Mobile customers (000s)										
Prepaid handset	3,724	3,604	3,532	3,423	3,423	3,371	3,346	3,503	3,381	3,381
Postpaid handset	5,335	5,428	5,557	5,683	5,683	5,734	5,763	5,820	5,824	5,824
Mobile broadband	1,113	1,139	1,159	1,175	1,175	1,181	1,184	1,198	1,243	1,243
Total mobile customers	10,172	10,171	10,247	10,281	10,281	10,285	10,293	10,522	10,448	10,448
Mobile ARPUs (A\$)										
Prepaid handset	19	19	18	18	19	18	19	18	18	18
Postpaid handset	42	41	41	42	42	38	38	38	37	37
Mobile broadband	22	21	20	20	21	19	19	19	20	19
Blended	32	31	31	31	31	29	29	29	29	29
Postpaid Handset (pre SFRS(I) 15 basis)	58	57	56	57	57	NA	NA	NA		NA
Data as % of service revenue	80%	79%	79%	78%	78%	84%	84%	84%	85%	85%
Retail Fixed²										
Standalone Telephony customers (000's)	88	87	94	95	95	66	63	59	55	55
Broadband customers (000's)										
On-net bundle and standalone broadband	653	635	607	557	557	480	377	284	228	228
HFC	395	391	381	352	352	303	232	168	135	135
ULL	258	244	226	205	205	176	145	116	94	94
Off-net bundle and standalone broadband	524	532	571	616	616	661	739	814	858	858
NBN	495	506	549	597	597	646	726	803	848	848
RDSL	29	26	22	19	19	15	13	12	10	10
Total Broadband	1,177	1,167	1,178	1,173	1,173	1,141	1,116	1,098	1,087	1,087
Total Fixed Customers	1,265	1,254	1,272	1,268	1,268	1,207	1,179	1,157	1,142	1,142
Mass Market Fixed										
Telephony customers (000's)										
HFC	402	399	387	358	358					
ULL	310	293	273	247	247					
Offnet (resale)	39	34	31	28	28					
NBN	488	520	560	608	608					
Broadband customers (000's)										
Business	24	24	24	23	23					
HFC	395	391	381	353	353					
ULL	322	303	282	255	255					
Total on-net	741	719	686	631	631					
Offnet (resale)	25	23	21	17	17					
NBN	483	516	540	590	590					
Total Broadband subscribers	1,249	1,257	1,247	1,238	1,238					

Note:

(1): With effect from 1 April 2019, the Group has adopted SFRS(I) 16, Leases, on prospective basis with no restatement to the comparatives.

(2): Review of our fixed disclosures to better align with the market.

Singapore Telecommunications Ltd

GROUP

S\$ Million	Quarterly FY2017/18 ⁽¹⁾				Quarterly FY2018/19				Quarterly FY2019/20 ⁽¹⁾				FY2018/19	FY2019/20
	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q		
Balance Sheet														
Current assets (excluding cash)	7,367	6,246	6,768	6,234	6,205	6,074	6,721	6,565	6,295	6,370	6,492	6,176	6,565	6,176
Cash and bank balances	632	651	841	525	625	707	637	513	579	551	576	1,000	513	1,000
Non-current assets	41,316	41,254	41,464	41,737	40,973	40,645	41,392	41,837	43,499	42,146	41,865	41,779	41,837	41,779
Total assets	49,315	48,151	49,073	48,496	47,803	47,425	48,750	48,915	50,373	49,067	48,933	48,955	48,915	48,955
Current liabilities	7,905	7,107	9,892	8,429	7,696	7,774	9,250	8,794	9,350	10,602	10,799	10,579	8,794	10,579
Non-current liabilities	12,523	11,064	9,632	10,355	9,660	10,744	10,571	10,311	11,078	10,917	11,263	11,562	10,311	11,562
Total liabilities	20,427	18,171	19,523	18,784	17,356	18,518	19,820	19,105	20,427	21,518	22,062	22,141	19,105	22,141
Net assets	28,887	29,980	29,550	29,712	30,447	28,907	28,930	29,810	29,946	27,549	26,871	26,814	29,810	26,814
Share capital	4,127	4,127	4,127	4,127	4,127	4,127	4,127	4,127	4,127	4,127	4,127	4,127	4,127	4,127
Retained earnings	25,992	27,118	26,474	27,269	28,101	27,026	26,740	27,513	27,784	25,373	24,890	25,448	27,513	25,448
Currency translation reserve (loss)	(228)	(420)	(667)	(1,284)	(1,416)	(1,967)	(1,819)	(1,768)	(1,670)	(1,657)	(1,880)	(2,444)	(1,768)	(2,444)
Other reserves	(999)	(834)	(360)	(376)	(361)	(268)	(97)	(35)	(262)	(254)	(215)	(342)	(35)	(342)
Equity attributable to shareholders	28,893	29,991	29,574	29,737	30,452	28,919	28,952	29,838	29,980	27,590	26,923	26,789	29,838	26,789
Minority interest	(5)	(12)	(24)	(26)	(5)	(11)	(22)	(28)	(34)	(41)	(52)	25	(28)	25
	28,887	29,980	29,550	29,712	30,447	28,907	28,930	29,810	29,946	27,549	26,871	26,814	29,810	26,814

Notes:

(1): With effect from 1 April 2019, the Group has adopted SFRS(I) 16, *Leases*, on prospective basis with no restatement to the comparatives.

Singapore Telecommunications Ltd

GROUP - Pre SFRS(I) adjustments

S\$ Million	Quarterly FY2016/17				Quarterly FY2017/18						
	1Q Total	2Q Total	3Q Total	4Q Total	1Q Total	2Q Total	3Q Total	4Q Total	FY2015/16	FY2016/17	FY2017/18
Income Statement											
Operating revenue	3,908	4,086	4,410	4,308	4,232	4,370	4,603	4,326	16,961	16,711	17,532
Operating expenses	(2,732)	(2,901)	(3,236)	(3,061)	(3,036)	(3,125)	(3,391)	(3,150)	(12,097)	(11,929)	(12,702)
Other income	1,176	1,186	1,174	1,247	1,197	1,245	1,213	1,177	4,864	4,782	4,830
	60	47	47	61	73	47	81	58	148	215	259
EBITDA	1,236	1,233	1,221	1,308	1,269	1,292	1,293	1,235	5,013	4,998	5,089
EBITDA margin (%)	31.6%	30.2%	27.7%	30.4%	30.0%	29.6%	28.1%	28.5%	29.6%	29.9%	29.0%
Share of associates' pre-tax profits	753	725	694	713	730	659	553	519	2,791	2,886	2,461
EBITDA & share of associates' pretax profits	1,989	1,958	1,915	2,022	1,999	1,951	1,846	1,754	7,804	7,884	7,550
Depreciation	(476)	(480)	(491)	(513)	(499)	(520)	(512)	(511)	(1,892)	(1,960)	(2,041)
Amortisation of intangibles	(67)	(69)	(71)	(72)	(73)	(79)	(74)	(73)	(257)	(279)	(299)
Depreciation & amortisation	(543)	(549)	(562)	(585)	(572)	(599)	(585)	(584)	(2,149)	(2,239)	(2,340)
EBIT	1,445	1,410	1,353	1,437	1,427	1,352	1,261	1,170	5,655	5,645	5,210
Net finance expense	(65)	(71)	(41)	(82)	(88)	(91)	(80)	(85)	(265)	(260)	(345)
Profit before EI and tax	1,380	1,338	1,312	1,355	1,340	1,261	1,180	1,085	5,390	5,385	4,865
Taxation	(441)	(374)	(342)	(380)	(435)	(337)	(290)	(280)	(1,597)	(1,536)	(1,343)
Profit after tax	939	965	970	975	904	924	890	805	3,793	3,849	3,523
Minority interests	4	4	6	8	6	6	8	2	13	22	21
Underlying net profit	943	969	976	983	910	929	898	807	3,805	3,871	3,544
Exceptional items (post-tax)	1	3	(3)	(20)	(18)	1,960	(8)	(26)	66	(18)	1,908
Net profit	944	972	973	963	892	2,889	890	781	3,871	3,853	5,451
Group Operating Revenue Composition											
Mobile communications	1,455	1,466	1,499	1,507	1,478	1,520	1,502	1,455	6,714	5,927	5,955
Data and Internet	784	812	831	893	835	875	887	831	3,138	3,319	3,427
Managed services	515	557	583	633	580	657	579	658	2,014	2,288	2,475
Business solutions	150	156	177	177	126	154	147	166	637	660	593
National telephone	268	271	263	261	251	251	234	228	1,128	1,062	963
International telephone	128	124	116	112	112	110	102	98	542	480	421
Sale of equipment	350	437	653	464	436	378	683	536	1,802	1,904	2,032
Pay television	85	89	93	90	93	98	90	88	285	356	369
Digital Businesses	136	141	154	135	282	285	332	214	476	566	1,113
Others	38	34	42	37	40	42	48	53	226	150	183
	3,908	4,086	4,410	4,308	4,232	4,370	4,603	4,326	16,961	16,711	17,532
Group Operating Expenses Composition											
Selling and administrative	717	722	768	716	722	726	768	707	3,056	2,922	2,923
Traffic expenses	381	386	405	403	393	405	411	406	2,212	1,576	1,616
Staff costs	618	638	628	640	669	680	654	650	2,434	2,523	2,652
Cost of sales	924	1,064	1,334	1,189	1,155	1,210	1,455	1,291	4,020	4,511	5,110
Repair and maintenance	90	90	93	104	93	94	97	84	359	377	368
Others	3	-	8	10	3	11	7	12	16	20	33
	2,732	2,901	3,236	3,061	3,036	3,125	3,391	3,150	12,097	11,929	12,702

Singapore Telecommunications Ltd

SINGAPORE - Pre SFRS(I) adjustments

S\$ Million	Quarterly FY2016/17				Quarterly FY2017/18						
	1Q Singtel	2Q Singtel	3Q Singtel	4Q Singtel	1Q Total	2Q Total	3Q Total	4Q Total	FY2015/16	FY2016/17	FY2017/18
Income Statement											
Operating revenue	1,884	1,920	2,078	2,047	2,041	2,095	2,182	2,078.0	7,663	7,928	8,396.3
Operating expenses	(1,305)	(1,352)	(1,562)	(1,557)	(1,479)	(1,528)	(1,669)	(1,603.0)	(5,524)	(5,776)	(6,279.6)
Other income	579	568	515	489	562	567	513	475.0	2,139	2,152	2,116.7
	4	16	18	23	15	15	12	22.0	48	62	63.9
EBITDA	583	584	534	513	577	582	525	497.0	2,187	2,213	2,180.6
EBITDA margin (%)	31.0%	30.4%	25.7%	25.0%	28.3%	27.8%	24.1%	23.9%	28.5%	27.9%	26.0%
Share of associates' pre-tax profits	753	725	694	713	730	659	552	519.4	2,791	2,886	2,460.6
EBITDA & share of associates' pre-tax profits	1,336	1,309	1,228	1,226	1,307	1,241	1,077	1,016.4	4,978	5,099	4,641.2
Depreciation & amortisation	(207)	(202)	(199)	(215)	(207)	(209)	(209)	(207.3)	(795)	(823)	(833.0)
EBIT	1,129	1,108	1,029	1,011	1,099	1,032	868	809.1	4,183	4,276	3,808.2
Net finance expense	(27)	(35)	(1)	(38)	(41)	(41)	(31)	(38.0)	(141)	(101)	(150.4)
Profit before EI and tax	1,102	1,072	1,028	973	1,058	991	838	771.1	4,042	4,174	3,657.8
Taxation	(358)	(297)	(259)	(266)	(350)	(255)	(195)	(184.8)	(1,198)	(1,180)	(985.7)
Profit after tax	743	776	768	707	708	735	643	586.3	2,844	2,994	2,672.1
Minority interests	4	4	6	8	6	6	8	1.7	13	22	21.1
Underlying net profit	747	780	774	714	714	741	651	588.0	2,856	3,016	2,693.2
Exceptional items ("EI") post-tax	23	4	(0)	(20)	(1)	1,960	(31)	(23.1)	96	7	1,904.2
Net profit	770	784	774	695	713	2,701	619	564.9	2,953	3,023	4,597.4
Singtel Operating Revenue Composition											
Mobile communications	525	520	526	511	506	506	509	487	2,116	2,082	2,008
Data and Internet	396	404	407	411	396	395	390	395	1,573	1,617	1,577
Managed services	369	390	407	486	427	456	428	501	1,395	1,652	1,811
National telephone	71	71	69	68	66	66	64	63	297	279	260
Sale of equipment	66	78	175	106	83	77	166	110	435	425	436
Business solutions	150	156	177	177	126	154	147	166	637	660	593
International telephone	95	87	82	77	74	73	69	66	394	341	281
Pay television	59	63	63	61	63	64	58	56	232	246	241
Digital Businesses	136	141	154	135	282	285	332	214	468	566	1,113
Others	17	12	19	14	18	20	19	20	118	61	77
	1,884	1,920	2,078	2,047	2,041	2,095	2,182	2,078	7,663	7,928	8,396
Singtel Operating Expenses Composition											
Selling and administrative	297	298	373	342	303	296	367	352.4	1,315	1,310	1,319
Traffic expenses	165	159	169	165	151	150	151	147.2	790	658	600
Staff costs	353	368	350	377	396	397	377	387.1	1,358	1,448	1,557
Cost of sales	459	495	624	629	594	644	734	666.1	1,915	2,206	2,638
Repair and maintenance	47	46	51	58	48	49	52	53.4	187	202	202
Others	(16)	(14)	(4)	(13)	(13)	(8)	(11)	(3.2)	(41)	(48)	(35)
	1,305	1,352	1,562	1,557	1,479	1,528	1,669	1,603.0	5,524	5,776	6,280
Depreciation	(181)	(175)	(173)	(188)	(179)	(180)	(185)	(183)	(700)	(717)	(727)

Singapore Telecommunications Ltd

OPTUS (\$\$) - Pre SFRS(I) adjustments

S\$ Million	Quarterly FY2014/15				Quarterly FY2015/16				Quarterly FY2016/17				Quarterly FY2017/18				FY2015/16	FY2016/17	FY2017/18
	1Q Optus	2Q Optus	3Q Optus	4Q Optus	1Q Optus	2Q Optus	3Q Optus	4Q Optus	1Q Optus	2Q Optus	3Q Optus	4Q Optus	1Q Total	2Q Total	3Q Total	4Q Total			
Income Statement																			
Operating revenue	2,409	2,494	2,535	2,436	2,397	2,334	2,467	2,100	2,024	2,167	2,332	2,261	2,191	2,275	2,422	2,248	9,298	8,784	9,136
Operating expenses	(1,730)	(1,764)	(1,835)	(1,693)	(1,753)	(1,644)	(1,801)	(1,376)	(1,428)	(1,549)	(1,673)	(1,503)	(1,557)	(1,597)	(1,722)	(1,547)	(6,573)	(6,153)	(6,422)
Other income	680	730	701	743	645	690	666	724	597	618	659	758	634	678	700	702	2,725	2,631	2,714
EBITDA	18	25	21	28	25	22	29	25	56	31	28	38	58	32	68	36	100	154	195
EBITDA margin (%)	698	755	721	771	670	712	695	749	653	649	687	796	692	710	768	738	2,825	2,784	2,909
Share of results of associates	29.0%	30.3%	28.5%	31.6%	27.9%	30.5%	28.2%	35.7%	32.2%	29.9%	29.5%	35.2%	31.6%	31.2%	31.7%	32.8%	30.4%	31.7%	31.8%
EBITDA & share of results of associates	698	755	721	771	670	712	695	749	653	649	687	796	693	710	769	738	2,826	2,785	2,909
Depreciation & amortisation	(358)	(355)	(351)	(353)	(348)	(339)	(334)	(333)	(336)	(347)	(363)	(370)	(365)	(390)	(376)	(377)	(1,354)	(1,416)	(1,507)
EBIT	341	400	371	418	322	373	361	416	317	302	324	426	328	320	392	361	1,472	1,369	1,402
Net finance expense	(27)	(21)	(45)	(40)	(26)	(36)	(31)	(31)	(38)	(36)	(40)	(44)	(47)	(50)	(50)	(47)	(124)	(158)	(194)
Profit before EI and tax	313	379	326	378	296	337	330	385	279	266	284	382	281	270	343	314	1,348	1,211	1,207
Taxation	(94)	(114)	(96)	(114)	(89)	(104)	(99)	(107)	(83)	(77)	(83)	(114)	(85)	(82)	(95)	(95)	(399)	(356)	(357)
Profit after tax	219	266	230	264	206	234	231	278	196	189	202	269	196	188	248	219	949	855	851
Minority interests	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Underlying net profit	219	266	230	264	206	234	231	278	196	189	202	269	196	188	248	219	949	855	851
Exceptional items ("EI") post-tax	(27)	-	-	(10)	(2)	(1)	(1)	(27)	(21)	(1)	(3)	-	(17)	-	23	(3)	(31)	(25)	3
Net profit	192	266	230	254	205	232	230	251	175	188	199	269	179	188	271	216	918	830	854
Optus Operating Revenue Composition																			
Mobile communications	1,285	1,312	1,308	1,245	1,222	1,191	1,212	972	930	946	973	996	972	1,014	993	969	4,597	3,845	3,947
Data and Internet	424	427	415	407	392	381	401	392	388	409	424	482	439	479	496	436	1,565	1,702	1,851
Managed services	137	160	144	171	147	146	178	148	146	167	176	147	154	201	152	158	619	636	664
National telephone	258	253	239	222	216	212	204	200	196	200	194	193	185	184	170	165	831	784	703
Sale of equipment	207	245	344	307	341	327	393	306	284	359	477	358	352	301	517	425	1,367	1,479	1,596
International telephone	56	54	45	43	41	38	36	33	33	37	34	35	37	38	33	32	148	139	140
Pay television	18	17	16	15	14	13	13	12	26	26	30	28	30	34	33	32	53	110	129
Digital Businesses	4	4	4	5	-	4	3	3	-	-	-	-	-	-	-	-	9	-	-
Others	22	21	20	21	23	24	27	35	22	22	23	23	22	23	29	32	108	89	106
	2,409	2,494	2,535	2,436	2,397	2,334	2,467	2,100	2,024	2,167	2,332	2,261	2,191	2,275	2,422	2,248	9,298	8,784	9,136
Optus Operating Expenses Composition																			
Selling and administrative	588	560	575	468	469	442	462	368	420	424	395	373	419	430	401	354	1,741	1,612	1,604
Traffic expenses	427	437	444	414	410	406	407	200	216	227	236	239	242	255	260	259	1,422	918	1,016
Staff costs	317	310	291	277	288	258	286	244	265	270	278	263	273	282	277	263	1,076	1,075	1,095
Cost of sales	343	398	475	469	528	482	590	505	465	570	711	560	561	566	721	625	2,104	2,305	2,473
Repair and maintenance	45	48	37	46	43	43	39	47	43	44	42	46	45	45	45	31	172	175	166
Others	11	12	13	20	16	14	17	11	19	14	12	23	17	18	18	15	58	68	68
	1,729.6	1,764.4	1,834.6	1,693.4	1,753	1,644	1,801	1,376	1,428	1,549	1,673	1,503	1,557	1,597	1,722	1,547	6,573	6,153	6,422
Depreciation	(327)	(324)	(321)	(313)	(308)	(299)	(292)	(292)	(295)	(305)	(318)	(325)	(320)	(339)	(327)	(328)	(1,192)	(1,243)	(1,314)

Singapore Telecommunications Ltd

OPTUS (A\$) - Pre SFRS(I) adjustments

A\$ Million	Quarterly FY2016/17				Quarterly FY2017/18						
	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	FY2015/16	FY2016/17	FY2017/18
	Optus	Optus	Optus	Optus	Optus	Optus	Optus	Optus	Optus	Optus	Optus
Income Statement											
Operating revenue	1,999	2,112	2,207	2,106	2,095	2,117	2,328	2,169	9,115	8,425	8,710
Operating expenses	(1,410)	(1,510)	(1,583)	(1,400)	(1,489)	(1,486)	(1,655)	(1,493)	(6,442)	(5,904)	(6,123)
Other income	589	602	624	706	607	631	673	676	2,673	2,521	2,587
	56	30	27	35	55	30	66	35	98	148	186
EBITDA	645	633	650	741	662	661	739	712	2,771	2,669	2,774
EBITDA margin (%)	32.3%	30.0%	29.4%	35.2%	31.6%	31.2%	31.7%	32.8%	30.4%	31.7%	31.8%
Share of results of associates	*	*	*	*	*	*	*	*	*	*	*
EBITDA & share of results of associates	645	633	650	741	662	661	739	712	2,771	2,669	2,774
Depreciation & amortisation	(332)	(338)	(343)	(344)	(349)	(363)	(362)	(363)	(1,327)	(1,358)	(1,436)
EBIT	313	295	307	397	314	298	377	348	1,444	1,312	1,338
Net finance (expense)/ income	(38)	(35)	(38)	(41)	(45)	(47)	(48)	(46)	(122)	(152)	(185)
Profit before EI and tax	276	260	269	356	269	252	330	303	1,322	1,160	1,153
Taxation	(82)	(75)	(78)	(106)	(81)	(76)	(91)	(91)	(392)	(341)	(340)
Underlying net profit	194	184	191	250	188	175	239	211	931	819	813
Exceptional items (post-tax)	(21)	(1)	(3)	-	(16)	-	23	(3)	(30)	(25)	4
Net profit	173	184	188	250	171	175	262	208	901	794	817

Singapore Telecommunications Ltd

ASSOCIATES - Pre SFRS(I) adjustments

	Quarterly FY2016/17				Quarterly FY2017/18				FY2015/16	FY2016/17	FY2017/18
	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q			
<u>Associates PBT before EI (\$ million)</u>											
Telkomsel	326	365	360	371	383	371	329	289	1,140	1,422	1,372
AIS	108	72	66	88	82	83	88	95	453	333	347
Bharti	176	172	142	90	103	83	38	(8)	698	580	216
Globe	90	59	66	74	81	59	44	81	313	288	266
Intouch	-	-	4	27	24	24	24	32	-	31	103
Regional associates subtotal	700	667	637	651	673	620	523	488	2,604	2,655	2,304
Others	53	58	58	63	61	29	29	31	184	231	150
Total	753	725	694	713	734	648	553	519	2,788	2,886	2,454
<u>Associates PAT after EI (\$ million)</u>											
Telkomsel	244	274	271	281	286	279	248	219	857	1,071	1,031
AIS	86	59	60	72	68	71	74	78	370	278	292
Bharti	93	92	48	36	35	30	25	(7)	316	270	83
Globe	64	37	56	50	57	62	30	54	235	208	202
Intouch	-	-	6	23	20	20	20	26	-	28	86
Regional associates subtotal	487	463	442	463	465	462	396	371	1,779	1,855	1,694
Others	41	49	48	55	50	25	24	30	151	194	129
Total	529	512	490	518	515	487	420	401	1,930	2,048	1,823
<u>Associates Dividends (\$ million)</u>											
Telkomsel	715	-	-	257	724	-	294	-	722	971	1,018
AIS	176	155	-	-	119	99	-	-	346	330	217
Bharti	-	17	-	-	-	13	-	35	28	17	48
Globe	40	40	40	41	40	39	38	37	157	160	153
Intouch	-	-	-	-	44	34	-	-	-	-	78
Regional associates subtotal	930	211	40	297	926	184	331	72	1,252	1,478	1,513
Others	15	110	20	33	35	63	12	25	98	178	134
Total	945	321	59	331	961	247	343	96	1,351	1,656	1,648
<u>Associates mobile subs ('000)</u>											
Telkomsel	157,387	163,699	173,919	169,367	178,001	190,362	196,322	192,752	153,613	169,367	192,752
AIS	39,355	39,914	41,031	40,648	40,474	40,186	40,056	40,050	38,928	40,648	40,050
Bharti	341,965	346,886	348,147	355,673	362,676	366,060	376,393	395,722	342,039	355,673	395,722
- India	255,735	259,941	265,853	273,648	280,647	282,047	290,113	304,192	251,237	273,648	304,192
- Africa	76,986	78,145	80,356	80,061	80,039	81,927	84,130	89,262	80,564	80,061	89,262
- South Asia	9,244	8,800	1,938	1,964	1,990	2,086	2,150	2,268	10,238	1,964	2,268
Globe	61,311	65,363	62,799	58,580	59,722	59,331	60,686	63,263	57,266	58,580	63,263
Intouch's share of AIS	-	-	NM	NM	NM	NM	NM	NM	-	NM	NM
Total	600,018	615,862	625,896	624,268	640,873	655,939	673,457	691,787	591,846	624,268	691,787

Singapore Telecommunications Ltd And Subsidiary Companies

SINGAPORE PRODUCT INFORMATION - Pre SFRS(I) adjustments

	Quarterly FY2016/17				Quarterly FY2017/18				FY2015/16	FY2016/17	FY2017/18
	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q			
International telephone											
IDD outgoing mins (mil)	702	696	658	626	590	563	526	496	3050	2681	2175
IDD ave collection rate (S\$/ min)	0.095	0.091	0.092	0.090	0.091	0.093	0.093	0.092	0.094	0.092	0.092
National telephone											
Res Fixed Working Lines (000s)	806	797	789	786	780	776	771	769	816	786	769
Biz Fixed Working Lines (000s)	708	700	691	681	672	663	654	645	716	681	645
Total Fixed Working Lines (000s)	1,514	1,497	1,480	1,467	1,452	1,439	1,425	1,414	1,532	1,467	1,414
Mobile communications											
Revenue ⁽¹⁾	525	520	526	511	506	506	509	487	2,116	2,082	2,008
mobile subscribers (000s)											
- Prepaid	1,773	1,774	1,738	1,745	1,714	1,675	1,679	1,636	1,773	1,745	1,636
-	-	1	(36)	7	(31)	(39)	4	(43)			
- Postpaid	2,330	2,341	2,350	2,392	2,414	2,423	2,430	2,449	2,328	2,392	2,449
- Total	2	11	9	42	22	9	7	19			
	4,103	4,115	4,088	4,137	4,128	4,098	4,109	4,085	4,101	4,137	4,085
	2	12	(27)	49	(9)	(30)	11	(24)			
mobile ARPU (S\$)											
- Prepaid	18	19	18	18	18	18	18	18	18	18	18
- Postpaid	70	69	69	67	65	64	64	61	72	68	64
- Blended	48	47	48	46	45	45	46	44	48	47	45
Acquisition cost per postpaid subs (S\$)	410	429	495	378	404	400	515	461	425	431	450
Data as % ARPU	53%	54%	56%	57%	60%	62%	63%	63%	50%	55%	62%
- non-SMS data	43%	45%	47%	49%	52%	54%	56%	56%	40%	46%	54%
Data and internet											
Total Fixed Broadband lines ('000)	600	602	605	609	613	617	617	619	599	609	619
Fibre Broadband lines ('000)	520	533	546	559	570	580	589	599	501	559	599
Singtel TV											
Total Singtel TV customers ('000)	416	412	409	408	404	404	401	395	423	408	395
On-the-go service customers ('000) ⁽²⁾	12	22	33	47	67	86	93	100	-	47	100
Number of households on triple/quad play services ('000)	498	498	500	503	500	505	508	509	500	503	509

Note (1): This comprises cellular service revenue in Singapore only and is determined net of bill rebates and prepaid sales discount, and includes revenue earned from broadband bundles. It excludes revenue earned from international calls classified under "International Telephone" revenue.

(2): Mainly customers who signed up for Cast OTT and Singtel TV Go companion apps

Singapore Telecommunications Ltd

OPTUS PRODUCT INFORMATION - Pre SFRS(I) adjustments

Product Information for Total Optus	FY2016/17 (A\$)					FY2017/18 (A\$)				
	Q1	Q2	Q3	Q4	YTD	Q1	Q2	Q3	Q4	YTD
Optus Mobile Revenue (A\$m)	1,242	1,319	1,417	1,305	5,283	1,314	1,274	1,505	1,404	5,496
Optus Mobile Service Revenue (A\$m)	963	970	966	973	3,872	977	991	1,001	983	3,953
Mobile										
Mobile customers (000s)										
Prepaid handset	3,657	3,636	3,679	3,743	3,743	3,725	3,701	3,672	3,705	3,705
Postpaid handset	4,683	4,774	4,864	4,947	4,947	5,001	5,076	5,203	5,304	5,304
Mobile broadband	997	1,010	1,030	1,032	1,032	1,039	1,050	1,077	1,097	1,097
Total mobile customers	9,336	9,420	9,573	9,722	9,722	9,765	9,827	9,952	10,106	10,106
Mobile ARPUs (A\$)										
Prepaid handset	21	22	21	22	21	20	21	20	20	20
Postpaid handset	48	47	46	46	47	46	46	46	44	46
Mobile broadband	21	20	20	19	20	21	20	21	21	21
Blended	34	34	34	34	34	33	34	34	33	33
Postpaid handset excluding DRP impact	58	59	59	59	58	59	60	60	59	59
Data as % of service revenue	74%	75%	78%	78%	76%	79%	79%	79%	79%	79%
Mass Market Fixed										
Telephony customers (000's)										
HFC	453	450	451	447	447	441	425	401	402	402
ULL	430	423	411	394	394	379	359	342	327	327
Offnet (resale)	19	52	55	57	57	60	52	45	43	43
NBN	134	162	190	225	225	277	350	415	456	456
Broadband customers (000's)										
Business	27	26	25	26	26	25	25	25	24	24
HFC	434	437	440	438	438	433	418	394	396	396
ULL	453	447	429	413	413	396	373	354	339	339
Total on-net	914	910	894	877	877	855	816	773	759	759
Offnet (resale)	31	36	40	42	42	41	39	34	32	32
NBN	136	164	192	228	228	279	351	416	453	453
Total Broadband subscribers	1,081	1,111	1,125	1,147	1,147	1,174	1,206	1,223	1,245	1,245

Singapore Telecommunications Ltd

GROUP - Pre SFRS(I) adjustments

S\$ Million	Quarterly FY2016/17				Quarterly FY2017/18						
	1Q Singtel	2Q Singtel	3Q Singtel	4Q Singtel	1Q Singtel	2Q Singtel	3Q Singtel	4Q Singtel	FY2015/16	FY2016/17	FY2017/18
Balance Sheet											
Current assets (excluding cash)	4,526	4,832	5,196	5,384	6,585	5,512	5,964	5,456	4,704	5,384	5,456
Cash and bank balances	966	585	848	534	632	651	841	525	462	534	525
Non-current assets	37,349	38,141	41,694	42,377	41,922	41,817	42,042	42,273	38,400	42,377	42,273
Total assets	42,840	43,558	47,738	48,294	49,138	47,979	48,846	48,254	43,566	48,294	48,254
Current liabilities	6,530	8,468	9,980	9,272	7,747	6,964	9,752	8,293	6,540	9,272	8,293
Non-current liabilities	10,886	10,047	10,798	10,808	12,524	11,037	9,590	10,307	12,023	10,808	10,307
Total liabilities	17,416	18,515	20,778	20,081	20,272	18,001	19,341	18,600	18,563	20,081	18,600
Net assets	25,424	25,043	26,960	28,214	28,867	29,979	29,505	29,654	25,003	28,214	29,654
Share capital	2,634	2,634	4,128	4,127	4,127	4,127	4,127	4,127	2,634	4,127	4,127
Retained earnings	29,401	28,667	28,529	29,494	30,386	31,528	30,820	31,601	28,457	29,494	31,601
Currency translation reserve (loss)	(5,491)	(5,128)	(4,596)	(4,508)	(4,735)	(4,928)	(5,157)	(5,773)	(4,940)	(4,508)	(5,773)
Other reserves	(1,131)	(1,136)	(1,109)	(900)	(906)	(760)	(261)	(276)	(1,161)	(900)	(276)
Equity attributable to shareholders	25,413	25,037	26,952	28,214	28,872	29,968	29,529	29,679	24,989	28,214	29,679
Minority interest and other reserve	10	6	8	*	(5)	11	(24)	(26)	13	*	(26)
	25,424	25,043	26,960	28,214	28,867	29,979	29,505	29,654	25,003	28,214	29,654

Notes:

“*” denotes less than S\$0.5 million

EXHIBITS I-N

Redacted In Their Entirety

EXHIBIT O

Contact

www.linkedin.com/in/annabel-lewis-0b676a2 (LinkedIn)

Top Skills

Data Privacy

Data Security

Licensing

Annabel Lewis

Chief Legal Officer
Boston

Summary

Business & Legal Leader in Tech & Cyber

Experience

Onapsis Inc.

Chief Legal Officer

July 2019 - Present (1 year 2 months)

Boston, Massachusetts

Legal / Corporate Development / Compliance

NetBrain Technologies Inc.

Chief Legal Officer

November 2018 - May 2019 (7 months)

Boston, Massachusetts

Head of Legal, Alliance Partnerships, & Corporate Operations

Business & legal advisor on company strategy incl. GTM, product strategy, and geo expansion into EMEA and APJ

Singtel

SVP, General Counsel & Corporate Secretary at Trustwave, a Singtel Company

September 2015 - November 2018 (3 years 3 months)

Head of Legal, Information Security, Risk, & Audit

Managed complex business litigation incl. data breach lawsuits / built compliance program incl. anti-corruption, data privacy and GDPR / developed IP strategy and patent portfolio / cultivated positive working environment between Sales and Legal / close advisor to Board

Trustwave

8 years 6 months

SVP, General Counsel & Corporate Secretary

January 2014 - September 2015 (1 year 9 months)

Helped grow company revenue 500%+ / S1 filing & IPO initiative / expansion into EMEA, LATAM, and APJ / built processes to support hyper growth / 15 acquisitions culminating in the \$850M valued sale of the company to Singtel

VP, Legal & Sr. Managing Counsel

April 2007 - January 2014 (6 years 10 months)

Kadets Law

Associate

2005 - 2007 (2 years)

Corporate law and real estate

Hanor & Black PLLC

Associate

2004 - 2005 (1 year)

Patent & trademark prosecution and litigation

Education

St. Mary's University School of Law

Doctor of Law (JD) cum laude/Honors Graduate · (2002 - 2005)

The University of Texas at Austin

Bachelor's degree, Biology (emphasis in genetics and microbiology) · (1997 - 2002)

Pewitt High School

Valedictorian/Advanced with Honors Graduate · (1997)

EXHIBIT P

A group of six young adults, three men and three women, are posing for a selfie outdoors. They are all smiling and looking at the camera. One woman in the foreground is holding a selfie stick with a smartphone attached. The group is dressed in casual to semi-formal attire. The background is a bright, slightly blurred outdoor setting.

Transforming with You

Annual Report 2016

Contents

Overview

An overview of our business, our performance, key achievements and value created, as well as our strategy moving forward

- 01** Financial Highlights
- 03** Chairman's Message
- 05** GCEO Review
- 09** Who We Are
- 11** The Value We Create
- 13** Board of Directors
- 18** Organisation Structure
- 19** Management Committee
- 22** Senior Management

Business Reviews

Insights into each of our business units

- 23** Group Consumer
- 37** Group Enterprise
- 43** Group Digital Life
- 49** Key Awards and Accolades

Governance and Sustainability

Our corporate governance, risk management and sustainability efforts

- 51** Governance & Sustainability Philosophy
- 53** Corporate Governance
- 81** Investor Relations
- 83** Risk Management Philosophy and Approach
- 91** Sustainability

Performance

Our financial performance

- 100** Group Five-year Financial Summary
- 102** Group Value Added Statements
- 103** Management Discussion and Analysis

Financials

Audited financial statements

- 113** Directors' Statement
- 122** Independent Auditors' Report
- 127** Consolidated Income Statement
- 128** Consolidated Statement of Comprehensive Income
- 129** Statements of Financial Position
- 130** Statements of Changes in Equity
- 134** Consolidated Statement of Cash Flows
- 137** Notes to the Financial Statements

Additional Information

Our shareholders, transactions with interested persons and other corporate information

- 222** Interested Person Transactions
- 223** Shareholder Information
- 225** Corporate Information
- 226** Contact Points



"Consumer habits are still evolving alongside the rapidly merging telecoms and internet space. The need for people and businesses to be connected is stronger than ever, which means more demand for seamless connectivity and data services."

A BOOST FOR ICT SERVICES

This new data paradigm presents opportunities for our ICT business. Our assets and capabilities have us well-positioned to capitalise on the shifts to cloud computing, enterprise mobility and smart city initiatives as public agencies and businesses look to exploit mobile capabilities to spur growth.

Cyber security has emerged as a critical issue for governments and businesses. As cyber threats grow in frequency and sophistication, company boards and managements are waking up to the urgent reality that their firms are not adequately protected against these threats and the associated reputational, business risks and costs. In this high-growth emerging market, our ambition is to build out a global business to be among the leaders in this space. Our acquisition of Trustwave last September brings with it a global customer base that we intend to build on and expand.

BUILDING OUT DIGITAL

Since beginning our transformation journey, we have refined our digital strategy to focus on three main areas: digital marketing, OTT video and data analytics where our telecom assets give us competitive advantage.

Amobee is our global digital marketing business that we continue to invest in as we build global scale. Voted the Most Innovative Tech Company, as well as Company of the Year, at the 2016

American Business Awards, Amobee's Brand Intelligence platform analyses and correlates more than 60 billion content engagements daily across the web, social media, video and mobile, helping businesses optimise their media strategies to improve brand awareness and engagement rates.

Our other businesses will take time to scale and mature. Our mobile streaming service, HOOQ, can now be found in India, Indonesia, the Philippines and Thailand, allowing us to tap into the growing demand for online entertainment in emerging markets as smartphone adoption rises. Our geoanalytics initiative, DataSpark, is securing more public contracts as agencies deploy its technology to optimise the planning of urban spaces and transport networks.

THE TRANSFORMATION CONTINUES

Transformation is a journey in which new opportunities emerge. Consumer habits are still evolving alongside the rapidly merging telecoms and internet space. The need for people and businesses to be connected is stronger than ever, which means more demand for seamless connectivity and data services. In short, the same motivations that set us on this path at the outset – reshaping the business to meet customers' evolving needs – are as strong, if not stronger today. So far, we have managed to deepen our customer engagement to compete in the new digital economy while maintaining our lead in the core telecoms business. We intend to continue delivering on both those counts going forward.

I would like to thank our directors, management and staff for their commitment to this transformation and also our many partners and stakeholders for their confidence in Singtel.

Our Board and management are committed to the highest standards of corporate governance and sustainable long-term value creation.

Yours sincerely,



Simon Israel
Chairman

Besides having to host and manage these services, we also had to secure them. This is where our investments in cyber security are also starting to pay off, supported by our ability to monitor traffic flows through our networks, and our trusted relationships with existing enterprise customers. In September 2015, we made a strategic move in acquiring Trustwave, a leading independent cyber security player with business in the US and around the world. A key priority for us this year is to leverage this Trustwave acquisition to create a global platform that can provide managed security services – 24/7.

Our move into Smart Nation solutions also made headway. This year, we secured a significant contract from the Singapore government to build the Land Transport Authority's next-generation Electronic Road Pricing or ERP project. Leading a consortium, we will build a system that will harness satellite tracking and our 4G network to collect and disseminate real-time traffic information. This will be the first time in the world that these capabilities will be implemented nationwide in an urban environment.

As Singapore moves towards becoming a Smart Nation, the majority of our customers are already on fibre broadband, enjoying ultra-high speeds and more competitive pricing levels. We have, in past years, enabled this nationwide fibre rollout through NetLink Trust, which owns our passive fibre infrastructure but operates as an independently managed business trust. This nationwide fibre network which now passes all homes in Singapore forms the backbone of the Singapore government's Smart Nation initiative. For regulatory reasons, we will progress plans to divest our stake in NetLink Trust to less than 25% by April 2018.

REFINING OUR DIGITAL STRATEGIES

Over the past four years, we have refined our digital strategy to focus on areas that contribute back to our core business and best leverage our telecom assets: digital marketing, OTT video and data analytics.

Amobee, our global digital marketing business, recorded strong growth in FY 2016 as it gained further traction among brands looking to increase the efficiency and effectiveness of their

advertising spend across new and multiple media platforms, be it social, mobile, video or email.

HOOQ, our OTT video joint venture with Sony Pictures Television and Warner Bros. Entertainment, is now available across Asia's most populous countries: India, Indonesia, the Philippines and Thailand, steadily adding more video streaming subscribers.

DataSpark, our advanced analytics start-up, is scoring more contracts from both public and private sector companies, which are using anonymised and aggregated telco data to gain insights that sharpen their business and operations planning.

While the results so far have been encouraging, it will be some time before all these businesses can ramp up to global scale and contribute meaningfully to our bottom line. We will continually review the progress of these investments.

Meanwhile, Singtel Innov8, our corporate venture fund, will continue to identify the latest innovations, products and technologies – giving the Group first dibs into monetisable new businesses that will augment our core business or further build on our digital strategy.

STRENGTHENING OUR TEAM

Our people are the foundation of our success. And I truly believe we have the right people and leadership with the necessary instincts for collaborating and innovating our way forward. Even so, we continue to develop the right talent and capabilities to help grow our company.

We have put in place long-term initiatives to attract and develop necessary talent in cyber security, cloud and analytics, having identified these as new growth areas for the business. Our employee engagement score for FY 2016 has improved further, and is quickly closing the gap with the benchmarks for top Global High Performing Companies. We have an energised team, excited about our future, and ready and willing to drive our necessary transformations.

CONTRIBUTING TO OUR COMMUNITIES

Our operations touch millions of lives in the region and it is important for us to give

Senior Management



CHIA WEE BOON

Chief Executive Officer, NCS
Group Enterprise



MARK CHONG

Chief Executive Officer,
International



HUI WENG CHEONG

Chief Operating Officer,
AIS



MURRAY KING

Chief Financial Officer,
Optus



ROBERT J. MCCULLEN

Chief Executive Officer and President,
Trustwave



SAMBA NATARAJAN

Chief Executive Officer,
Group Digital Life



JOHN PAITARIDIS

Managing Director,
Optus Business



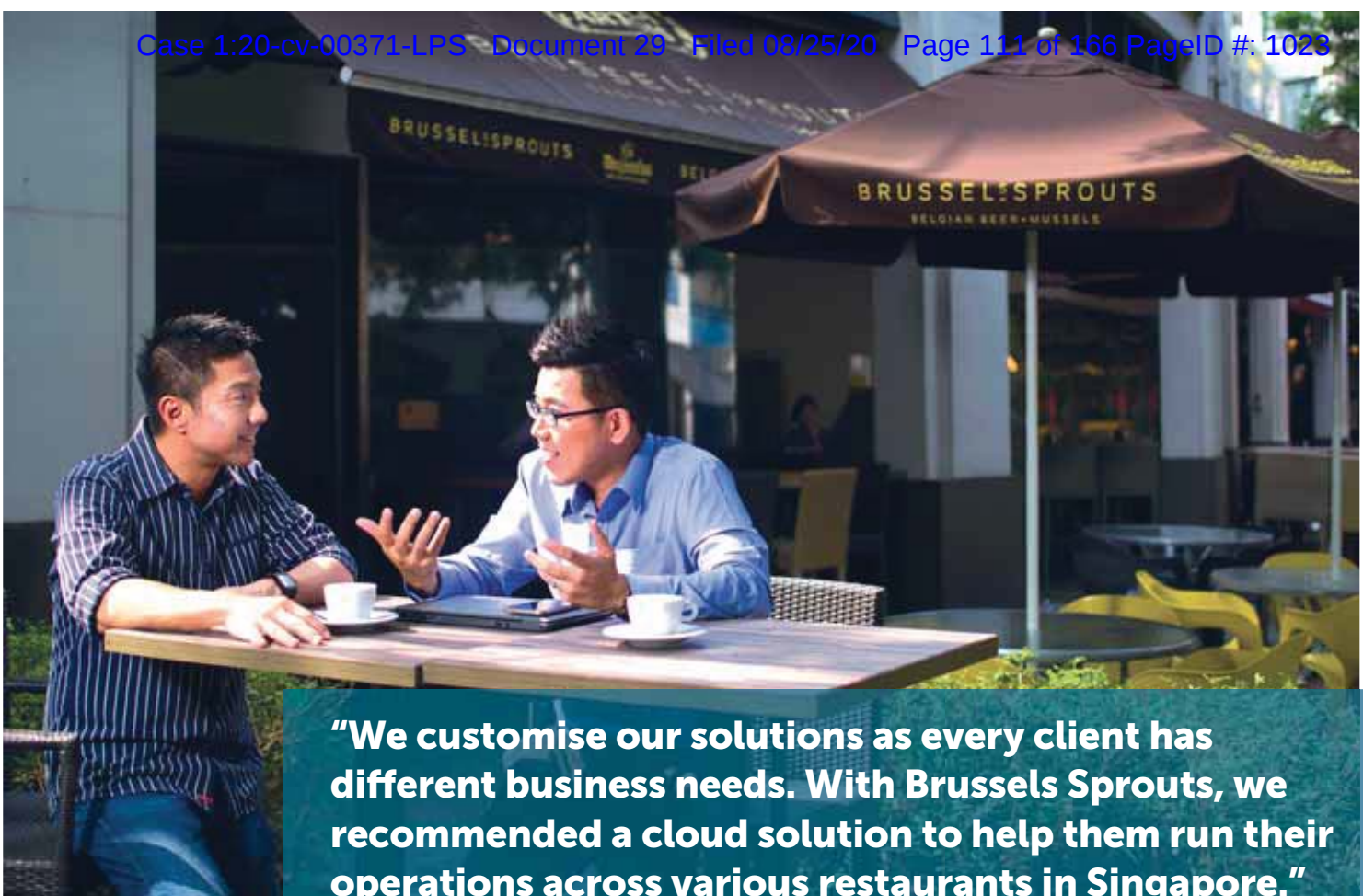
TAY SOO MENG

Group Chief Technology Officer



WILLIAM WOO

Managing Director,
Enterprise Data & Managed Services
Group Enterprise



"We customise our solutions as every client has different business needs. With Brussels Sprouts, we recommended a cloud solution to help them run their operations across various restaurants in Singapore."

— Jason Tan Jie Sheng,
Territorial Sales Manager, Singtel (right)
with Gavin Chen, CEO of Brussels Sprouts (left)

We have been growing our cyber security capabilities organically and through investments and partnerships with FireEye, Akamai and Palo Alto Networks, in anticipation of this trend. With our 2015 acquisition of Trustwave, the largest independent managed security services provider in North America, we can now provide differentiated security solutions for different markets and industries and meet the growing demand for real-time, round-the-clock managed security services.

We have also broken new ground in maritime cyber security globally by partnering global mobile satellite communications company Inmarsat to deploy Trustwave's managed security services to defend against cyber attacks.

We are growing our leadership in the enterprise cyber security space with the launch of the Singtel Cyber Security Institute or CSI in April

2016. An advanced cyber range and educational institute, the CSI will meet the growing regional need for skilled cyber security expertise and raise cyber preparedness among boards and C-suites. It is the first of

its kind in the region to enhance the cyber defence capabilities of cyber operations teams and equip company boards and senior management with cyber awareness, crisis and communications management skills.

Reach for the public cloud with a faster, private connection.

Enjoy a more reliable, direct and secure connection to major cloud computing platforms with the MPLS-based Singtel Cloud Access. It is now easier for your business to create private connections between public cloud, data centres and on-premise infrastructure.

www.singtel.com
For local enquiries: 1800singtel
For international enquiries: gcp@singtel.com

Copyright © 2015 Singtel Telecommunications Ltd (STL) 192012445. All rights reserved. All other trademarks mentioned in this document are the property of their respective owners.

AN INFECTED COMPUTER CAN SERIOUSLY HURT YOUR BUSINESS.

Protect your business with Singtel Managed Security Services, powered by Trustwave. Beyond just anti-virus, we deliver email protection for your business. With Singtel Managed Security Services, you are protected before and during cyber attacks.

ONLY \$6.42/mth per user Unlimited security features for	Defend 24/7 monitoring against all cyber threats for your office email and computers that have been blocked.	Inform Daily summary of alerts and malware attacks that have been blocked.	Investigate 24/7 backup and forensic reporting to recover from attacks.
---	--	--	---

Get protection from cyber attacks now, call us at 1800-763-1111 or visit www.singtel.com/SecuritySolutions/SA

Trustwave helps businesses fight cybercrime, protect data and reduce security risk. With cloud and managed security services, integrated intelligence and threat security experts, offer the best and most effective. Trustwave helps businesses to transform how they manage their information security and compliance programs. With this three-pronged business, we succeed in the Trustwave "TrustKeeper" cloud platform, through which Trustwave delivers a robust, efficient and cost-effective threat, vulnerability and compliance management.

A Singtel Company
Trustwave
Smart security to protect

1800singtel | 1800 763 1111 | Singtel Asia Company | www.singtel.com

Copyright © 2015 Singtel Telecommunications Ltd. All rights reserved.

For the year ended 31 March 2016, the Group performed in line with the guidance issued during the year. Net profit grew 5.5% in constant currency terms. The strong underlying performance was underpinned by its core business driven mainly by higher mobile data usage and improved contributions from the associates. With the Singapore Dollar strengthening against the Australian Dollar and the Indonesian Rupiah, net profit increased 2.4% to S\$3.87 billion. Foreign currency movements negatively impacted net profit by S\$119 million or 3.1 percentage points.

Trustwave, Inc. ("**Trustwave**"), a newly acquired cyber security company consolidated from 30 September 2015, contributed S\$147 million in operating revenue, S\$5 million in EBITDA and S\$27 million in net loss⁽¹⁾.

The Group's operating revenue declined by 1.5% to S\$16.96 billion, impacted by the steep decline of 9% of the Australian Dollar against the Singapore Dollar and the reduction in mobile termination rates⁽²⁾ in Australia from 1 January 2016 ("**rates change**"). In constant currency terms, operating revenue would have grown 4.1% with growth across all the business units. The rates change reduced operating revenue by S\$188 million but had minimal impact on profitability. EBITDA declined by 1.5% to S\$5.01 billion but in constant currency terms would have increased by 4.1%.

Group Consumer, the largest business segment, recorded lower operating revenue of 4.6%. In constant currency terms, operating revenue would have grown 3.0% (up 4.8% excluding the rates change). EBITDA declined 1.2% but in constant currency terms would have increased strongly by 6.5% on strong cost management, and lower mobile customer acquisition and retention costs in Australia as penetration of device repayment plans increased.

Group Enterprise saw operating revenue grew 1.3% while EBITDA declined 3.9%. Excluding fibre rollout

and Trustwave, both revenue and EBITDA were stable. On the same basis and in constant currency terms, operating revenue grew 2.8% and EBITDA remained stable. The higher operating revenue, despite the slowing global economy, was driven mainly by higher ICT and cloud services.

Group Digital Life, which is focused on digital marketing, regional premium OTT video and data analytics, saw a 45% rise in operating revenue with full year's contributions from Kontera and Adconion acquired in September 2014 quarter. Negative EBITDA fell 24% reflecting increased scale at Amobee and effective cost management, partially offset by HOOQ's start-up losses.

The Group and its associates continued to record strong customer growth. The combined mobile customer base reached 605 million⁽³⁾ in 25 countries as at 31 March 2016, up 8.8% or 49 million from a year ago.

The associates' post-tax contributions rose 9.5% to S\$1.93 billion, and would have increased 11% excluding the currency translation impact with higher earnings at Telkomsel and NetLink Trust.

Telkomsel registered strong double-digit growth in revenue and EBITDA, boosted by higher voice and data usage. Airtel delivered higher revenue and EBITDA on strong data growth, improved operating margins in India as well as lower fair value losses in Africa but was offset by higher depreciation and spectrum related costs in India. AIS reported stable service revenue while earnings were impacted by 2G to 3G/4G handset migration costs. Globe saw higher profits from growth in mobile data and customer base, as well as one-off gains. NetLink Trust recorded higher revenue and EBITDA boosted by increased fibre penetration in Singapore.

Depreciation and amortisation charges were stable and would have

increased 5.9% in constant currency terms. The higher depreciation charges was due to increased investments in mobile networks including LTE deployment in Singapore and Australia, while amortisation charges increased due mainly to acquired intangibles of Trustwave and investments in spectrums. Consequently, the Group's EBIT rose 2.7% to S\$5.66 billion, and would have been up 6.0% in constant currency terms.

Net finance expense increased 22% on higher interest expense from higher average borrowings as well as an increase in interest rates.

Excluding the one-off tax credit last year, the increase in tax expense of 6.1% in constant currency terms reflected higher profits and higher withholding taxes on increased dividends from the associates.

Underlying net profit was stable at S\$3.81 billion and in constant currency terms would have increased 4.0% from last year. Excluding Trustwave and the one-off tax credit last year, underlying net profit was up 2.4%, and would have increased 5.8% in constant currency terms.

The Group's net exceptional gain of S\$66 million mainly comprised gains on sale of venture investments of S\$96 million and share of Airtel's net exceptional gains of S\$65 million, partially offset by the currency translation loss of S\$56 million reclassified from equity upon loss of joint control of PBTL, and various one-off charges.

The Group has successfully diversified its earnings base through its expansion and investments in overseas markets. Hence, the Group is exposed to currency movements. On a proportionate basis if the associates are consolidated line-by-line, operations outside Singapore accounted for three-quarters of both the Group's proportionate revenue and EBITDA.

Notes:

⁽¹⁾ Include amortisation of acquired intangibles and acquisition financing cost.

⁽²⁾ Mobile termination rates are the fees charged by mobile operators for receiving calls and messages on their networks.

⁽³⁾ Excluding Pacific Bangladesh Telecom Limited ("**PBTL**") (45%-owned joint venture) which the Group has ceased to exercise joint control.

Notes to the Financial Statements

For the financial year ended 31 March 2016

2.2 Group Accounting

The accounting policy for investments in subsidiaries, associates and joint ventures in the Company's financial statements is stated in **Note 2.4**. The Group's accounting policy on goodwill is stated in **Note 2.15.1**.

2.2.1 Subsidiaries

Subsidiaries are entities (including structured entities) controlled by the Group. Control exists when the Group has power over the entity, is exposed, or has rights, to variable returns from its involvement with the entity and has the ability to affect those returns by using its power over the entity. Power is demonstrated through existing rights that give the Group the ability to direct activities that significantly affect the entity's returns. The Group reassesses whether or not it controls an investee if facts and circumstances indicate that there are changes to one or more of the elements of control listed above. Subsidiaries are consolidated from the date that control commences until the date that control ceases. All significant inter-company balances and transactions are eliminated on consolidation.

2.2.2 Associates

Associates are entities over which the Group has significant influence. Significant influence is the power to participate in the financial and operating policy decisions of the investee but is not control or joint control over those policies.

Investments in associates are accounted for in the consolidated financial statements using the equity method of accounting. Equity accounting involves recording the investment in associates initially at cost, and recognising the Group's share of the post-acquisition results of associates in the consolidated income statement, and the Group's share of post-acquisition reserve movements in reserves. The cumulative post-acquisition movements are adjusted against the carrying amount of the investments in the consolidated statement of financial position.

In the consolidated statement of financial position, investments in associates include goodwill on acquisition identified on acquisitions completed on or after 1 April 2001, net of accumulated impairment losses. Goodwill is assessed for impairment as part of the investment in associates.

When the Group's share of losses in an associate equals or exceeds its interest in the associate, including loans that are in fact extensions of the Group's investment, the Group does not recognise further losses, unless it has incurred or guaranteed obligations in respect of the associate.

Unrealised gains resulting from transactions with associates are eliminated to the extent of the Group's interest in the associate. Unrealised losses are eliminated in the same way as unrealised gains, but only to the extent that there is no evidence of impairment.

2.2.3 Joint ventures

Joint ventures are joint arrangements whereby the parties that have joint control of the arrangement have rights to the net assets of the joint arrangements. Joint control is the contractually agreed sharing of control of an arrangement, which exists only when decisions about the relevant activities require unanimous consent of the parties sharing the control.

The Group's interest in joint ventures is accounted for in the consolidated financial statements using the equity method of accounting.

In the consolidated statement of financial position, investments in joint ventures include goodwill on acquisition identified on acquisitions completed on or after 1 April 2001, net of accumulated impairment losses. Goodwill is assessed for impairment as part of the investment in joint ventures.

The Group's interest in its unincorporated joint operations is accounted for by recognising the Group's assets and liabilities from the joint operations, as well as expenses incurred by the Group and the Group's share of income earned from the joint operations, in the consolidated financial statements.

Unrealised gains resulting from transactions with joint ventures are eliminated to the extent of the Group's interest in the joint venture. Unrealised losses are eliminated in the same way as unrealised gains, but only to the extent that there is no evidence of impairment.

Notes to the Financial Statements

For the financial year ended 31 March 2016

43.3 Significant subsidiaries incorporated outside Singapore and Australia (Cont'd)

	Name of subsidiary	Principal activities	Country of incorporation/ operation	Percentage of effective equity interest held by the Group	
				2016 %	2015 %
33.	Singtel Taiwan Limited	Provision of telecommunications services and all related activities	Taiwan	100	100
34.	Singtel Ventures (Cayman) Pte Ltd	Investment holding	Cayman Islands	100	100
35.	Sudong Sdn. Bhd.	Management, provision and operations of a call centre for telecommunications services	Malaysia	100	100
36.	Trustwave Holdings, Inc.	Provision of managed security services	USA	98	—
37.	Trustwave Limited	Provision of managed security services	United Kingdom	98	—
38.	Viridian Limited	Investment holding	Mauritius	100	100

All companies are audited by a member firm of Deloitte Touche Tohmatsu Limited except for the company denoted (*) which is audited by another firm.

Notes:

⁽¹⁾ The place of the business of the subsidiaries are the same as their country of incorporation, unless otherwise specified.

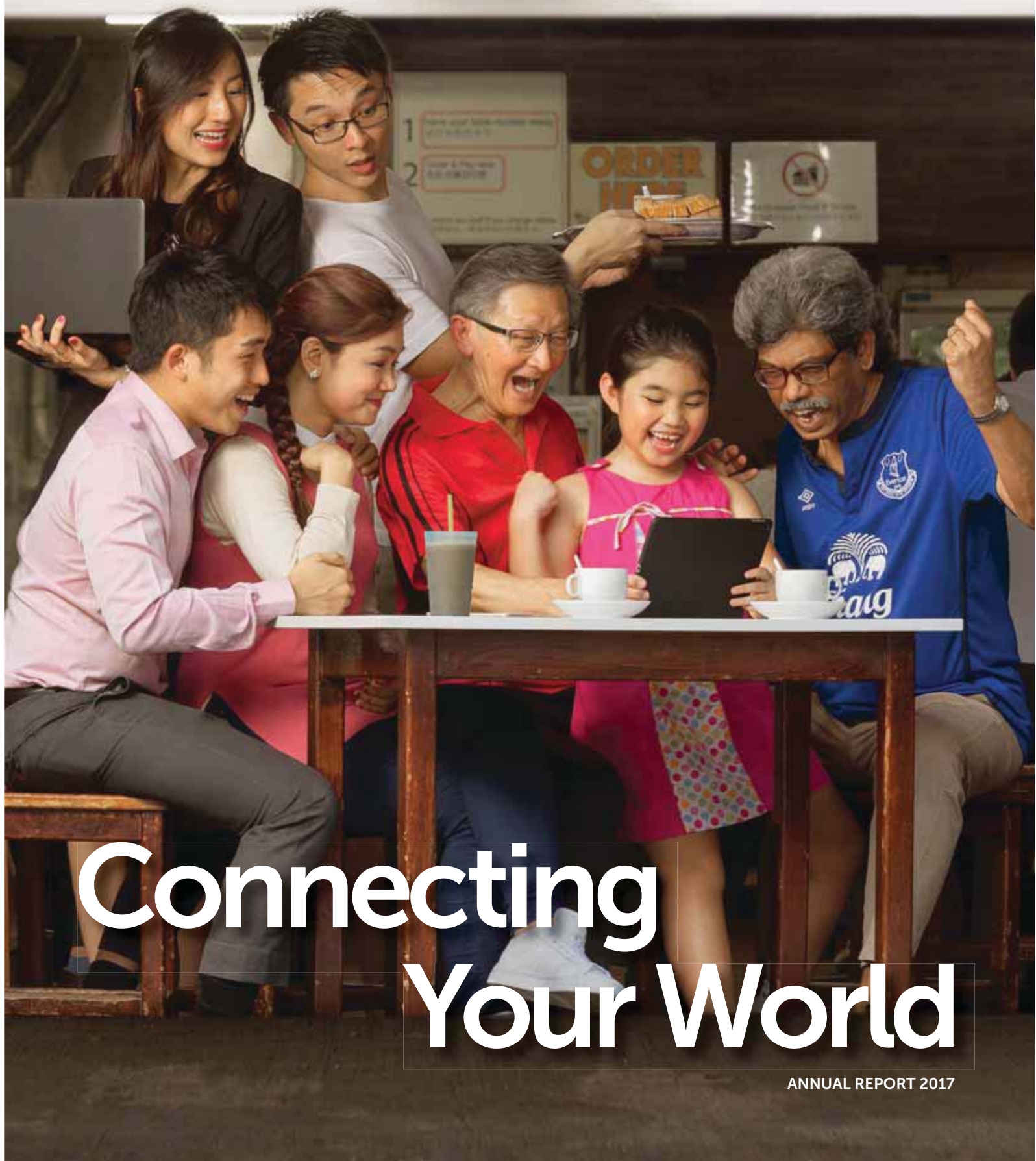
⁽²⁾ The company has operations mainly in the USA, Australia, Israel, Singapore and the United Kingdom.

⁽³⁾ Subsidiary's financial year-end is 31 December.

43.4 Associates of the Group

	Name of associate	Principal activities	Country of incorporation/ operation	Percentage of effective equity interest held by the Group	
				2016 %	2015 %
1.	2359 Media Pte. Ltd. ⁽²⁾	Development and design of mobile-based advertising	Singapore	28.6	—
2.	ADSB Telecommunications B.V. ⁽³⁾	Dormant	Netherlands	—	25.6
3.	APT Satellite Holdings Limited ⁽⁴⁾	Investment holding	Bermuda	20.3	20.3
4.	APT Satellite International Company Limited ⁽⁴⁾	Investment holding	British Virgin Islands	28.6	28.6
5.	HOPE Technik Pte Ltd	Provision of high performance unique engineering solutions	Singapore	21.3	—

EXHIBIT Q



Connecting Your World

ANNUAL REPORT 2017

Table of Contents

OVERVIEW

An overview of our businesses, our performance, key achievements and value created, as well as our strategy moving forward

- 1 Financial Highlights
- 3 Achievements in FY 2017
- 5 Chairman's Message
- 7 GCEO Review
- 11 Who We Are
- 13 Our Businesses
- 14 Our Strategy
- 15 The Value We Create
- 17 Board of Directors
- 22 Organisation Structure
- 23 Management Committee
- 28 Senior Management

BUSINESS REVIEWS

Insights into each of our business units

- 29 Group Consumer
- 43 Group Enterprise
- 51 Group Digital Life
- 59 Key Awards and Accolades

GOVERNANCE AND SUSTAINABILITY

Our corporate governance, risk management and sustainability efforts

- 61 Governance and Sustainability Philosophy
- 63 Corporate Governance
- 91 Investor Relations
- 93 Risk Management Philosophy and Approach
- 101 Sustainability

PERFORMANCE

Our financial performance

- 110 Group Five-year Financial Summary
- 112 Group Value Added Statements
- 113 Management Discussion and Analysis

FINANCIALS

Audited financial statements

- 123 Directors' Statement
- 132 Independent Auditor's Report
- 137 Consolidated Income Statement
- 138 Consolidated Statement of Comprehensive Income
- 139 Statements of Financial Position
- 140 Statements of Changes in Equity
- 144 Consolidated Statement of Cash Flows
- 147 Notes to the Financial Statements

ADDITIONAL INFORMATION

Our shareholders, transactions with interested persons and other corporate information

- 228 Interested Person Transactions
- 229 Shareholder Information
- 231 Corporate Information
- 232 Contact Points



Achievements in FY 2017

The Group has achieved a lot since our last annual report. We launched new products and services, bolstered our core and digital capabilities, and deepened our relationships with our regional associates.

Launched Cyber Security Training for C-Suites



The Singtel Cyber Security Institute in Singapore is the first of its kind in Asia Pacific to hone cyber skills and preparedness of businesses and governments.



Launched All-in-one Mobile Payments

Introduced Singtel Dash, Singapore's first all-in-one mobile payments solution for transit, retail and money transfers.



Extended Global Connectivity

Formed a strategic alliance with Airtel in India to provide high speed data connectivity through

370 points of presence in **325** cities worldwide.



Established Content Creation Arm

Globe in the Philippines set up Globe Studios and Globe Live to create original shows and world-class live entertainment events.

APRIL 2016

MAY 2016

JUNE 2016

OCTOBER 2016

NOVEMBER 2016



Launched Cyber Security Services in Japan

Partnered TIS Inc to provide Trustwave's cyber security services in Japan to help businesses build cyber resilience and protect critical infrastructure.



Deepened Relations with Regional Associates

Increased effective interests in AIS and Airtel in the high-growth Thai and Indian markets through acquisition of shares in Intouch Holdings and Bharti Telecom.



Launched Security Operations Centre in Australia

Optus Advanced Security Operations Centre in Australia helps protect enterprises against cyber threats.



Invested in Cyber R&D

Established NUS-Singtel Cyber Security R&D Lab to create innovative cyber security solutions for a smarter, safer Singapore.

Dear Shareholders,

FY 2017 was a challenging year as competition intensified across markets for both our consumer and enterprise businesses. Taken in this context, Singtel delivered a resilient performance while continuing to make significant investments for the future. Our net profit for the year was stable at S\$3.85 billion, underpinned by growth in mobile data, ICT and digital services.

INVESTING FOR THE FUTURE

We continue to invest in the digital transformation we began five years ago, transforming our core business and investing to grow to scale new global businesses in digital marketing and cyber security. Transformation is at the heart of repositioning Singtel to remain relevant to our customers as well as building new sources of revenue for the mid to long term.

STRENGTHENING OUR NETWORKS POSITION

Network performance is a key competitive differentiator for Singtel, and increasingly important with the growing consumption of video and the demands that places on network performance. We continue to invest in networks ahead of demand to ensure a leading customer experience.

It is notable that the technology investment cycle is compressing – it took eight years to go from 2G to 3G and only four years to go to 4G. We are now implementing 4.5G and in the exploratory stage of 5G networks.

At the same time, the cost of spectrum has soared given it is finite in nature and required for growth. Spectrum auctions around the region have been fiercely contested by incumbents as well as new entrants. Singtel has emerged with strong spectrum holdings, providing the Group with competitive advantage.

BUILDING OUR LEADING POSITIONS IN THE REGION

Beyond the developed markets in Singapore and Australia, we are making the investments needed to build on our leading positions across the region. Last year, we increased our effective interests in our associates in Thailand and India by acquiring stakes in Intouch Holdings and Bharti Telecom.

We believe both markets are favourably positioned for mobile revenue growth given their younger population demographics and data growth. While the entry of a new operator in the Indian telecoms industry has triggered unprecedented industry disruption and consolidation, we believe this will lead to a healthier industry structure for the long term.

CAPTURING NEW GROWTH IN DIGITAL

As the public and private sectors increasingly go digital, demand for ICT-based solutions such as cloud, software as a service and cyber security are providing growth opportunities.

Cyber security is a high-growth sector where we have established a global platform by leveraging our acquisition of Trustwave, a US-based leading managed security services provider. We are building out a global cyber security business which we expect to become a key growth driver in our future. Coupled with our existing ICT assets and capabilities, we are well placed to provide a comprehensive set of managed services with carriage solutions that will create more value in the long term.

In digital marketing, Amobee's recent acquisition of Turn, a global technology platform for marketers and agencies, adds programmatic capabilities and brings Amobee to scale. Amobee is now in a stronger position to capture the global digital marketing opportunity.

OUR WORK CONTINUES

I am encouraged to see our investments in our core and digital transformation delivering tangible results. It shows our efforts over the last five years are making a difference. In fact, we are now in a much stronger position to compete and thrive in this new economy and are well positioned to participate in the opportunities that will emerge around Smart Nation. Amid this fast-changing world, our Board and management remain committed to the highest standards of corporate governance and sustainable long-term value creation.

I would like to thank our directors, management and employees for their unstinting commitment to this journey. We do realise that there is still much to do and our work continues.

Yours sincerely,



SIMON ISRAEL
Chairman

Senior Management



CHIA WEE BOON

Chief Executive Officer
NCS
Group Enterprise



HUI WENG CHEONG

Chief Operating Officer
AIS



MURRAY KING

Chief Financial Officer
Optus



ROBERT J. MCCULLEN

Chief Executive Officer & President
Trustwave
Group Enterprise



JOHN PAITARIDIS

Managing Director
Optus Business
Group Enterprise



KIM PERELL

Chief Executive Officer
Amobee
Group Digital Life



WILLIAM WOO

Managing Director
Enterprise Data & Managed Services
Group Enterprise

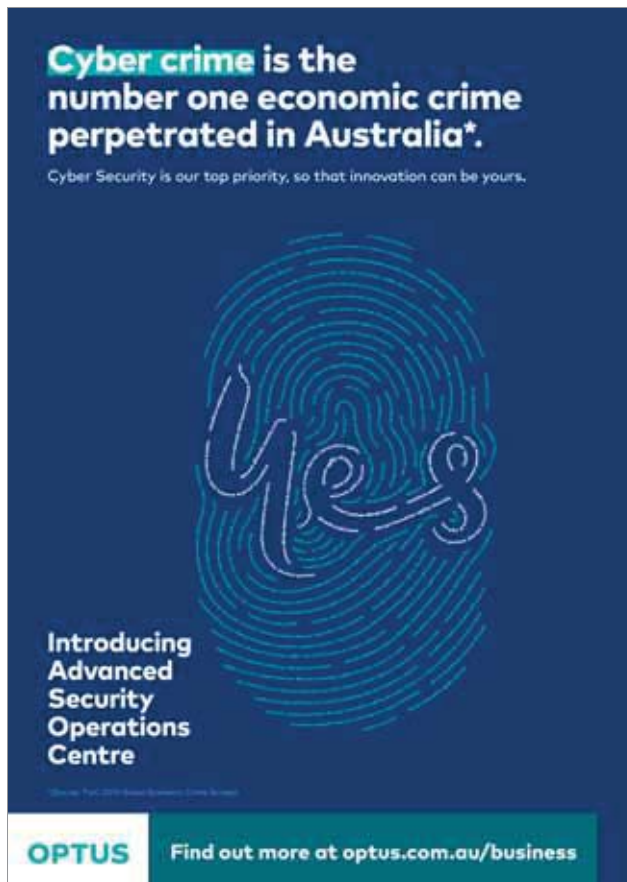
Group Enterprise

professionals from undergraduate to postdoctoral level. It will also develop intellectual property that can be commercialised through our global network of product engineering and development centres.

We launched the Optus Advanced Security Operations Centre (ASOC) in Sydney, Australia, and we will

soon operate a new ASOC in Tokyo, Japan. The two centres add to our existing global network of seven ASOCs which monitor cyber threats round the clock, help enterprises build cyber resilience and protect their critical infrastructure. Trustwave, our cyber security arm, provides managed security services, including comprehensive threat intelligence,

threat data analytics, and advanced security automation for incident response, backed by its elite SpiderLabs team. We also partnered our regional associate Globe to provide managed security services in the Philippines. The services will be delivered through Globe's ASOC in Manila, which will be powered by Trustwave.



We set up the Singtel Cyber Security Institute in Singapore. Our advanced cyber range and educational institute is the first of its kind in the region to provide holistic training for company boards, management, and technology and operations personnel to deal with cyber attacks.

ENABLING THE SMART CITY VISION

As cities grow, city planners increasingly recognise that cities need to be smart and sustainable to overcome the attendant environmental, economic and social challenges. They rely on smart technology solutions for the efficient and effective delivery of public services, better traffic management, and a safer home and living environment.

In Singapore, we support the country's vision of becoming the world's first Smart Nation by 2025 with our advanced capabilities in smart city operating platforms, data analytics and agile application development. These capabilities are being deployed in a number of

What the media said

"In the last two years, Singtel has accelerated efforts to grow the business – securing partnerships with global big names, and launching new facilities in cyber security. It is approaching the field of cyber security in trailblazer fashion."
– Jacquelyn Cheok, The Business Times

EXHIBITS R-U

Redacted In Their Entirety

EXHIBIT V

Annual Report 2019

Reimagining Your Future



Singtel

Reimagining Your Future

Much has changed over Singtel's 140-year history. Technology and innovation has made the mobile phone central to our daily lives. Fitting into the palm of our hands, they serve as gateways to an exciting world of entertainment, information and services. We now stand on the cusp of 5G – an era of hyper-connectivity and newer technologies that will further revolutionise the way we work and play.

As a leading communications technology provider, we're proud to be enablers of such change. Innovation has always been at the core of our business. Our purpose is to keep on pushing boundaries and making breakthroughs, both in our networks and services, so how we live our lives, conduct our businesses, entertain ourselves, keep improving. We are here for the long haul at Singtel, and we're reimagining your future to bring a better one to you.

Table of Contents

Overview

An overview of our businesses, our performance, key achievements and value created, as well as our strategy moving forward

1	Financial Highlights
3	FY 2019 Achievements
5	Chairman's Message
7	GCEO Review
9	Who We Are
11	Our Businesses and Strategy
13	The Value We Create
15	Board of Directors
21	Organisation Structure
22	Management Committee
28	Senior Management

Business Reviews

Insights into each of our business units

29	Group Consumer
41	Group Enterprise
47	Group Digital Life
53	Key Awards and Accolades

Governance and Sustainability

Our corporate governance, risk management and sustainability efforts

55	Governance and Sustainability Philosophy
57	Corporate Governance
87	Investor Relations
89	Risk Management Philosophy and Approach
100	Sustainability



Performance

Our financial performance

- 107 Group Five-year Financial Summary
- 110 Group Value Added Statements
- 111 Management Discussion and Analysis

Financials

Audited financial statements

- 121 Directors' Statement
- 131 Independent Auditors' Report
- 137 Consolidated Income Statement
- 138 Consolidated Statement of Comprehensive Income
- 139 Statements of Financial Position
- 140 Statements of Changes in Equity
- 144 Consolidated Statement of Cash Flows
- 147 Notes to the Financial Statements

Additional Information

Our shareholders, transactions with interested persons and other corporate information

- 250 Interested Person Transactions
- 251 Additional Information on Directors Seeking Re-election
- 261 Shareholder Information
- 263 Corporate Information
- 264 Contact Points



Scan here to view the
Singtel Annual Report 2019 online.

FY 2019 Achievements

We are focused on connecting and empowering everyone, consumers and businesses alike, in new and meaningful ways. This means growing our digital capabilities and investing in innovation and emerging technologies such as 5G and IoT to bring the smart, connected future closer.

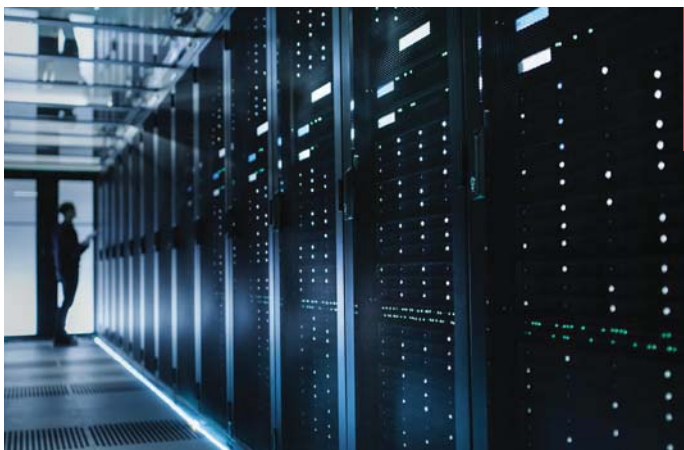


Advanced 5G in Australia and Singapore

- Optus introduced Australia's first 5G commercial fixed wireless service.
- Singtel launched Singapore's first 5G pilot network.

Enhanced cyber security capabilities

- Consolidated cyber assets globally under the Trustwave brand to form one of the industry's most comprehensive cyber security companies.
- Established the first Global Telco Security Alliance with AT&T, Etisalat, SoftBank and Telefónica to create one of the world's biggest managed security services platforms.



Strengthened IoT and cloud capabilities

- Struck partnerships with Microsoft and China Mobile to enable enterprises to deploy their IoT devices across networks seamlessly.
- AIS expanded cloud business and data centres with the acquisition of CS Loxinfo to provide end-to-end digital solutions to enterprises in Thailand.

Chairman's Message

Dear Shareholders,

FY 2019 was more than just a challenging year. I would characterise it as somewhat of a 'perfect storm' with intensifying competition across all markets, particularly India and Indonesia, plus the added backdrop of heightened economic uncertainty. These factors, coupled with regional currencies moving significantly against us and reduced contributions from our smaller stake in NetLink Trust, contributed to a 21% decline in our underlying net profit to S\$2.83 billion.

Your Board has proposed the payment of a final dividend of 10.7 cents per share. If approved, this will bring the total full year dividend to 17.5 cents per share.

RIISING TO CHALLENGES

Last year, I signalled that competition was escalating across the region, with operators aggressively competing for market share.

In India, we have seen an unprecedented situation, where a new entrant investing more than US\$40 billion, has waged a price war, driving the industry into losses.

While this has been painful in the short term, we have arrived at a three-player market, creating a better long-term market structure for when the market normalises.

Airtel has weathered this storm and defended its market share. Airtel undertook a rights issue in May which Singtel has supported to protect our

investment and ensure Bharti can fund its growth.

It is your Board's belief that India will remain a major driver of industry growth, supported by the government's Digital India initiative.

In Indonesia, Telkomsel weathered intense price competition, particularly during the government-mandated registration exercise for prepaid SIM cards. With the recovery of the market, we expect Telkomsel to return to growth.

STRONG CORE PERFORMANCES

Despite challenges, we had strong performances in Singapore and Australia. Our consumer businesses gained mobile market share in both countries as our investments in networks, content and digitalisation paid off.

Both markets also laid the groundwork for 5G. Optus introduced Australia's first 5G commercial service while Singtel launched Singapore's first 5G pilot network. New technologies like 5G will converge with IoT and AI to usher in an era of hyper-connectivity that will redefine whole industries and consumer lifestyles. Our 5G investments are part of longer-term plans to position us for future growth.

GROWING NEW GLOBAL BUSINESSES

Part of our digital transformation involved making calculated investments in new businesses that would thrive in the future economy. Building out our digital businesses: in cyber security, we consolidated the

Group's operations and resources into a single global entity under the Trustwave brand to form one of the industry's most comprehensive global cyber security companies. Our digital marketing business Amobee has achieved scale, while the acquisition of Videology, a software provider for the high-growth advanced TV and video advertising segments, positions us strongly for a converged media landscape.

Your Board is aware that the value of these investments is not being recognised in our share price and management intends to unlock this value at the appropriate time. We are also leveraging our regional scale and partnerships to drive a digital ecosystem across our mobile customer base of more than 690 million.

DEEPENING SUSTAINABILITY EFFORTS

As the sustainability conversation evolves, so has Singtel's efforts in this space. To reduce our carbon footprint even further to align with the global climate agenda, we are exploring long-term renewable energy supply options to help us fulfil our aspiration to be carbon neutral. Our efforts have not gone unnoticed and we continue to be recognised globally in areas such as climate change, governance and diversity. We were one of four Singapore firms and the only Southeast Asian communications company to be listed in the 2019 Bloomberg Gender-Equality Index.

cornerstone of a digital economy. Last year, we launched Singapore's first 5G pilot network at one-north with Ericsson. We also partnered with Ericsson and Singapore Polytechnic to open the nation's first live 5G facility – 5G Garage – on campus which serves as a training centre, test bed and ideation lab to develop Singapore's own 5G ecosystem.

PROTECTING ENTERPRISES

As we move towards a hyper-connected digital future, the risk of cyber threats becomes even greater. To safeguard enterprises against a growing slew of fast-evolving cyber threats, we consolidated our cyber security assets under the Trustwave brand, to form one of the industry's most comprehensive global cyber security companies. We continue to develop our cyber security capabilities to position ourselves to

lead and shape the cyber security sphere. Our global network of Advanced Security Operations Centres is now supported by the new Trustwave SpiderLabs Fusion Centre in Chicago, a cutting-edge cyber security command centre providing unprecedented threat hunting capabilities through pioneering threat intelligence. We also acquired Hivint, an award-winning cyber security consulting company in Australia, enhancing our consulting capabilities.

To further complement our network, we welcomed AT&T as a member to the Global Telco Security Alliance that we formed with Etisalat, Softbank and Telefónica, greatly increasing the Alliance's global presence and resources. We also partnered with Argus, a global leader in automotive cyber security, whose solutions are being

integrated into Singtel's managed security services. The partnership will facilitate the future introduction of connected cars and new technologies such as autonomous vehicles.

STRENGTHENING CORE CAPABILITIES

Strong core capabilities are key to powering new technologies and helping customers accelerate their own digital journey. Even as we develop new services, we continue to strengthen and digitalise our core. We launched Liquid Infrastructure, a next-generation data-driven, highly agile, intelligent platform that integrates physical and virtual network services. The platform, designed for use with services such as optimised cloud access, virtual network function and IoT, allows enterprises to configure their networks with ease and deploy resources when needed.



Singtel executives demonstrating how IoT and AI can enhance companies' competitive advantage to Singapore's Minister for Communications and Information S Iswaran (third from left) at MWC Barcelona 2019.

Independent Auditors' Report

Members of Singapore Telecommunications Limited

For the financial year ended 31 March 2019

The key audit matter

How the matter was addressed in our audit

Impairment assessment of goodwill (Cont'd)

Global Cyber Security CGU

Subsequent to the reorganisation of the Group's cyber security business, with effect from 1 April 2018, management has assessed and considered the combined cyber security businesses of the Group, including Trustwave, to constitute one CGU.

The Group performed impairment assessments for each of the CGUs by estimating the recoverable amounts. The recoverable amount is the discounted sum of individually forecasted cash flows for each year and the value of the cash flows for the years thereafter using a long-term growth rate. As the recoverable amount for each of the CGUs was calculated to be in excess of the respective carrying amounts, no impairment was determined.

Forecasting of future cash flows is a highly judgmental process which requires estimation of revenue growth rates, profit margins, discount rates and future economic conditions.

Refer to Note 24 to the financial statements for the impairment assessments.

In particular, our procedures included:

Optus, Amobee and Global Cyber Security

We assessed the reasonableness of the key assumptions used by management in developing the cash flow forecasts and the discount rates used in computing the recoverable amounts, which included but are not limited to:

- Agreeing the cash flow forecasts used in the impairment model to Board approved forecasts and budgets;
- Considering management's expectations of the future business developments and corroborated certain information with market data; we also considered planned operational improvements to the businesses and how these plans would impact future cash flows and whether these were appropriately reflected in the cash flow forecasts used;
- Challenging the appropriateness of cash flow forecasts used by comparing against historical trends and recent performance and industry trends. Where relevant, assessing whether budgeted cash flows for prior years were achieved to assess forecasting accuracy;
- Comparing the discount rates and terminal growth rates to observable market data; and
- Performing a sensitivity analysis of the key assumptions used to determine which reasonable changes to assumptions would change the outcome of the impairment assessment.

Findings

We found the identification of CGUs to be reasonable and appropriate.

We found the key assumptions and estimates used in determining the recoverable amounts to be within a supportable range.

Share of joint ventures' reported contingent liabilities relating to regulatory litigations and tax disputes

The Group's significant joint ventures have a number of on-going disputes and litigations with their local regulators and tax authorities.

Significant judgement is required by management in assessing the likelihood of the outcome of each matter and whether the risk of loss is remote, possible or probable and whether the matter is considered a contingent liability to be disclosed.

Please refer to Note 41 to the financial statements for 'Significant Contingent Liabilities of Associates and Joint Ventures'.

Our audit procedures included:

- Inquiring with management and legal counsel of the joint ventures to understand the process and internal controls relating to the identification, assessment and recognition of the disputes and litigations.
- Reviewing the audit working papers of the auditors of the joint ventures ('Component Auditors'), in particular their assessment on the regulatory litigations and tax disputes that may have a material impact to the financial statements.
- Discussing with the Component Auditors on their evaluation of the probability and magnitude of losses relating to the disputes and litigations, and their conclusions reached in accordance with SFRS(I) 1-37 *Provisions, Contingent Liabilities and Contingent Assets*.

Notes to the Financial Statements

For the financial year ended 31 March 2019

2.12.1 Subsidiaries

Subsidiaries are entities (including structured entities) controlled by the Group. Control exists when the Group has power over the entity, is exposed, or has rights, to variable returns from its involvement with the entity and has the ability to affect those returns by using its power over the entity. Power is demonstrated through existing rights that give the Group the ability to direct activities that significantly affect the entity's returns. The Group reassesses whether or not it controls an investee if facts and circumstances indicate that there are changes to one or more of the elements of control listed above. Subsidiaries are consolidated from the date that control commences until the date that control ceases. All significant inter-company balances and transactions are eliminated on consolidation.

2.12.2 Associates

Associates are entities over which the Group has significant influence. Significant influence is the power to participate in the financial and operating policy decisions of the investee but is not control or joint control over those policies.

Investments in associates are accounted for in the consolidated financial statements using the equity method of accounting. Equity accounting involves recording the investment in associates initially at cost, and recognising the Group's share of the post-acquisition results of associates in the consolidated income statement, and the Group's share of post-acquisition reserve movements in reserves. The cumulative post-acquisition movements are adjusted against the carrying amount of the investments in the consolidated statement of financial position.

Where the Group's interest in an associate reduces as a result of a deemed disposal, any gain or loss arising as a result of the deemed disposal is taken to the consolidated income statement.

Where the Group increases its interest in its existing associate and it remains as an associate, the incremental cost of investment is added to the existing carrying amount without considering the fair value of the associate's identifiable assets and liabilities.

In the consolidated statement of financial position, investments in associates include goodwill on acquisition identified on acquisitions completed on or after 1 April 2001, net of accumulated impairment losses. Goodwill is assessed for impairment as part of the investment in associates.

When the Group's share of losses in an associate equals or exceeds its interest in the associate, including loans that are in fact extensions of the Group's investment, the Group does not recognise further losses, unless it has incurred or guaranteed obligations in respect of the associate.

Unrealised gains resulting from transactions with associates are eliminated to the extent of the Group's interest in the associate. Unrealised losses are eliminated in the same way as unrealised gains, but only to the extent that there is no evidence of impairment.

2.12.3 Joint ventures

Joint ventures are joint arrangements whereby the parties that have joint control of the arrangement have rights to the net assets of the joint arrangements. Joint control is the contractually agreed sharing of control of an arrangement, which exists only when decisions about the relevant activities require unanimous consent of the parties sharing the control.

The Group's interest in joint ventures is accounted for in the consolidated financial statements using the equity method of accounting.

Where the Group's interest in a joint venture reduces as a result of a deemed disposal, any gain or loss arising as a result of the deemed disposal is taken to the consolidated income statement.

EXHIBIT W

The background of the entire page is a photograph of three business professionals in a high-tech digital environment. On the left, a man in a white shirt and blue tie points at a large, curved digital screen displaying colorful, abstract data visualizations. In the center, a woman in a dark blue dress looks on with her hand near her chin. On the right, another man in a pink shirt is partially visible, gesturing towards the screen. The background is dark with vertical streaks of light and faint, glowing digital patterns.

Ready, set, DIGITAL!

Annual Report 2018

Table of Contents

Overview

An overview of our businesses, our performance, key achievements and value created, as well as our strategy moving forward

1	Financial Highlights
3	FY 2018 Achievements
5	Chairman's Message
8	GCEO Review
11	Who We Are
13	Our Businesses and Strategy
15	The Value We Create
17	Board of Directors
27	Organisation Structure
28	Management Committee
34	Senior Management

Business Reviews

Insights into each of our business units

35	Group Consumer
49	Group Enterprise
55	Group Digital Life
61	Key Awards and Accolades

Governance and Sustainability

Our corporate governance, risk management and sustainability efforts

63	Governance and Sustainability Philosophy
65	Corporate Governance
97	Investor Relations
99	Risk Management Philosophy and Approach
108	Sustainability

Performance

Our financial performance

116	Group Five-year Financial Summary
118	Group Value Added Statements
119	Management Discussion and Analysis

Financials

Audited financial statements

129	Directors' Statement
139	Independent Auditor's Report
145	Consolidated Income Statement
146	Consolidated Statement of Comprehensive Income
147	Statements of Financial Position
148	Statements of Changes in Equity
152	Consolidated Statement of Cash Flows
155	Notes to the Financial Statements

Additional Information

Our shareholders, transactions with interested persons and other corporate information

250	Interested Person Transactions
251	Shareholder Information
253	Corporate Information
254	Contact Points

The Group performed in line with its guidance for the financial year ended 31 March 2018.

Net profit for the year hit a new high, rising a robust 42% to S\$5.45 billion. This was due to exceptional divestment gains from NetLink Trust and a strong performance from the core business.

Operating revenue surged 4.9% and EBITDA rose 1.8%, reflecting strong execution in Australia Consumer and the digital businesses following the acquisition of Turn in April 2017. Revenue from ICT and digital businesses increased a strong 19% to S\$4.18 billion and contributed 24% of the Group's revenue, up from 21% last year.

Depreciation and amortisation charges increased on higher investments in mobile infrastructure network and spectrum across the Group.

Consequently, the Group's EBIT (before the associates' contributions) was stable.

In the emerging markets, the regional associates continued to win new customers and drive data growth with investments in network and spectrum. The customer base of the

Group and its regional associates reached 706 million in 21 countries as at 31 March 2018, up 11% or 68 million from a year ago. Singtel has strengthened its collaborations with the regional associates to build an ecosystem of digital services by leveraging the Group's strengths and customer base across these countries.

The associates' post-tax underlying profit contributions declined by 11% on weaker earnings from Airtel and Telkomsel as well as lower contribution from NetLink NBN Trust following the reduction in economic interest of 75.2% in July 2017. The decline was partly mitigated by higher contribution from Intouch (acquired in November 2016).

Airtel's results were impacted by continued intense competition with aggressive pricing led by a new player and further aggravated by mandated cuts in mobile termination rates in India, partly mitigated by continued positive growth momentum in Africa. Telkomsel's earnings fell on softer revenue growth amid heightened price competition in data and steep declines in voice and SMS revenues, coupled with higher depreciation charges and a weaker Indonesian Rupiah against the Singapore Dollar.

Including the associates' contributions, the Group's EBIT declined by 7.7% to S\$5.21 billion.

Net finance expense increased 33% on lower dividend income from the Southern Cross consortium, decline in net interest income from NetLink Trust with the repayment of unitholder loan in July 2017, as well as higher interest expense on increased average borrowings.

With lower associates' contributions, higher depreciation and amortisation charges as well as increased net finance expense, underlying net profit declined by 8.4% for the year.

The Group has successfully diversified its earnings base through its expansion and investments in overseas markets. Hence, the Group is exposed to currency movements. On a proportionate basis if the associates are consolidated line-by-line, operations outside Singapore accounted for three-quarters of both the Group's proportionate revenue and EBITDA.

EXHIBIT X

Contact

www.linkedin.com/in/kevinkilraine
(LinkedIn)

Kevin K.

Finance Executive
Macquarie Park

Summary

CFO/Finance Professional with extensive business, consulting and commercial experience in the telecoms and ICT sectors.

Specialties: Performance improvement, business & system process analysis, operational review and process design

Strategic analysis, market analysis and business planning

Financial analysis, modelling and structuring

Business risk analysis

Project management

Tendering and contract & service level negotiation

Due diligence support & expert advisory and commercial & regulatory advisory in telecoms, media and high-tech

Product and customer profitability analysis, margin enhancement and revenue assurance

Experience

Optus

VP, Finance and Transformation, Group IT

June 2018 - Present (2 years 3 months)

Sydney, Australia

Trustwave

Chief Financial Officer

April 2016 - June 2018 (2 years 3 months)

Chicago, Illinois

Optus

8 years 2 months

Vice President, Finance, Optus Business

August 2011 - April 2016 (4 years 9 months)

Sydney, Australia

Director, Corporate Services, Optus Networks

October 2008 - September 2011 (3 years)

General Manager, Transformation
March 2008 - October 2008 (8 months)

KPMG

Associate Director, Information Communications & Entertainment
Advisory

March 2003 - March 2008 (5 years 1 month)

In my role at KPMG I focussed on strategic advisory and performance improvement projects for clients in the telecommunications, media, software and related industries. I have focussed on these industries for the last 13 years. I am also the Australian lead for KPMG's global margin enhancement product suite for the telecommunications industry: Revenue Assurance, Cost Management, Construction Management and Profitability Enhancement.

In 2004 I co-authored KPMG's thought leadership paper titled "Leaders or Laggards: Australia's Broadband Future" and I presented on this and related subjects to Telstra, Singtel Optus and the National Broadband Strategy Implementation Group. I was also a contributing author on KPMG's thought leadership piece "Voice over IP: Decipher and Decide. Understanding and managing the technology risks of adoption". In 2006, I co-authored KPMG's thought leadership piece "Fostering investment in broadband infrastructure – the need for regulatory certainty".

BearingPoint

3 years 2 months

Senior Manager

October 2001 - February 2003 (1 year 5 months)

Senior Manager

January 2000 - September 2001 (1 year 9 months)

KPMG

Manager Information Risk Management

September 1994 - December 1999 (5 years 4 months)

Education

Institute of Chartered Accountants in Ireland

FCA, Management and financial accounting, Tax, Audit, Law & Management
Information Systems · (1992 - 1995)

Dublin City University
PDA, Accounting and Finance · (1991 - 1992)

University College Dublin
BE, Electronic Engineering · (1987 - 1991)

EXHIBIT Y



(/en-us/)

**TECHNOLOGY**

Secure Email Gateway

A single solution that delivers advanced protection against today's sophisticated email-based threats, extensive policy controls, and in-depth data security and compliance management.

GET YOUR TRIAL (/EN-US/RESOURCES/SECURITY-RESOURCES/TRIAL-SOFTWARE/TRUSTWAVE-SEG-TRIAL-WITH-SQL-EXPRESS/)

TALK TO SALES

Make Email Safer

Protecting your email environment against spam, malware, phishing attacks, business email compromise, account takeover, ransomware and more is one of your top priorities. Trustwave Secure Email Gateway multi-layered intelligence and detection engine performs deep analysis of your inbound email traffic, in real-time, to protect your users from cyber threats, enables you to integrate the workflow of your email content into business processes, while scrutinizing outbound email traffic to prevent your proprietary data, intellectual property, confidential documents and financial records from electronically leaving the building.

What a Secure Email Gateway Brings to You

- ✓ Complete email protection against phishing, business email compromise
- ✓ Sophisticated, multi-layered approach that reduces false positives
- ✓ Powerful data loss protection to help safeguard your intellectual property and achieve regulatory compliance
- ✓ Syslog support for Security Intelligence and Event Management (SIEM) integration
- ✓ Domain protection from unauthorized use with Domain-based Message Authentication, Reporting and Conformance (DMARC)
- ✓ Detection of forged sender addresses in emails with Domain Keys Identified Mail (DKIM)
- ✓ Microsoft Azure Information Protection and Rights Management Services (AIP/RMS) integration
- ✓ Granular and flexible policy engine to enable workflow integration with your custom business processes

✓ Comprehensive management controls

(/en-us/)



✓ Built-in industry, machine and human intelligence from elite Trustwave Spider Labs email security researchers

✓ Around-the-clock support via online, email and phone, plus maintenance updates

✓ Easy integration with Trustwave Managed Security Services for more in depth endpoint, database and network threat protection

Layering Secure Email Gateway with Office 365 or other web-based email gateways

Email security add-ons like Exchange Online Protection (EOP) or Advanced Threat Protection (ATP) are somewhat effective at blocking massive spam and known threats, but they will not reliably stop highly targeted business email compromise, phishing, spear phishing or zero-day attacks.

Layering Secure Email Gateway with your Office 365 or other web-based email gateways delivers advanced protection from ordinary to sophisticated attacks by proactively detecting suspicious email, removing them from end user access and shielding well-intentioned end users from falling prey to known and targeted attacks – all at a per user cost far less than an E5 license subscription.

Deployment Options

CLOUD

Cloud provides leading protection against spam, phishing, malware, blended and targeted attacks using a constant flow of product updates and enhancements. Achieve enhanced email security, minimize complexity, and save money by complementing your Office 365, G-Suite or other web-based email gateways with Cloud.



(/en-us/)



ON PREMISE

Gain industry leading protection against spam, phishing, malware, blended and targeted attacks by retaining on-site control and granularity of the data in your environment with an on-premises solution.

SERVICE PROVIDER EDITION

Grow your business with an end-to-end email security service – all with the flexibility and granularity that empowers you to provide the exact service your customer required while maintaining full ownership of customer relationships.

Comprehensive Protection



Advanced Detection and Filtering

Stops external phishing, business email compromise and other threats by scanning for email anomalies, inconsistencies, and malicious behavior in the email's structure, content, attachment, and links.



Comprehensive Email Archiving

Provides a systematic approach to save and protect the data contained in email messages to enable fast retrieval. This tool plays an essential role at companies in which data permanence is a priority.



Necessary Advanced Threat Protection

Thwart malicious content and URLs and deliver real-time, zero-day protection against phishing, blended and targeted threats.



Simple, Advanced Email Encryption

Email users can securely send emails containing sensitive or confidential information and documents to any recipient around the globe without requiring the recipient to download or install any software.



Time of Click URL Scanning

Validates every URL and webpage at the time of click and not just at the time of receipt to ensure you are protected anytime and from any device.



Extensive Policy Controls

Implement custom policy configurations based on trigger points, content filtering and other policies for greater control.



Customizable Business Email Compromise (BEC) Protection



Avoid targeted phishing and BEC attacks through the combination of email security measures, employee education and best practices.



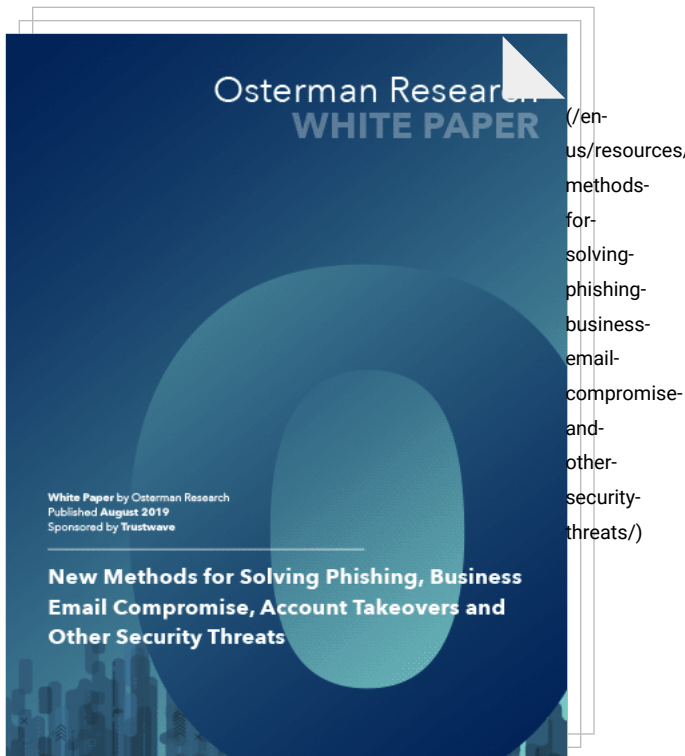
Image Analyzer

Automatically scans and sorts images entering the company via email into two categories – offensive and pornographic and normal and acceptable. Protects employees, customers, and suppliers from exposure to inappropriate and illegal content reducing and removing legal liability.



Data Loss Prevention (DLP)

Scan outbound emails and attachments to provide full DLP-level inspection to manage confidential data and meet stringent industry and regulatory requirements.



WHITE PAPER

New Methods for Solving Phishing, Business Email Compromise and Other Security Threats

As organizations become more complex with the introduction of new tools and technology that aims to accelerate business processes, the attack landscape has expanded, offering an even greater opportunity for digital marauders to take advantage of the environment. This whitepaper dives into the latest findings on these threats and others, but more importantly, advises what you can do to thwart them.

GET YOUR COPY NOW ([/EN-US/RESOURCES/LIBRARY/DOCUMENTS/NEW-METHODS-FOR-SOLVING-PHISHING-BUSINESS-EMAIL-COMPROMIS](/en-us/resources/library/documents/new-methods-for-solving-phishing-business-email-compromise-and-other-security-threats/)

ALL UPDATES

DOCUMENTS

BLOGS

TRIALS

Additional Resources

(/en-us/resources/library/documents/secure-email-gateway-cloud/)

Nov 12, 2019

Secure Email Gateway Cloud (/en-us/resources/library/doc email-gateway-cloud/)

DATA SHEET

(/en-us/resources/library/documents/in-out-and-around-360-security-for-office-365/)

Mar 15, 2019

In, Out and Around: 360° Security for Office 365 (/en-us/resources/library/doc out-and-around-360 WHITE PAPER

(/en-us/resources/library/documents/trustwave-email-archiving/)

Nov 12, 2019

Trustwave Email Archiving (/en-us/resources/library/doc email-archiving/)

DATA SHEET

(/en-us/resources/library/documents/not-disturb-blocking-email-threat-the-door/)

Jun 19, 2019

Do Not Disturb! Blocking Email Threats at the Door (/en-us/resources/library/doc not-disturb-blocking-email-threat-the-door CASE STUDY

<

>

Ready to Get Started?

Our specialists are ready to tailor our security service solutions to fit the needs of your organization.

FIRST NAME: *

LAST NAME: *

WORK EMAIL: *

JOB ROLE: *

Select...

COMPANY NAME: *

https://www.trustwave.com/en-us/services/technology/secure-email-gateway/ 5/7

INDUSTRY: *

Select...

(/en-us/)

COUNTRY: *

Select...

PHONE NUMBER: *

☐

Keep me updated with the latest security news and research

I'M INTERESTED



- (https://www.linkedin.com/company/trustwave/)

SERVICES (/EN-US/SERVICES/)

Managed Security (/en-us/services/managed-security/)

Security Testing (/en-us/services/security-testing/)

Technology (/en-us/services/technology/)

Consulting (/en-us/services/consulting/)

Education (/en-us/services/education/)

RESOURCES (/EN-US/RESOURCES/)

Blogs & Stories (/en-us/resources/blogs/)

Resource Library (/en-us/resources/library/)

Security Resources (/en-us/resources/security-resources/)

Events & Webinars (/en-us/resources/upcoming/)
- (https://www.facebook.com/Trustwave/)

CAPABILITIES (/EN-US/CAPABILITIES/)

By Topic (/en-us/capabilities/by-topic/)

By Industry (/en-us/capabilities/by-industry/)

By Mandate (/en-us/capabilities/by-mandate/)

COMPANY (/EN-US/COMPANY/)

About Trustwave (/en-us/company/about-us/)

Careers (https://jobs.jobvite.com/trustwave)

Newsroom (/en-us/company/newsroom/)

Contact (/en-us/company/contact/)

Support (/en-us/company/support/)
- STAY INFORMED

Sign up to receive the latest security news and trends from Trustwave.

email@example.com

SUBSCRIBE

No spam, unsubscribe at any time.
- LEGAL (/EN-US/LEGAL-DOCUMENTS/)

TERMS OF USE (/EN-US/LEGAL-DOCUMENTS/TERMS-OF-USE/)

PRIVACY POLICY (/EN-US/LEGAL-DOCUMENTS/PRIVACY-POLICY/)

UNITED STATES - ENGLISH
- https://www.trustwave.com/en-us/services/technology/secure-email-gateway/

6/7



Secure Email Gateway, Make Email Safe, Trustwave
Copyright © 2020 Trustwave Holdings, Inc.
(en-us)
All rights reserved.



EXHIBIT Z



FREQUENTLY ASKED QUESTIONS

Trustwave SEG Blended Threat Module

Table of Contents

- 1 What is a Blended Threat?..... 2
- 2 What is the Blended Threat Module?..... 2
- 3 How Does the BTM Work? 2
- 4 How Do I Enable the BTM? 3
 - 4.1 SEG Cloud 3
 - 4.2 SEG Premises 3
- 5 What URLs Does the BTM Rewrite and Check? 4
- 6 What Do End Users See? 5
- 7 Can I Bypass the BTM for Some Users or URLs? 7
 - 7.1 SEG Cloud 7
 - 7.2 SEG Premises 8
- 8 What Reporting on BTM is Available? 10
- 9 Can I Report URLs to Trustwave?..... 10
- About Trustwave 12

1 What is a Blended Threat?

A Blended Threat is an attempt to compromise information security that uses multiple vectors. Blended Threat email messages are typically crafted so that they appear to be from a trusted sender. They contain links to a website hosting malicious code, or attempting to entice the user into providing personal information. Blended Threat emails are sometimes targeted to a specific individual or individuals.

2 What is the Blended Threat Module?

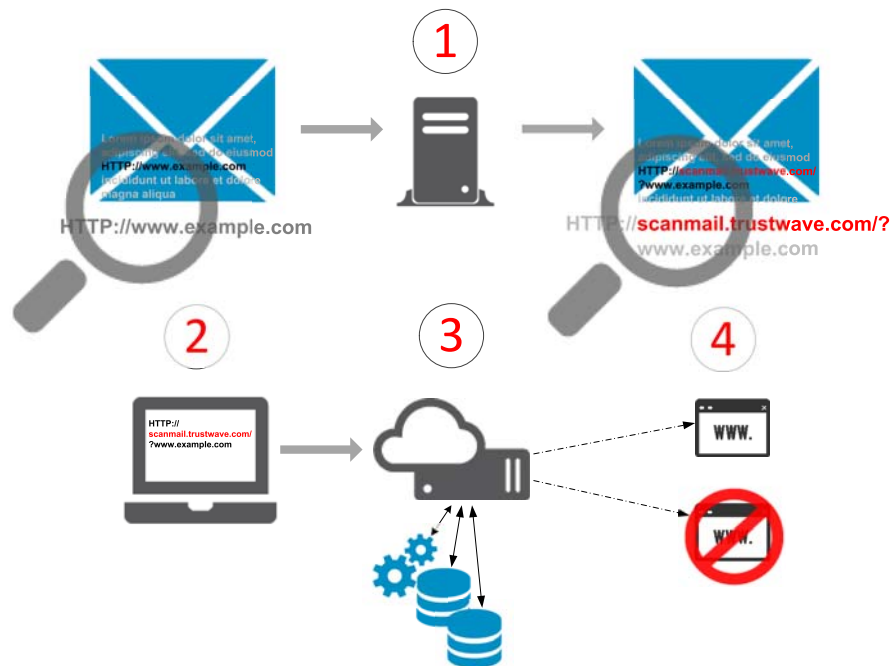
The Trustwave SEG Blended Threat Module uses a number of validation methods, including real-time behavioral analysis and content inspection as well as information from a number of industry standard sources, to identify and block sites that serve suspicious or malicious code.

Because validation is performed in real time by a cloud service when a link is clicked, it provides superior effectiveness in catching and neutralizing new exploits for all users on any device from any location.

3 How Does the BTM Work?

The BTM functions as follows:

1. SEG scans email messages and rewrites URL links before delivering the email.
2. Clicking a link invokes the Trustwave Link Validator cloud service.
3. The Link Validator passes the URL to one or more validation services.
4. Depending on the results of validation, the Link Validator redirects the request to the original site, or blocks the request, as described below.

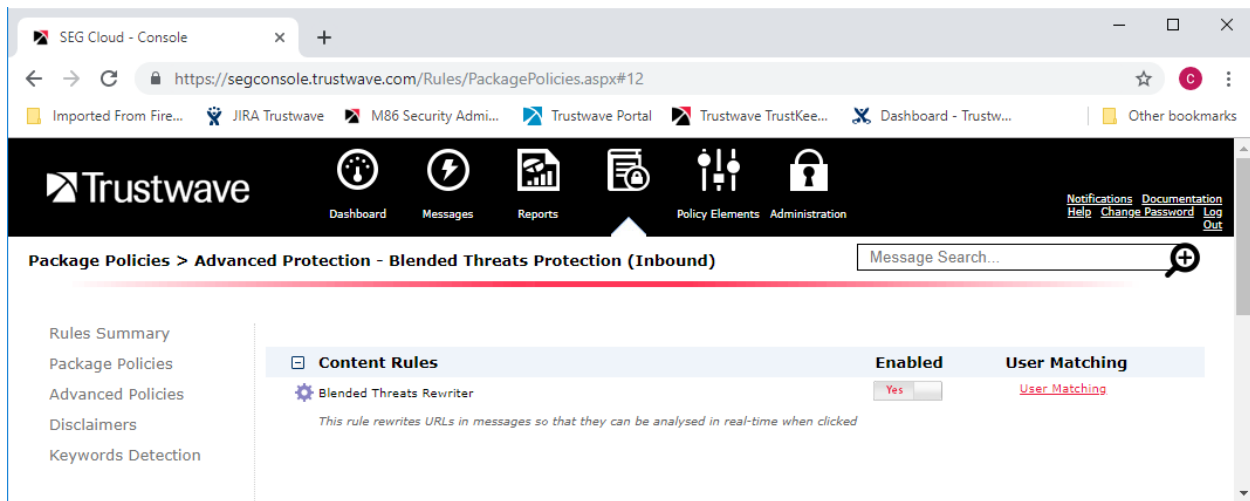


4 How Do I Enable the BTM?

The BTM is implemented as a Rule Action in SEG.

4.1 SEG Cloud

Customers who have purchased the Advanced Protection package see this Package in the Customer Console. The Package contains a single rule, which is enabled by default. The customer can choose to bypass scanning for some users, as described later in this document.



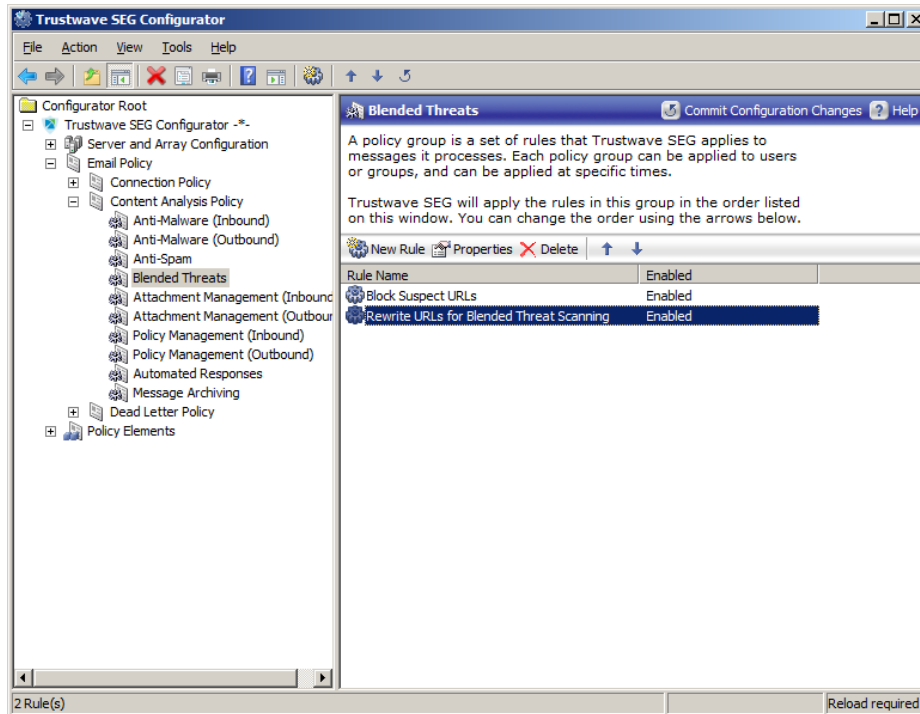
4.2 SEG Premises

SEG Premises requires Web access from the Array Manager server. The required URLs are:

- <https://mailmarshal.licensing.marshall.com> (used to validate licensing for this feature)
- <https://stats.scanmail.trustwave.com> (used to retrieve information about URL rewriting activity from the cloud service)

Trustwave SEG Blended Threat Module FAQ - May 15, 2019

SEG includes a default Policy Group (Blended Threats), and a Rule to enable the BTM. This rule is disabled by default because the BTM is separately licensed. To use the rule, simply enable it and then commit configuration. Customers who have not licensed this feature will not be able to enable this rule.



Note: SEG Premises installations that were upgraded from version 6.9 or below do not include this default rule. The customer must create a rule using the action *Rewrite URLs in the message for Blended Threat Scanning*. This rule should be placed after anti-virus and spam blocking rules.

5 What URLs Does the BTM Rewrite and Check?

The BTM attempts to rewrite any link or text in the body of an email message that might be clickable when the user reads the message. In HTML message bodies, the link location (href) is rewritten. In both HTML and plain text message bodies, text URLs are rewritten.

The BTM does not rewrite links in attached files such as PDF or Office documents. The BTM does rewrite links in attached email messages.

Links that may be rewritten include text that “looks like” a URL either with or without the protocol part like http:// as well as IPv4 and IPv6 addresses and obfuscated links.

In SEG Premises only, the BTM also rewrites text links in the message subject.

The BTM does not rewrite URLs of the customer’s local domains (domains used for inbound email delivery), or private network IP addresses.

For full technical details of the types of links that are rewritten and excluded from rewriting, see Trustwave Knowledge Base article [Q14548](#).

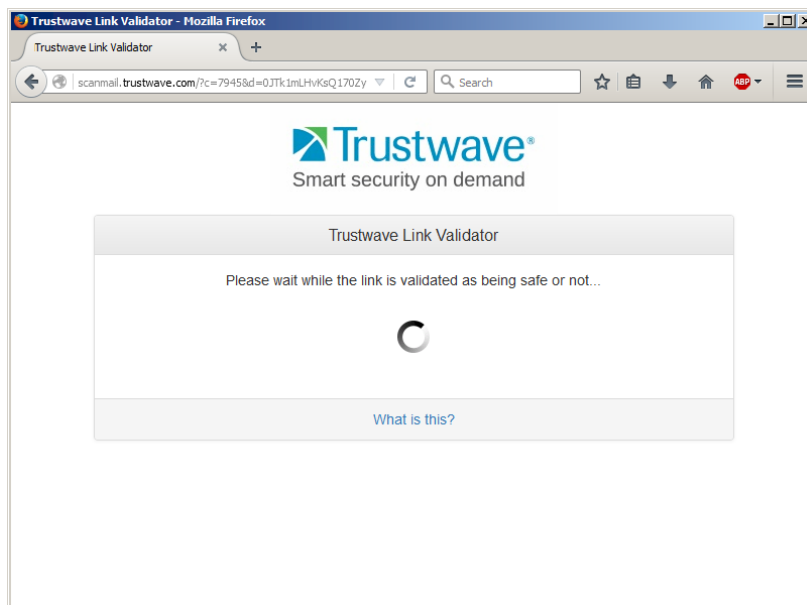
6 What Do End Users See?

When a user opens a message, if the message is displayed in plain text all links will be visibly altered. HTML messages will not be visibly altered, but hovering over a link shows the rewritten URL.

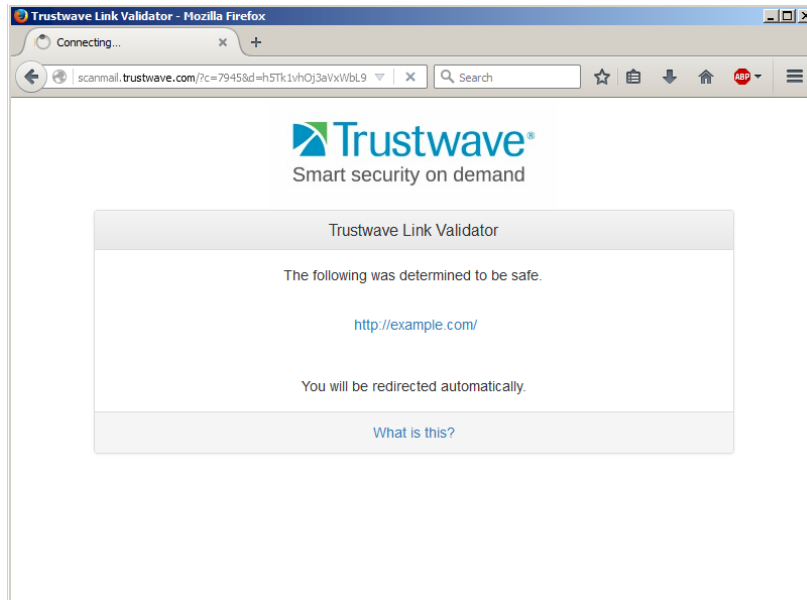
The URL of the Link Validator cloud service accessed by the email clients is:

<http://scanmail.trustwave.com/>

When the user clicks a link, the URL is passed to the Trustwave Link Validator for evaluation. An information page displays briefly.

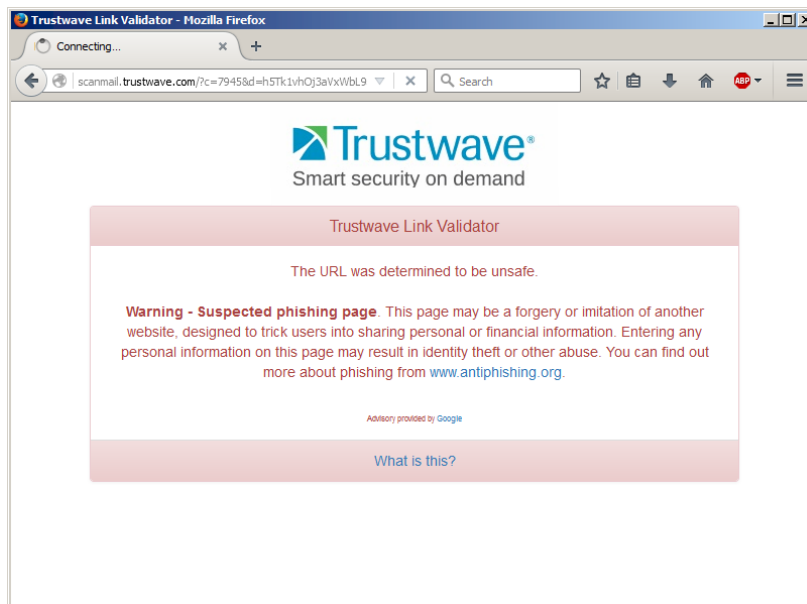


When a result is available it is reported.



If the result is “safe”, the user is automatically redirected to the original URL.

If the result is “unsafe”, a block page displays. In some cases a link with more specific information about the block source is included.



If the validator cannot check the URL, the user will be informed and will be offered the opportunity to click through to the site without validation.

This could occur if

- the BTM license of the customer company that originally rewrote the URL is expired
- the validator encounters an error accessing the site

7 Can I Bypass the BTM for Some Users or URLs?

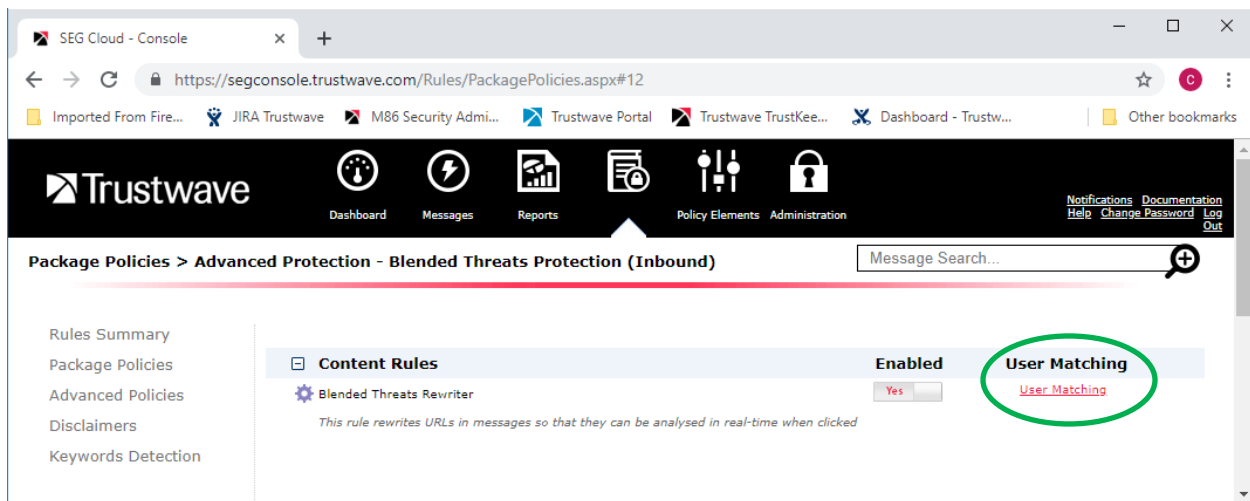
You can configure BTM to not rewrite some URLs, or not rewrite content for some users.



Caution: Trustwave strongly recommends you do not bypass rewriting if at all possible. “Trusted” sites and “busy executive” users are among the highest risks for Blended Threats.

7.1 SEG Cloud

To bypass BTM rewriting, configure User Matching on the Blended Threats Scanner Rule. You can choose to bypass rewriting for messages that are addressed to certain internal users, or from certain external addresses. For testing purposes only, you can choose only to rewrite messages addressed to, or from, specific addresses.

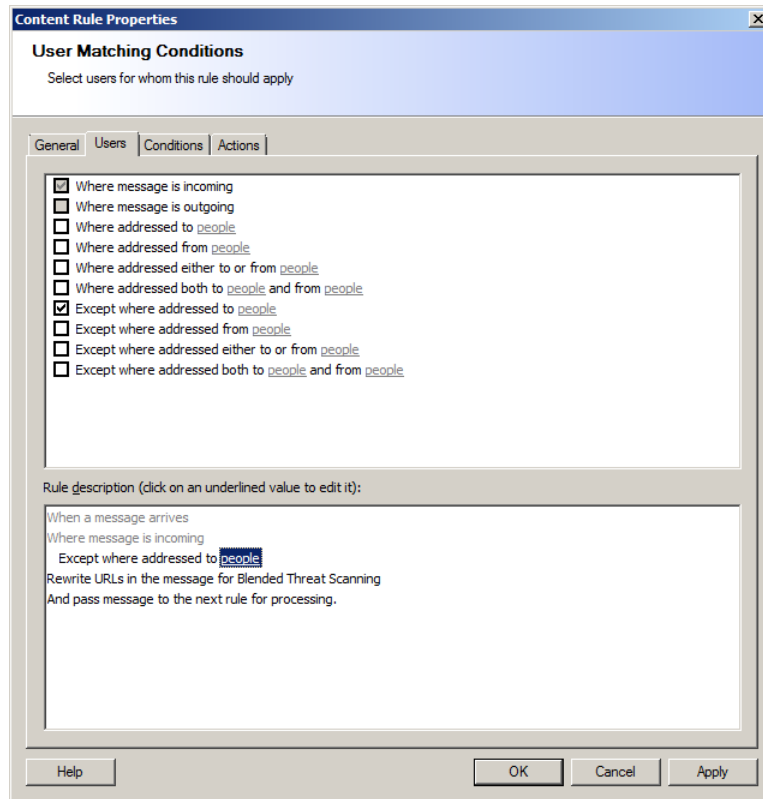


For more information about User Matching, see Help for this page of the Customer Console.

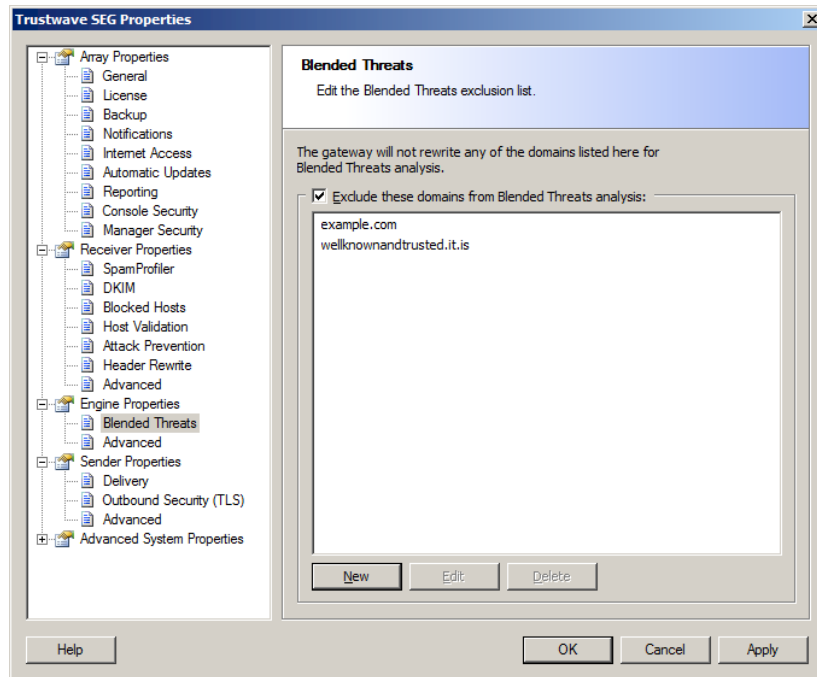
Trustwave SEG Blended Threat Module FAQ - May 15, 2019

7.2 SEG Premises

To bypass BTM rewriting, you can add User Matching conditions to the Rewrite URLs for Blended Threat Scanning Rule.

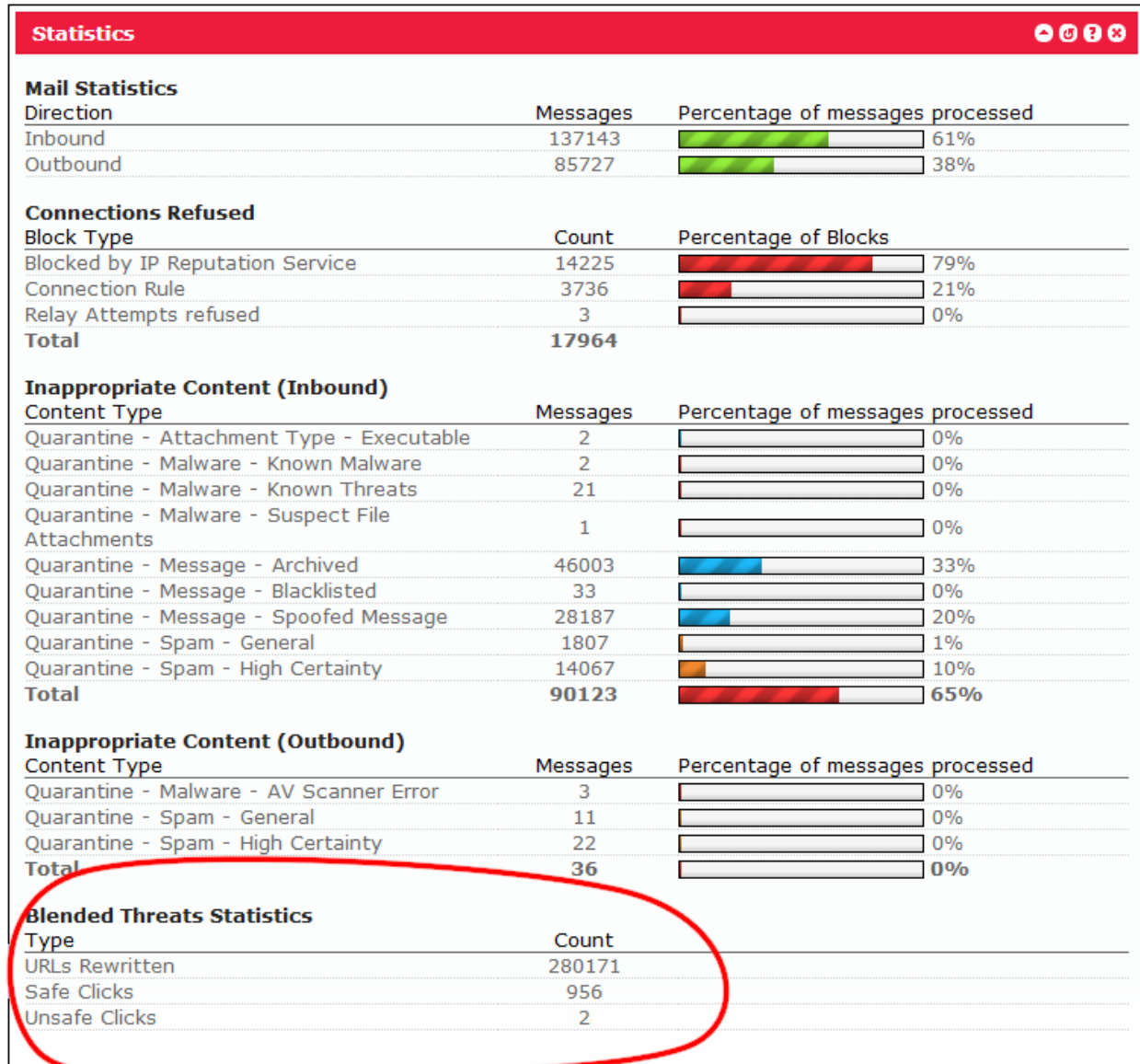


You can also exclude specific domains from rewriting. In the SEG Configurator, navigate to Trustwave SEG Properties > Blended Threats.



8 What Reporting on BTM is Available?

Statistics of URLs rewritten, “safe” clicks, and “unsafe” clicks display on the SEG Premises Console Dashboard and the SEG Cloud Customer Console Dashboard.



9 Can I Report URLs to Trustwave?

If you find a URL that you think is wrongly classified by BTM validation, you can report it to Trustwave using the web form at <https://www.trustwave.com/support/submit-URL.asp>

Trustwave SEG Blended Threat Module FAQ - May 15, 2019

Use this form to report URLs that should be blocked by BTM, or blocked URLs that you believe are legitimate and safe.

About Trustwave

Trustwave helps businesses fight cybercrime, protect data and reduce security risk. With cloud and managed security services, integrated technologies and a team of security experts, ethical hackers and researchers, Trustwave enables businesses to transform the way they manage their information security and compliance programs. More than three million businesses are enrolled in the Trustwave TrustKeeper® cloud platform, through which Trustwave delivers automated, efficient and cost-effective threat, vulnerability and compliance management. Trustwave is headquartered in Chicago, with customers in 96 countries. For more information about Trustwave, visit <https://www.trustwave.com>.

EXHIBIT AA



DATA SHEET

Secure Email Gateway Service Provider Edition

► COMPLETE EMAIL PROTECTION, PURPOSE-BUILT FOR SERVICE PROVIDERS

Benefits

● Purpose-Built for Service Providers

Multi-tenancy, scalability and redundancy that meets the needs of even the largest service provider environments

● Adapt and Manage to Your Needs

Provide the exact service your customers require – you decide exactly what can and cannot be done based on your business needs

● Ensured Service Level Commitments

Supports even the most stringent service level agreements for uptime, spam and virus detection

When adopting new technologies, too often, service providers are asked to lower their service level standards or implement patched-together solutions that aren't intended to support service provider environments. As a service provider, broadening your portfolio with email security should be a business enabler that easily fits into your operating processes.

Trustwave Secure Email Gateway Service Provider Edition (SPE) is a market leading solution for managed and internet service providers that empowers you to grow your business with an end-to-end email security service – all with the flexibility and granularity that empowers you to provide the exact service your customers require while maintaining full ownership of the customer.

Overview

Built on the award-winning Trustwave Secure Email Gateway, Trustwave SPE was designed from the ground up for service provider environments to help you manage your common business issues as well, such as administration, policy management, provisioning and workflow.

Trustwave SPE provides anti-spam, anti-virus, content and compliance management and encryption services within a centrally managed, highly scalable architecture that empowers you to easily offer a wide range of email security services to any size business.

- Gain significant recurring revenue stream through subscription business model
- Modular service options and flexible pricing plans
- Purpose-built architecture, featuring multi-tenancy, scalability and redundancy
- Simplified administration and provisioning to manage your customer engagements
- Easily adapt and manage based on your and your customer's business requirements

Multi-Tenancy, Scalability and Redundancy

Trustwave SPE is purpose-built to meet the needs of even the largest service provider environments. Management, reporting and configuration are multi-tenant and capable of administering thousands of different customers across multiple nodes within a single Trustwave SPE installation – all linked together and managed from the Array Manager.

Trustwave SPE features a highly scalable architecture that is currently used in environments supporting hundreds of thousands of users. It is also redundant by design. Email processing nodes can be connected in load-balanced, redundant arrays ensuring always-on availability while allowing for maintenance and support.

Adapt and Manage Based on Your Needs

Unlike other solutions, Trustwave SPE provides unmatched flexibility and granularity that empowers you to provide the exact service your customers require. You define the service and service levels that meet your requirements, allowing you to fully align with your customer's needs. Need a special policy for just one customer? No problem with Trustwave SPE because you decide what can or cannot be done.

Extensive Service Offerings

With Trustwave SPE you can offer your customers a range of email security services that can be tailored according to your requirements, including:

- Email security (anti-spam and anti-virus)
- Content security
- Encryption

Simplified Administration and Provisioning

Trustwave SPE is a true managed solution for deployment in large, multi-server environments, making it easy to manage policies, user accounts and messages spread across multiple servers – all simplified with a centralized management console.

Comprehensive logging assists with diagnostics and troubleshooting while administrative auditing provides tracking of who has made changes, when the changes were made and what was changed. Billing and accounting systems can be integrated through exporting of report and log records. Trustwave SPE also provides an API for full integration with external applications, such as those for billing and provisioning new customers.

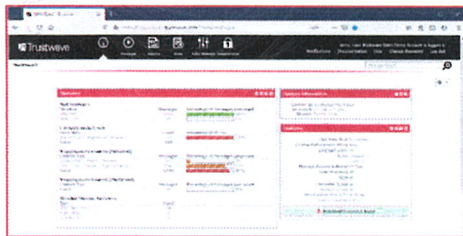
Flexible and Comprehensive Reporting

Trustwave SPE provides extensive reporting capabilities for you and your customers. You can easily schedule automatic generation of reports or run reports on demand, and reports can cover a range of criteria, including bandwidth usage, cost apportioning, triggered rules and reports by domain, customer, customer group or department.

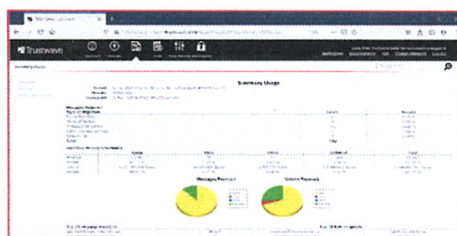
Service-Level Commitments

Trustwave understands that you want to offer the highest levels of assurance and reliability to your customers. Trustwave SPE is capable of supporting even the most stringent service level agreements, including:

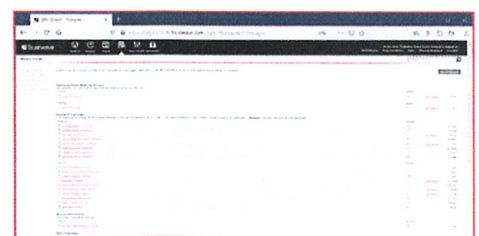
- **Uptime:** Trustwave SPE architecture can achieve network uptimes of 99.999%
- **Spam Filtering:** Trustwave SPE can achieve spam blocking rates of 99.97% or better with a false positive rate of 0.001%
- **Virus Blocking:** Trustwave SPE can use a range of scanners to deliver 100% detection of known viruses, plus security policies can quickly be implemented to block new virus outbreaks before scanners are updated



Administrator Dashboard



Reporting



Policy Configuration and Management

"The deployment of Trustwave Secure Email Gateway Service Provider Edition has proved to be popular with our current clients and strengthens our offering to new customers. It has proven to be an attractive and compelling offering that has positively supported us in recruiting new customers."

– Topsec Technology



EXHIBIT AB



DATA SHEET

Trustwave Secure Email Gateway Cloud

► CYBERSECURITY STARTS HERE - PROTECT YOUR BUSINESS BY MAKING YOUR EMAIL SAFER

Benefits

Unparalleled Email Security

- Advanced Threat Protection
- Protection Against Fraud and Spoofing
- Dynamic Malware Analysis

Superior Compliance and Data Protection

- Prevent Loss of Sensitive Data
- Meet Stringent Compliance Requirements
- Integrate with Microsoft Azure Rights Management Service

Powerful Management Controls

- Advanced Policy Engine
- Management and Reporting

What started as a cost-effective way for people to send and receive messages, email is now the de facto communications tool with billions of users worldwide. Email now extends far beyond sending and receiving simple messages and has transformed into a collaboration, transactional, delivery tool and file repository, and is the primary channel for attackers to gain access to your company.

Stop Fraud and Spoofing

Fact. Cybercrime is increasing. You know cybercriminals want your sensitive and valuable data and access to unsuspecting employees. And to stay several steps ahead of your security team, they continually develop increasingly sophisticated methods to gain access. As a result of these intensifying threats, your security team is tasked with stopping an ever-increasing number of sophisticated phishing or social engineering attacks, malicious attachments and ransomware attacks.

Make Email Safer

Protecting your email environment against spam, malware, phishing attacks, business email compromise, account takeover, ransomware and more while managing complex compliance policies should be one of your top priorities yet it can be a daunting challenge. Trustwave Secure Email Gateway Cloud multi-layered intelligence and detection engine filters your inbound email traffic, in real-time, to protect your users from cyber threats and spam while scrutinizing outbound email traffic to prevent your data and intellectual property from electronically leaving the building.

Secure your Office 365 and other email gateway environments

Upgrading to the most expensive Office 365 enterprise tier just to get the advanced threat protection you need may not be financially feasible. And relying solely on the native capabilities of Office 365 to protect against evolving phishing, spear phishing, business email compromise, and ransomware attacks is just not "good enough."

By investing in a modern-day single source secure email gateway solution, you are giving your security staff the added tools they need to get a leg up on cybercriminals and their sophisticated threats.

Trustwave Secure Email Gateway Cloud delivers you:

- Complete email protection against phishing, business email compromise
- Sophisticated, multi-layered approach that reduces false positives
- Powerful data loss protection to help safeguard your intellectual property and achieve regulatory compliance
- Integration with Microsoft Azure Rights Management Service (RMS) to ensure RMS protected content is validated before leaving your environment
- Syslog support for Security Intelligence and Event Management (SIEM) integration
- Domain protection from unauthorized use with Domain-based Message Authentication, Reporting and Conformance (DMARC)
- Detection of forged sender addresses in emails with Domain Keys Identified Mail (DKIM)
- Granular and flexible policy engine
- Comprehensive management controls
- Built-in intelligence from elite Trustwave Spider Labs email security researchers
- Around-the-clock support via online, email and phone, plus maintenance updates
- Easy integration with Trustwave Managed Security Services for more in depth endpoint, database and network protection
- A lower cost per user, per year

Optional Security Modules

Email Archiving	<ul style="list-style-type: none"> • Provides a systematic approach to save and protect the data contained in email messages to enable fast retrieval. This tool plays an essential role at companies in which data permanence is a priority.
Email Encryption	<ul style="list-style-type: none"> • Company email users can securely send emails containing sensitive or confidential information and documents to any recipient around the globe without requiring the recipient to download or install any software.
Blended Threat	<ul style="list-style-type: none"> • Identifies, catches, neutralizes and blocks, in real-time, websites that serves up suspicious or malicious code to company users.
Image Analyzer	<ul style="list-style-type: none"> • Automatically scans and sorts images entering and leaving the company via email into two categories – offensive and pornographic and normal and acceptable – stopping the offensive and pornographic. • Protects employees, customers, and suppliers from exposure to inappropriate and illegal content reducing and removing legal liability.
Supported Antivirus	<ul style="list-style-type: none"> • Keep your existing anti-virus scanners from Sophos, McAfee, Kaspersky and Bitdefender.

Integrate with Microsoft Azure Information Protection (AIP) and Rights Management Services (RMS)

Microsoft AIP and RMS enables restricted access to documents and emails that are specific to identified individuals within your company and prevents others from viewing or editing these documents - even if they are sent outside the company.

Trustwave is the only secure email gateway solution with the ability to open, analyze and apply policies for data loss protection and acceptable use, then re-encrypt any RMS protected files and emails to ensure sensitive data does not leak from your company.

