PAUL ANDRE (State Bar No. 196585)
pandre@kramerlevin.com
LISA KOBIALKA (State Bar No. 191404)
lkobialka@kramerlevin.com
JAMES HANNAH (State Bar No. 237978)
jhannah@kramerlevin.com
AUSTIN MANES (State Bar No. 284065)
amanes@kramerlevin.com
KRAMER LEVIN NAFTALIS & FRANKEL LLP
990 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 752-1700
Facsimile: (650) 752-1800

*Attorneys for Plaintiff*
FINJAN, INC.

**IN THE UNITED STATES DISTRICT COURT**

**FOR THE NORTHERN DISTRICT OF CALIFORNIA**

FINJAN, INC., a Delaware Corporation,

Plaintiff,

v.

CARBON BLACK, INC., a Delaware Corporation,

Defendant.

Case No.:

**COMPLAINT FOR PATENT INFRINGEMENT**

**DEMAND FOR JURY TRIAL**

**COMPLAINT FOR PATENT INFRINGEMENT**

Plaintiff Finjan, Inc. ("Finjan") files this Complaint for Patent Infringement and Demand for Jury Trial against Carbon Black, Inc. ("Defendant" or "Carbon Black") and alleges as follows:

**THE PARTIES**

1. Finjan is a Delaware Corporation with its principal place of business at 2000 University Avenue, Suite 600, E. Palo Alto, California 94303.

2. Defendant is a Delaware Corporation with its headquarters and principal place of business at 1100 Winter Street in Waltham, Massachusetts 02451. Defendant maintains a regular and established place of business in this District at 530 Lytton Avenue, 2nd Floor, Suite 240 in Palo Alto, California 94301. Defendant's website (https://www.carbonblack.com/contact-us/) lists 530 Lytton Avenue in Palo Alto, California as one of its physical addresses under the title "Our Locations." On information and belief, Defendant was formerly known as "BIT9, Inc." and "BIT 9, Inc." Defendant may be served through its agent for service of process, The Corporation Trust Company, at Corporation Trust Center, 1209 Orange Street in Wilmington, Delaware 19801.

**JURISDICTION AND VENUE**

3. This action arises under the Patent Act, 35 U.S.C. § 101 *et seq*. This Court has original jurisdiction over this controversy pursuant to 28 U.S.C. §§ 1331 and 1338.

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

5. This Court has personal jurisdiction over Defendant. Upon information and belief, Defendant regularly and continuously does business in this District and has infringed or induced infringement, and continues to do so, in this District. In addition, this Court has personal jurisdiction over Defendant because minimum contacts have been established with this forum and the exercise of jurisdiction would not offend traditional notions of fair play and substantial justice.

**INTRADISTRICT ASSIGNMENT**

6. Pursuant to Local Rule 3-2(c), Intellectual Property Actions are assigned on a district-wide basis.

## FINJAN'S INNOVATIONS

7. 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 a pioneer in developing proactive security technologies capable of detecting previously unknown and emerging online security threats, recognized today under the umbrella term "malware." These technologies protect networks and endpoints by identifying suspicious patterns and behaviors of content delivered over the Internet. Finjan has been awarded, and continues to prosecute, numerous patents covering innovations 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 over $65 million in R&D investments.

8. 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 online security drew equity investments from two major software and technology companies, the first in 2005 followed by the second in 2006. Finjan generated millions of dollars in product sales and related services and support revenues through 2009, when it spun off certain hardware and technology assets in a merger. Pursuant to this merger, Finjan was bound to a non-compete and confidentiality agreement, under which it could not make or sell a competing product or disclose the existence of the non-compete clause. Finjan became a publicly traded company in June 2013, capitalized with $30 million. After Finjan's obligations under the non-compete and confidentiality agreement expired in March 2015, Finjan re-entered the development and production sector of secure mobile products for the consumer market.

**FINJAN'S ASSERTED PATENTS**

9. On October 12, 2004, U.S. Patent No. 6,804,780 ("the '780 Patent"), titled SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES, was issued to Shlomo Touboul. A true and correct copy of the '780 Patent is attached to this Complaint as Exhibit A and is incorporated by reference herein.

10. All rights, title, and interest in the '780 Patent have been assigned to Finjan, who is the sole owner of the '780 Patent. Finjan has been the sole owner of the '780 Patent since its issuance.

11. The '780 Patent is generally directed towards methods and systems for generating a downloadable ID. By generating an identification for each examined downloadable, the system may allow for the downloadable to be recognized without reevaluation. Such recognition increases efficiency while also saving valuable resources, such as memory and computing power.

12. On November 28, 2000, U.S. Patent No. 6,154,844 ("the '844 Patent"), titled SYSTEM AND METHOD FOR ATTACHING A DOWNLOADABLE SECURITY PROFILE TO A DOWNLOADABLE, was issued to Shlomo Touboul and Nachshon Gal. A true and correct copy of the '844 Patent is attached to this Complaint as Exhibit B and is incorporated by reference herein.

13. All rights, title, and interest in the '844 Patent have been assigned to Finjan, who is the sole owner of the '844 Patent. Finjan has been the sole owner of the '844 Patent since its issuance.

14. The '844 Patent is generally directed towards computer networks, and more particularly, provides a system that protects devices connected to the Internet from undesirable operations from web-based content. One of the ways this is accomplished is by linking a security profile to such web-based content to facilitate the protection of computers and networks from malicious web-based content.

15. On March 18, 2014, U.S. Patent No. 8,677,494 ("the '494 Patent"), titled MALICIOUS MOBILE CODE RUNTIME MONITORING SYSTEM AND METHODS, was issued to Yigal Mordechai Edery, Nimrod Itzhak Vered, David R. Kroll, and Shlomo Touboul. A true and correct copy of the '494 Patent is attached to this Complaint as Exhibit C and is incorporated by reference herein.

16. All rights, title, and interest in the '494 Patent have been assigned to Finjan, who is the sole owner of the '494 Patent. Finjan has been the sole owner of the '494 Patent since its issuance.

17. The '494 Patent is generally directed towards a method and system for deriving security profiles and storing the security profiles. One of the ways this is accomplished is by deriving a security profile for a downloadable, which includes a list of suspicious computer operations, and storing the security profile in a database.

18. On March 20, 2012, U.S. Patent No. 8,141,154 ("the '154 Patent"), titled SYSTEM AND METHOD FOR INSPECTING DYNAMICALLY GENERATED EXECUTABLE CODE, was issued to David Gruzman and Yuval Ben-Itzhak. A true and correct copy of the '154 Patent is attached to this Complaint as Exhibit D and is incorporated by reference herein.

19. 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.

20. The '154 Patent is generally directed towards a gateway computer protecting a client computer 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.

21. The '780 Patent, the '844 Patent, the '494 Patent, and the '154 Patent, as described in paragraphs 9–20 above, are collectively referred to as the "Asserted Patents" herein.

**FINJAN'S NOTICE OF INFRINGEMENT TO DEFENDANT**

22. Finjan and Defendant's patent discussions date back to December 2015. Finjan contacted Defendant on or about December 17, 2015, regarding a potential license to Finjan's patents, including the '780, '844, '494, and '154 Patents. Finjan identified and described the following products made, used, or sold by Defendant as infringing Finjan's Patents: Bit9 + Carbon Black Solution, the Bit9 Security Platform, and the Bit9 + Carbon Black Threat Intelligence Cloud.

23. Finjan delivered another letter to Defendant on or about January 21, 2016, which described in detail how Defendant's products practice the claim elements of the Asserted Patents. Finjan's letter on or about January 21, 2016, also described Finjan's successes before the U.S. Patent

and Trademark Office's Patent Trial and Appeal Board ("PTAB"), including the fact that no claims of the Asserted Patents had been determined to be unpatentable.

24. On or about February 18, 2016, Finjan provided Defendant with exemplary claim charts detailing how the '844, '494, and '154 Patents read on Defendant's products. Specifically, this presentation identified how the '844, '494, and '154 Patents read on: Carbon Black Endpoint Solution; Endpoint Threat Detection; Cb Enterprise; and Cb Threat Intel. This presentation on or about February 18, 2016, also identified the '780 Patent and described that Defendant's Cb Response, Cb Enterprise, and Cb Threat Intel all perform the invention claimed in the '780 Patent.

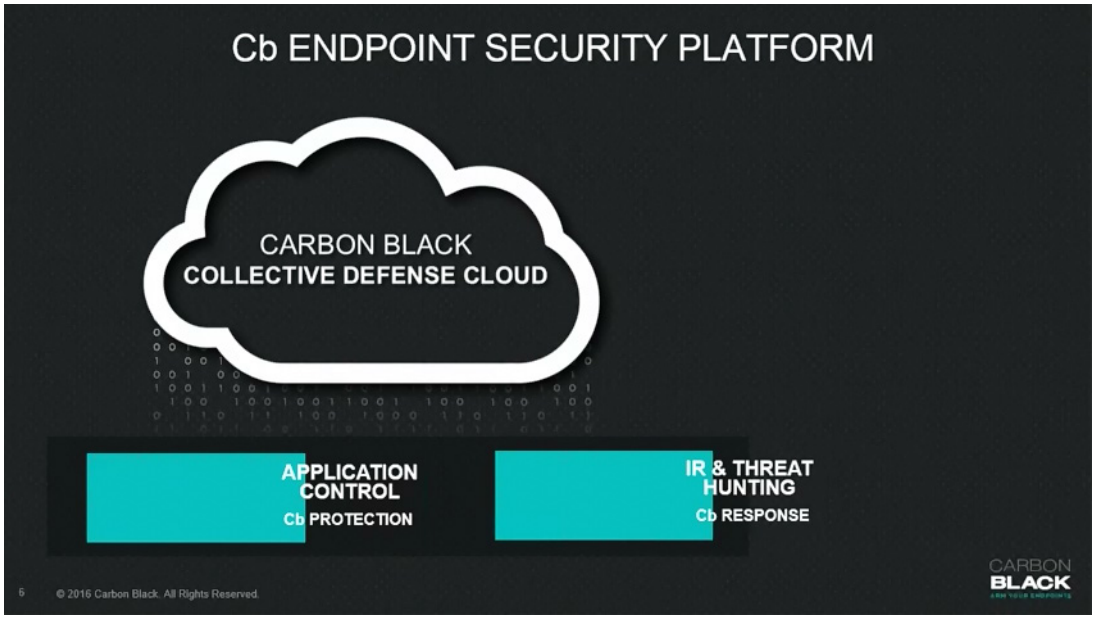
25. From February 2016 until in or around February 2018, Finjan attempted to engage Defendant in licensing discussions. Finjan met with Defendant in person in Boston in August 2017, during which meeting Finjan explained in detail how each of the Asserted Patents reads on each of the Accused Products. Finjan has diligently pursued Carbon Black regarding its infringement, and has engaged in at least eighteen meetings, by telephone, video, or in person, over more than two years in an attempt to engage Carbon Black in licensing discussions. Despite Finjan's earnest and consistent efforts, Defendant refused to take a license to Finjan's patents. At no time has Defendant provided any reasonable explanation—legal or otherwise—countering Finjan's exemplary claim charts as to how any of the Accused Products do not infringe any of the Asserted Patents.

**Carbon Black**

26. Defendant makes, uses, sells, offers for sale, and/or imports into the United States and this District products and services that utilize the Cb Predictive Security Cloud, Cb Response, Cb Defense, Cb Defense for VMware, and Cb Protection (formerly known as Carbon Black Enterprise Protection/Bit9 Security Platform/Bit9 Party Suite) products, services, and technologies (collectively, "Accused Products"). *See* Ex. E (https://www.carbonblack.com/products/).

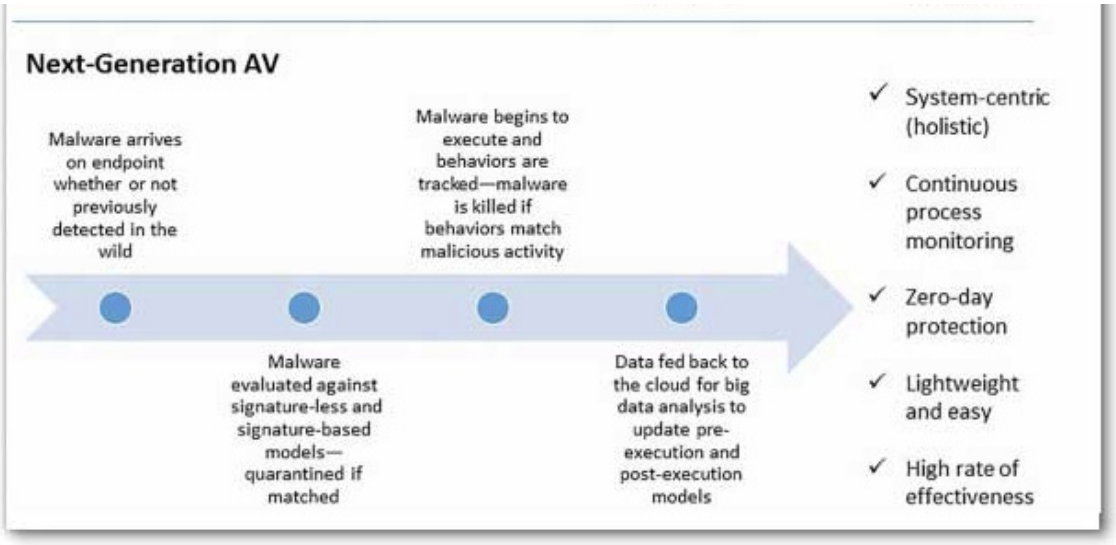
27. All Carbon Black Accused Products operate in a similar manner and utilize the same infringing technologies described herein. For example, Carbon Black utilizes lightweight agents on endpoints with its Next-Generation Anti-Virus ("NGAV") and Endpoint Detection and Response

("EDR") technologies that interact with the Carbon Black Cloud (sometimes referred to as the Carbon Black Collective Defense Cloud) utilizing Collective Intel and Detonation technologies.



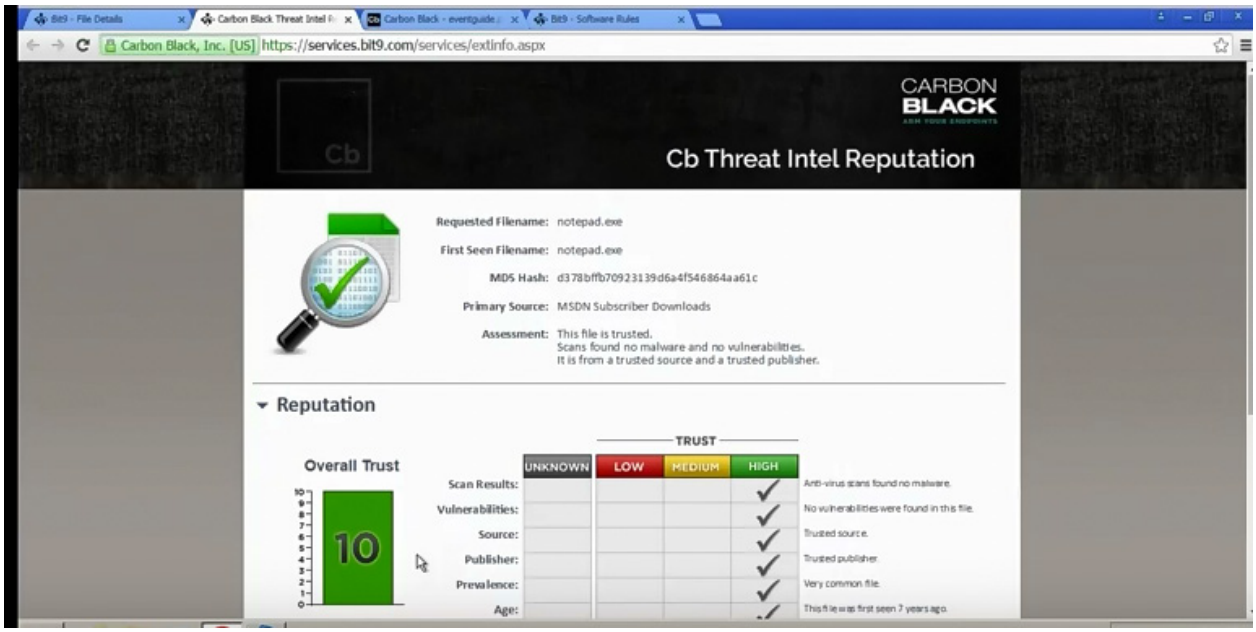

*See, e.g.*, https://www.youtube.com/watch?v=WQm-hYHAv8g.

28. As shown below, Carbon Black's NGAV and EDR technologies provide behavioral analysis of potential malware and security against zero-day attacks.




NGAV capabilities also reach beyond use of indicators of compromise (IOCs), metadata such as virus signatures, IP addresses, file hashes and URLs—all of which demonstrate that potentially malicious activity has occurred.

Ex. F (https://www.carbonblack.com/2016/12/20/replacing-traditional-antivirus-with-next-gen-antivirus-visualizing-ngav-and-evaluation-architecture/).

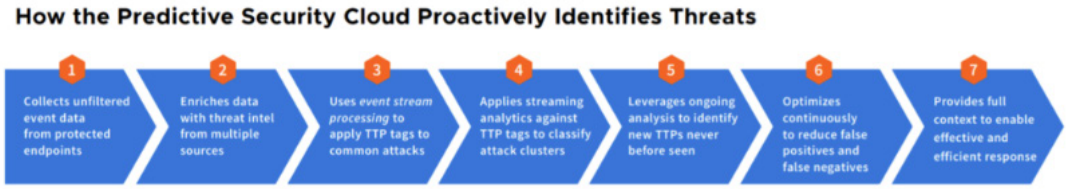



*See*, https://www.youtube.com/watch?v=WQm-hYHAv8g (showing an example of a threat score result or intel reputation for an application).

**Cb Predictive Security Cloud**

29. Defendant's Cb Predictive Security Cloud interacts with Cb Defense, Cb Defense for VMware, and Cb ThreatSight to provide "next-generation security services through the cloud." *See* Ex. G (https://www.carbonblack.com/products/cb-predictive-security-cloud/).

30. As shown below, Cb Predictive Security Cloud collects data from Carbon Black endpoint agents to provide protection against future attacks.



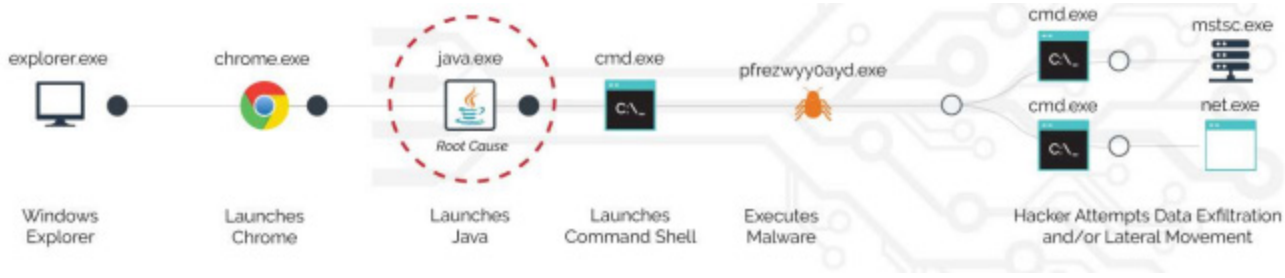

Ex. H (https://www.carbonblack.com/2018/01/23/what-is-the-cb-predictive-security-cloud-psc/).

31. As further shown below, Cb Predictive Security Cloud utilizes the same infringing technologies as the other Accused Products including NGAV, EDR, Collective Intel, and Detonation.


*See* Ex. I (https://www.carbonblack.com/2017/10/10/carbon-blacks-vision-predictive-security-cloud/).

**Cb Response**

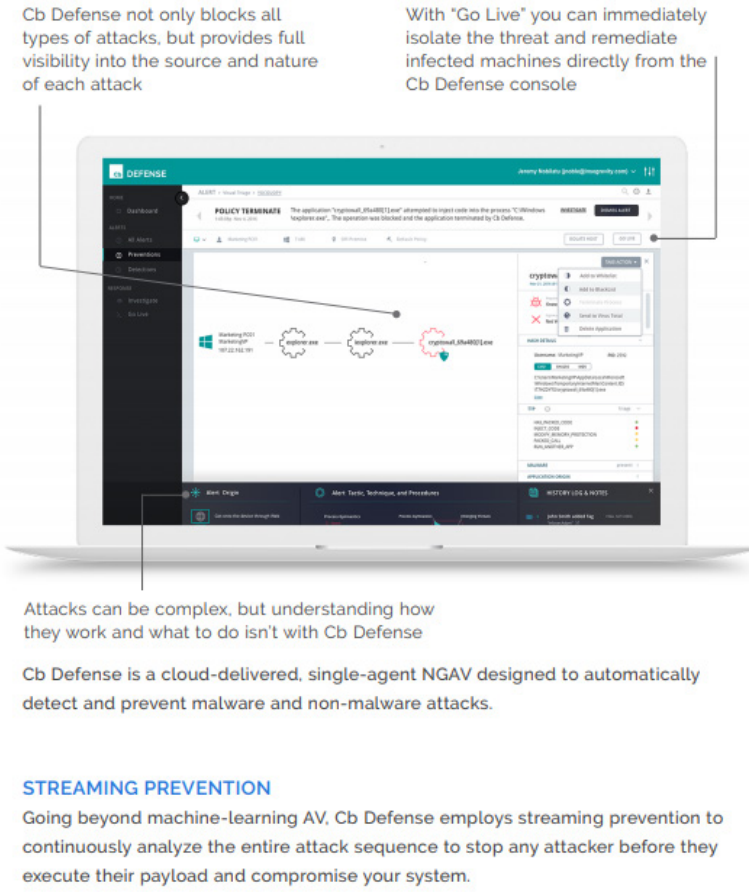
32. Defendant's Cb Response (formerly Cb Enterprise Response, on information and belief) is a "market-leading IR and threat hunting solution" that "continuously records and captures all endpoint activity." *See* Ex. J (https://www.carbonblack.com/company/news/press-releases/carbon-blacks-cb-response-6-1-scales-largest-enterprises-empowers-socs-ir-teams-gain-complete-endpoint-visibility-conclusive-root-cause-within-minutes/).




*See, e.g.*, Ex. K (https://cdn.www.carbonblack.com/wp-content/uploads/2017/04/CB_Response_Data_Sheet_web_fin-1.pdf).

**Cb Defense and Cb Defense for VMware**

33. Defendant's Cb Defense (and related Cb Defense for VMware) operates as a lightweight software agent at an endpoint and utilizes Carbon Black's cloud technologies to prevent malicious attacks. *See, e.g.*, Ex. L (Cb_Defense_ds_web-1.pdf).




*See* Ex. L (Cb_Defense_ds_web-1.pdf).

**Cb Protection**

34. Defendant's Cb Protection (formerly known as Carbon Black Enterprise Protection/Bit9 Security Platform/Bit9 Party Suite) is sold as licensed software that includes an on-premise Management Console, Cb Protection Agent (a light weight software that runs on endpoints), and a subscription to Cb Protection software (including Cb Collective Defense Cloud, maintenance, and support).

## DEFENDANT'S INFRINGEMENT OF FINJAN'S PATENTS

35. Defendant has been and is now infringing, and will continue to infringe, the Asserted Patents in this Judicial District and elsewhere in the United States by, among other things, making, using, importing, selling, and/or offering for sale its Cb Predictive Security Cloud, Cb Response, Cb Defense, Cb Defense for VMware, and Cb Protection (formerly known as Carbon Black Enterprise Protection/Bit9 Security Platform/Bit9 Party Suite) products and services ("Accused Products").

36. In addition to directly infringing the Asserted Patents pursuant to 35 U.S.C. § 271(a), either literally or under the doctrine of equivalents, or both, Defendant indirectly infringes all the Asserted Patents by instructing, directing, and/or requiring others, including its customers, purchasers, users, and developers, to perform all or some of the steps of the method claims, either literally or under the doctrine of equivalents, or both, of the Asserted Patents.

## COUNT I

**(Direct Infringement of the '780 Patent pursuant to 35 U.S.C. § 271(a))**

37. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

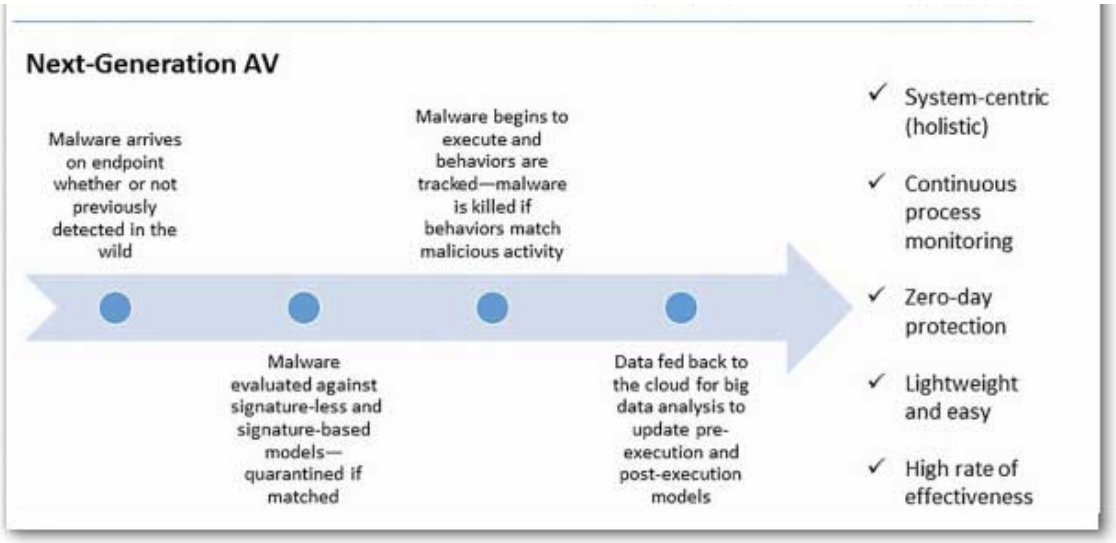
38. Defendant has infringed Claims 1-18 of the '780 Patent in violation of 35 U.S.C. § 271(a).

39. Defendant's infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

40. Defendant's acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of Finjan.

41. Defendant's infringement includes, but is not limited to, the manufacture, use, sale, importation and/or offer for sale of Defendant's products and services, including its Cb Predictive Security Cloud, Cb Response, Cb Defense, Cb Defense for VMware, and Cb Protection (formerly known as Carbon Black Enterprise Protection/Bit9 Security Platform/Bit9 Party Suite) products and services (collectively, the "'780 Accused Products").

42. The '780 Accused Products embody the patented invention of the '780 Patent and infringe the '780 Patent because they practice a method of obtaining a downloadable that includes one or more references to software components required to be executed by the downloadable, fetching at least one software component required to be executed by the downloadable, and performing a hashing function on the downloadable and the fetched software components to generate a downloadable ID. For example, as shown below, the '780 Accused Products provide gateway security to end users, where they receive downloadables that include one or more references to executable software components, including .exe files, .pdf files, and other downloadables that might exhibit malicious behavior.




NGAV capabilities also reach beyond use of indicators of compromise (IOCs), metadata such as virus signatures, IP addresses, file hashes and URLs—all of which demonstrate that potentially malicious activity has occurred.

Ex. F (https://www.carbonblack.com/2016/12/20/replacing-traditional-antivirus-with-next-gen-antivirus-visualizing-ngav-and-evaluation-architecture/).

43. The '780 Accused Products will also fetch at least one software component required to be executed by the downloadable.

## Endpoints

### GET /status/{hash}

The status endpoint returns data about the status of the inspection.

**Parameters**

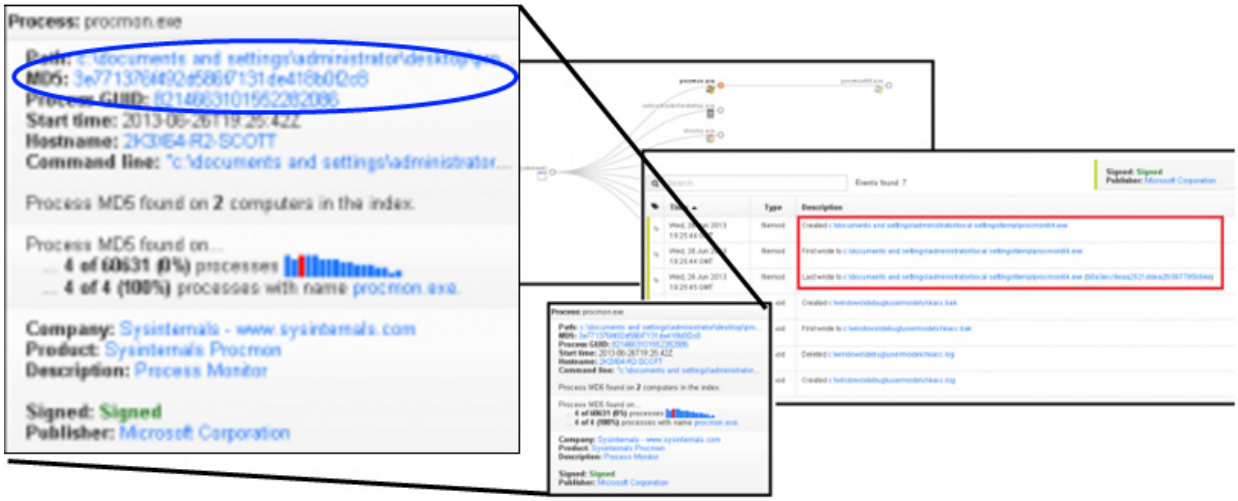
| in | name | type | required | description |
|---|---|---|---|---|
| path | hash | string | true | Hex string of either MD5 or SHA256 checksum of submitted binary |

**Response**


```
{
  "metadata": {
    "magic": "PE32 executable for MS Windows (native) Intel 80386 32-bit",
    "md5": "a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0",
    "mime": "application/octet-stream",
    "name": "2c018e375986cb29a76910850eb83bb0c14ed22c2d00194692e27955f3707f67.exe",
    "sha1": "a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0",
    "sha256": "a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0",
    "size": "4134122"
  }
```

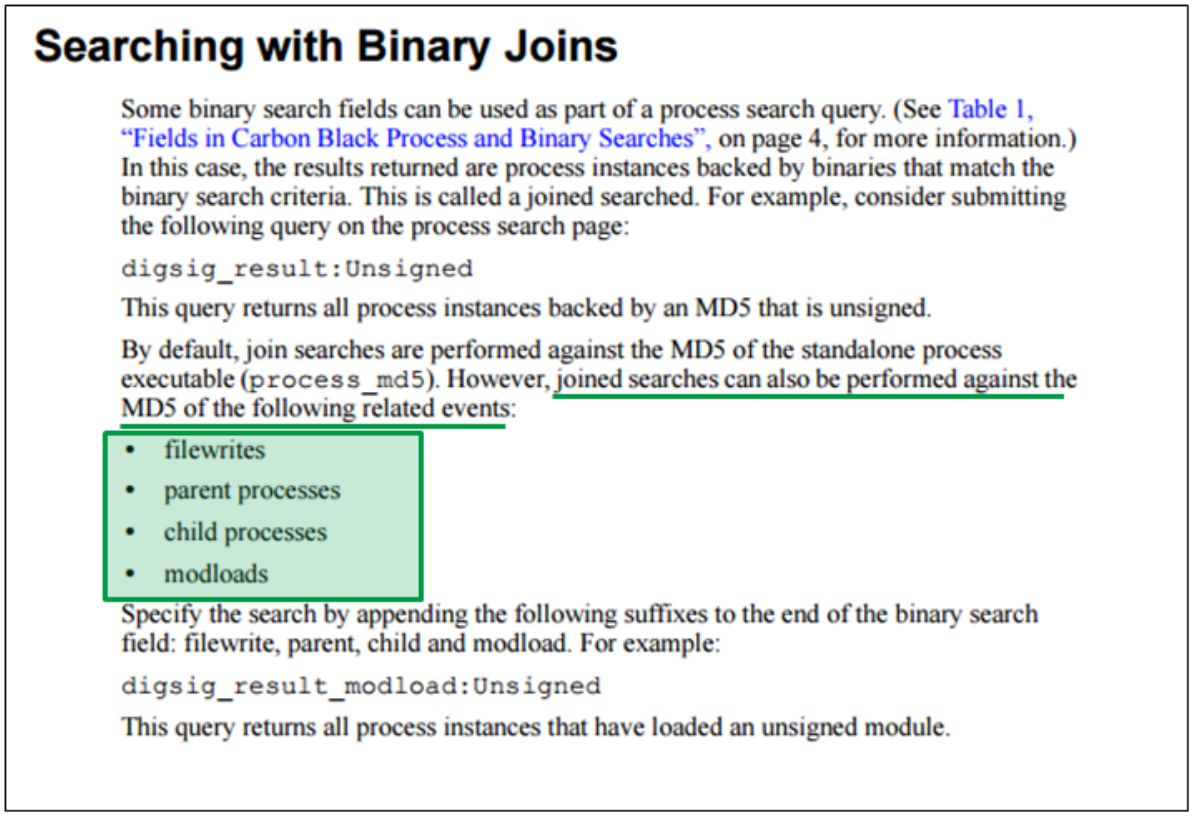

Ex. M (https://developer.carbonblack.com/reference/collective-defense-cloud/1/inspection-api/) (emphasis added) (showing that Carbon Black generates downloadable IDs using MD-5, SHA1, or SHA256 hashing functions).

44. The '780 Accused Products perform a hashing function (such as MD-5, SHA1, or SHA256) on the downloadable to generate a downloadable ID, as shown above and below. The '780 Accused Products hash files and components that are referenced by the downloadable as part of creating a downloadable ID, such as dropped files.




This was on my x64 system. The top-left element is the process tree, and shows the procmon.exe process with a child process named procmon64.exe. That explains how a single procmon executable runs on both x64 and x86 architectures—it's actually two executables. But how did procmon64.exe get there? The answer is in the process activity list, the right-central pane. Highlighted in red, it shows that procmon.exe recognized it was on an x64 system, created a new file called procmon64.exe in the temp directory, then executed it. (It also shows the MD5 hash of the file: b0a3ecc9eaa2521ddea2fc067785b84e.) Everything else happened in the procmon64.exe process.

Ex. N (https://www.carbonblack.com/2014/04/30/carbon-black-for-techies-a-distributed-process-monitor/) (emphasis added).



## Searching with Binary Joins

Some binary search fields can be used as part of a process search query. (See Table 1, "Fields in Carbon Black Process and Binary Searches", on page 4, for more information.) In this case, the results returned are process instances backed by binaries that match the binary search criteria. This is called a joined searched. For example, consider submitting the following query on the process search page:

```
digsig_result:Unsigned
```

This query returns all process instances backed by an MD5 that is unsigned.

By default, join searches are performed against the MD5 of the standalone process executable (`process_md5`). However, joined searches can also be performed against the MD5 of the following related events:

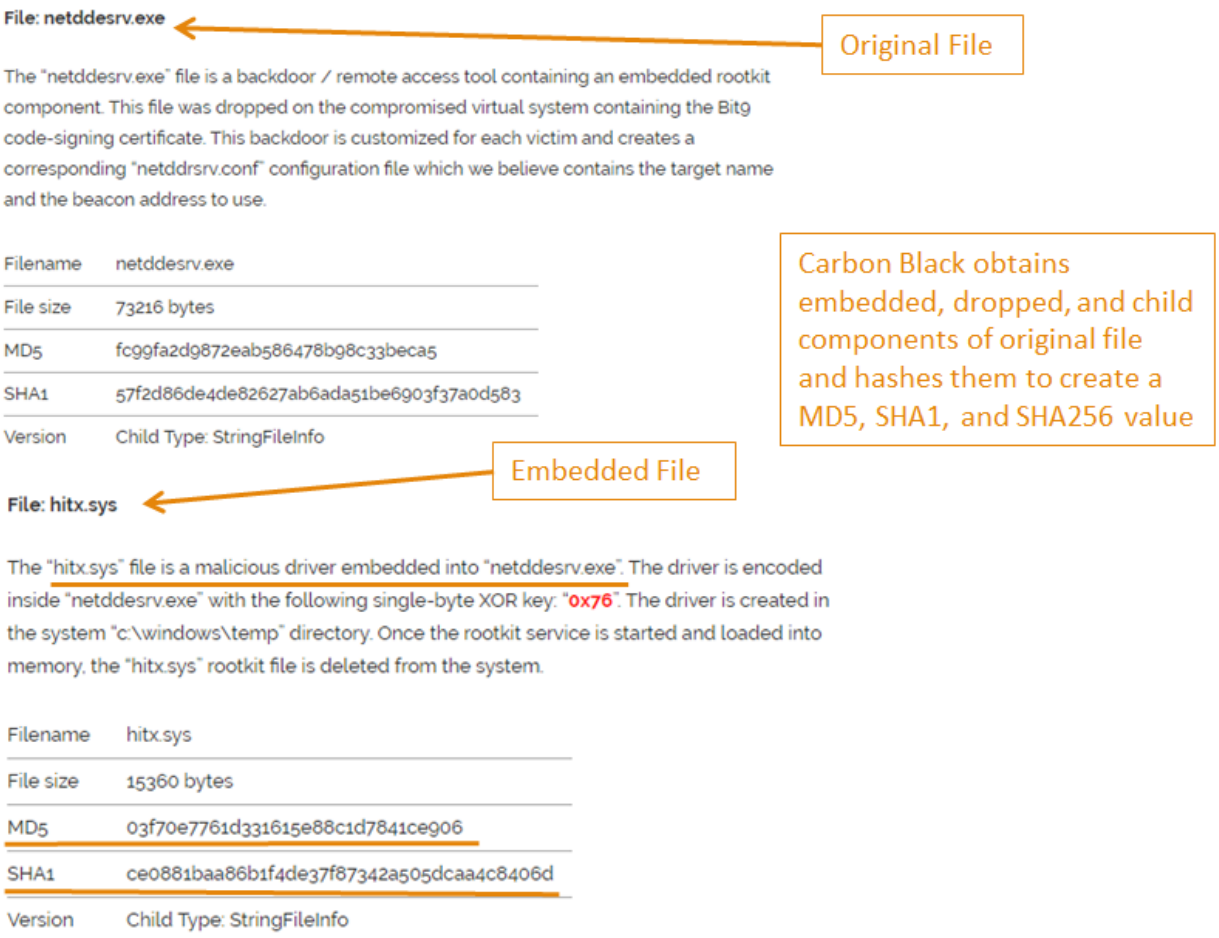
- filewrites
- parent processes
- child processes
- modloads

Specify the search by appending the following suffixes to the end of the binary search field: filewrite, parent, child and modload. For example:

```
digsig_result_modload:Unsigned
```

This query returns all process instances that have loaded an unsigned module.

Ex. O (https://developer.carbonblack.com/resources/query_overview.pdf) (emphasis added).




Ex. P (https://www.carbonblack.com/2013/02/25/bit9-security-incident-update/) (emphasis added).

45. Defendant's infringement of the '780 Patent has injured Finjan in an amount to be proven at trial.

46. Defendant has been specifically long-aware of Finjan's patents, including the '780 Patent, and has acted recklessly and egregiously with conduct that is willful, wanton, malicious, bad-faith, deliberate, wrongful, and flagrant by its continued infringing activity despite possessing specific knowledge of its infringement of the '780 Patent. Defendant has had specific knowledge of its infringement of the '780 Patent since at least in or about February 2016, when Finjan specifically identified and described the '780 Patent and how the '780 Patent reads on Defendant's Cb Protection, Cb Response, and Cb Threat Intel.

47. On information and belief, despite its knowledge of the '780 Patent and its knowledge of its own infringement of that patent since at least in or about February 2016, Defendant made no

effort to design its products or services around the '780 Patent in order to avoid infringement. Instead, on information and belief, Defendant incorporated infringing technology into additional products, such as those identified in this Complaint. All of these actions demonstrate Defendant's blatant and egregious disregard for, and willful infringement of, Finjan's patent rights.

48. Despite its knowledge of the Asserted Patents and being provided representative claim charts of the Asserted Patents, Defendant has sold and continues to sell the Accused Products and Services in complete and reckless disregard of Finjan's patent rights. As such, Defendant has acted recklessly and continues to willfully, wantonly, and deliberately engage in acts of infringement of the '780 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 the '780 Patent pursuant to 35 U.S.C. § 271(b))**

49. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

50. Defendant has induced infringement of at least Claims 1-8 of the '780 Patent under 35 U.S.C. § 271(b).

51. In addition to directly infringing the '780 Patent, Defendant indirectly infringes the '780 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including customers, purchasers, users and developers, to perform some of the steps of the method claims, either literally or under the doctrine of equivalents, of the '780 Patent, where all the steps of the method claims are performed by either Defendant or its customers, purchasers, users, and developers, or some combination thereof. Defendant knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users and developers, to infringe by practicing, either themselves or in conjunction with Defendant, one or more method claims of the '780 Patent, including Claims 1-8.

52. Defendant knowingly and actively aided and abetted the direct infringement of the '780 Patent by instructing and encouraging its customers, purchasers, users, and developers to use the

'780 Accused Products. Such instruction and encouragement includes, but is not limited to, advising third parties to use the '780 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the '780 Patent, advertising and promoting the use of the '780 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the '780 Accused Products in an infringing manner.

53. Defendant updates and maintains an HTTP site with Defendant's administration guides, user guides, operating instructions, and training and certifications which cover in depth aspects of operating the Accused Products. *See, e.g.*, Ex. Q (https://www.carbonblack.com/resources/support/).

**COUNT III**

**(Direct Infringement of the '844 Patent pursuant to 35 U.S.C. § 271(a))**

54. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

55. Defendant has infringed and continues to infringe Claims 1-44 of the '844 Patent in violation of 35 U.S.C. § 271(a).

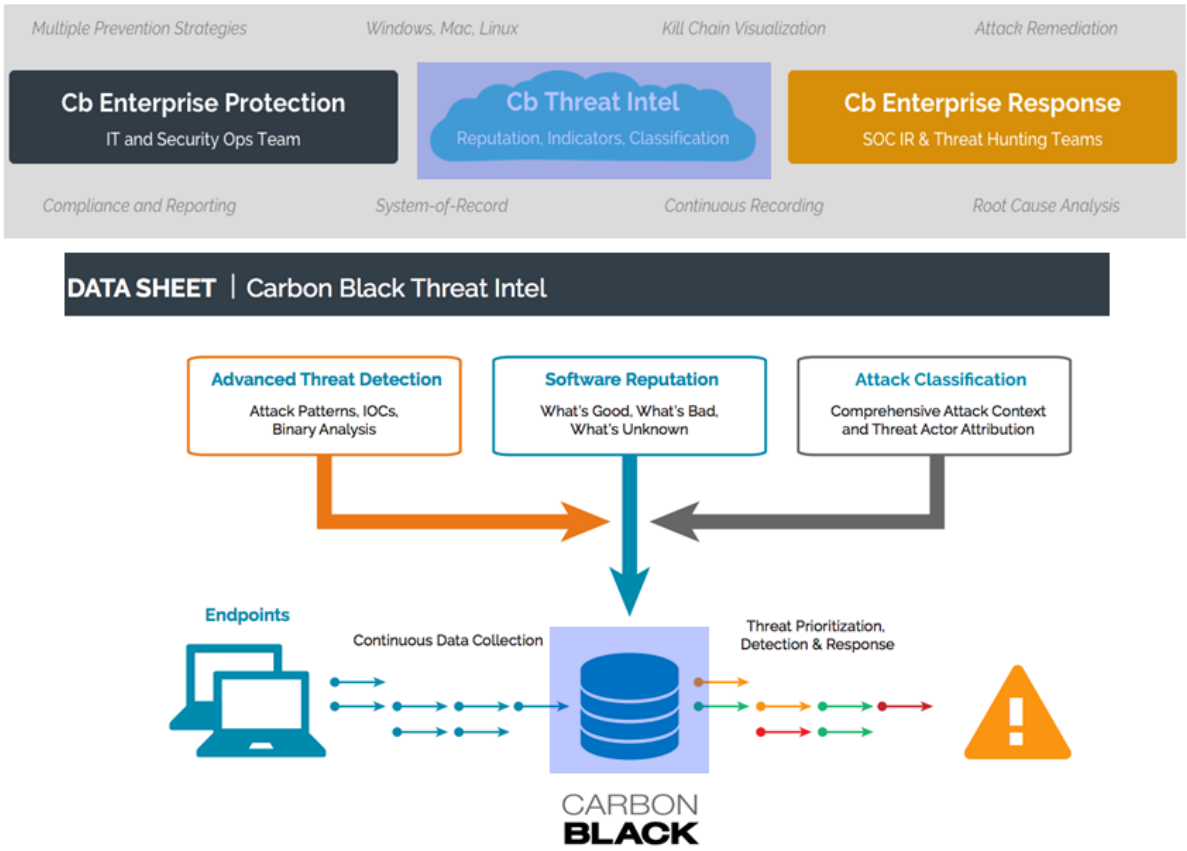
56. Defendant's infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

57. Defendant's acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of Finjan.

58. Defendant's infringement includes the manufacture, use, sale, importation and/or offer for sale of Defendant's products and services, including the Cb Predictive Security Cloud, Cb Response, Cb Defense, Cb Defense for VMware, and Cb Protection (formerly known as Carbon Black Enterprise Protection/Bit9 Security Platform/Bit9 Party Suite) (collectively, the "'844 Accused Products").

59. The '844 Accused Products embody the patented invention of the '844 Patent and infringe the '844 Patent because they practice a method of receiving by an inspector a downloadable,

generating by the inspector (e.g., Carbon Black's Advanced Threat Detection and Advanced Threat Indicators) a first downloadable security profile that identifies suspicious code in the received downloadable, and linking by the inspector the first downloadable security profile to the downloadable before a web server makes the downloadable available to web clients. *See* Ex. R (Cb_Endpoint_Threat_Detection_v2.pdf) ; Ex. S (https://www.carbonblack.com/wp-content/uploads/2016/02/2016_cb_threat_intel2.pdf). For example, as shown below, the '844 Accused Products provide security to end users, where incoming downloadables (e.g., PDFs with JavaScript, EXE files, or JavaScript embedded within an HTML file) are received by the '844 Accused Products.




Ex. R (Cb_Endpoint_Threat_Detection_v2.pdf) (emphasis added); Ex. S (https://www.carbonblack.com/wp-content/uploads/2016/02/2016_cb_threat_intel2.pdf) (emphasis added).

60. Carbon Black's Endpoint Threat Protection generates a downloadable security profile that analyzes suspicious behavior and captures a list of suspicious code (identified as

"SuspiciousActivities" or "CommandName") that are performed by the downloadable using a variety of rules and "detonation."


```
{
  "metadata": {
    "magic": "PE32 executable for MS Windows (native) Intel 80386 32-bit",
    "md5": "a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0",
    "mime": "application/octet-stream",
    "name": "2c018e375986cb29a76910850eb83bb0c14ed22c2d00194692e27955f3707f67.exe",
    "sha1": "a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0",
    "sha256": "a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0",
    "size": "4134122"
  },
  "report_url": "https://analysis.carbonblack.com/report/g",
  "results": {
    "analysis_summary": "bad",
    "detonation": {
      "data": [
        {
          "te": {
            "CPULevelDetection": "false",
            "SuspiciousActivities": {
              "SuspiciousEvent": {
                "SuspiciousActivity": [
                  {
                    "Path": "[low confidence] Behaves like a known malware ( Generic.MALWARE.x )"
                  }
                ],
                "Type": "SuspiciousActivityEvent"
              }
            },
            "System": {
              "OsInfo": "Microsoft Windows 7 32 bit, Office 2003, Office 2007, Adobe Acrobat Reader 9.0, Adobe Fl
              "OsRev": "53",
              "OsUID": "7e6fe36e-889e-4c25-8704-56378f0830df",
              "Osname": "Windows 7"
            },
            "reportDate": "Tue Sep 27 10:39:09 2016"
      "status": "complete"
    },
    "score": 100,
    "score_factors": {
      "detonation": {
        "score": 8,
        "verdict": "suspicious"
      },
      "strings_analysis": {},
      "subfile": {
        "score": 100,
        "verdict": "bad"
      },
      "yara": {
        "score": 100,
        "verdict": "bad"
      }
    },
```

```
"yara": {
  "data": [
    {
      "generic": {
        "matches": [
          {
            "meta": {
              "confidence": 8,
              "description": "Detects Sauron/Strider/Remsec based on rich trash headers",
              "severity": 10
            },
            "namespace": "production.yar",
            "rule": "sauron_strider_trash"
          }
```


*See* Ex. M (https://developer.carbonblack.com/reference/collective-defense-cloud/1/inspection-api/) (identifying suspicious code, suspicious malware, YARA rule hits, "detonation" analysis).

61. As shown below, Carbon Black's products include information about YARA rule hits and descriptions, which can be used to detect suspicious code.

**Yara**

**Schema**

- (object)
  - `data` (array): Yara data results
  - (object)
    - `matches` (array): List of yara rules that matched on this binary
    - (object)
      - `meta` (object): Metadata about Yara rule that fired
      - `condidence` (integer: int32): Confidence factor in Yara rule
      - `description` (string): Description of Yara rule
      - `severity` (integer: int32)
      - `rule` (string): Name of Yara rule
  - `status` (string): Status of Yara analysis

*See* Ex. M (https://developer.carbonblack.com/reference/collective-defense-cloud/1/inspection-api/) (showing YARA schema).

62. As shown below, Carbon Black's StringsAnalysis schema includes information about the string hits and descriptions, which can be used to detect suspicious code.

**StringsAnalysis**

**Schema**

- (object)
  - `data` (array): generic object wrapper
  - (object)
    - `ascii_strings` (string): ascii strings
    - `unicode_strings` (string): unicode strings
  - `status` (string): Status of StringsAnalysis

*See* Ex. M (https://developer.carbonblack.com/reference/collective-defense-cloud/1/inspection-api/) (showing StringAnalysis schema).

63. As shown below, Carbon Black's Detonation schema includes information about the detonation, which can be used to detect suspicious code.

**Detonation**

**Schema**

- (object)
  - `data` (array): List of data sections
  - (object)
    - `te` (object): Emulation telemetry data
    - `System` (object)
      - `OsInfo` (string): Description of OS
      - `OsRev` (string): OS Rev of Sandbox environment
      - `OsUID` (string): unique identifier for Sandbox environment
      - `Osname` (string): Name of OS (e.g. Windows 8.1)
    - `Activities` (object): Set of activities observed during execution on the sandbox
      - `Command` (array): list of Commands performed during execution
      - (object)
        - `Action` (string): Name of action performed. e.g. QueryKey, Read,
        - `CommandName` (string: RegistryEvent, FileSystemEvent, NetworkEvent, SuspiciousActivityEvent, ProcessEvent, NetworkHTTPEvent): Type of command performed. e.g. RegistryEvent, FileSystemEvent
    - `SuspiciousActivities` (object): Set of behaviours observed during execution on the sandbox
      - `SuspiciousEvent` (object)
      - `Type` (string): type of suspicious activity observed during execution
      - `SuspiciousActivity` (array): list of observed behaviours during execution on sandbox
        - (object)
        - `Path` (string)
    - `av` (object): Antivirus Scanner Information
    - `signature_name` (string): Malware signature name
  - `status` (string): Status of Detonation

*See* Ex. M (https://developer.carbonblack.com/reference/collective-defense-cloud/1/inspection-api/) (showing Detonation schema).

64. As shown below, Carbon Black's ScoreFactors and Report schemas includes information about the downloadable, including scores related to a downloadable's suspiciousness.

**ScoreFactors**

**Schema**

- (object)
  - `detonation` (object): Detonation score information
  - `score` (integer: int32): Score of detonation
  - `verdict` (string: good, bad, suspicious, unknown): Enum of verdict from detonation
  - `yara` (object): Yara score information
  - `score` (integer: int32): Score of Yara
  - `verdict` (string: good, bad, suspicious, unknown): Enum of verdict from Yara
  - `cb_reputation` (object)
  - `score` (integer: int32): Score of CB reputation
  - `prevalence` (object): Prevalence
  - `score` (integer: int32): Factor for community prevalence

*See* Ex. M (https://developer.carbonblack.com/reference/collective-defense-cloud/1/inspection-api/) (showing Detonation schema stored in a security profile).

65. As shown below, Carbon Black's Endpoint Threat generates a downloadable security profile that analyzes suspicious behavior and captures a list of suspicious code.

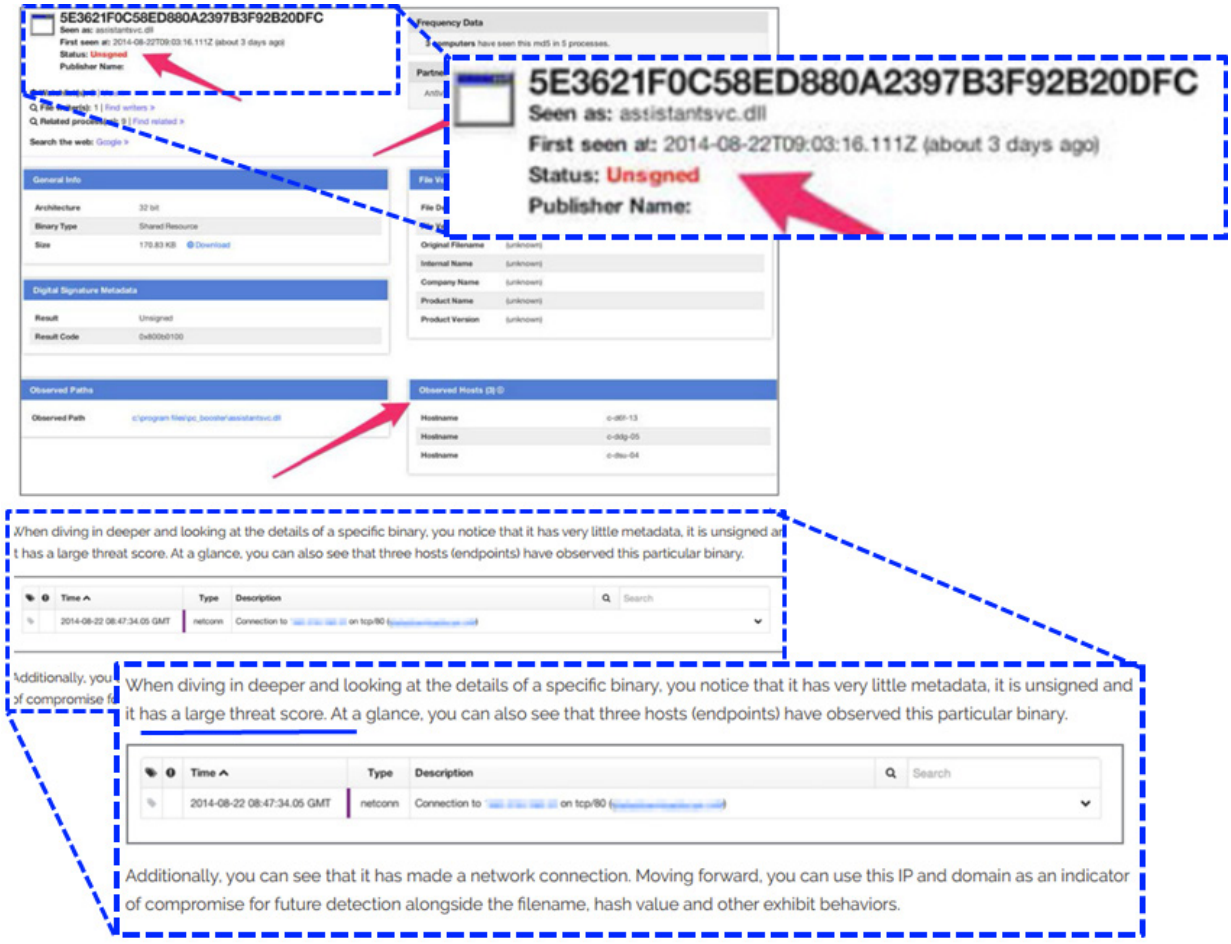
| Suspicious Application Behavior | Example |
|---|---|
| • Possible exploit of document-handling application<br>• Shell execution from document-handling application<br>• Unexpected command shell use<br>• File execution from recycle bin | • User opens an email .DOC attachment, and a hidden malware executable attempts to map the network using shell commands |
| **Suspicious Executable Properties** | **Example** |
| • Suspicious executable based on location<br>• Suspicious executable based on name<br>• Suspicious executable based on extension | • A common non-executable file name is dropped into and run from a recycle bin or temp folder such as a file with a PDF or GIF extension |
| **Process Injection** | **Example** |
| • Possible password hash tool execution<br>• Suspicious process injection | • Malware inject into MS Local Security Authority Subsystem Service (LSASS) gaining access to password cache on an endpoint |
| **System Configuration Tampering** | **Example** |
| • Possible name resolution tampering<br>• Unusual change to startup configuration<br>• Possible file hiding | • Malware arrives and tampers with system configuration: Explorer file view, firewall settings, IP address settings |

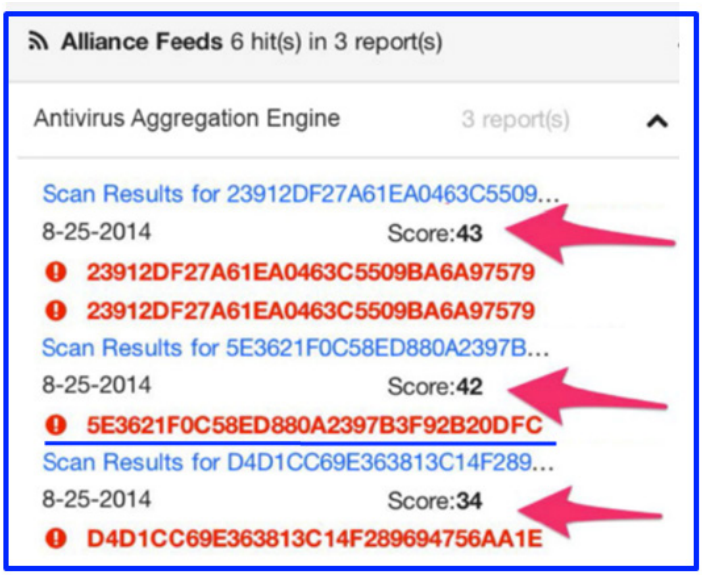
Ex. R (Cb_Endpoint_Threat_Detection_v2.pdf) (emphasis added).

> **Advanced Threat Indicators (ATI)**, developed by the Carbon Black threat research team, monitor and examine many system facets, including files, registry, process and memory execution, to identify potential compromise or infection in real time. ATIs also can examine the recorded history of endpoint activity that

Ex. R at (Cb_Endpoint_Threat_Detection_v2.pdf) (emphasis added).

66. Carbon Black links the downloadable security profile to the downloadable before it is made available to the client. For example, Carbon Black uses rules to determine a "score" on whether the content is malicious and links the downloadable security profile to the downloadable to prevent access to the downloadable via a blocking mechanism.






*See* Ex. T (2016_cb_wp_threat_hunting.pdf) (emphasis added)).

67. Defendant's infringement of the '844 Patent has injured Finjan in an amount to be proven at trial.

68. Defendant has been specifically long-aware of Finjan's patents, including the '844 Patent, and has acted recklessly and egregiously with conduct that is willful, wanton, malicious, bad-faith, deliberate, wrongful, and flagrant by its continued infringing activity despite possessing specific knowledge of its infringement of the '844 Patent. Defendant has had specific knowledge of its infringement of the '844 Patent since at least on or about December 2015, when Finjan specifically identified and described the following products made, used, or sold by Defendant as infringing the '844 Patent: Bit9 + Carbon Black Solution, the Bit9 Security Platform, and the Bit9 + Carbon Black Threat Intelligence Cloud. Finjan also provided Defendant with a claim chart on or about February 2016 specifically describing how the '844 Patent reads on its products.

69. On information and belief, despite its knowledge of the '844 Patent and its knowledge of its own infringement of that patent since at least in or about December 2015, Defendant made no effort to design its products or services around the '844 Patent in order to avoid infringement. Instead, on information and belief, Defendant incorporated infringing technology into additional

products, such as those identified in this Complaint. All of these actions demonstrate Defendant's blatant and egregious disregard for, and willful infringement of, Finjan's patent rights.

70. Despite its knowledge of the Asserted Patents and being provided representative claim charts of the Asserted Patents, Defendant has sold and continues to sell the Accused Products and Services in complete and reckless disregard of Finjan's patent rights. As such, Defendant has acted recklessly and continues to willfully, wantonly, and deliberately engage in acts of infringement of the '844 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 IV**
**(Indirect Infringement of the '844 Patent pursuant to 35 U.S.C. § 271(b))**

71. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

72. Defendant has induced and continues to induce infringement of one or more claims of the '844 Patent under 35 U.S.C. § 271(b).

73. In addition to directly infringing the '844 Patent, Defendant indirectly infringes the '844 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including customers, purchasers, users and developers, to perform some of the steps of the method claims of the '844 Patent, either literally or under the doctrine of equivalents, where all the steps of the method claims are performed by either Defendant or its customers, purchasers, users and developers, or some combination thereof. Defendant knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users and developers, to infringe by practicing, either themselves or in conjunction with Defendant, one or more method claims of the '844 Patent, including Claims 1-14 and 23-31.

74. Defendant knowingly and actively aided and abetted the direct infringement of the '844 Patent by instructing and encouraging its customers, purchasers, users and developers to use the '844 Accused Products. Such instruction and encouragement includes, but is not limited to, advising third parties to use the '844 Accused Products in an infringing manner, providing a mechanism through

which third parties may infringe the '844 Patent, advertising and promoting the use of the '844 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the '844 Accused Products in an infringing manner.

75. Defendant updates and maintains an HTTP site with Defendant's administration guides, user guides, operating instructions, and training and certifications which cover in depth aspects of operating the Accused Products. *See, e.g.*, Ex. Q (https://www.carbonblack.com/resources/support/).

**COUNT V**

**(Direct Infringement of the '494 Patent pursuant to 35 U.S.C. § 271(a))**

76. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

77. Defendant has infringed Claims 3-5 and 7-18 of the '494 Patent in violation of 35 U.S.C. § 271(a).

78. Defendant's infringement is based upon literal infringement or, in the alternative, infringement under the doctrine of equivalents.

79. Defendant acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization or license of Finjan.

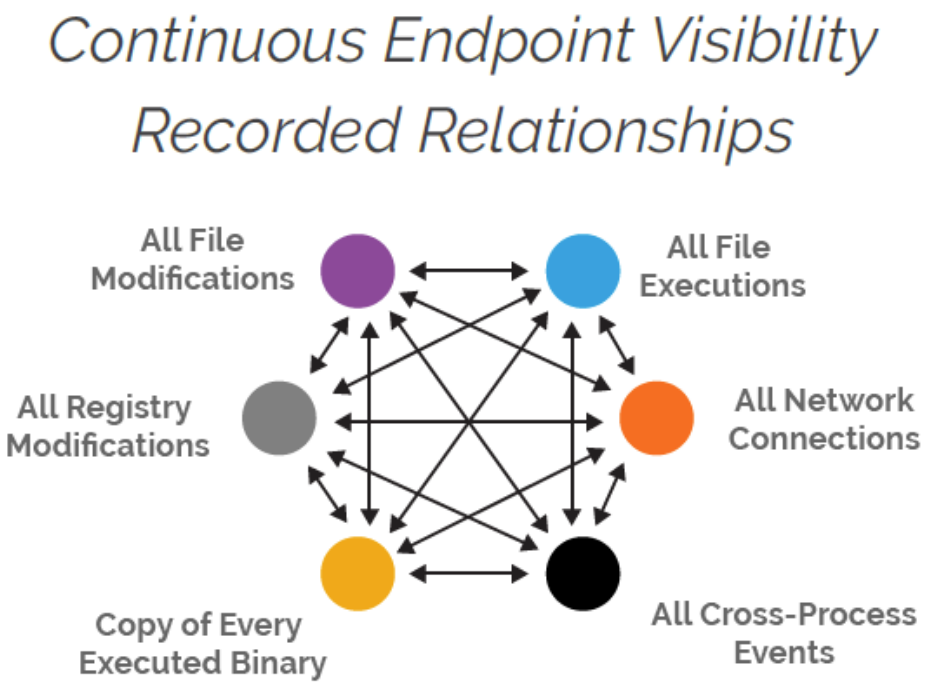
80. Defendant's infringement includes, but is not limited to, the manufacture, use, sale, importation and/or offer for sale of Defendant's products and services, including its Cb Predictive Security Cloud, Cb Response, Cb Defense, Cb Defense for VMware, and Cb Protection (formerly known as Carbon Black Enterprise Protection/Bit9 Security Platform/Bit9 Party Suite) products and services (collectively, the "'494 Accused Products").

81. The '494 Accused Products embody the patented invention of the '494 Patent and infringe the '494 Patent because they practice a system for managing downloadables comprising a receiver for receiving an incoming downloadable, a scanner for deriving security profile data for the downloadable, including a list of suspicious computer operations that may be attempted by the downloadable, and a database manager for storing the downloadable security profile data in a

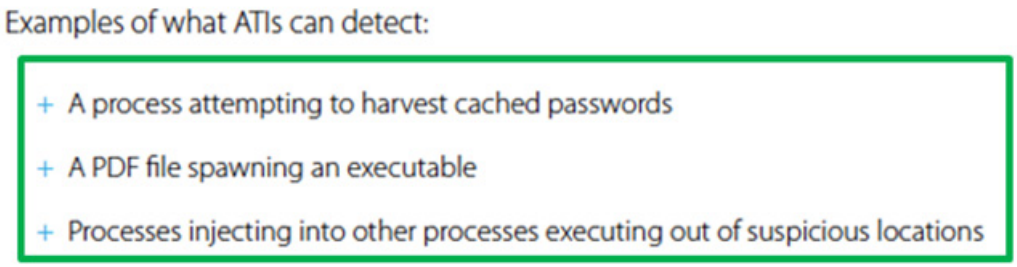
database. For example, as shown below, the '494 Accused Products provide security to end users, where incoming downloadables are received by the '494 Accused Products. For example, Carbon Black's Advanced Threat Indicators (ATI) derive security profile data for the downloadable, which includes a list of suspicious computer operations that may be attempted by the downloadable. As shown below, Carbon Black's Accused Products and Services receive incoming downloadables such as JavaScript and Java, and monitor their actions for suspicious operations.

**Advanced Threat Indicators (ATI)**, developed by the Carbon Black threat research team, monitor and examine many system facets, including files, registry, process and memory execution, to identify potential compromise or infection in real time. ATIs also can examine the recorded history of endpoint activity that

Ex. R (Cb_Endpoint_Threat_Detection_v2.pdf) (emphasis added).

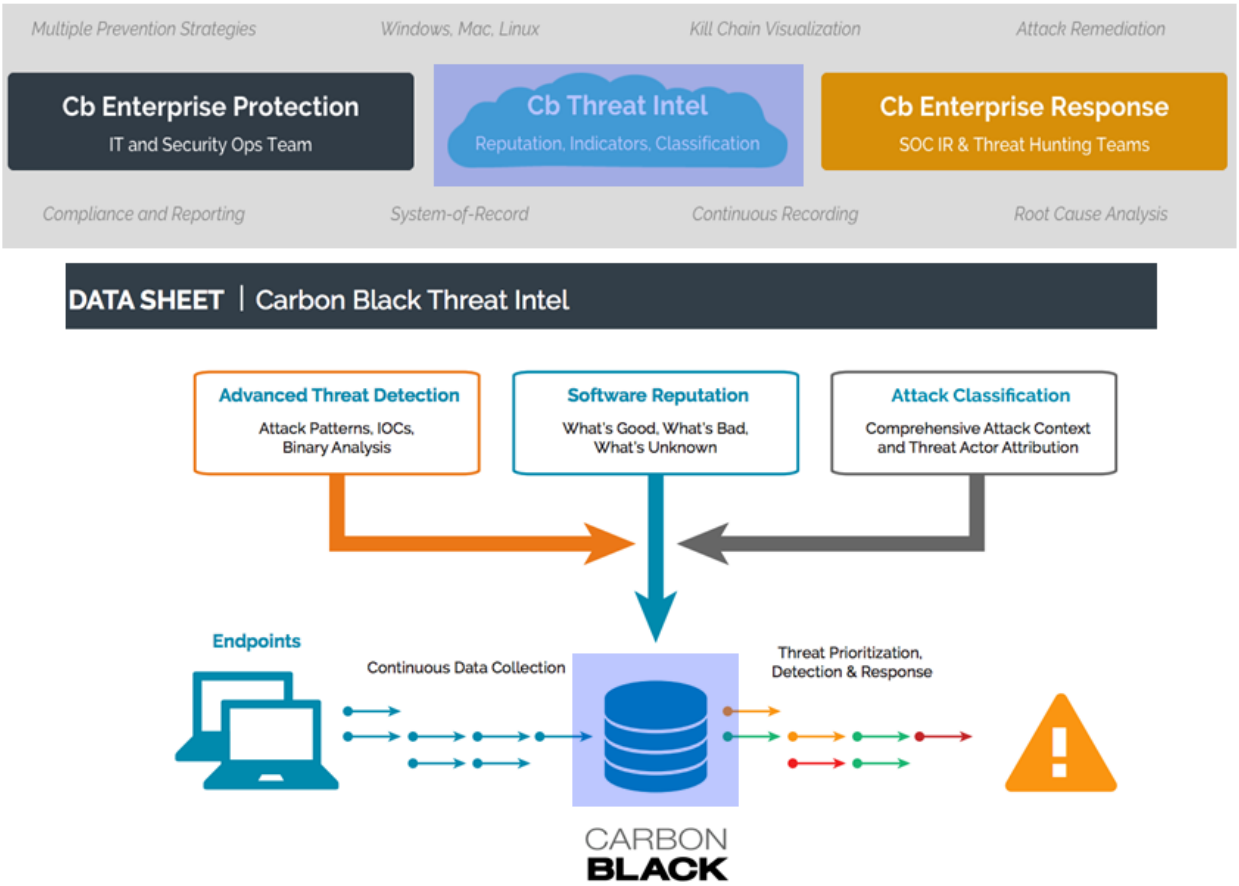



*See* Ex. T (2016_cb_wp_threat_hunting.pdf).




Ex. U (data-breach-detection-what-you-need-to-know.pdf) (emphasis added).

82. As shown below, Carbon Black's Endpoint Threat Protection performs static and dynamic analyses on the downloadable and then stores the downloadable security profile data in databases (such as the Carbon Black's Continuous Data Collection database) and provides reports of that data.




Ex. R (Cb_Endpoint_Threat_Detection_v2.pdf) (emphasis added) ; Ex. S (https://www.carbonblack.com/wp-content/uploads/2016/02/2016_cb_threat_intel2.pdf).

83. As shown below, Carbon Black's Endpoint Threat Protection derives security profile data identifying suspicious operations using a variety of rules and "detonation" and stores them in a database.


```
{
  "metadata": {
    "magic": "PE32 executable for MS Windows (native) Intel 80386 32-bit",
    "md5": "a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0",
    "mime": "application/octet-stream",
    "name": "2c018e375986cb29a76910850eb83bb0c14ed22c2d00194692e27955f3707f67.exe",
    "sha1": "a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0",
    "sha256": "a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a0",
    "size": "4134122"
  },
  "report_url": "https://analysis.carbonblack.com/report/g",
  "results": {
    "analysis_summary": "bad",
    "detonation": {
      "data": [
        {
          "te": {
            "CPULevelDetection": "false",
            "SuspiciousActivities": {
              "SuspiciousEvent": {
                "SuspiciousActivity": [
                  {
                    "Path": "[low confidence] Behaves like a known malware ( Generic.MALWARE.x )"
                  }
                ],
                "Type": "SuspiciousActivityEvent"
              }
            },
            "System": {
              "OsInfo": "Microsoft Windows 7 32 bit, Office 2003, Office 2007, Adobe Acrobat Reader 9.0, Adobe Fl
              "OsRev": "53",
              "OsUID": "7e6fe36e-889e-4c25-8704-56378f0830df",
              "Osname": "Windows 7"
            },
            "reportDate": "Tue Sep 27 10:39:09 2016"
    "status": "complete"
  },
  "score": 100,
  "score_factors": {
    "detonation": {
      "score": 8,
      "verdict": "suspicious"
    },
    "strings_analysis": {},
    "subfile": {
      "score": 100,
      "verdict": "bad"
    },
    "yara": {
      "score": 100,
      "verdict": "bad"
    }
  },
```

```
"yara": {
  "data": [
    {
      "generic": {
        "matches": [
          {
            "meta": {
              "confidence": 8,
              "description": "Detects Sauron/Strider/Remsec based on rich trash headers",
              "severity": 10
            },
            "namespace": "production.yar",
            "rule": "sauron_strider_trash"
          }
```


*See* Ex. M (https://developer.carbonblack.com/reference/collective-defense-cloud/1/inspection-api/) (identifying YARA rule hits and "detonation" analysis).

84. As shown below, Carbon Black's YARA rules schema includes information about the YARA rule hits and descriptions, which can be used to detect suspicious operations.

**Yara**

**Schema**

- (object)
  - `data` (array): Yara data results
  - (object)
    - `matches` (array): List of yara rules that matched on this binary
    - (object)
      - `meta` (object): Metadata about Yara rule that fired
      - `condidence` (integer: int32): Confidence factor in Yara rule
      - `description` (string): Description of Yara rule
      - `severity` (integer: int32)
      - `rule` (string): Name of Yara rule
  - `status` (string): Status of Yara analysis

*See* Ex. M (https://developer.carbonblack.com/reference/collective-defense-cloud/1/inspection-api/) (showing YARA schema).

85. As shown below, Carbon Black's StringsAnalysis schema includes information about the string hits and descriptions, which can be used to detect suspicious operations.

**StringsAnalysis**

**Schema**

- (object)
  - `data` (array): generic object wrapper
  - (object)
    - `ascii_strings` (string): ascii strings
    - `unicode_strings` (string): unicode strings
  - `status` (string): Status of StringsAnalysis

*See* Ex. M (https://developer.carbonblack.com/reference/collective-defense-cloud/1/inspection-api/) (showing StringAnalysis schema).

86. As shown below, Carbon Black's Detonation schema includes information about the detonation, which can be used to detect suspicious operations.

**Detonation**

**Schema**

- (object)
  - `data` (array): List of data sections
  - (object)
    - `te` (object): Emulation telemetry data
    - `System` (object)
      - `OsInfo` (string): Description of OS
      - `OsRev` (string): OS Rev of Sandbox environment
      - `OsUID` (string): unique identifier for Sandbox environment
      - `Osname` (string): Name of OS (e.g. Windows 8.1)
    - `Activities` (object): Set of activities observed during execution on the sandbox
      - `Command` (array): list of Commands performed during execution
      - (object)
        - `Action` (string): Name of action performed. e.g. QueryKey, Read,
        - `CommandName` (string: RegistryEvent, FileSystemEvent, NetworkEvent, SuspiciousActivityEvent, ProcessEvent, NetworkHTTPEvent): Type of command performed. e.g. RegistryEvent, FileSystemEvent
    - `SuspiciousActivities` (object): Set of behaviours observed during execution on the sandbox
      - `SuspiciousEvent` (object)
      - `Type` (string): type of suspicious activity observed during execution
      - `SuspiciousActivity` (array): list of observed behaviours during execution on sandbox
        - (object)
        - `Path` (string)
    - `av` (object): Antivirus Scanner Information
    - `signature_name` (string): Malware signature name
  - `status` (string): Status of Detonation

*See* Ex. M (https://developer.carbonblack.com/reference/collective-defense-cloud/1/inspection-api/) (showing Detonation schema stored in a security profile).

87. As shown below, Carbon Black's ScoreFactors and Report schemas includes information about the downloadable, including scores related to a downloadable's suspiciousness.

**ScoreFactors**

**Schema**

- (object)
  - `detonation` (object): Detonation score information
  - `score` (integer: int32): Score of detonation
  - `verdict` (string: good, bad, suspicious, unknown): Enum of verdict from detonation
  - `yara` (object): Yara score information
  - `score` (integer: int32): Score of Yara
  - `verdict` (string: good, bad, suspicious, unknown): Enum of verdict from Yara
  - `cb_reputation` (object)
  - `score` (integer: int32): Score of CB reputation
  - `prevalence` (object): Prevalence
  - `score` (integer: int32): Factor for community prevalence

*See* Ex. M (https://developer.carbonblack.com/reference/collective-defense-cloud/1/inspection-api/) (showing Detonation schema stored in a security profile).

88. Defendant's infringement of the '494 Patent has injured Finjan in an amount to be proven at trial.

89. Defendant has been specifically long-aware of Finjan's patents, including the '494 Patent, and has acted recklessly and egregiously with conduct that is willful, wanton, malicious, bad-faith, deliberate, wrongful, and flagrant by its continued infringing activity despite possessing specific knowledge of its infringement of the '494 Patent. Defendant has had specific knowledge of its infringement of the '494 Patent since at least in or about December 2015, when Finjan specifically identified and described the following products made, used, or sold by Defendant as infringing the '494 Patent: Bit9 + Carbon Black Solution, the Bit9 Security Platform, and the Bit9 + Carbon Black Threat Intelligence Cloud. Finjan also provided Defendant with a claim chart on or about February 2016 specifically describing how the '494 Patent reads on its products.

90. On information and belief, despite its knowledge of the '494 Patent and its knowledge of its own infringement of that patent since at least in or about December 2015, Defendant made no effort to design its products or services around the '494 Patent in order to avoid infringement.

Instead, on information and belief, Defendant incorporated infringing technology into additional products, such as those identified in this Complaint. All of these actions demonstrate Defendant's blatant and egregious disregard for, and willful infringement of, Finjan's patent rights.

91. Despite its knowledge of the Asserted Patents and being provided representative claim charts of the Asserted Patents, Defendant has sold and continues to sell the Accused Products and Services in complete and reckless disregard of Finjan's patent rights. As such, Defendant has acted recklessly and continues to willfully, wantonly, and deliberately engage in acts of infringement of the '494 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 VI**
**(Indirect Infringement of the '494 Patent pursuant to 35 U.S.C. § 271(b))**

92. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

93. Defendant has induced infringement of at least Claims 3-5 and 7-9 of the '494 Patent under 35 U.S.C. § 271(b).

94. In addition to directly infringing the '494 Patent, Defendant indirectly infringes the '494 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including customers, purchasers, users and developers, to perform one or more of the steps of the method claims, either literally or under the doctrine of equivalents, of the '494 Patent, where all the steps of the method claims are performed by either Defendant, its customers, purchasers, users, and developers, or some combination thereof. Defendant knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users, and developers, to infringe by practicing, either themselves or in conjunction with Defendant, one or more method claims of the '494 Patent, including Claims 3-5 and 7-9.

95. Defendant knowingly and actively aided and abetted the direct infringement of the '494 Patent by instructing and encouraging its customers, purchasers, users, and developers to use the '494 Accused Products. Such instruction and encouragement includes, but is not limited to, advising

third parties to use the '494 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the '494 Patent, advertising and promoting the use of the '494 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the '494 Accused Products in an infringing manner.

96. Defendant updates and maintains an HTTP site with Defendant's administration guides, user guides, operating instructions, and training and certifications which cover in depth aspects of operating the Accused Products. *See, e.g.*, Ex. Q (https://www.carbonblack.com/resources/support/).

**COUNT VII**

**(Direct Infringement of the '154 Patent pursuant to 35 U.S.C. § 271(a))**

97. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

98. Defendant has infringed and continues to infringe Claims 1-12 of the '305 Patent in violation of 35 U.S.C. § 271(a).

99. Defendant's infringement is based upon literal infringement or, in the alternative, infringement under the doctrine of equivalents.

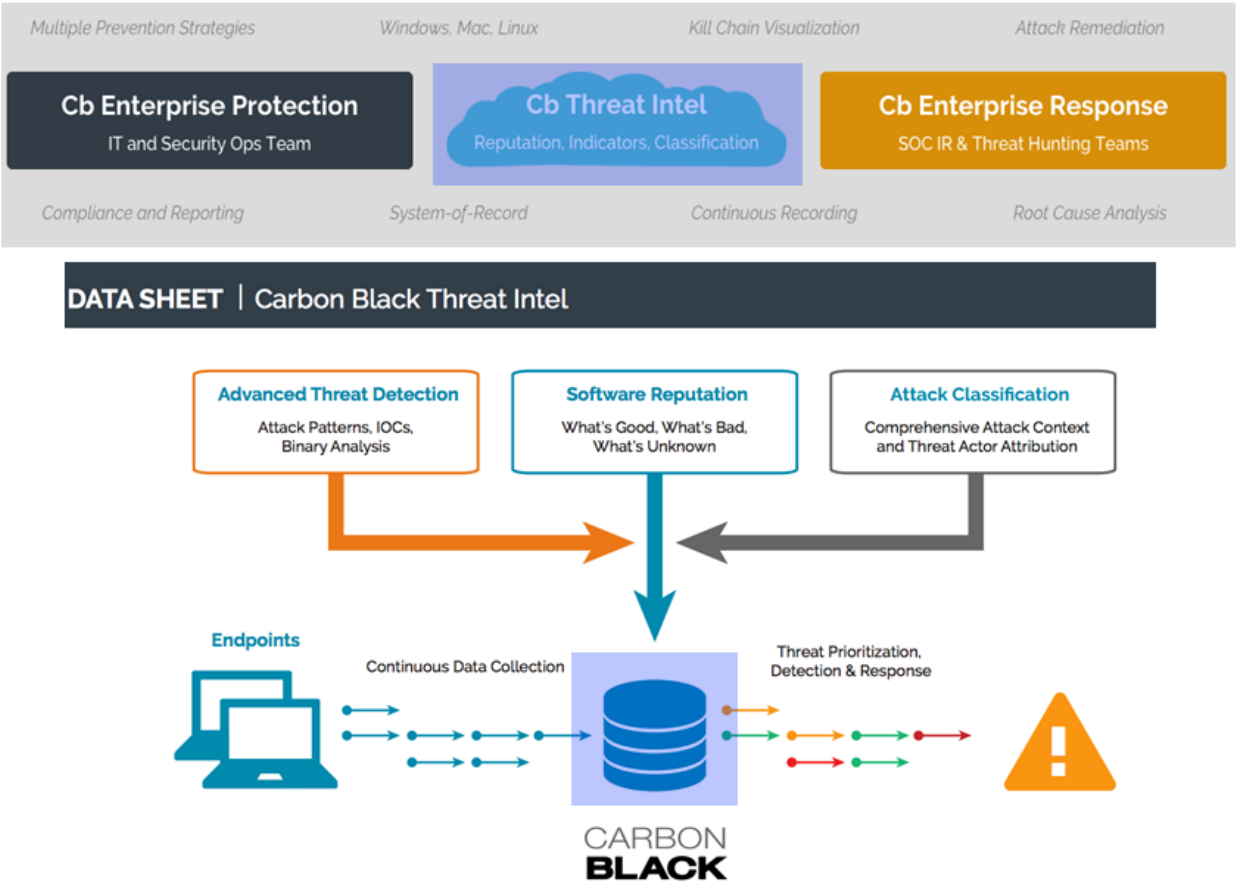
100. Defendant acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization or license of Finjan.

101. Defendant's infringement includes, but is not limited to, the manufacture, use, sale, importation and/or offer for sale of Defendant's products and services, including the Cb Predictive Security Cloud, Cb Response, Cb Defense, Cb Defense for VMware, and Cb Protection (formerly known as Carbon Black Enterprise Protection/Bit9 Security Platform/Bit9 Party Suite) (collectively, the "'154 Accused Products").

102. The '154 Accused Products embody the patented invention of the '154 Patent and infringe the '154 Patent because they utilize and/or incorporate 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

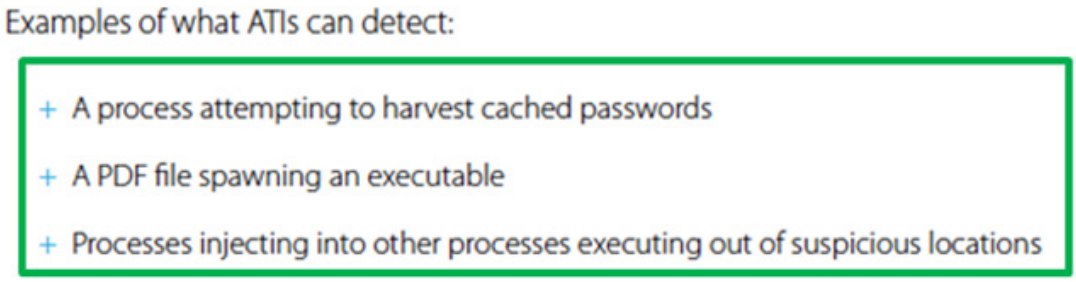
an input, and (ii) for invoking a second function with the input, only if a security computer indicates that such invocation is safe; a transmitter for transmitting the input to the security computer for inspection, when the first function is invoked; and a receiver for receiving an indication from the security computer whether it is safe to invoke the second function with the input.

103. For example, as shown below, the '154 Accused Products act as a content processor to process content or data received over the network, where that content includes a call to a first function that contains an input. This input is sent from the lightweight agent on the endpoint to a security computer that is located on premise or to the security cloud for inspection.




Ex. R (Cb_Endpoint_Threat_Detection_v2.pdf) (emphasis added); Ex. S (https://www.carbonblack.com/wp-content/uploads/2016/02/2016_cb_threat_intel2.pdf).

104. The '154 Accused Products can invoke second functions only if they are determined to be safe after receiving an indication from the on-premise security computer or the cloud security computer.




Ex. U (data-breach-detection-what-you-need-to-know-pdf) (emphasis added).

105. As a result of Defendant's unlawful activities, Finjan has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Finjan and Defendant both compete in the security software space, as described for example in paragraphs 7-8 and 22-34 above. And Finjan is actively engaged in licensing its patent portfolio, as described for example in paragraphs 7-8 and 22-34 above. Defendant's continued infringement of the Asserted Patents causes harm to Finjan in the form of price erosion, loss of goodwill, damage to reputation, loss of business opportunities, inadequacy of money damages, and direct and indirect competition. Monetary damages are insufficient to compensate Finjan for these harms. Accordingly, Finjan is entitled to and seeks a preliminary and/or permanent injunctive relief.

106. Defendant's infringement of the '154 Patent has injured and continues to injure Finjan in an amount to be proven at trial.

107. Defendant has been specifically long-aware of Finjan's patents, including the '154 Patent, and has acted recklessly and egregiously with conduct that is willful, wanton, malicious, bad-faith, deliberate, wrongful, and flagrant by its continued infringing activity despite possessing specific knowledge of its infringement of the '154 Patent. Defendant has had specific knowledge of its infringement of the '494 Patent since at least on or about December 2015, when Finjan specifically identified and described the following products made, used, or sold by Defendant as infringing the

'154 Patent: Bit9 + Carbon Black Solution, the Bit9 Security Platform, and the Bit9 + Carbon Black Threat Intelligence Cloud. Finjan also gave Defendant a claim chart in or about February 2016 specifically describing how the '154 Patent reads on its products.

108. On information and belief, despite its knowledge of the '154 Patent and its knowledge of its own infringement of that patent since at least in or about December 2015, Defendant made no effort to design its products or services around the '154 Patent in order to avoid infringement. Instead, on information and belief, Defendant incorporated infringing technology into additional products, such as those identified in this Complaint. All of these actions demonstrate Defendant's blatant and egregious disregard for, and willful infringement of, Finjan's patent rights.

109. Despite its knowledge of the Asserted Patents and being provided representative claim charts of the Asserted Patents, Defendant has sold and continues to sell the Accused Products and Services in complete and reckless disregard of Finjan's patent rights. As such, Defendant has acted recklessly and continues to willfully, wantonly, and deliberately engage 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.

## PRAYER FOR RELIEF

WHEREFORE, Finjan prays for judgment and relief as follows:

A. An entry of judgment holding that Carbon Black has infringed the '780 Patent, the '844 Patent, the '494 Patent, and the '154 Patent, and is continuing to infringe the '154 Patent; and has induced infringement of the '780 Patent, the '844 Patent, and the '494 Patent;

B. A preliminary and permanent injunction against Carbon Black and its officers, employees, agents, servants, attorneys, instrumentalities, and/or those in privity with them, from continuing to infringe the '154 Patent, and for all further and proper injunctive relief pursuant to 35 U.S.C. § 283;

C. An award to Finjan of such past damages as it shall prove at trial against Carbon Black that are adequate to fully compensate Finjan for Carbon Black's infringement of the '780 Patent, the '844 Patent, the '494 Patent, and the '154 Patent, said damages to be no less than a reasonable

royalty;

D. A determination that Carbon Black's infringement has been willful, wanton, and deliberate and that the damages against it be increased up to treble on this basis or for any other basis in accordance with the law;

E. 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;

F. An accounting of all infringing sales and revenues, together with post judgment interest and prejudgment interest from the first date of infringement of the '780 Patent, the '844 Patent, the '494 Patent, and the '154 Patent; and

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

Respectfully submitted,

Dated: March 21, 2018

By: */s/ Paul J. Andre*

Paul J. Andre (State Bar No. 196585)
Lisa Kobialka (State Bar No. 191404)
James Hannah (State Bar No. 237978)
Austin Manes (State Bar No. 284065)
KRAMER LEVIN NAFTALIS
& FRANKEL LLP
990 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 752-1700
Facsimile: (650) 752-1800
pandre@kramerlevin.com
lkobialka@kramerlevin.com
jhannah@kramerlevin.com
amanes@kramerlevin.com

*Attorneys for Plaintiff*
FINJAN, INC.

**DEMAND FOR JURY TRIAL**

Finjan demands a jury trial on all issues so triable.

Respectfully submitted,

Dated: March 21, 2018

By: */s/ Paul J. Andre*

Paul J. Andre (State Bar No. 196585)
Lisa Kobialka (State Bar No. 191404)
James Hannah (State Bar No. 237978)
Austin Manes (State Bar No. 284065)
KRAMER LEVIN NAFTALIS
& FRANKEL LLP
990 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 752-1700
Facsimile: (650) 752-1800
pandre@kramerlevin.com
lkobialka@kramerlevin.com
jhannah@kramerlevin.com
amanes@kramerlevin.com

*Attorneys for Plaintiff*
FINJAN, INC.