

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF CALIFORNIA

FINJAN, INC.,

Plaintiff,

v.

JUNIPER NETWORK, INC.,

Defendant.

No. C 17-05659 WHA

**ORDER GRANTING IN PART  
EARLY MOTION FOR SUMMARY  
JUDGMENT ON '494 PATENT**

**INTRODUCTION**

In this patent infringement action, each side moves for early summary judgment on one asserted claim among many. For the reasons stated below, patent owner's motion is **GRANTED IN PART.**

**STATEMENT**

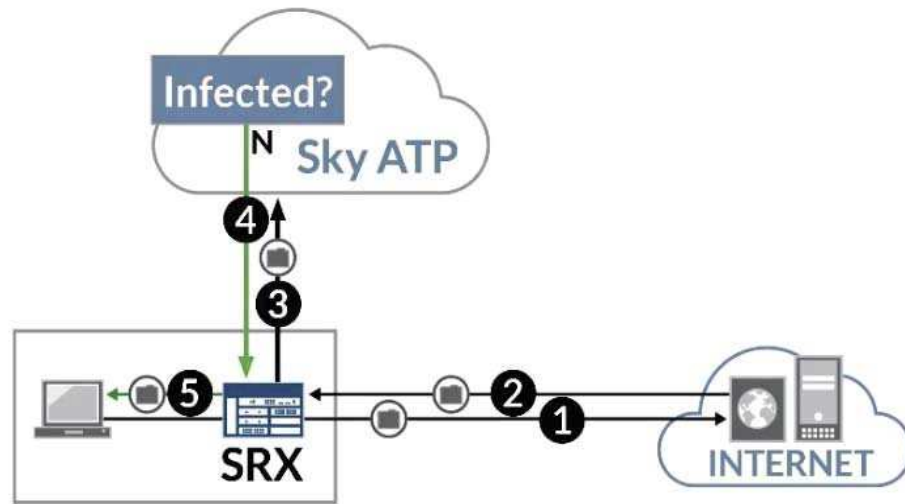
**1. THE '494 PATENT.**

United States Patent No. 8,677,494 ("the '494 patent") relates to malware detection. It is generally directed to systems and methods for protecting devices from suspicious "Downloadables" — "an executable application program, which is downloaded from a source computer and run on the destination computer" (Dkt. No. 126 at 6). These Downloadables may be used to deliver malicious code without the user's knowledge.

Specifically, the '494 patent's claims involve three basic steps: (1) receive a Downloadable; (2) scan the Downloadable to generate security profile data ("Downloadable

1 Security Profile (DSP) data”), which includes a list of suspicious computer operations that  
2 the Downloadable may attempt to perform; and (3) store the security profile in a database  
3 (’494 patent 21:20–25, 22:8–16).

4 **2. OVERVIEW OF ACCUSED PRODUCTS.**



16 **A. SRX Gateways.**

17 Juniper’s SRX Gateways are network appliances and software that act as firewalls to  
18 protect a computer on a network from receiving malicious content. Once the SRX intercepts an  
19 incoming file, it determines whether it is a Downloadable type that should be analyzed (such as  
20 HTML, Microsoft documents, EXE files). If so, it then sends the entire file to the cloud-based  
21 Sky ATP for analysis.

22 **B. Sky ATP.**

23 Sky ATP is a cloud-based scanning system that inspects files with its “Malware  
24 Analysis Pipeline” to determine the threat level posed by the Downloadable. The Malware  
25 Analysis Pipeline in Sky ATP scans an unrecognized Downloadable using (1) a conventional  
26 antivirus check; (2) static analysis; and (3) dynamic analysis. Static analysis involves analyzing  
27 the Downloadable’s contents without actually running the file. Dynamic analysis, on the other  
28 hand, analyzes the Downloadable’s contents by executing and observing the file in a safe,

1 simulated environment called a “sandbox.” This multi-stage pipeline analysis renders a  
2 “verdict,” *i.e.* how dangerous the file is, which is returned to the SRX the next time it  
3 encounters the Downloadable.

4 **3. FINJAN’S MOTION ON CLAIM 10 OF THE ’494 PATENT.**

5 According to Finjan, Juniper infringes Claim 10 of the ’494 patent because the accused  
6 products “receive Downloadables from servers on the Internet, scan these Downloadables using  
7 dynamic and static analysis to generate a behavioral profile, and store the resulting behavioral  
8 profile in a results database” (Dkt. No. 98 at 2).

9 Finjan now moves for summary judgment of direct infringement of Claim 10 based on  
10 (1) Juniper’s SRX Gateways used in combination with Sky ATP; and (2) Sky ATP alone (Dkt.  
11 No. 98 at 1). Juniper opposes on three grounds: (1) non-infringement; (2) invalidity based on  
12 unpatentable subject matter and indefiniteness; and (3) Finjan’s failure to mark (Dkt. No. 126  
13 at 1–2). Discovery relating to this round of early summary judgment informed both sides how  
14 the accused system works. This order follows full briefing and oral argument.

15 **ANALYSIS**

16 **1. LEGAL STANDARD.**

17 Summary judgment is proper when there is no genuine dispute of material fact and the  
18 moving party is entitled to judgment as a matter of law. FRCP 56(a). A genuine dispute of  
19 material fact is one that “might affect the outcome of the suit under the governing law.”  
20 *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 247–48 (1986). In deciding a motion for  
21 summary judgment, we must accept the non-movant’s non-conclusory evidence and draw all  
22 justifiable inferences in its favor. *Id.* at 255.

1           **2.        INFRINGEMENT (OR NON-INFRINGEMENT).**

2           Claim 10 states ('494 patent at 22:7–16) (emphasis added):

3           A system for managing Downloadables, comprising:

4                     a receiver for receiving an incoming Downloadable;

5                     a Downloadable *scanner* coupled with said receiver, for deriving  
6                     security profile data for the Downloadable, including a *list of*  
7                     *suspicious computer operations* that may be attempted by the  
8                     Downloadable; and

9                     a *database manager* coupled with said Downloadable scanner, for  
10                     storing the Downloadable security profile data in a database.

11           To prove infringement, Finjan must show that Juniper's accused products meet each  
12           properly construed limitation of Claim 10 either literally or under the doctrine of equivalents.

13           *See Deering Precision Instruments, LLC v. Vector Distribution Sys., Inc.*, 347 F.3d 1314, 1324  
14           (Fed. Cir. 2003). To establish literal infringement, all of the elements of the claim, as correctly  
15           construed, must be present in the accused products. *TechSearch, LLC v. Intel Corp.*, 286 F.3d  
16           1360, 1371 (Fed. Cir. 2002). Finjan may also establish infringement under the doctrine of  
17           equivalents by "showing that the difference between the claimed invention and the accused  
18           product [is] insubstantial," including "by showing on a limitation by limitation basis that the  
19           accused product performs substantially the same function in substantially the same way with  
20           substantially the same result as each claim limitation of the patented product." *Crown*  
21           *Packaging Tech., Inc. v. Rexam Beverage Can Co.*, 559 F.3d 1308, 1312 (Fed. Cir. 2009).

22           To determine whether summary judgment of non-infringement (or infringement) is  
23           warranted, this order will first construe Claim 10 to determine its scope and then determine  
24           whether the properly construed Claim 10 reads on Juniper's accused products. *See Pitney*  
25           *Bowes, Inc. v. Hewlett-Packard Co.*, 182 F.3d 1298, 1304 (Fed. Cir. 1999).

26           Claim terms "are generally given their ordinary and customary meaning," *i.e.*, "the  
27           meaning that the term would have to a person of ordinary skill in the art in question at the  
28           time of the invention." *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–13 (Fed. Cir. 2005).  
Claim construction examines the claim language itself, the specification, and, if in evidence,  
the prosecution history. *Amgen Inc. v. Hoechst Marion Roussel, Inc.*, 314 F.3d 1313, 1324

1 (Fed. Cir. 2003). When legal “experts” offer views on claim construction that conflict with each  
2 other or with the patent itself, such conflict does not create a question of fact or relieve the court  
3 of its obligation to construe the claim according to the tenor of the patent. *Markman v. Westview*  
4 *Instruments, Inc.*, 52 F.3d 967, 983 (Fed. Cir. 1995).

5 Here, the parties dispute the following terms: (1) “list of suspicious computer  
6 operations”; (2) “suspicious computer operations”; (3) “scanner”; (4) and “database manager.”  
7 This order will construe these terms in deciding the issue of infringement.

8 **A. “List of Suspicious Computer Operations.”**

9 This order construes the limitation “list of suspicious computer operations” as “list of  
10 computer operations in a received Downloadable that are deemed hostile or potentially hostile.”

11 Significantly, the ’494 patent is a continuation of United States patent application Serial  
12 No. 08/964,388, now United States Patent No. 6,092,194 (the ’194 patent), entitled “System and  
13 Method for Protecting a Computer and a Network from Hostile Downloadables.” The later  
14 ’494 patent incorporated the ’194 patent by reference. The ’494 patent’s specification itself  
15 provides no clarity as to the limitations at issue, so this order will look to the earlier ’194 patent’s  
16 specification for guidance.

17 The ’194 patent uses, perhaps confusingly, the term “list” in multiple ways, two of which  
18 concern the dispute over the term “list of suspicious computer operations.” For our immediate  
19 purposes, we must distinguish between a pre-existing master list of suspicious computer  
20 operations versus a shorter list of suspicious computer operations freshly derived from a specific  
21 Downloadable. This duality of usage within the specification has allowed each side to construe  
22 the list in Claim 10 in two different ways. This order, however, holds that the list of suspicious  
23 computer operations referenced in Claim 10 is one derived from the specific Downloadable  
24 under scrutiny.<sup>1</sup>

---

25  
26  
27 <sup>1</sup> The ’194 patent specification further refers to two more lists — “a list of all files to be accessed by  
28 the Downloadable code” and an “access control list” (’194 patent at 5:53–54, 6:21) — but these lists do not  
contribute to the problem at hand.

1 Let's start with the pre-existing master list. As between the two patents, only the '194  
2 patent discloses any embodiment for deriving security profile data. That embodiment is found in  
3 a description of Figure 7, which illustrates the process for decomposing a Downloadable to  
4 derive DSP data ('194 patent at 9:24–29) (emphasis added):

5 The code scanner . . . resolves a respective command in the machine  
6 code, and in step 715 determines whether the resolved command is  
7 suspicious (e.g., *whether the command is one of the operations*  
8 *identified in the list described above with reference to [Figure] 3). . . .*  
9 [I]f the code scanner in step 715 determines that the resolved command  
10 is suspect, then the code scanner 325 in step 720 decodes and registers  
11 the suspicious command . . . as DSP data.

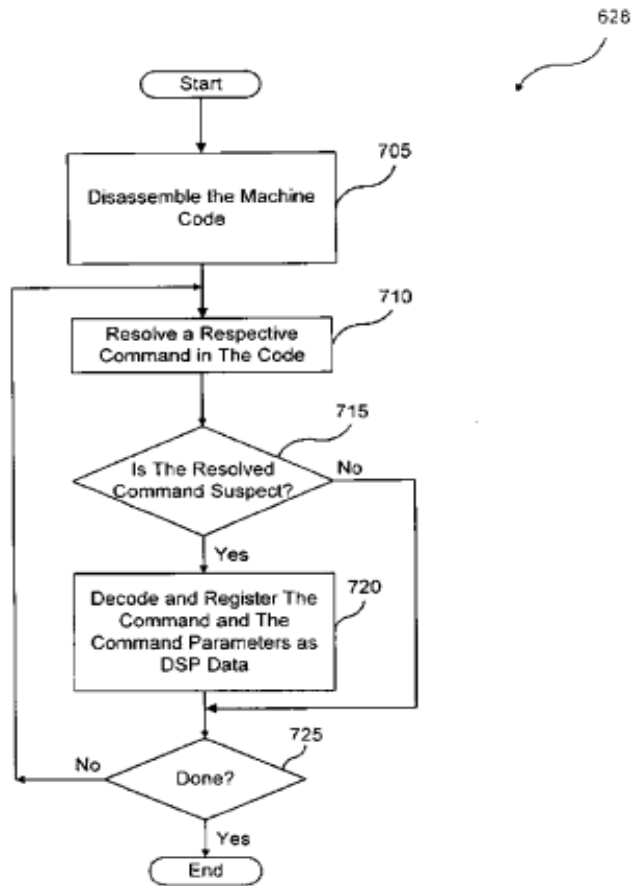


FIG. 7

22 In essence, as described in Figure 7, the code scanner (1) “disassemble[s] the machine  
23 code of the Downloadable”; (2) “resolves a respective command in the machine code;” and  
24 (3) “determines whether the resolved command is suspicious” ('194 patent at 9:20–29). If the  
25  
26  
27  
28

1 resolved command is determined to be suspicious, then the code scanner (4) “decodes and  
2 registers the suspicious command . . . as DSP data” (*id.* at 9:34–37).

3 In turn, a description of Figure 3 (which Figure 7 references) also includes the following  
4 example master list (*id.* at 5:58–6:4):

5 An Example List of Operations Deemed Potentially Hostile  
6 File operations: READ a file, WRITE a file;  
7 Network operations: LISTEN on a socket, CONNECT to  
8 a socket, SEND data, RECEIVE data, VIEW  
9 INTRANET;  
10 Registry operations: READ a registry item, WRITE a  
11 registry item;  
12 Operating system operations: EXIT WINDOWS, EXIT  
13 BROWSER, START PROCESS/THREAD, KILL A  
14 PROCESS/THREAD, CHANGE PROCESS/  
15 THREAD PRIORITY, DYNAMICALLY LOAD A  
16 CLASS/ LIBRARY, etc.; and  
17 Resource usage thresholds; memory, CPU, graphics, etc.

18 Specifically, a code scanner may identify a computer operation as suspicious by  
19 checking whether it is on the master “list described above with reference to [Figure] 3” —  
20 which most conceivably refers to the disclosed “Example List of Operations Deemed  
21 Potentially Hostile.”

22 The adjective “master” is the Court’s own word choice, not the specification’s, but it  
23 captures the function served by the passages just quoted.

24 The second list referenced in the specification is the shorter list compiled of suspicious  
25 operations derived only from a received Downloadable. In the preferred embodiment, that list  
26 is generated by comparing the operations in the Downloadable to the master list of suspicious  
27 operations. When there is a match, that specific operation goes on the second list.

28 The description of Figure 3 — which Figure 7 references in connection with  
determining whether a command within a Downloadable is suspicious — further includes the  
following embodiment (’194 patent at 5:50–54):

The code scanner 325 may generate the DSP data 310 as a list of  
all operations in the Downloadable code which could ever be  
deemed potentially hostile and a list of all files to be accessed by  
the Downloadable code.

1 For example, if the master list contains 200 commands, all predetermined as suspicious,  
2 the commands in the received Downloadable code would then be checked against this master  
3 list, resulting in a second list specific to the Downloadable based on the matched hits of, say,  
4 twenty commands.

5 With at least two different “lists” in play in the specification, the question is then,  
6 *which* list does Claim 10 refer to? Reading the claim language and specification together as a  
7 whole, the claimed “list of suspicious computer operations” in Claim 10 refers to a list of  
8 computer operations found *in the received Downloadable code* that have been culled out as  
9 suspicious.

10 *First*, the Claim 10 language itself indicates a list derived for a specific Downloadable,  
11 *not* a pre-existing list. This is apparent when the limitation is read in the claim’s context —  
12 “deriving security profile data *for the Downloadable*, including a list of suspicious computer  
13 operations that may be attempted *by the Downloadable*.” The context of this language  
14 indicates that the list referenced in Claim 10 is tied to operations found within the  
15 Downloadable code. This reading is further supported by the term’s parallel usage in Claim 1,  
16 which more clearly indicates that the “list of suspicious computer operations” is part of the  
17 security profile data derived specifically for a received Downloadable (*see* ’494 patent at  
18 21:20–23).

19 *Second*, the specification supports this construction. For example, the Downloadable  
20 security profile data, which includes the list at issue, is derived specifically for a received  
21 Downloadable. The specification says that the Downloadable’s derived security profile data  
22 can then be compared against “the access control list” (yet another list), which “contains  
23 criteria indicating whether to pass or fail the Downloadable” (’194 patent at 6:13–23).  
24 While this important pass-fail step is not itself recited or reached in Claim 10, it illustrates  
25 that the “list of suspicious computer operations” within the Downloadable security profile data  
26 is necessarily limited to a specific Downloadable, not the pre-existing master list; otherwise,  
27 comparison with the access control list would be pointless. Moreover, the specification  
28 discloses that “the present invention may identify Downloadables that perform *operations*



1 *deemed suspicious*” and that it “may examine the Downloadable code to determine whether the  
2 code contains any suspicious operations, and thus may allow or block the Downloadable  
3 accordingly” (*id.* at 2:32–37).

4 This order therefore mostly agrees with Finjan on this limitation, as the purpose of the  
5 Downloadable security profile data is to look at code within a received Downloadable and  
6 compile a list tailored to that file (*see* Tr. 99:6–9). It therefore rejects Juniper’s assertion that  
7 Claim 10 includes *both* the pre-existing master list and the subset list of suspicious operations  
8 found in a Downloadable code (Tr. 100:19–102:4). In so arguing, Juniper embraces a  
9 construction of this limitation by a panel of the PTAB — “a list of all operations that could  
10 ever be deemed potentially hostile” — in *Symantec Corporation & Blue Coat Systems LLC v.*  
11 *Finjan, Inc.*, IPR2015–01892, Paper No. 58 at 12 (P.T.A.B. Mar. 15, 2017) (Dkt. No. 126 at  
12 11). The same PTAB panel affirmed this construction in *Palo Alto Networks, Inc. & Blue*  
13 *Coat Systems LLC v. Finjan, Inc.*, IPR2016–00159, Paper No. 50 at 33–35 (P.T.A.B. Apr. 11,  
14 2017). The panel based its construction on the aforementioned embodiment in the ’194 patent  
15 included in the following description of Figure 3, “list of all operations in the Downloadable  
16 code which could ever be deemed potentially hostile” (’194 patent at 9:24–29). This  
17 construction, however, remains dictum, as the Board’s decision did not ultimately turn on its  
18 adopted construction. *See Symantec*, IPR2015–01892 Paper No. 58 at 12. Anyway, this order  
19 disagrees with the panel’s construction.

20 Using ellipses, Juniper justifies the panel’s dictum by quoting “all operations . . . which  
21 could ever be deemed potentially hostile” from the aforementioned embodiment, this to assert  
22 that the claimed list must refer to a pre-existing master list. This, however, is a sleight of hand.  
23 Counsel’s ellipses delete crucial limiting language, namely “in the Downloadable code,”  
24 *i.e.*, the ’194 patent actually says “a list of all operations *in the Downloadable code* which  
25 could ever be deemed potentially hostile.” Once this language is read in full without ellipses,  
26 the list refers to what is found within the four corners of the received Downloadable code.  
27 This cannot refer to the master list. The Court is disappointed that Juniper’s counsel would use  
28 this sleight of hand. Once read in light of its true scope, this embodiment is fully consistent

1 with this order’s adopted construction. Nor would it necessarily violate, as Juniper argues, the  
2 principle that “a claim interpretation that excludes a preferred embodiment from the scope of  
3 the claim is rarely, if ever, correct.” *Accent Packaging, Inc. v. Leggett & Platt, Inc.*, 707 F.3d  
4 1318, 1326 (Fed. Cir. 2013) (quoting *On-Line Techs., Inc. v. Bodenseewerk Perkin-Elmer*  
5 *GmbH*, 386 F.3d 1133, 1138 (Fed. Cir. 2004)).

6 This order finds that there is no genuine dispute that Juniper’s accused products meet  
7 this limitation. The accused system’s pre-existing master list, Juniper says, does not flag *all*  
8 operations that have been known to be suspicious or potentially hostile, including the example  
9 operation “CHANGE PROCESS/THREAD PRIORITY” given in the patent (Tr.  
10 101:22–105:4; Dkt. No. 126 at 24–25). But as discussed above, the ’494 patent does not claim  
11 the pre-existing list — it only claims the list of computer operations within a specific  
12 Downloadable deemed hostile or potentially hostile. Juniper’s Malware Analysis Pipeline  
13 *does* compile a list of operations within a received Downloadable identified as hostile or  
14 potentially hostile (Dkt. No. 98, Exh. 11; Cole Decl. ¶¶ 34–37, 41). Juniper offers no evidence  
15 (under this order’s construction) to the contrary.

16 Juniper’s proposed construction would impose a seemingly impossible standard to  
17 meet. Juniper’s proposed “list of *all operations* which *could ever* be deemed potentially  
18 hostile” would require a list of every operation (not just in the received Downloadable but in  
19 every possible Downloadable) that has been and could ever be used in a potentially hostile  
20 manner. As Juniper would have it, this list would have to be universally exhaustive and thus  
21 impossible to meet, for the imagination of hackers never sleeps in devising new ways to cheat.<sup>2</sup>

### 22 B. “Suspicious Computer Operations.”

23 This order next rejects Juniper’s contention that the term “suspicious” in this context is  
24 indefinite. “[A] patent is invalid for indefiniteness if its claims, read in light of the  
25 specification delineating the patent, and the prosecution history, fail to inform, with reasonable  
26 certainty, those skilled in the art about the scope of the invention.” *Nautilus, Inc. v. Biosig*

---

27  
28 <sup>2</sup> For added clarity, this order therefore adopts Finjan’s proposed construction with this modification,  
*i.e.*, “list of computer operations *in a received Downloadable* that are deemed hostile or potentially hostile.”

1 *Instruments, Inc.*, 134 S. Ct. 2120, 2124 (2014). “Indefiniteness must be proven by clear and  
2 convincing evidence.” *Sonix Tech. Co., Ltd. v. Publications Int’l, Ltd.*, 844 F.3d 1370, 1377  
3 (Fed. Cir. 2017). Here, Juniper fails to show by clear and convincing evidence that  
4 determining whether or not a computer operation is “suspicious” is subjective and thus  
5 inherently certain.

6 At issue here are essentially two distinct steps at which a computer operation is  
7 “deemed” suspicious. First, a human (say, a cyber security engineer) decides which computer  
8 operations, known to be capable of performing in a hostile manner (such as a WRITE  
9 command), to put on the pre-existing master list. This step necessarily requires that the human  
10 deem — this is the subjective part — an operation suspicious. Second, the patented system  
11 deems (or not) a computer operation in a received Downloadable code suspicious by checking  
12 it against the master list. If it’s on the master list, too bad — it’s suspicious. If it’s not, great,  
13 it’s not suspicious.

14 Once a human composes the master list, the subjective part is over. That part is *not*  
15 covered by the patent. All that is covered is the comparison. This is objective because the  
16 operation is either on the master list or not.

17 Juniper contends that the term “suspicious” is inherently subjective because “there is no  
18 standard or commonly accepted list of ‘suspicious’ computer operations” and that it requires a  
19 subjective determination (Dkt. No. 126 at 9–10). It further points to Finjan’s statement in the  
20 *Symantec* IPR proceeding that “there is no *a priori* understanding of what constitutes a  
21 ‘suspicious computer operation.’ ” See *Symantec*, IPR2015–01892 Paper No. 58 at 9. Juniper  
22 (and Finjan) is right in arguing that there is no *a priori* understanding of “suspicious,” as the  
23 patent itself describes legitimate operations such as WRITE commands as “potentially hostile”  
24 (Dkt. No. 126 at 9–10; ’194 patent at 5:59).

25 But this allegedly subjective inquiry happens in the *first* step as the master list is being  
26 compiled. That this initial determination by a human that an operation is suspicious may be an  
27 inherently subjective exercise, as argued by Juniper, is irrelevant to the definiteness of Claim  
28 10. That step, important as it may be, is not part of the claimed invention.

1           Again, what is claimed is the *objective* second step, where an operation found in an  
2 incoming Downloadable is deemed suspicious because that operation had been included in the  
3 master list (*see* '194 patent at 5:59). As such, Juniper's reliance on *Interval Licensing LLC v.*  
4 *AOL, Inc.*, 766 F.3d 1364, 1371–74 (Fed. Cir. 2014), *Datamize, LLC v. Plumtree Software,*  
5 *Inc.*, 417 F.3d 1342 (Fed. Cir. 2005), and *International Test Solutions, Inc. v. Mipox*  
6 *International Corporation*, No. C 16–00791 RS, 2017 WL 1367975, at \*4 (N.D. Cal. Apr. 10,  
7 2017) (Judge Richard Seeborg), is unavailing. Those decisions involved “facially subjective”  
8 limitations that “provide[d] little guidance” on its own (“unobtrusive manner” in *Interval*  
9 *Licensing*, 766 F.3d at 1371–74 ) or were “completely dependent on a person’s subjective  
10 opinion” (“aesthetically pleasing” in *Datamize*, 417 F.3d at 1350).

11           Here, on the other hand, “suspicious” as claimed and described in the specification is  
12 sufficiently definite such that a person of ordinary skill in the art can apply the claim language  
13 with reasonable certainty. *Nautilus*, 134 S. Ct. at 2124. As Finjan points out, a person of  
14 ordinary skill in the art “would be able to apply the claim language” by observing whether an  
15 accused system uses a pre-existing master list of computer operations “deemed hostile or  
16 potentially hostile to create a Downloadable security profile that includes a list of operations  
17 that were deemed suspicious according to the rules of the system” (Dkt. No. 184 at 5–6).  
18 Accordingly this order finds that Juniper fails to show by clear and convincing evidence that  
19 this limitation is indefinite.

20           Note well that in saving this claim from indefiniteness by excluding the master list from  
21 the invention, Finjan has made the claim even more abstract than before — a problem we will  
22 address below.

23           **C. “Scanner.”**

24           Based on the claim language and specification of the '494 and '194 patents, this order  
25 mostly agrees with Finjan and therefore adopts its proposed construction, with modification.  
26  
27  
28

1 This order construes “scanner” as “software that searches code to identify suspicious patterns  
2 or suspicious computer operations.”<sup>3</sup>

3 The Claim 10 language and the ’194 patent’s specification describe the role of the  
4 “code scanner” as deriving or resolving the Downloadable Security Profile data of a received  
5 Downloadable (’494 patent at 22:9–10; ’194 patent at 5:41–42). The ’194 patent specification  
6 further explains that the code scanner “determines whether the resolved command is  
7 suspicious” and “may search the code for any pattern, which is undesirable or suggests that the  
8 code was written by a hacker” (194 patent at 5:54–57; 9:24–26). The specification thus  
9 supports this order’s construction of Claim 10’s scanner as software searching code to identify  
10 suspicious patterns or suspicious computer operations, whether static or dynamic.

11 This order rejects Juniper’s attempt to construe this limitation as “a static analyzer that  
12 uses parsing techniques to decompose the code.” Juniper concentrates its fire on an  
13 embodiment in the ’194 specification, which describes a “code scanner” that “uses  
14 *conventional parsing techniques to decompose the code . . .* of the Downloadable into the DSP  
15 data” (’194 patent at 5:42–45) (emphasis added). “While claims are to be interpreted in light  
16 of the specification . . . it does not follow that limitations from the specification may be read  
17 into the claims.” *Comark Comm’ns, Inc. v. Harris Corp.*, 156 F.3d 1182, 1186 (Fed. Cir.  
18 1998). Further, courts are “cautioned against limiting the claimed invention to preferred  
19 embodiments or specific examples in the specification.” *Texas Instruments, Inc. v. United*  
20 *States Int’l Trade Comm’n*, 805 F.2d 1558, 1563 (Fed. Cir. 1986). In fact, the ’194 patent  
21 elsewhere describes other embodiments of the code scanner, such as “disassembling machine  
22 code” (194 patent at 9:23–24), which renders Juniper’s construction too narrow.

23 Juniper points to Finjan’s arguments in *Symantec Corporation v. Finjan, Inc.*,  
24 IPR2015–01892, Paper 27 at 29 (P.T.A.B. June 21, 2016) (Patent Owner Response) to set up a

---

26 <sup>3</sup> Finjan requests judicial notice of *Finjan, Inc. v. Cisco Systems, Inc.*, No. C 17–00072 BLF, 2018 WL  
27 3537142 (N.D. Cal. July 23, 2018), where Judge Beth Freeman (who presided over the *Blue Coat*, 2015 WL  
28 363000 decision both parties rely on) construed the same limitation. A court may judicially notice a fact that is  
not subject to reasonable dispute because it “can be accurately and readily determined from sources whose  
accuracy cannot reasonably be questioned.” FRE 201(b). Accordingly, Finjan’s request for judicial notice is  
**GRANTED.**

1 disclaimer. To distinguish an earlier particular reference, which had described dynamic  
2 analysis, Finjan argued that the reference taught against the use of scanners (Dkt. No. 126 at 8,  
3 Exh. 12 at 29). By implication, Juniper asserts Finjan conceded that anything using dynamic  
4 analysis cannot be a scanner within the meaning of Claim 10. That is, Juniper posits, Finjan  
5 disclaimed the use of a dynamic analyzer as the claimed scanner. This chain of inferences,  
6 however, is insufficient to establish disclaimer by Finjan. Even recognizing that “applicants  
7 rarely submit affirmative disclaimers,” a prosecution disclaimer still requires “clear and  
8 unambiguous disavowal of claim scope.” *Saffran v. Johnson & Johnson*, 712 F.3d 549, 559  
9 (Fed. Cir. 2013) (citations omitted). The prior statement in question made by Finjan did not  
10 purport to limit the claim language itself, but rather purported to explain away a prior art  
11 reference. Even if we held Finjan to its statement that the reference taught against use of  
12 scanners, and even if the reference did use “dynamic analysis,” Juniper cites no Federal Circuit  
13 authority holding that a patent owner’s statement that a reference taught away from a claim  
14 limitation rises to the level of disclaimer as to claim scope. Therefore, given that the standard  
15 for finding a disclaimer is “demanding,” this order is unwilling to hold that “scanner” excludes  
16 dynamic analysis. *Avid Tech., Inc. v. Harmonic, Inc.*, 812 F.3d 1040, 1045 (Fed. Cir. 2016).

17 Under the adopted construction of “scanner,” *i.e.* “software that searches code to  
18 identify suspicious patterns or suspicious computer operations,” this order finds that Juniper’s  
19 accused products meet this limitation. Finjan argues that Juniper’s SRX Gateways with Sky  
20 ATP, and Sky ATP alone — which includes the Malware Analysis Pipeline involving both  
21 static and dynamic analyzers — constitute a Downloadable “scanner” (Dkt. No. 98 at 20).  
22 The evidence shows that the Malware Analysis Pipeline indeed generates a threat level  
23 “verdict” by searching a received Downloadable’s code to identify suspicious operations or  
24 patterns (Cole Decl. ¶ 35; Dkt. No. 154, Exh. 5 at 121:11-22). Juniper does not dispute that it  
25 meets this limitation under this order’s construction and thus does not point to any evidence in  
26 the record to the contrary. Accordingly, this order finds that Juniper’s accused products meet  
27 this limitation.  
28

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**D. “Database Manager.”**

This order adopts Juniper’s proposed construction, “a program or programs that control a database so that the information it contains can be stored, retrieved, updated and sorted,” which comes verbatim from Finjan’s own explanation of this limitation in a former IPR proceeding.

Specifically, Juniper’s proposed construction comes from Finjan itself in *Palo Alto Networks, Inc. & Blue Coat Systems LLC v. Finjan, Inc.*, IPR2016–00159, Paper No. 50 at 49 (P.T.A.B. Apr. 11, 2017). To overcome prior art, Finjan explicitly stated that a person of ordinary skill in the art “would ‘understand[] the term “database manager” to mean “a program or programs that control a database so that the information it contains can be stored, retrieved, updated and sorted.’ ” *Id.* at 49 (alteration in original) (citing Patent Owner’s Response, Paper 17 at 43–44 (Aug. 12, 2016)). Now Finjan tries to walk back its previous statements, asserting that the plain and ordinary meaning already includes Juniper’s interpretation such that Juniper’s proposed construction adds unnecessary limitations. This order finds, however, that Finjan’s statement in the IPR proceeding amounted to a clear and unmistakable disavowal of claim scope. *Saffran*, 712 F.3d at 559. Finjan itself defined this limitation in order to avoid invalidation and is now stuck with it.

Nevertheless, there is no genuine dispute that the accused system meets this limitation. Sky ATP stores results in three different storage solutions provided by Amazon: (1) DynamoDB, (2) S3, and (3) MySQL (Dkt. No. 126 at 26). ResultsDB management is an interface overlaying these three storage components. Juniper contends that its ResultsDB management does not constitute a “database manager.” Rather, it asserts, *Amazon*, which runs the underlying storage components (*i.e.*, DynamoDB, S3, and MySQL), acts as the “database manager” and controls its own storage products (Dkt. No. 126 at 32; Rubin ¶ 84). And, because ResultsDB is merely an interface, Juniper argues, it cannot *directly* sort data contained within DynamoDB or S3 and thus does not meet the proper construction.

This order disagrees. *First*, Juniper’s assertion that ResultsDB is “just an interface” and that Amazon controls its databases is belied by its expert, who testified that ResultsDB

1 indeed makes the determination of whether a result is stored in DynamoDB or S3 (Dkt. No.  
2 154, Exh. 5 at 140:4–20). *Second*, Juniper’s attempt to require that a database manager sort  
3 data *directly* within a database is unpersuasive, at least on this record. The construction “a  
4 program or programs that control a database so that the information it contains can be . . .  
5 sorted” simply requires that the database manager have the capability to sort the information  
6 contained within a database; it does not indicate *where* that information must be sorted. Here,  
7 Juniper admits that “ResultsDB can retrieve data from DynamoDB or S3 *and then* sort the data  
8 that was retrieved” (Dkt. No. 126 at 32) (emphasis in original). That “the data actually stored  
9 in DynamoDB or S3 remains as is” is irrelevant for the purposes of this construction (*see*  
10 *ibid.*). This order therefore finds that ResultsDB meets this limitation.

#### 11 E. “Database.”

12 Both parties agree to construe “database” as “a collection of interrelated data organized  
13 according to a database schema to serve one or more applications” (Dkt. No. 126 at 6).  
14 Unfortunately, this “stipulation” has led to satellite litigation over its meaning, so the  
15 stipulation has done no good.

16 Finjan points to Juniper’s ResultsDB, which allegedly refer “both to the software  
17 components of Sky ATP that manage the results” and the “underlying databases that physically  
18 store the results for future use” (Dkt. No. 98 at 21, Exh. 11; Cole Decl. ¶¶ 57–61). This, Finjan  
19 argues, is the “database” where results of the Malware Analysis Pipeline are stored. Juniper  
20 responds that ResultsDB is simply an interface to the three underlying databases and is thus not  
21 a true database itself (Dkt. No. 126 at 27, Exh. 3 at 56:25–57:8; 55:13–25). The parties further  
22 dispute whether ResultsDB or DynamoDB are organized according to a “database schema”  
23 (Dkt. Nos. 97-30, 126 at 27–28; Rubin Decl. ¶¶ 61–66; Cole Decl. ¶¶ 64, 66), and whether the  
24 three storage components are “interrelated” (Dkt. Nos. 98 at 22, 126 at 29–30; Cole Decl. ¶ 59  
25 Rubin Decl. ¶ 68). The parties also dispute whether ResultsDB functions as a database under  
26 the doctrine of equivalents.

27 The Court has tried hard to understand the record submitted as to whether the accused  
28 system includes a “database” within the meaning of Claim 10. Factual disputes regarding



1 whether ResultsDB constitutes a “database” — either literally or under the doctrine of  
2 equivalents — while thin, preclude a determination one way or the other on the record  
3 provided with the degree of certainty required for summary judgment, particularly when  
4 viewing the record in light most favorable to Juniper. This issue will have to be tried to a jury.  
5 The Court will postpone any further claim construction on this limitation until the jury is  
6 instructed so that the Court will have the benefit of the trial record before construing the term.

7 **F. Deriving Downloadable Security Profile**  
8 **Before Storing.**

9 This order generally agrees with Juniper that Claim 10 includes a timing requirement,  
10 *i.e.*, the list of suspicious computer operations cannot be simultaneously derived and stored in a  
11 database. It disagrees, however, with Juniper’s interpretation of this timing requirement.

12 In IPR2015–01892, Finjan distinguished from prior art by asserting that the ’494 patent  
13 required “storing the [Downloadable security profile] data in a database” to be construed  
14 such that it is clear “the [Downloadable security profile] data is only placed in the database  
15 upon derivation of the profile, including the list of suspicious computer operations” (Dkt. No.  
16 126, Exh. 12 at 16). “Deriving” and “storing” the Downloadable security profile data therefore  
17 are separate steps.

18 Juniper contends Sky ATP does not meet the claim element “a database manager  
19 coupled with said Downloadable scanner, for storing the Downloadable security profile data in  
20 a database” because it stores the Downloadable security profile data *before* the alleged list of  
21 suspicious computer operations is derived (Dkt. No. 126 at 33). Specifically, Juniper contends  
22 it does not infringe because results from the Malware Pipeline Manager’s multiple analysis  
23 engines (the static and dynamic analyzers) — each of which separately analyze files — are  
24 stored at different times, depending on when the engine finishes its analysis (and thus the  
25 Downloadable security profile data is built up iteratively) (Dkt. No. 126 at 33–34; Rubin  
26 ¶¶ 91–93). This order disagrees. The claim language and Finjan’s argument in the IPR  
27 proceeding do not require that the Downloadable security profile data, including the list of  
28 suspicious computer operations, be fully derived before they are stored in a database. In other

1 words, Claim 10 does not require the *entire* Downloadable security profile be derived before  
2 any security profile data (*e.g.* a suspicious compute operation) is stored in a database.

3 **3. VALIDITY (OR INVALIDITY).**

4 Juniper argues that Claim 10 is invalid under Section 101 for failing to meet the  
5 two-part *Alice* test. Under well-established Supreme Court precedent, laws of nature, natural  
6 phenomena, and abstract ideas remain patent-ineligible under Section 101. *See, e.g., Ass’n*  
7 *for Molecular Pathology v. Myriad Genetics, Inc.*, 569 U.S. 576, 589 (2013) (citations and  
8 quotations omitted). The Supreme Court has set forth a two-step “framework for  
9 distinguishing patents that claim laws of nature, natural phenomena, and abstract ideas from  
10 those that claim patent-eligible applications of those concepts.” Under this framework, a court  
11 must first “determine whether the claims at issue are directed to one of those patent-ineligible  
12 concepts.” If so, then the court must further “consider the elements of each claim both  
13 individually and ‘as an ordered combination’ to determine whether the additional elements  
14 ‘transform the nature of the claim’ into a patent-eligible application.” *Alice Corp. Pty. Ltd. v.*  
15 *CLS Bank Int’l*, 134 S. Ct. 2347, 2355 (2014) (quoting *Mayo Collaborative Servs. v.*  
16 *Prometheus Labs., Inc.*, 566 U.S. 66 (2012)).

17 **A. Alice Step One.**

18 At step one, courts must first examine the “patent’s ‘claimed advance’ to determine  
19 whether the claims are directed to an abstract idea.” *Finjan, Inc. v. Blue Coat Systems, Inc.*,  
20 879 F.3d 1299, 1303 (Fed. Cir. 2018). “[T]he first step in the *Alice* inquiry . . . asks whether  
21 the focus of the claims is on the specific asserted improvement in computer capabilities . . . or,  
22 instead, on a process that qualifies as an ‘abstract idea’ for which computers are invoked  
23 merely as a tool.” *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1335–36 (Fed. Cir. 2016).

24 This order agrees with Juniper that Claim 10 of the ’494 patent is directed to an abstract  
25 idea. It broadly claims the fundamental practice of collecting data, analyzing data, and storing  
26 results, a concept that is inherently needed for virtually any variation of data analysis, storage,  
27 and retrieval. *See Intellectual Ventures I LLC v. Symantec Corp.*, 838 F.3d 1307, 1318 (Fed.  
28 Cir. 2016) (citing *Alice*, 134 S.Ct. at 2356).

1           *Finjan, Inc. v. Blue Coat Systems, Inc.*, 879 F.3d 1299 (Fed. Cir. 2018), is  
2 distinguishable. There, the United States Court of Appeals for the Federal Circuit held the  
3 United States Patent No. 6,154,844 (the '844 patent) patent eligible under step one due to the  
4 patent's "behavior-based" approach to virus scanning. *Id.* at 1304. Representative Claim 1 of  
5 the '844 patent "scans a downloadable and attaches the virus scan results to the downloadable  
6 in the form of a newly generated file: a 'security profile that identifies suspicious code in the  
7 received Downloadable.'" *Ibid.* The appellate court held that this "behavior-based" virus  
8 scan that analyzed a downloadable's code was a non-abstract improvement on traditional,  
9 "code-matching" virus scans, which "simply look for the presence of known viruses."

10           Here, on the other hand, the '494 patent has a different focus. Claim 10 does not recite  
11 "a new kind of file," *i.e.* a security profile, "that enables a computer security system to do  
12 things it could not do before." *See Blue Coat*, 879 F.3d at 1305. Rather, Claim 10 recites  
13 deriving "security profile *data*." Ultimately, the thrust of Claim 10 is on analyzing a file and  
14 extracting information — which, once washed of its technological context, is merely an  
15 abstract idea. *See Intellectual Ventures I LLC v. Symantec Corp.*, 838 F.3d 1307, 1314 (Fed.  
16 Cir. 2016) (claims involving filtering email for spam and viruses held directed to an abstract  
17 idea).

18           Unlike the '844 patent, which recites attaching the security profile to the Downloadable  
19 before allowing the file to reach a user (which added a "protective step"), Claim 10 of the '494  
20 patent does not itself recite any step beyond the mere identification of suspicious operations  
21 within a received Downloadable (and then storing the information somewhere). *See Finjan,*  
22 *Inc. v. Blue Coat Sys., LLC*, No. C 15–03295 BLF, 2016 WL 7212322, at \*10 (N.D. Cal. Dec.  
23 13, 2016) (Judge Beth Labson Freeman), 2016 WL 7212322, at \*10. It stops short of claiming  
24 any non-fundamental, routine step, such as comparing the security profile with the access  
25 control list or any kind of protective measure. As such, Claim 10 is directed to an abstract idea  
26 rather than an improvement on computer functionality. This finding in line with rulings made  
27 by two other courts in our district. *Id.* at \*9–10; *Finjan, Inc. v. Sophos, Inc.*, 244 F. Supp. 3d  
28 1016, 1059–1060 (N.D. Cal. 2017) (Judge William H. Orrick).

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**B. Alice Step Two.**

The Supreme Court has described step two as “a search for an inventive concept — *i.e.*, an element or *combination of elements* that is sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the ineligible concept itself.” *Alice*, 134 S. Ct. at 2355 (quotations and citation omitted) (emphasis added). Juniper contends that Claim 10 of the ’494 patent contains no inventive concept sufficient to transform its patent-ineligible subject matter into a patentable invention under *Alice* step two.

At this juncture, this order will postpone on reaching the issue of whether Claim 10 survives under *Alice* step two. Rather, the Court will wait to have the benefit of the trial record before determining whether Claim 10 contains an inventive concept such that it is patent eligible.

**4. SECTION 287.**

Juniper further alleges that Finjan is not entitled to summary judgment on its infringement claim on the now-expired ’494 patent because it has not met its burden of showing compliance with Section 287’s marking requirements.

Section 287 “advises a patent owner to mark his patented article with a notice of his patent rights. Failure to do so limits his recovery of damages to the period after the infringer receives notice of the infringement.” *Motorola, Inc. v. United States*, 729 F.2d 765, 768 (Fed.Cir. 1984) (citing 35 U.S.C. § 287). Moreover, Section 287 is “a limitation on damages, and *not an affirmative defense*.” *Arctic Cat Inc. v. Bombardier Recreational Prod. Inc.*, 876 F.3d 1350, 1366 (Fed. Cir. 2017) (citations omitted) (emphasis added). Accordingly, this order declines to reach the issue of marking on Finjan’s motion for summary judgment of infringement. A jury will have to decide.

**CONCLUSION**

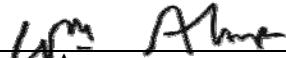
For the foregoing reasons, Finjan’s motion for summary judgment is **GRANTED IN PART**. In sum, the following issues will be decided at trial: (1) whether the accused products meet the “database” limitation; (2) Juniper’s Section 101 invalidity defense; (3) Juniper’s

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

Section 287 defense on damages; and (4) the extent of damages. A separate order will address the trial schedule. Please, we will have no more motion practice directed to Claim 10.

**IT IS SO ORDERED.**

Dated: August 24, 2018.

  
\_\_\_\_\_  
WILLIAM ALSUP  
UNITED STATES DISTRICT JUDGE