

1 PAUL J. ANDRE (State Bar No. 196585)
pandre@kramerlevin.com
2 LISA KOBIALKA (State Bar No. 191404)
lkobialka@kramerlevin.com
3 JAMES HANNAH (State Bar No. 237978)
jhannah@kramerlevin.com
4 KRAMER LEVIN NAFTALIS
5 & FRANKEL LLP
990 Marsh Road
6 Menlo Park, CA 94025
Telephone: (650) 752-1700
7 Facsimile: (650) 752-1800
8 *Attorneys for Plaintiff*
9 FINJAN, INC.

10
11 **IN THE UNITED STATES DISTRICT COURT**
12 **FOR THE NORTHERN DISTRICT OF CALIFORNIA**
13 **OAKLAND DIVISION**

14 FINJAN, INC., a Delaware Corporation,
15 Plaintiff,
16 v.
17 SOPHOS INC., a Massachusetts Corporation,
18 Defendant.

Case No.: 14-CV-01197-SBA

**PLAINTIFF FINJAN, INC.'S OPENING
CLAIM CONSTRUCTION BRIEF**

Judge: Hon. Sandra B. Armstrong

TABLE OF CONTENTS

	Page(s)
I. INTRODUCTION	1
II. STATEMENT OF FACTS	2
A. Background of the Technology.....	2
B. Summary of Finjan’s Patents	2
1. The ‘918 Patent	3
2. The ‘926 Patent	4
3. The ‘494 Patent	4
4. The ‘844 Patent	5
5. The ‘580 Patent	5
6. The ‘780 Patent	5
7. The ‘289 Patent	6
8. The ‘154 Patent	6
III. ARGUMENT	6
A. Finjan’s Proposed Terms	7
1. CODE-C (the ‘918 Patent: Claims 12 ,22)	8
2. Database (the ‘926 Patent: Claim 22, the ‘494 Patent: Claims: 1, 10)	10
3. Means-Plus-Function Claim Terms (3 Terms)	12
a) “means for receiving a Downloadable”	13
b) “means for generating a first Downloadable security profile that identifies suspicious code in the received Downloadable”	14
c) “means for linking the first Downloadable security profile to the Downloadable before a web server makes the Downloadable available to web clients”	15
B. Sophos’ Proposed Terms for Construction	16
1. Security Context (the ‘918 Patent: Claims 12, 22)	17
2. Certificate Creator (the ‘580 Patent: Claim 1)	18
3. Protocol Appender (the ‘580 Patent: Claim 1)	20
IV. CONCLUSION.....	22

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Aventis Pharms. Inc. v. Amino Chems. Ltd.</i> , 715 F.3d 1363 (Fed. Cir. 2013).....	7, 16
<i>Funai Elec. Co. v. Daewoo Elecs. Corp.</i> , 616 F.3d 1357 (Fed. Cir. 2010).....	10, 21
<i>Hoechst Celanese Corp. v. BP Chems. Ltd.</i> , 78 F.3d 1575 (Fed. Cir. 1996).....	19
<i>Markman v. Westview Instruments, Inc.</i> , 52 F.3d 967 (Fed. Cir. 1995)(en banc), <i>aff'd</i> , 517 U.S. 370 (1996)	6
<i>Noah Sys., Inc. v. Intuit Inc.</i> , 675 F.3d 1302 (Fed. Cir. 2012).....	12
<i>O2 Micro Intl. Ltd. v. Beyond Innovation Tech. Co.</i> , 521 F.3d 1351 (Fed. Cir. 2008).....	12
<i>Phillips v. AWH Corp.</i> , 415 F.3d 1303 (Fed. Cir. 2005)(en banc).....	6, 19
<i>SuperGuide Corp. v. DirecTV Enterprises, Inc.</i> , 358 F.3d 870 (Fed. Cir. 2004).....	9
<i>Thorner v. Sony Computer Entm't Am. LLC</i> , 669 F.3d 1362 (Fed. Cir. 2012).....	7, 16
<i>Vitronics Corp. v. Conceptronic, Inc.</i> , 90 F.3d 1576 (Fed. Cir. 1996).....	9
Statutes	
35 U.S.C. § 112(6)	13, 14, 15
35 U.S.C. § 112(f).....	13
Other Authorities	
MPEP § 2111.01	8, 9

1 **I. INTRODUCTION**

2 Finjan was founded in 1995 with the goal of proactively shielding against a new generation of
3 computer virus threats spawned on the Internet. Through over a decade of research and after spending
4 over \$65 million in research and development, Finjan developed a visionary suite of anti-malware
5 technologies that protect countless potential victims around the globe. Finjan's portfolio of patents
6 reflects its extensive and comprehensive development of innovative technology to protect against these
7 new threats. Long acknowledged by the industry as a significant innovation, numerous companies
8 have taken a license under its patents.¹ Sophos, however, has refused to do so, even though its
9 products employ Finjan's patented technology. Because Sophos has chosen not to respect Finjan's
10 patents, design around Finjan's patented inventions, or to take a reasonable license, Finjan was
11 compelled to file this action to protect the value of its patents for its licensees and shareholders who
12 believe in the value of Finjan's innovations. In particular, this action is to rectify Sophos' infringement
13 of eight of Finjan's patents covering these security technologies.

14 Finjan wrote the claims of the patents-in-suit using clear language understood by those of skill
15 in the art. The claims generally stand on their own without reference to the intrinsic record because the
16 meaning is unambiguously described in the language of the claims. As a result, Finjan submits that the
17 claim terms of Finjan's Patents generally do not require construction. Finjan and Sophos, however, do
18 disagree on the meaning of eight terms from five of the eight patents-in-suit, including a term that has
19 previously been agreed upon by one of Sophos' competitors in another litigation, and three are clear
20 but are to be construed by law as means-plus-function elements. Finjan's constructions for these terms
21 are supported by the specification and claims, and reflect the fundamental clarity in the claims
22 language of Finjan's patents.

23 Sophos' definitions, on the other hand, violate a variety of claim construction tenants. Most
24 notably, Sophos seeks to change well-understood claim terms even though no explicit disavowal exists
25

26 ¹ Finjan has licensed its patent portfolio to six companies in agreements worth over \$100 million in
27 total.
28

1 in the intrinsic record. Absent a clear indication in the intrinsic record, a well-understood term should
 2 be afforded its plain and ordinary meaning. This principle alone dictates that the Finjan's proposed
 3 plain and ordinary constructions for these terms should govern.

4 **II. STATEMENT OF FACTS**

5 **A. Background of the Technology**

6 Computers are constantly under attack from computer viruses propagating on the Internet.
 7 Viruses have proven to be one of the most intractable, not to mention costly, problems with computers.
 8 This is particularly the case since the advent of the "always on" Internet connection, giving computer
 9 hackers around the clock access to steal private information, disable systems, or worse. Hackers have
 10 also become increasingly sophisticated in developing viruses. There is no "silver bullet" to protect a
 11 computer from every attack. The Internet is simply too large, viruses are changing too fast, and the
 12 hackers have become too clever at disguising viruses. Finjan's visionary patented technology protect
 13 against a vast majority of these threats at various levels in the Internet architecture by detecting
 14 abnormal behaviors and reacting to new unauthorized encroachments *before* a breach can occur, as
 15 opposed to the less effective anti-virus software that can only prevent previously identified viruses,
 16 often referred to as signature-based scanning software.

17 **B. Summary of Finjan's Patents**

18 Finjan pioneered new technologies to protect computers and networks by using behavior-based
 19 technology, which focuses on what incoming program code intends to do, as opposed to traditional
 20 signature-based scanning. Traditional signature based virus scanning looked for an exact copy or
 21 "fingerprint" of a previously seen virus, which was adequate when viruses were created a slow rate.
 22 Finjan's novel technology allowed it to outsmart the hackers by detecting new and unknown viruses
 23 that hackers tried to hide through obfuscation (a technique of hiding executable code so it is difficult to
 24 read and understand) and through polymorphism (when a hacker creates multiple different versions of
 25 viruses). While criminals continue to create new and innovative viruses at an alarming rate, Finjan's
 26 patented technologies understand the actual bad behavior of a virus and describe techniques for
 27 detecting them with proper analysis and through the creation of a "profile" for the content.
 28

1 Accordingly, by targeting and analyzing the viruses' behavior, Finjan's patented technologies
 2 effectively stem the tide of malicious code based attacks. At a conceptual level, this is similar to a
 3 police officer determining that a person holding a gun, wearing a mask and following directions to a
 4 bank has the "profile" of someone likely to try to rob that bank, while previous system focused on
 5 identifying specific known criminals.

6 Finjan also discovered that an effective way to stop viruses was to prevent them from entering a
 7 computer network to begin with. This way, a protected network can stop viruses before its starts to
 8 propagate across the numerous computers and systems inside the company's network. With this key
 9 insight, Finjan developed technology that operate as network components, such as a security gateway
 10 and as part of the "cloud," allowing a company to catch viruses before they run amok on a network.
 11 Network components, such as a security gateway, catch viruses early because they can inspect
 12 communication between an external computer or network and a protected computer or network. At a
 13 conceptual level, the idea is similar to the use of a physical gateway for a castle—the gateway serves
 14 as a point to inspect traffic entering and exiting the castle.

15 The eight patents asserted against Sophos' products in this case are: U.S. Patent Nos. 6,154,844
 16 ("844 Patent"), 6,804,780 ("780 Patent"), 7,613,918 ("918 Patent"), 7,613,926 ("926 Patent"),
 17 7,757,289 ("289 Patent"), 8,141,154 ("154 Patent"), 8,566,580 ("580 Patent"), and 8,677,494 ("494
 18 Patent") (collectively "Finjan Patents"). Exs. 1-8.² The Finjan Patents relate to a suite of technologies
 19 for protecting computers from viruses downloaded through the Internet. The Finjan Patents describe
 20 different aspects of protection, providing computers with multiple layers of protection. Finjan and
 21 Sophos dispute the meaning of eight elements for the '918 Patent, '926 Patent, '494 Patent, '844 Patent
 22 and '580 Patent.

23 **1. The '918 Patent**

24 The '918 Patent protects computer from potentially malicious content, *i.e.* content that may be
 25 a virus. *See* Ex. 3 (the '918 Patent, Abstract). The '918 Patent generally covers mitigating harm from
 26 _____

27 ² All citations to exhibits are to exhibits attached to the Declaration of James Hannah filed herewith.
 28

1 potentially malicious content by using restricted security contexts that are associated with certain
2 computer accounts and deriving a profile for code received from the Internet. *Id.* The created profile
3 is combined with the content and sent to a computer for processing to determine whether the code is
4 safe. *Id.*

5 **2. The ‘926 Patent**

6 The ‘926 Patent is related to a system for protecting computers on a network from malicious
7 content. *See* Ex. 4 (the ‘926 Patent, Abstract). Specifically, the ‘926 Patent describes systems and
8 methods for performing an operation on content received over the network and deriving an identifier
9 for that content. *Id.* The identifier is used to find one or more profiles for the content on the computer
10 system that includes suspicious operations the content may attempt. A representation of the profile and
11 the content are sent to a destination computer. *Id.* In this manner, there is no need for the content to be
12 scanned if the profile has already been created. *Id.*

13 **3. The ‘494 Patent**

14 The ‘494 Patent generally covers a system for receiving a downloadable³ and creating a profile
15 for the downloadable to be stored in a database. *See* Ex. 8 (the ‘494 Patent, Abstract). The ‘494 Patent
16 discloses deriving a security profile for the downloadable that includes a list of suspicious operations
17 that may be attempted by the downloadable. *Id.* The ‘494 Patent then discloses storing the
18 downloadable profile in a database. *Id.* Additional information about the downloadable can also be
19 stored in the database, such as the date and time the profile was derived and URL from which the
20 downloadable originated. *Id.* at Col. 21, ll. 26-28. The profile can be derived a number of different
21 ways, including by disassembling the downloadable to allow suspicious operations to be more easily
22 detected. *Id.* at Col. 22, ll. 4-6.

23
24
25
26 ³ “Downloadable” is a concept coined by Finjan and the parties have agreed that the term means “an
27 executable application program, which is downloaded from a source computer and run on the
28 destination computer.”

1 **4. The ‘844 Patent**

2 The ‘844 Patent relates to inspecting a downloadable and associating a profile to the
3 downloadable indicating suspicious (*i.e.*, hostile or potentially hostile) operations that may be
4 attempted by the downloadable. *See* Ex. 1 (the ‘844 Patent, Abstract). In this way, the system is able
5 to characterize the behavior of the downloadable to determine whether it is malicious. *Id.* To generate
6 this profile, known as a downloadable security profile (“DSP”), the ‘844 Patent generally includes a
7 content inspector that identifies suspicious operations or code in a downloadable and linking the DSP
8 to the downloadable. *Id.* The content inspector generally uses a set of rules, which may include a list
9 of operations, or code patterns deemed suspicious. *Id.* This list of suspicious operations or code
10 patterns can be used to generate a DSP indicating the different combinations of malicious operations
11 present in the downloadable. *Id.* at Col. 2, l. 65-Col. 3, l. 2. After the DSP has been created and
12 identified for a particular downloadable, it can be used to determine whether to allow the
13 downloadable into a network or to be delivered to a computer. *Id.*

14 **5. The ‘580 Patent**

15 The ‘580 Patent is generally directed towards a system for efficient secure communication
16 between a client and a server through security computers. *See* Ex. 7 (the ‘580 Patent, Abstract). The
17 claims generally cover a system with a first security computer connected to a client computer with a
18 Secured Socket Layer (“SSL”) connector, and a second security computer coupled together with the
19 first security computer, where the second security computer is coupled with a server with an SSL
20 connector. *Id.* Through the use of certificates, the result is to improve efficiency by reducing the
21 number of communications between servers, thus reducing traffic in a network, and thereby reducing
22 latency, while still providing a secure communications. *Id.*

23 **6. The ‘780 Patent**

24 The ‘780 Patent relates to systems and techniques for generating an ID for a downloadable.
25 The ID is generated by a process called “hashing.” *See* Ex. 2 (the ‘780 Patent, Abstract). Hashing is a
26 mathematical function that can be applied to data to allow more efficient determination of whether the
27 data was previously seen. *Id.* The ‘780 Patent describes hashing the downloadable along with
28

1 referenced components to generate the ID for the downloadable. *Id.* The ID generated can be applied
 2 to one component of the downloadable, to a subset of the components, to all of the components of a
 3 downloadable or stored for later use. *Id.* Finjan and Sophos do not dispute the meaning of the ‘780
 4 Patent’s terms.

5 **7. The ‘289 Patent**

6 The ‘289 Patent generally covers a system and method for inspecting dynamically generated
 7 executable code. *See* Ex. 5 (the ‘289 Patent, Abstract). The claims generally cover receiving content
 8 with an original call function and replacing the original call function with a substitute call function,
 9 and then determining whether it is safe to invoke the original call function, thereby protecting the
 10 client computer from dynamically generated malicious code. *Id.* Finjan and Sophos do not dispute the
 11 meaning of the ‘289 Patent’s terms.

12 **8. The ‘154 Patent**

13 The ‘154 Patent relates to protecting a computer from dynamically generated executable code.
 14 *See* Ex. 6 (the ‘154 Patent, Abstract). Prior systems only protected against malicious content that was
 15 static. However, the Patent describes how hackers can obfuscate content in a manner where its true
 16 nature is only revealed when dynamically generated. *Id.* The ‘154 Patent provides a unique type of
 17 behavioral analyses that protects against such dynamically generated malicious content. *Id.* Finjan and
 18 Sophos do not dispute the meaning of the ‘154 Patent’s terms.

19 **III. ARGUMENT**

20 Finjan’s constructions follow the canons of claim construction and should be adopted here.
 21 The purpose of claim construction is to define the proper scope of the invention and to give meaning to
 22 claim language when the jury might otherwise misunderstand a claim term in the context of the patent.
 23 *See Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 976 (Fed. Cir. 1995)(en banc), *aff’d*, 517
 24 U.S. 370 (1996); *see also Phillips v. AWH Corp.*, 415 F.3d 1303, 1316 (Fed. Cir. 2005)(en banc)(“The
 25 construction that stays true to the claim language and most naturally aligns with the patent’s
 26 description of the invention will be, in the end, the correct construction.”). Finjan has identified five
 27 terms amongst the eight asserted patents that the Court should construe. In one instance, Finjan
 28

1 proposes minor clarifications to a claim term that is keeping with the intrinsic record and easily
 2 understood by the fact-finder. For the term “database,” construction is necessary because Sophos is
 3 applying the term in an unreasonably broad manner. The remaining three terms require construction
 4 because, as a matter of law, they are “means-plus-function” elements.

5 For the terms Sophos has selected, it proposes unnecessary limitations in an attempt to support
 6 its non-infringement position, circumventing the plain language and altering the scope of the claims.
 7 *See Aventis Pharms. Inc. v. Amino Chems. Ltd.*, 715 F.3d 1363, 1373 (Fed. Cir. 2013) (“Courts are
 8 required therefore to ‘look to the words of the claims themselves . . . to define the scope of the patented
 9 invention.’”) (citation omitted); *see also Thorner v. Sony Computer Entm’t Am. LLC*, 669 F.3d 1362,
 10 1366 (Fed. Cir. 2012) (“We do not read limitations from the specification into claims; we do not
 11 redefine words. Only the patentee can do that.”). In the specific case of the term “database,” the one
 12 term that Sophos argues no construction is necessary. However, Sophos attempts to broaden the
 13 definition beyond the scope of the patent and the plain understanding of the term in an attempt salvage
 14 an untenable invalidity position.

15 **A. Finjan’s Proposed Terms**

16 Finjan drafted the claims of the Finjan Patents in a manner that an ordinary person skilled in the
 17 art⁴ could understand. There are only a few claim terms in the asserted patents that require
 18 construction given the clear drafting of the claim language.⁵ For these terms, Finjan provides
 19 constructions that are consistent with the specifications and easy for the fact-finder to understand.
 20 Sophos’ proposed constructions, however, contradict the clear specifications of Finjan’s Patents, create
 21 ambiguity, or simply misstate how a person of ordinary skill in the art would understand the claim.

22 _____
 23
 24 ⁴ A person of ordinary skill in the art has a bachelor’s degree in computer science or related field, and
 25 (1) two years of industry experience and/or (2) an advanced degree in computer science or related
 26 field. *See* Declaration of Nenad Medvidovic in Support of Finjan’s Opening Claim Construction Brief
 (“Medvidovic Decl.”) ¶ 12.

27 ⁵ Finjan and Sophos agreed on the proper construction of three terms used in the Finjan Patents—
 28 “Downloadable,” “CODE-A,” and “CODE-B.” Dkt. 54 at 1.

1 **1. CODE-C (the ‘918 Patent: Claims 12 ,22)**

Term in Dispute	Finjan’s Proposed Construction	Sophos’ Proposed Construction
CODE-C	combined code	combined code created at the gateway computer

6 CODE-C is a term coined by Finjan for the ‘918 Patent and has no readily understood meaning
7 outside the context of the ‘918 Patent and claims. However, Finjan included a clear definition for the
8 use of the term within the ‘918 Patent.⁶ Finjan proposes that “CODE-C” be construed using this
9 definition of “combined code.” Finjan’s proposed construction is consistent with the claims, for
10 example Claim 12 of the ‘918 Patent states:

11 12. A computer security system for a gateway computer, comprising:
12 a receiver for receiving content including
13 ...
14 a code packager, coupled with said security context generator, for packaging (i)
15 information about the computer account determined by said security context
16 generator and (ii) CODE-A, with (iii) executable wrapper code ("CODE-B"),
17 into a combined code ("CODE-C"); and
18 a transmitter, coupled with said code packager, for forwarding CODE-C to the
19 client computer for processing.

20 Ex. 3 (‘918 Patent at Col. 12, ll. 32-57) (emphasis added).

21 Furthermore, the specification of the ‘918 Patent repeatedly defines CODE-C as the combined
22 code of CODE-A and CODE-B.⁷ See e.g., *id.* at Abstract (“combining (i) information about the
23 determined computer account name and (ii) CODE-A, with executable wrapper code (‘CODE-B’) into
24

25 ⁶ “An applicant is entitled to be his or her own lexicographer and may rebut the presumption that claim
26 terms are to be given their ordinary and customary meaning by clearly setting forth a definition of the
27 term that is different from its ordinary and customary meaning(s).” MPEP § 2111.01: Plain Meaning,
28 citing *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994).

⁷ The parties were able to come to an agreement for the construction of CODE-A and CODE-B, which
similarly takes the definition as defined by specification without extraneous limitations. Dkt. No. 54 at
1.

1 combined code ('CODE-C')) (emphasis added). As shown, CODE-C means "combined code".

2 *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996) ("It is well-settled that, in
3 interpreting an asserted claim, the court should look first to the intrinsic evidence of record, *i.e.*, the
4 patent itself, including the claims, the specification and, if in evidence, the prosecution history.")
5 (citing *Markman*, 52 F.3d at 979). For this reason alone Finjan's proposed construction should be
6 adopted.

7 Sophos does not dispute that Finjan's construction of CODE-C is proper, as it too includes
8 "combined code" in its proposed construction. However, instead of stopping there, Sophos adds a
9 limitation requiring a gateway computer to create CODE-C. Sophos imports this extraneous limitation
10 into every claim based on an example embodiment, in contravention of the canons of claim
11 construction. *SuperGuide Corp. v. DirecTV Enterprises, Inc.*, 358 F.3d 870, 875 (Fed. Cir. 2004) ("[I]t
12 is important not to import into a claim limitations that are not part of the claim."); *see also* MPEP §
13 2111.01. Nowhere in the specification does the Finjan limit CODE-C to the example embodiment of
14 creating CODE-C on a gateway computer. Further, some claims of the '918 Patent require a code
15 packager to create CODE-C on a gateway computer, while other claims do not. *Cf.* Claims 12 and 35
16 with Claims 1, 21 and 28. Therefore, Sophos' proposed construction should be rejected because it
17 improperly imports a limitation from the specification for some claims and be superfluous for other
18 claims. Thus, the Court should adopt Finjan's proposed construction.

19 What is more, the specification identifies seven additional embodiments that do not require a
20 gateway computer, let alone creating CODE-C on a gateway computer, in contrast only two disclosed
21 embodiments of the invention are "a computer security system for a gateway computer." Ex. 3 ('918
22 Patent, Col. 4, l. 10-Col. 6, l. 8). The seven embodiments do not require or suggest that the CODE-C
23 must always be created on a gateway computer, and allow for its creation at any location.
24 Furthermore, some example embodiments of the invention CODE-C to reside on computer-readable
25 storage medium, and, therefore do not require or suggest that it must be resident on a gateway
26 computer. *See e.g., id.* at Col. 4, ll. 47-62; Col. 5, ll. 24-35; Col. 5, l. 63-Col. 6, l. 8; Claims 21, 33,
27 and 36. Sophos' proposed construction would read out these embodiments by requiring CODE-C to be
28

created on a gateway computer while the claim requires a computer-readable storage medium. *Funai Elec. Co. v. Daewoo Elecs. Corp.*, 616 F.3d 1357, 1371 (Fed. Cir. 2010) (rejecting claim construction that excluded an example embodiment).

2. Database (the ‘926 Patent: Claim 22, the ‘494 Patent: Claims: 1, 10)

Term in Dispute	Finjan’s Proposed Construction	Sophos’ Proposed Construction
Database	a collection of interrelated data organized according to a database schema to serve one or more applications	no construction necessary

Finjan requests that the Court clarify “database” as its plain and ordinary meaning of “a collection of interrelated data organized according to a database schema to serve one or more applications.” Medvidovic Decl., ¶¶ 30-31; *see also* Ex. 9 (IBM Dictionary definition of “database”).

The use of the term database can be seen in Claim 1 of the ‘494 Patent, which states:

1. A computer-based method, comprising the steps of:
receiving an incoming Downloadable;

deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable;
and

storing the Downloadable security profile data in a database.

Ex. 8 (‘494 Patent at Col. 21, ll. 19-25) (emphasis added).

Finjan requests this clarification of “database” because in its Invalidity Contentions, Sophos applies the term in a manner that is impermissibly broad compared to the ordinary understanding of “database” to one of ordinary skill in the art. For example, in its Invalidity Contentions, Sophos relies on simple files, such as a log file, for the “database.” *See e.g.*, Ex. 10 (Sophos’ Invalidity Contentions H-25 at 12) (“It would have been obvious to one of ordinary skill in the art to store or log information related to an incoming program, as such was a well-known way to achieve at least the benefits of improved speed and accuracy of program classification, including classification of malware, and of

1 more efficient use of system resources.”)(emphasis added); *see also* Medvidovic Decl., ¶¶ 32-33. As
 2 explained below, one of ordinary skill in the art would not understand a log file to be a database.

3 A person of ordinary skill in the art would understand from reading the specification and claims
 4 of the ‘926 and ‘494 Patents that database is a collection of data stored related to downloadable
 5 security profiles and schemas related to the downloadable security profile, and not an unstructured
 6 collection of data on a computer such as a log file. Medvidovic Decl., ¶¶ 32-33. Indeed, in prior
 7 litigations where this term was at issue, Sophos’ competitor agreed with Finjan on the construction of
 8 database for the same patent. *See Finjan, Inc. v. Websense, Inc.*, Case No. 13-cv-4398, Dkt. No. 93
 9 (N.D. Cal.). A computer system uses a database to store structured data accessible for later use by an
 10 application program. The structure used by the database for storing this data is called the “database
 11 schema” and allows the database to be easily organized, managed and searched to allow an application
 12 program to use the data. This understanding contrasts with the typical understanding of a “log file,”
 13 which does not necessarily have such a structured organization of data.

14 The plain and ordinary meaning of database used by Sophos is broader than intended by the
 15 inventor. *See* Medvidovic Decl., ¶ 30. The claim language of the asserted patents all relate to the
 16 storage of data within the database in the context of the security profile or the downloadable security
 17 profile. *See e.g.*, Ex. 4 (the ‘926 Patent, Claims 1, 8, 15, 22, 29, and 30); *see also* Ex. 8 (‘494 Patent,
 18 Claims 1, 2, and 10). The system actively uses these security profiles to detect malware and manage
 19 the system, not just for archival storage. Medvidovic Decl., ¶ 31. Sophos’ proposed construction
 20 would allow the term to mean any type of storage, such as a simple log file. This is incorrect, as the
 21 log files disclosed in the prior art references have a different typical use, for example for occasional
 22 manual analysis by an administrator or as a historical record for long term storage, and not for storing
 23 related, structured data, with well-defined data formats, for active update and retrieval of security
 24 profile information. Medvidovic Decl., ¶¶ 32-33. Furthermore, the ‘780 Patent discloses the use of
 25 log files, and does not equate them with databases. *See e.g.*, Ex. 4 (the ‘926 Patent, Col. 4, l. 17).
 26 Indeed, the ‘780 Patent, which is incorporated by reference by the ‘926 Patent, shows as separate
 27 components a security database and an events log. Ex. 2 (the ‘780 Patent, Fig. 2). Thus, Finjan’s
 28

1 construction is proper because it is consistent with how a person of ordinary skill in the art would
 2 understand the term at the time of invention and the specification.

3 Accordingly, the Court should construe or clarify the term “database” to apply as one of
 4 ordinary skill in the art would understand it to mean and not in the impermissibly broad manner
 5 Sophos seeks in support of its invalidity. *O2 Micro Intl. Ltd. v. Beyond Innovation Tech. Co.*, 521 F.3d
 6 1351, 1362 (Fed. Cir. 2008) (“When the parties present a fundamental dispute regarding the scope of a
 7 claim term, it is the court's duty to resolve it.”).

8 **3. Means-Plus-Function Claim Terms (3 Terms)**

9 The parties have identified different functions and structures for the means-plus-function
 10 elements recited in claim 43 of the ‘844 Patent. Finjan proposes that the functions be the verbatim text
 11 recited in the claim elements while Sophos’ proposes that the mean-plus-function elements are
 12 indefinite despite the presumption that the claim is valid.

13 Finjan’s constructions are proper because they are the very function set forth directly in the
 14 claim element. Medvidovic Decl., ¶¶ 12, 15, 18. For example, one of the disputed claim elements
 15 states that it is a “means for receiving a Downloadable.” Thus, the claim recites the exact function for
 16 this element, namely “receiving a Downloadable.” The other two elements are similarly easy to
 17 determine a function for, undercutting Sophos’ claim the terms are indefinite. Further, a person of
 18 ordinary skill in the art would be able to recognize and identify the structure corresponding to the
 19 functions from reading the specification of the ‘844 Patent. Medvidovic Decl., ¶¶ 12-14. Therefore,
 20 the means-plus-function claim elements in dispute cannot be indefinite. *Noah Sys., Inc. v. Intuit Inc.*,
 21 675 F.3d 1302, 1312 (Fed. Cir. 2012) (means-plus-functions are not indefinite if a person of ordinary
 22 skill is able to “recognize the structure in the specification and associate it with the corresponding
 23 function in the claim.”) (citations omitted).

a) “means for receiving a Downloadable”

Term in Dispute	Finjan’s Proposed Construction	Sophos’ Proposed Construction
means for receiving a Downloadable	Governed by 35 U.S.C. § 112(6): Function: receiving a Downloadable Structure: Downloadable file interceptor	Indefinite

As noted above, Finjan’s construction for the function is set forth in the plain language of the claim element. Thus, the proper function for the “means for receiving a Downloadable” is “receiving a Downloadable.” Medvidovic Decl., ¶ 12.

The intrinsic record also fully supports the structure for performing this function. The specification of the ‘844 Patent provides that the “Downloadable file interceptor” performs the relevant function of receiving a downloadable. For example, the ‘844 Patent states “[m]ethod 700 begins with the Downloadable file interceptor 505 in step 705 receiving a Downloadable file” and “[t]he generic protection engine 500 includes a Downloadable file interceptor 505 for intercepting incoming Downloadables (i.e., Downloadable files) for inspection...” Ex. 1 (the ‘844 Patent, Col. 9, ll. 21-22; Col. 7, ll. 44-46) (emphasis added). Here, the specification clearly identifies that the “Downloadable file interceptor” structure performs the function of “receiving a Downloadable file.” Thus, a person of ordinary skill in the art would be able to identify, with reasonable certainty, the structure and corresponding function because the specification clearly identifies the structure and function. Medvidovic Decl., ¶¶ 12-14. Accordingly, the proper structure for this means-plus-function term is a “Downloadable file interceptor.” See 35 U.S.C. § 112(f) (limitations are “construed to cover the corresponding structure, material, or acts described in the specification and equivalents thereof.”); Medvidovic Decl., ¶ 13.

b) “means for generating a first Downloadable security profile that identifies suspicious code in the received Downloadable”

Term in Dispute	Finjan’s Proposed Construction	Sophos’ Proposed Construction
means for generating a first Downloadable security profile that identifies suspicious code in the received Downloadable	Governed by 35 U.S.C. § 112(6): Function: generating a first Downloadable security profile that identifies suspicious code in the received Downloadable Structure: content inspection engine	Indefinite

Finjan’s construction for this claim element is also based on the plain language of the claim. For the claim element “means for generating a first Downloadable security profile that identifies suspicious code in the received Downloadable,” Finjan proposes the function “generating a first Downloadable security profile that identifies suspicious code in the received Downloadable.” Thus, Finjan’s proposed construction for the function should be adopted. Medvidovic Decl., ¶ 15.

The ‘844 Patent discloses that the corresponding structure for “generating a first Downloadable security profile that identifies suspicious code in the received Downloadable” is a content inspection engine. Medvidovic Decl., ¶ 16. Specifically, the ‘844 Patent provides that “a content inspection engine [] uses a set of rules to generate a Downloadable security profile corresponding to a Downloadable.” Ex. 1 (‘844 Patent, Abstract) (emphasis added); *see also* id. at Col. 7, ll. 62-63 (“a local content inspection engine 525 generates a DSP[Downloadable security profile]”) (emphasis added). In addition, the “Downloadable security profile” identifies suspicious code in the received Downloadable because the Downloadable security profile “preferably includes a list of all potentially hostile or suspicious computer operations that may be attempted by the Downloadable, and may also include the respective arguments of these operations.” *Id.* at Col. 4, ll. 4-7 (emphasis added).

Therefore, a person of ordinary skill in the art would understand, with reasonable certainty, that the content inspection engine would generate the downloadable security profile and that the downloadable

security profile would identify suspicious code in the received downloadable. Medvidovic Decl., ¶¶ 15-17. Thus, Finjan's structure is the correct one because they are the structures disclosed to perform the requisite function.

c) **“means for linking the first Downloadable security profile to the Downloadable before a web server makes the Downloadable available to web clients”**

Term in Dispute	Finjan's Proposed Construction	Sophos' Proposed Construction
means for linking the first Downloadable security profile to the Downloadable before a web server makes the Downloadable available to web clients	Governed by 35 U.S.C. § 112(6): Function: linking the first Downloadable security profile to the Downloadable before a web server makes the Downloadable available to web clients Structure: content inspection engine	Indefinite

For the claim element “means for linking the first Downloadable security profile to the Downloadable before a web server makes the Downloadable available to web clients,” Finjan again proposes the plain language function “linking the first Downloadable security profile to the Downloadable before a web server makes the Downloadable available to web clients.” Thus, Finjan's proposed construction is the correct one and should be adopted. Medvidovic Decl., ¶ 18.

The '844 Patent specification also discloses that the corresponding structure for “linking the first Downloadable security profile to the Downloadable before a web server makes the Downloadable available to web clients” is the content inspection engine. Medvidovic Decl., ¶ 19. Specifically, the '844 Patent provides that “[t]he first content inspection engine may link to the Downloadable ... [and] [a]dditional content inspection engines may generate and link additional Downloadable security profiles to the Downloadable.” Ex. 1 ('844 Patent, Abstract) (emphasis added); *see also id.* at Col. 3, 1. 66-Col. 4, 1. 4 (The inspector 125 includes a content inspection engine 160 ... for attaching the

[Downloadable security profile] to the Downloadable.”) (emphasis added); *id.* at Col. 8, ll. 49-51 (“The content inspection engine 160 in step 630 attaches the DSP[Downloadable security profile] 215 ...to the [] Downloadable 150.”) (emphasis added). As noted by the specification, the term “linking” “indicate[s] an association between the Downloadable 205 and the [Downloadable security profile] 215.” *Id.* at Col. 6, ll. 20-21. In addition, the “Downloadable security profile” is linked to the Downloadable prior to being transmitted to the client computer by inspector. *See id.* at Col. 5, ll. 3-5 (“The inspector 125 then transmits the signed inspected Downloadable 195 to the web server 185 for addition to web page data 190 and web page deployment.”) (emphasis added). Therefore, a person of ordinary skill in the art would understand, with reasonable certainty, that the content inspection engine would link the downloadable security profile to the downloadable prior to making it available to the web client via the web server and inspector. Medvidovic Decl., ¶¶ 18-20. Thus, Finjan’s structure is the correct one because they are the structures disclosed to perform the requisite function.

B. Sophos’ Proposed Terms for Construction

Sophos has identified terms for construction that one of ordinary skill in the art, as well as laypersons, readily understand. As such, no construction is necessary beyond the plain and ordinary meaning of the terms. Sophos, nonetheless, seeks constructions which violate the tenants of claim construction by replacing terms and adding extraneous limitations, thereby, circumventing the plain language and altering the scope of the claims. *See Aventis Pharms.*, 715 F.3d at 1373 (“Courts are required therefore to ‘look to the words of the claims themselves . . . to define the scope of the patented invention.’”) (citations omitted); *see also Thorner*, 669 F.3d at 1366 (“We do not read limitations from the specification into claims; we do not redefine words. Only the patentee can do that.”).

1 **1. Security Context (the ‘918 Patent: Claims 12, 22)**

Term in Dispute	Finjan’s Proposed Construction	Sophos’ Proposed Construction
security context	No construction necessary	an environment in which a software application is run, which may limit resources that the application is permitted to access or operations that the application is permitted to perform

2 Sophos asks the Court to construe the term “security context.” This is unnecessary because it is
3 well understood term by a person of ordinary skill in the art when read with the claims. Medvidovic
4 Decl., ¶¶ 26-29. The claims define the term and describe the proper scope of the claim. For example
5 claims 12, states in part:

6 12. A computer security system for a gateway computer, comprising:
7 a receiver for receiving content including
8 potentially malicious executable code ("CODE-A"), intended for downloading at
9 a client computer, wherein the client computer manages a plurality of computer
10 accounts for logging in to the client computer, and wherein each computer
11 account of the plurality of computer accounts has associated therewith a *security*
12 *context* within which an executable running on the client computer under such
13 *account is processed*;
14 ...

15 Ex. 3 (the ‘918 Patent, Col. 12, ll. 32-42) (emphasis added).

16 As shown in the Claim 12, the claims already require that a computer account is associated
17 with the security context and that a security context is something within which a running executable is
18 processed, *i.e.* an environment for processing the executable. As such, the claims adequately define
19 the term and any additional construction would be superfluous and only serve to confuse the fact-
20 finder.
21
22
23
24
25
26
27
28

Sophos argues that security context must have additional limitations and relies on a description of the term “security context” that, admittedly, is included in the specification of the ‘918 Patent. However, Sophos’ construction is unnecessary and potentially opens the door for Sophos to make improper arguments. Sophos’ proposed construction can be broken into two parts. The first part is the description of a security context as “an environment in which a software application is run.” Finjan does not dispute that this is accurate description, only that it is redundant based on the language of the claims. Namely, that the claims already require that the executable is run in a particular security context. As such, there is no need to include this portion of the construction.

In the second part of its proposed construction, Sophos adds that the security context “may limit resources that the application is permitted to access or operations that the application is permitted to perform.” As shown, this section does not include a limitation on the term because it is only what the security context “may” do. As such, there is no need to include the limitation and to do so would confuse the fact-finder. Furthermore, Sophos’ proposed construction of the term could be used by Sophos as an attempt to make the improper argument that the security context must limit resources an application can access or operations it can perform, rather than it being something it “may” do. As such, Sophos’ proposed construction should be rejected.

2. Certificate Creator (the ‘580 Patent: Claim 1)

Term in Dispute	Finjan’s Proposed Construction	Sophos’ Proposed Construction
certificate creator	No construction necessary	security gateway component that creates a signed certificate for attributes of a server certificate

Sophos attempts to import limitations into the term “certificate creator,” a term that needs no construction and should be given its plain and ordinary meaning. Indeed, Sophos attempts to limit the term by requiring the certificate creator to be part of the security gateway based on an example embodiment and despite adequate description of the term in the clear language of the claim. The term “certificate creator” is only used in Claim 1 of the ‘580 Patent:

1. A system for secure communication, comprising:

a first security computer comprising:

a certificate creator, (i) for receiving attributes of a server computer's signed certificate within a reply message generated by a second security computer and communicated to the first security computer, the signed certificate being used to authenticate the server computer, and (ii) for creating a proxy signed certificate from the received attributes;

a certificate cache for storing and retrieving the attributes of the server computer's signed certificate; and

a first SSL connector, for connecting to a client computer and for performing a first SSL handshake with the client computer using the proxy signed certificate created by said certificate creator; and ...

Ex. 7 ('580 Patent, Col. 7, ll. 46-61) (emphasis added).

As shown in Claim 1, the claim itself provides a significant description for the operation of the certificate creator already. Sophos' construction is incompatible with the claim because the claim requires that the certificate creator be part of the "first security computer" not a security gateway as Sophos' proposed construction would require. Furthermore, Sophos proposed construction contradicts claim differentiation, because dependent Claim 3 adds the limitation to first security computer to being a "network gateway computer." Under Sophos' proposed construction, Claim 3 would be superfluous, because the certificate creator would already be on a security gateway computer. *Phillips*, 415 F.3d at 1315 ("the presence of a dependent claim that adds a particular limitation gives rise to a presumption that the limitation in question is not present in the independent claim.") (citation omitted). Thus, Sophos' proposed construction should be rejected.

The inventor provided no special meaning to the term "certificate creator" and a person of ordinary skill in the art would understand the term in the context of the specification. *Medvidovic Decl.*, ¶¶ 34-36; *see also Hoechst Celanese Corp. v. BP Chems. Ltd.*, 78 F.3d 1575, 1578, (Fed. Cir. 1996) ("A technical term used in a patent document is interpreted as having the meaning that it would be given by persons experienced in the field of the invention, unless it is apparent from the patent and the prosecution history that the inventor used the term with a different meaning."). In fact, the term is

clear is self-defining and is simply a component that creates certificates in the manner described in the claim. The construction proposed by Sophos would alter this clear and well-understood ordinary meaning. Therefore, the plain and ordinary meaning of “certificate creator” should govern.

3. Protocol Appender (the ‘580 Patent: Claim 1)

Term in Dispute	Finjan’s Proposed Construction	Sophos’ Proposed Construction
protocol appender	No construction necessary	an apparatus that appends certificate attributes within a protocol request

Similarly, Sophos violates the rules of claim construction with its construction of “protocol appender.” First, Claim 1 of the ‘580 Patent, the only claim including this term, includes the structure of a “protocol appender” in the claims itself, and requires no further construction. Claim 1 of the ‘580 patent recites:

1. A system for secure communication, comprising: a first security computer comprising:

...

a second security computer communicatively coupled with said first security computer via a non-SSL connection for receiving a connection request message therefrom, the connection request message including cached attributes of the signed certificate, comprising:

...

a protocol appender, for appending the current attributes of the signed certificate within the reply message communicated to said first security computer, when said certificate comparator determines that the cached attributes of the signed certificate do not match the current attributes of the signed certificate.

Ex. 7 (the ‘580 Patent, Col. 7, l. 46-Col. 8, l. 20) (emphasis added). As shown, Claim 1 specifically defines the term. Nothing in the specification of the ‘580 Patent requires the term to be construed, as no explicit definition is provided for the term.

Sophos’ proposed construction, on the other hand, is directly contrary to the specification. The specification of the ‘580 Patent clearly shows in one embodiment, the protocol appender “is used in

performing step 1135 of FIG. 3 and step 1265 of FIG. 4B,” *i.e.* “append server certificate attributes to the header.” Ex. 7 (the ‘580 Patent, Col. 7, ll. 16-17; Figs. 3, 4B). However, a few sentences later, the specification also provides another embodiment by stating the protocol appender “for appending the hash value to a protocol message” and also “is used in performing step 1220 of FIG. 4A,” *i.e.* “append fingerprint/hash to connection request.” *Id.* at Col. 7, ll. 24-27; Fig. 4A. Thus, Sophos’ proposed construction would read out the second embodiment of protocol appender because their definition would not include appending a fingerprint/hash to a protocol message. *Funai Elec.*, 616 F.3d at 1371 (rejecting claim construction that excluded an example embodiment).

Further, the claims themselves identify which embodiment of the protocol appender it intends to use. Notably Claim 2 uses protocol appender on first security computer differently than the protocol appender on the second security computer as described in Claim 1. In Claim 1, as shown above, the protocol appender on the second security computer is used for “for appending the current attributes of the signed certificate within the reply message communicated to said first security computer, when said certificate comparator determines that the cached attributes of the signed certificate do not match the current attributes of the signed certificate.” In Claim 2, shown below, the protocol appender is used on the first security computer “for appending the hash value derived by said first security computer certificate encoder within a request message communicated to said second security computer.”

The system of Claim 1 wherein said first security computer further comprises:

a certificate encoder for deriving a hash value of the cached attributes of the signed certificate; and

a protocol appender, for appending the hash value derived by said first security computer certificate encoder within a request message communicated to said second security computer, ...

Ex. 7 (the ‘580 Patent, Col. 8, ll. 21-28) (emphasis added).

Because Sophos' proposed construction is based on one embodiment, when applied to other embodiments, the result creates confusion and unintended limitations not supported by the specification. While the protocol appender performs multiple functions, it does not necessarily perform these functions at the same time or even on the same computer. Thus, Sophos' proposed construction should be rejected.

Additionally, the inventor provided no special meaning to the term "protocol appender" and a person of ordinary skill in the art would understand the term in the context of the specification. Medvidovic Decl., ¶¶ 37-39. Therefore, Finjan's proposed plain and ordinary meaning of "protocol appender" should govern.

IV. CONCLUSION

For the reasons set forth above, Finjan respectfully requests that the Court construe all of the disputed terms of the Finjan Patents in accordance with Finjan's constructions.

Respectfully submitted,

Dated: December 1, 2014

By: /s/ James Hannah

Paul J. Andre
Lisa Kobialka
James Hannah
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

Attorneys for Plaintiff
FINJAN, INC.