

EXHIBIT 2

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

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION**

FINJAN, INC.,
Plaintiff,
v.
CISCO SYSTEMS, INC.,
Defendant.

Case No. 17-cv-00072-BLF

**ORDER CONSTRUING CLAIMS IN
U.S. PATENT NOS. 6,154,844; 6,804,780;
7,647,633; 8,141,154; 8,677,494**

[Re: ECF 100, 112, 127]

United States District Court
Northern District of California

Plaintiff Finjan, Inc. (“Finjan”) brings this patent infringement lawsuit against Defendant Cisco Systems, Inc. (“Cisco”), alleging infringement of five of Finjan’s patents directed to computer and network security: U.S. Patent Nos. 6,154,844 (“the ’844 patent”); 6,804,780 (“the ’780 patent”); 7,647,633 (“the ’633 patent”); 8,141,154 (“the ’154 patent”); and 8,677,494 (“the ’494 patent”) (collectively, the “Asserted Patents”). The Court held a tutorial on June 7, 2018 and a *Markman* hearing on June 15, 2018 for the purpose of construing ten disputed terms in the ’844, ’780, ’633, ’154, and ’494 patents.

I. BACKGROUND

The Asserted Patents are directed to network security technologies that detect online threats from malware. Finjan asserts that Cisco’s products and services infringe the Asserted Patents. *See generally* Second. Am. Compl., ECF 55. Each patent is summarized below.

A. The ’844 Patent

The ’844 patent is titled “System and Method for Attaching a Downloadable Security Profile to a Downloadable” and was issued on November 28, 2000. Ex. 1 to Hannah Decl. (the ’844 patent), ECF 100-3. This patent claims systems and methods for inspecting Downloadables

1 for suspicious code or behavior according to a set of rules and generating a profile of the results
2 from the inspection. *See, e.g., id.* at 1:62–3:7. In some embodiments, a content inspection engine
3 generates a security profile and links that profile to a Downloadable. *Id.* at 2:3–11. The profile
4 can include certificates that are later read by a protection engine to determine whether or not to
5 trust the profile. *Id.* at 2:20–48. By providing verifiable profiles, the claimed systems and
6 methods may efficiently protect computers from hostile Downloadables. *Id.* at 2:61–3:7.

7 **B. The '494 Patent**

8 The '494 patent is titled “Malicious Mobile Code Runtime Monitoring System and
9 Methods” and was issued on March 18, 2014. Ex. 2 to Hannah Decl. (the '494 patent), ECF 100-
10 4. The patent provides “[p]rotection systems and methods . . . for protecting one or more personal
11 computers (“PCs”) and/or other intermittently or persistently network accessible devices or
12 processes from undesirable or otherwise malicious operations” *Id.* at 2:51–55. To achieve
13 this goal, some embodiments utilize a protection engine in order to identify executable code. *Id.*
14 at 11:65–12:14, 12:38–47.

15 **C. The '780 Patent**

16 The '780 patent is titled “System and Method for Protecting a Computer and a Network
17 From Hostile Downloadables” and was issued on October 12, 2004. Ex. 3 to Hannah Decl. (the
18 '780 patent), ECF 100-5. This patent teaches the generation of a re-usable ID for downloaded
19 files so that future iterations of those files can be easily identified. For instance, the patent
20 discloses that an ID generator can compute an ID that identifies a Downloadable by fetching
21 components of the Downloadable and performing a hashing function on the fetched components.
22 *See, e.g., id.* at 2:12–16.

23 **D. The '633 Patent**

24 The '633 patent is titled “Malicious Mobile Code Runtime Monitoring System and
25 Methods” and was issued on January 12, 2010. Ex. 4 to Hannah Decl. (the '633 patent), ECF 100-
26 6. The patent provides systems and methods for protecting devices on an internal network from
27 code, applications, and/or information downloaded from the Internet that performs malicious
28 operations. *Id.* at Abstract. At a high level, some embodiments include a protection engine that

1 resides on a network server and monitors incoming information for executable code. *Id.* at 2:20–
 2 3:4. Upon detection of executable code, the protection engine deploys a “mobile protection code”
 3 and protection policies to a downloadable-destination. *Id.* col. 3:5–21. At the destination, the
 4 Downloadable is executed, typically within a sandboxed environment, and malicious or potentially
 5 malicious operations that run or attempt to run are intercepted and neutralized by the mobile
 6 protection code according to set protection policies. *See id.* at 3:22–40.

7 E. The '154 Patent

8 The '154 patent is titled “System and Method for Inspecting Dynamically Generated
 9 Executable Code” and was issued on March 20, 2012. Ex. 5 to Hannah Decl. (the '154 patent),
 10 ECF 100-7. The patent concerns “new behavioral analysis technology [that] affords protection
 11 against dynamically generated malicious code,” which are viruses generated at runtime. *Id.* at
 12 4:32–34; *see also id.* at 3:32–33. In some embodiments, a gateway computer receives content
 13 from the internet, where the content includes a call to an original function and an input. *Id.* at
 14 5:26–32. The gateway computer modifies the received content by replacing the call to the original
 15 function with a corresponding call to a substitute function. *Id.* at 5:32–35. The substitute function
 16 sends the input to a security computer, which determines whether it is safe to invoke the original
 17 function with the input at a client computer. *Id.* at 5:35–43. In this approach, the patent provides
 18 technology that protects computers from dynamically generated malicious code.

19 II. LEGAL STANDARD

20 A. General Principles

21 Claim construction is a matter of law. *Markman v. Westview Instruments, Inc.*, 517 U.S.
 22 370, 387 (1996). “It is a ‘bedrock principle’ of patent law that ‘the claims of a patent define the
 23 invention to which the patentee is entitled the right to exclude,’” *Phillips v. AWH Corp.*, 415 F.3d
 24 1303, 1312 (Fed. Cir. 2005) (en banc) (internal citation omitted), and, as such, “[t]he appropriate
 25 starting point . . . is always with the language of the asserted claim itself,” *Comark Commc 'ns, Inc.*
 26 *v. Harris Corp.*, 156 F.3d 1182, 1186 (Fed. Cir. 1998).

27 Claim terms “are generally given their ordinary and customary meaning,” defined as “the
 28 meaning the term would have to a person of ordinary skill in the art in question . . . of the

1 effective filing date of the patent application.” *Phillips*, 415 F.3d at 1313 (internal citation
2 omitted). The court reads claims in light of the specification, which is “the single best guide to the
3 meaning of a disputed term.” *Id.* at 1315; *see also Lighting Ballast Control LLC v. Philips Elecs.*
4 *N. Am. Corp.*, 744 F.3d 1272, 1284-85 (Fed. Cir. 2014) (en banc). Furthermore, “the
5 interpretation to be given a term can only be determined and confirmed with a full understanding
6 of what the inventors actually invented and intended to envelop with the claim.” *Phillips*, 415
7 F.3d at 1316 (quoting *Renishaw PLC v. Marposs Societa’ per Azioni*, 158 F.3d 1243, 1250 (Fed.
8 Cir. 1998)). The words of the claims must therefore be understood as the inventor used them, as
9 such understanding is revealed by the patent and prosecution history. *Id.* The claim language,
10 written description, and patent prosecution history thus form the intrinsic record that is most
11 significant when determining the proper meaning of a disputed claim limitation. *Id.* at 1315–17;
12 *see also Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996).

13 Evidence external to the patent is less significant than the intrinsic record, but the court
14 may also consider such extrinsic evidence as expert and inventor testimony, dictionaries, and
15 learned treatises “if the court deems it helpful in determining ‘the true meaning of language used
16 in the patent claims.’” *Phillips*, 415 F.3d at 1318 (quoting *Markman*, 52 F.3d at 980). However,
17 extrinsic evidence may not be used to contradict or change the meaning of claims “in derogation
18 of the ‘indisputable public records consisting of the claims, the specification and the prosecution
19 history,’ thereby undermining the public notice function of patents.” *Id.* at 1319 (quoting
20 *Southwall Techs., Inc. v. Cardinal IG Co.*, 54 F.3d 1570, 1578 (Fed. Cir. 1995)).

21 **B. Means-Plus-Function Claims**

22 Paragraph 6 of 35 U.S.C. § 112 provides for means-plus-function claiming: “An element in
23 a claim for a combination may be expressed as a means . . . for performing a specified function . . .
24 and such claim shall be construed to cover the corresponding structure, material, or acts described
25 in the specification and equivalents thereof.”¹ When a claim uses the term “means” to describe a
26

27
28 ¹ Paragraph 6 of 35 U.S.C. § 112 was replaced with newly designated § 112(f) when the America
Invents Act (“AIA”) Pub. L. No. 112-29. took effect on September 16, 2012. Because the

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.