IRELL & MANELLA LLP
Jonathan S. Kagan (SBN 166039)
jkagan@irell.com
Joshua Glucoft (SBN 301249)
jglucoft@irell.com
1800 Avenue of the Stars, Suite 900
Los Angeles, California 90067-4276
Telephone: (310) 277-1010
Facsimile: (310) 203-7199

Rebecca Carson (SBN 254105)
rcarson@irell.com
Dennis Courtney (SBN 307646)
dcourtney@irell.com
Ingrid Petersen (SBN 313927)
ipetersen@irell.com
Kevin Wang (SBN 318024)
kwang@irell.com
840 Newport Center Drive, Suite 400
Newport Beach, California 92660-6324
Telephone: (949) 760-0991
Facsimile: (949) 760-5200

Attorneys for Defendant
JUNIPER NETWORKS, INC.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

FINJAN, INC., a Delaware Corporation, Plaintiff, vs. JUNIPER NETWORKS, INC., a Delaware Corporation, Defendant.	Case No. 3:17-cv-05659-WHA **RESPONSIVE BRIEF REGARDING INVALIDITY OF CLAIM 10 OF U.S. PATENT NO. 8,677,494 UNDER 35 U.S.C. § 101**

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Finjan's ill-fated effort to resuscitate Claim 10 is based upon the argument that Claim 10 implements a new "behavior-based scanning technique." Even a cursory reading of the claim, however, demonstrates that Claim 10 does not describe how to use "behavior-based" scanning to protect a user computer. Finjan's effort to save Claim 10 by comparing it with patents that do implement "behavior-based" protection is thus misplaced. Moreover, even if Claim 10 did incorporate "behavior-based" protection, clear and convincing evidence ***from this case*** demonstrates that this purportedly inventive concept was old hat by 1996.

A. Finjan's Attempts To Equate Claim 10 To The '844 Patent Are Misplaced.

Finjan argues that "[t]he elements of Claim 10 describe a behavior-based scanning technique" to address problems in "Downloadables," and purportedly "describes ***exactly how to protect against them***." Dkt. 535 at 5:6-8 (emphasis added). Finjan then repeatedly cites the Federal Circuit's analysis of U.S. Patent No. 6,154,844 in *Finjan, Inc. v. Blue Coat Sys., Inc.*, 879 F.3d 1299 (Fed. Cir. 2018) as if it were dispositive of the § 101 analysis for any patent that supposedly covers "behavior-based" malware analysis. *See, e.g.*, Dkt. 565 at 3:4-5; 8:10-11. This attempt to conflate Claim 10 with claims in an entirely different patent is mistaken.

First, although Finjan argues that "Claim 10 provides the same benefits as those recognized by the Federal Circuit as patent eligible," Dkt. 565 at 8:14-15, it provides no factual support for this argument (or any other similarity between the '494 and '844 patents). Indeed, contrary to Finjan's allegations, Dkt. 565 at 3:5-6, the '844 patent is ***not*** a parent to the '494 patent, *see, e.g.*, IPR2017-02154, Paper 8 at 10-11 (claims in '844 patent have a November 6, 1997 priority date, after the November 8, 1996 claimed priority date for the '494 patent).

In fact, *Blue Coat* actually undermines Finjan's argument, as it turns upon differences between Claim 10 and the '844 patent. While the '844 Patent claims steps after determining whether or not "suspicious code" may actually be computer virus, Claim 10 recites only a system for generating and storing a list of operations that may or may not be indicative of a virus. Dkt. 564 at 5:18-26 (reciting a system for receiving a "Downloadable" and deriving/storing a list of "suspicious" operations in a database). Claim 10 does not recite ***doing*** anything with this list, much less ***how*** to use the list to detect a virus (via a "behavior-based" process or otherwise). Dkt. 189 (MSJ Order) at 5-8 (the "list of suspicious operations" must be compared against a separate "access control" list to decide whether to pass or fail a Downloadable, but "this important pass-fail step is ***not*** itself recited or reached in Claim 10") (emphasis added). Claim 10 recites only "the familiar progression of acquiring and analyzing information of a desired type to extract results from that information," without even purporting to describe how to extract those results, and is not inventive. *Procter & Gamble Co. v. QuantifiCare Inc.*, 288 F. Supp. 3d 1002, 1027 (N.D. Cal. 2017).

By contrast, the '844 Patent generates a "security profile" that identifies suspicious code, which it then links "to the Downloadable before a web server makes the Downloadable available to web clients"—thus "attach[ing] . . . ***virus scan results to the downloadable in the form of a newly generated file***." *Blue Coat*, 879 F.3d at 1304 (emphasis added). The Federal Circuit found this approach was not abstract because it "allow[ed] access to be tailored for different users and ensures that threats are identified before a file reaches a user's computer." *Id.* at 1305. Because Claim 10 (as this Court has already found) recites only the generation and storage of information, it does not and cannot describe how to generate virus scan results or use those results to allow or deny access to user computers. Dkt. 189 at 19:10-13.

B. Behavior-Based Scanning Was Well-Known, Routine And Conventional.

Even if Claim 10 actually implemented "behavior-based" scanning—which it does not—Finjan's contention that behavior-based malware analysis was new in the computer security field as of 1996 is contrary to the evidentiary record in this case. As one example, Juniper introduced a research paper by David J. Stang published in 1995 that states that "[t]he idea of behavior blocking is not entirely new," and identifies several behavior blockers available in the market as of 1995. Tr. Ex. 1069-6 ("*Smart* behavior blocking has been in use worldwide for several years."). Stang also describes the use of "heuristic" scanning, (*i.e.*, a form of static analysis that looks for suspicious operations or code patterns and can detect unknown viruses), and notes that products employing heuristic analysis had been around for years. *Id.* at 9 ("Products able to do heuristic analysis of static code (*i.e.* a file or sector which was stored on a drive) and conclude whether or not the code contained a virus have been around for years."). Indeed, Morton Swimmer's 1995 research paper confirms in the "Current State of the Art" section that heuristics were already being used to detect

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.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**