UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SYMANTEC CORPORATION, Plaintiff, v. ZSCALER, INC., Defendant.	Case No. 17-cv-04426-JST **ORDER DENYING JUDGMENT ON THE PLEADINGS** Re: ECF No. 190

United States District Court
Northern District of California

Defendant Zscaler, Inc. moves for judgment on the pleadings as to Plaintiff Symantec Corporation's patent infringement claims for claim 1 and claim 5 of U.S. Patent No. 7,735,116 ("the '116 patent") because the claims are directed to patent-ineligible subject matter. ECF No. 190. The Court DENIES the motion for judgment on the pleadings.

I. BACKGROUND

The parties compete in the computer security software field. ECF No. 18 at 5; ECF No. 10 at 5. Symantec alleges that Zscaler's cloud-based security products infringe seven of its patents. ECF No. 139 ¶ 18. In a related case, Symantec alleges that Zscaler's products infringe an additional seven patents. Symantec v. Zscaler, 17-cv-4414-JST, ECF No. 1 ¶ 15. The Court previously granted Zscaler's motion to dismiss two patents in suit on the grounds of ineligibility. ECF No. 173. The Court also granted Zscaler leave to amend its invalidity contentions to assert a contention against the '116 patent. ECF No. 185. The '116 patent generally claims a relational, hierarchical system for sharing security checks between different security functions in a unified threat management ("UTM") system. ECF No. 1-1 at 79.[1]

[1] Symantec asks the Court to consider its second amended complaint ("SAC") in deciding the motion. ECF No. 194 at 8 (citing Aatrix Software, Inc. v. Green Shades Software, Inc., 882 F.3d

United States District Court
Northern District of California

II. LEGAL STANDARD

"After the pleadings are closed—but early enough not to delay trial—a party may move for judgment on the pleadings." Fed. R. Civ. P. 12(c). The analysis for Rule 12(c) motions for judgment on the pleadings is "substantially identical to [the] analysis under Rule 12(b)(6)." Chavez v. United States, 683 F.3d 1102, 1108 (9th Cir. 2012) (citation and quotation marks omitted). "A judgment on the pleadings is properly granted when, taking all the allegations in the non-moving party's pleadings as true, the moving party is entitled to judgment as a matter of law." Fajardo v. Cty. of Los Angeles, 179 F.3d 698, 699 (9th Cir. 1999) (citation omitted); see also Brooks v. Dunlop Mfg. Inc., No. C 10–04341 CRB, 2011 WL 6140912, at *3 (N.D. Cal. Dec. 9, 2011).

Under section 101 of the Patent Act "abstract ideas are not patentable." Alice Corp. Pty. v. *CLS Bank Int'l*, 134 S. Ct. 2347, 2354 (2014). However, "an invention is not rendered ineligible for patent simply because it involves an abstract concept." Id. Courts must distinguish between patents that claim abstract ideas, on the one hand, and patents "that claim patent-eligible applications of those concepts," on the other hand. Id. at 2355. To draw this distinction, courts engage in a two-step analysis.

In step one, courts determine whether the claims at issue are "directed to an abstract idea." Id. at 2356-57. Courts look to whether claims are "directed to a specific improvement" or "to a specific implementation of a solution to a problem." Enfish, LLC v. Microsoft Corp., 822 F.3d 1327, 1338, 1339 (Fed. Cir. 2016). For software patents, this inquiry "often turns on whether the claims focus on 'the specific asserted improvement in computer capabilities'" or "on a process that qualifies as an 'abstract idea' for which computers are invoked merely as a tool." Finjan, Inc. v. Blue Coat Sys., Inc., 879 F.3d 1299, 1303 (Fed. Cir. 2018) (quotation omitted). "The purely functional nature of the claim confirms that it is directed to an abstract idea, not a concrete embodiment of that idea." Affinity Labs of Texas, LLC v. Amazon.com Inc., 838 F.3d 1266, 1269 (Fed. Cir. 2016). A claim that could be performed by a human, excising generic computer

1121, 1125-1130 (Fed. Cir. 2018)). The Court declines this procedurally improper request. Moreover, in a concurrently filed order, the Court denies Symantec's motion for leave to file its SAC.

United States District Court
Northern District of California

implemented steps, is often abstract. Intellectual Ventures I LLC v. Alstom S.A., 838 F.3d 1307, 1318 (Fed. Cir. 2016). The same principle applies to claims that "only contain generalized software components arranged to implement an abstract concept on a computer." Accenture Glob. Servs., GmbH v. Guidewire Software, Inc., 728 F.3d 1336, 1345 (Fed. Cir. 2013).

If the court concludes in step one that the claims are directed to an abstract issue, the court must then "consider the elements of each claim both individually and as an ordered combination" to determine "whether it contains an inventive concept sufficient to transform the claimed abstract idea into a patent-eligible application." Alice, 134 S. Ct. at 2355, 2357 (internal quotation marks omitted). A claim recites an inventive concept "when the claim limitations involve more than performance of well-understood, routine, [and] conventional activities previously known to the industry." Berkheimer v. HP Inc., 881 F.3d 1360, 1367 (Fed. Cir. 2018) (quotation omitted). In some cases, when improvements in the specification are captured in the claims, whether an element or combination of elements is well-understood becomes a question of fact. Id. at 1368-699; see also Cellspin Soft, Inc. v. Fitbit, Inc., No. 17-CV-05928-YGR, 2018 WL 1610690, at *10 n.12 (N.D. Cal. Apr. 3, 2018) (distinguishing Berkheimer where the plaintiff failed "to identify any portion of the specification which describe[d] the purportedly inventive" concept); Uniloc USA, Inc. v. Apple Inc., No. C 18-00358 WHA, 2018 WL 2287675, at *7 (N.D. Cal. May 18, 2018) (same). Both steps are informed by the claims and the specification. See Amdocs (Israel) Ltd. v. Openet Telecom, Inc., 841 F.3d 1288, 1299 (Fed. Cir. 2016).[2]

III. DISCUSSION

The '116 patent is titled "System and Method for Unified Threat Management with a Relational Rules Methodology." ECF No. 1-1 at 79. According to the specification, various kinds of software were developed to guard against a host of different attacks. Id. at 99. The defenses involved included "anti-virus software, anti-spam software, firewalls (both software and

[2] The Federal Circuit has expressed "some doubt" as to whether it is appropriate to dismiss a claim on patent eligibility grounds prior to claim construction. Aatrix Software, Inc. v. Green Shades Software, Inc., 882 F.3d 1121, 1125 (Fed. Cir. 2018). But see MyMail, Ltd. v. ooVoo, LLC, No. 17-CV-04487-LHK, 2018 WL 1367385, at *4 (N.D. Cal. Mar. 16, 2018) (dismissing claims as ineligible without claim construction after Aatrix). The Court need not address that question because it denies the motion for judgment on the pleadings.

hardware), defenses against Denial-of-Service (DOS) attacks, anti-phishing technology, and so forth. Id. These different software-based defenses developed as a "'jumble' of separate programs or appliances," leading to a great deal of complexity and redundancy as IT administrators deployed software with overlapping capabilities. Id. (internal quotation marks in original). The prior art placed those functions together in one UTM on a security gateway, but "security checks [were] invoked at each decision point and the results [were] not shared among security features[,] leading to a duplication of the checks and inefficient processing of rules." Id. at 101. The '116 patent's hierarchical and relational approach to security eliminates this redundancy and "detects and rejects bad data [] as soon as possible." Id. at 102.

A. Claim 1

Claim 1 recites

> A method of controlling access to a networked device, the method comprising:
>
> > receiving an incoming message packet by a security gateway coupled to said networked device;
> >
> > evaluating the received message packet to determine if the received message packet is compliant with a first test, the first test corresponding to a first level of a security hierarchy implemented by said security gateway, wherein the security hierarchy establishes a relationship between security functions from a lowest level to a highest level; and
> >
> > the received packet is rejected at the earliest possible operation in the processing of the packet in the security hierarchy;
>
> forwarding the received packet and an indication of its compliance with the first test for subsequent processing upon the received packet complying with the first test; and
>
> dropping the received packet whereby no further processing of the received packet is performed upon the received packet not complying with the first test.

ECF No. 1-1 at 111.

Zscaler argues claim 1 is abstract because "[s]tripped of computer jargon," it "boils down to . . . functional results: (i) receiv[ing] a packet; (ii) subject[ing] the packet to a first test in a sequence of tests; and then (iii) forward[ing] the packet for further tests if it passes, or else drop[ping] the packet if it fails." ECF No. 190 at 10. Zscaler analogizes the claim to a human resources manager receiving a job application, checking if there are open positions, and dropping the application if not, but checking further for requisite training or experience if so. Id. at 11. Symantec's own description in its brief makes clear that claim 1 addresses an abstract concept: organizing security tests into an information sharing hierarchy. ECF No. 194 at 16 (describing "a security hierarchy that establishes a relationship between security functions, forwarding the packet with an indication of compliance, and rejecting packets at the earliest possible operation"). The Federal Circuit held that "[u]sing organizational and product group hierarchies . . . is an abstract idea that has no particular concrete or tangible form or application. It is a building block, a basic conceptual framework for organizing information, similar to the claims involving collecting, recognizing, and storing data in Content Extraction and the claims in CyberSource." Versata Dev. Grp., Inc. v. SAP Am., Inc., 793 F.3d 1306, 1333–34 (Fed. Cir. 2015) (citing Content Extraction & Transmission LLC v. *Wells Fargo Bank, National Ass'*n, 776 F.3d 1343 (Fed. Cir. 2014); CyberSource Corp. v. Retail Decisions, Inc., 654 F.3d 1366 (Fed. Cir. 2011)). Because claim 1 does nothing more than relate security tests or functions in a hierarchy, and share information, it is abstract. See FairWarning IP, LLC v. Iatric Sys., Inc., 839 F.3d 1089, 1094 (Fed. Cir. 2016) (finding claims "directed to collecting and analyzing information to detect misuse and notifying a user when misuse is detected" abstract because they are "merely directed to a combination of these abstract-idea categories").

However, construing the claims in the manner most favorable to Symantec, Entler v. Gregoire, 872 F.3d 1031, 1043 (9th Cir. 2017); Aatrix Software, Inc. v. Green Shades Software, Inc., 882 F.3d 1121, 1124 (Fed. Cir. 2018), the ordered combination of elements in claim 1 is inventive, at least at this preliminary stage. The specification makes clear that while the method of placing disparate security functions together on a single UTM was in the prior art, organizing that UTM's functions or tests in any relational or hierarchical manner that shared information between the various tests was not. ECF No. 1-1 at 99 (noting disadvantages with known UTM appliances); see also id. at 100-101 (describing that tests were bolted onto UTMs without sharing results between tests). These improvements are captured in claim 1, for example, through language describing that message packets go to a test at "a first level of a security hierarchy," and an indication of compliance passes between tests. ECF No. 1-1 at 111. Based on the patent's discussion of the novelty of a hierarchical organization and information sharing system for UTMs, the "question of whether a claim element or combination of elements is well-understood, routine and conventional to a skilled artisan in the relevant field is a question of fact." Berkheimer, 881 F. 3d at 1368.

B. Claim 5

Claim 5 recites

> A method of controlling access to a networked device, the method comprising:
>
> > receiving a plurality of incoming message packets by a security gateway coupled to said networked device;
> >
> > identifying, at a level of a security hierarchy implemented by said security gateway, a subset of the plurality of incoming message packets as being an attack on the networked device, wherein the security hierarchy establishes a relationship between security functions from a lowest level to a highest level;
> >
> > determining a plurality of indicator parameters of the identified subset of attacking message packets;
> >
> > dynamically defining an attack defense processing rule as a function of the determined plurality of indicator parameters, wherein said attack defense processing rule may be at any level of said security hierarchy; and
> >
> > applying the attack defense processing rule to subsequently received incoming message packets to fend off the identified attack.

ECF No. 1-1 at 111.

Claim 5 adds some detail to the patent's general process, for example by determining indicator parameters for an incoming packet, dynamically defining a rule based on those indicators, and applying that rule to future attacks. Id. Zscaler analogizes the claim to sorting mail: After noting characteristics of unwanted mail, such a bulk-rate stamp, an assistant might develop a rule and throw away mail with that characteristic in the future. ECF No. 190 at 13.

Zscaler's analogy overlooks that the rules are applied hierarchically, but as discussed, a hierarchical arrangement will not keep a claim from abstraction. See *Versata*, 793 F.3d at 1333–34; see also *Fitbit Inc. v. AliphCom*, No. 16-CV-00118-BLF, 2017 WL 819235, at *10 (N.D. Cal. Mar. 2, 2017), *reconsideration denied*, No. 16-CV-00118-BLF, 2017 WL 3129989 (N.D. Cal. July 24, 2017) (finding abstract the "general idea of data collection and reporting, but just applied in the narrower context of reporting cumulative activity level").

Symantec argues the claim is not abstract because it dynamically defines rules at specific levels in the hierarchy and applies those rules in subsequent attacks. ECF No. 194 at 23 (explaining the "multi-layered approach" "establishes a relationship between security functions from a lowest level to a highest level"). Nothing in the patent, however, describes in what way dynamically defining improves functionality, both because the phrase fails to describe how it dynamically defines, and because it does not explain that dynamically defining improves any computer function. Symantec also argues that by "dynamically defining" a rule, claim 5 can "fend off a newly identified attack." ECF No. 194 at 25. But neither Symantec's reference nor the Court's own review reveals patent text that supports this argument. See ECF No. 194 at 22 (asserting "[t]he solution to the problem of fending off newly identified threats is captured in Claim 5" without describing at all that, or how, claim 5 identifies new threats); ECF No. 1-1 at 111. In *Finjan*, the Federal Circuit concluded that a patent that behaviorally scanned a downloadable file, and attached the scan results to that file, was not abstract because behavior-based scanning improved computer functionality, and attaching the result allowed for "granular information about potentially suspicious code." *Finjan*, 879 F.3d at 1304. Claim 5 here is distinguishable from the claim at issue in *Finjan* because that patent claimed a specific method, behavioral scanning and attaching, to improve functionality and to avoid abstraction, whereas here the patent simply describes a result: hierarchical scanning. *Id.* at 1304-1305 (distinguishing the non-abstract patent because it specifically describes how the result is carried out).[3] On

[3] The phrase or term that comes closest to explaining "how" in claim 5 is "dynamically defining." ECF No. 1-1 at 111. The Court will soon construe this term following a *Markman* hearing. The Court's conclusion that claim 5 is abstract is only bolstered by Symantec's proposal to either not construe dynamically define, or alternatively to define it as "in response to the attack," neither of

balance, claim 5 is abstract.

But at this procedural stage, the claim is saved at the inventiveness step. Unlike claim 1, claim 5 fails to capture one of the ’116 patent’s purported inventive features: sharing information between the related tests or functions. ECF No. 1-1 at 100-101. Claim 5 says nothing about information sharing. Id. at 111. But it may be that the security hierarchy alone improved on the prior art. See ECF No. 1-1 at 101 [specification] (“Advantageously, the security hierarchy facilitates configurable degrees of security protection.”); id. (“[T]he URR provides for dropping undesired traffic at the earliest point of the security hierarchy.”). As Symantec explains, by utilizing a hierarchy, the ’116 patent rejects data as soon as possible, which improves upon prior UTMs which always scanned each of several tests. ECF No. 194 at 29. Like claim 1, claim 5 captures the specification’s claimed improvement in the form of setting up a relational, hierarchical system for uniting the various functions. ECF No. 1-1 at 111 (“[T]he security hierarchy establishes a relationship between security functions from a lower level to a highest level[.]”). At the least, the specification raises an issue of fact as to inventiveness. See Berkheimer, 881 F. 3d at 1368.

CONCLUSION

For the aforementioned reasons, the Court DENIES Zscaler’s motion for judgment on the pleadings.

IT IS SO ORDERED.

Dated: July 23, 2018

Jon S. Tigar

JON S. TIGAR
United States District Judge

which offers guidance on how the result of hierarchical scanning is carried out. ECF No. 145-1 at 5-6.