IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

GOSECURE, INC. Plaintiff, v. CROWDSTRIKE, INC., and CROWDSTRIKE HOLDINGS, INC. Defendants.	)))))))))))	**Case No. 1:24-cv-00526-DII**

PLAINTIFF'S OPPOSITION TO DEFENDANTS' MOTION TO DISMISS

TABLE OF CONTENTS

I. Introduction 1

II. Background 1

A. Technological Problems With Existing Computer Network Security Systems 2

B. The Patentee's Specific Technological Solution 2

III. Legal Standards 5

A. Motions To Dismiss Under Rule 12(b)(6) 5

B. Patent-Eligibility Under 35 U.S.C. § 101 5

IV. The Patents Claim Eligible Subject Matter Under 35 U.S.C. § 101 7

A. *Alice* Step 1: The Independent Claims Recite Improved Network Technology 7

B. *Alice* Step 2: The Independent Claims Add An Inventive Concept 14

C. The Dependent Claims Provide Additional Details Supporting Eligibility 16

V. GoSecure's Complaint Plausibly Alleges Infringement 17

VI. GoSecure's Complaint Plausibly Alleges Pre-suit Indirect and Willful Infringement 19

VII. If Necessary, GoSecure Requests Leave To Amend 20

TABLE OF AUTHORITIES

Page(s)

CASES

Aatrix Software, Inc. v. Green Shades Software, Inc.,
882 F.3d 1121 (Fed. Cir. 2018)..... 6, 16, 20

Alice Corp. v. CLS Bank Int'l,
573 U.S. 208 (2014).....5, 6

Amdocs (Israel) Ltd. v. Openet Telecom, Inc.,
841 F.3d 1288 (Fed. Cir. 2016)..... 14, 15

Ancora Techs., Inc. v. HTC America, Inc.,
908 F.3d 1343 (Fed. Cir. 2018)..... 11, 14

Ashcroft v. Iqbal,
556 U.S. 662 (2009).....5

Bascom Global Internet Servs. v. AT&T Mobility,
827 F.3d 1341 (Fed. Cir. 2016).....6, 15

Berkheimer v. HP Inc.,
881 F.3d 1360 (Fed. Cir. 2018).....6

Bot M8 LLC v. Sony Corp. of Am.,
4 F.4th 1342 (Fed. Cir. 2021) 17, 18

CardioNet, LLC v. InfoBionic, Inc,
955 F.3d 1358 (Fed. Cir. 2020)..... 17

Cellspin Soft, Inc. v. Fitbit, Inc.,
927 F.3d 1306 (Fed. Cir. 2019).....16

Contiguity, LLC v. Conduent Bus. Servs., LLC,
No. 23-cv-00038-XR, 2024 WL 252068 (W.D. Tex. Jan. 22, 2024).....19

Cooperative Entertainment, Inc. v. Kollective Tech., Inc.,
50 F.4th 127 (Fed. Cir. 2022) 16

CosmoKey Sols. GmbH & Co. KG v. Duo Sec. LLC,
15 F.4th 1091 (Fed. Cir. 2021) 1, 6, 15

Cuvillier v. Taylor,
503 F.3d 397 (5th Cir. 2007).....5

DDR Holdings, LLC v. Hotels.com, L.P.,
773 F.3d 1245 (Fed. Cir. 2014).....15

Electric Power Grp., LLC v. Alstom S.A.,
830 F.3d 1350 (Fed. Cir. 2016).....12

Enfish, LLC, v. Microsoft Corp.,
822 F.3d 1327 (Fed. Cir. 2016)..... 6, 7, 12

Finjan, Inc. v. Blue Coat Sys., Inc.,
879 F.3d 1299 (Fed. Cir. 2018).....*passim*

Global-Tech Appliances, Inc. v. SEB S.A.,
563 U.S. 754 (2011).....19

In re Katrina Canal Breaches Litig.,
495 F.3d 191 (5th Cir. 2007).....5

In re Killian,
45 F.4th 1373 (Fed. Cir. 2022) 12

Int'l Bus. Machines Corp. v. Zillow Grp., Inc.,
50 F.4th 1371 (Fed. Cir. 2022) 12

Intellectual Ventures I LLC v. Symantec Corp.,
838 F.3d 1307 (Fed. Cir. 2016).....13

Invs. LDC v. Phillips,
401 F.3d 638, 641 (5th Cir. 2005) 18

Koninklijke KPN N.V. v. Gemalto M2M GmbH,
942 F.3d 1143 (Fed. Cir. 2019).....11

Lone Star Fund V (U.S.), L.P. v. Barclays Bank PLC,
594 F.3d 383 (5th Cir. 2010).....5

MAZ Encryption Techs. LLC v. BlackBerry Ltd.,
No. 6:15-CV-1167, 2016 WL 9275008 (E.D. Tex. June 7, 2016), 2016 WL
9275397 (June 27, 2016).....18

Mobile Acuity Ltd. v. Blippar Ltd.,
--- F.4th ----, 2024 WL 3659127 (Fed. Cir. 2024).....16

Monolithic Power Sys., Inc. v. Silergy Corp.,
127 F. Supp. 3d 1071 (N.D. Cal. 2015).....20

Nalco Co. v. Chem-Mod, LLC,
883 F.3d 1337 (Fed. Cir. 2018).....17

Network Sys. Techs., LLC v. Qualcomm Inc.,
No. 1:22-cv-01331, 2023 WL 11833572 (W.D. Tex. July 21, 2023).....19

Packet Intelligence LLC v. NetScout Sys., Inc.,
965 F.3d 1299 (Fed. Cir. 2020) 11

Pederson v. Zoho Corp.
No. 1:23-cv-71-DII, 2023 WL 3612333 (W.D. Tex. May 23, 2023) 18

PersonalWeb Techs. LLC v. Google LLC,
8 F.4th 1310 (Fed. Cir. 2021) 12

Repairify, Inc. v. Keystone Auto. Indus., Inc.,
610 F. Supp. 3d 897 (W.D. Tex. 2022) 17

SRI Int'l, Inc. v. Cisco Sys., Inc.,
930 F.3d 1295 (Fed. Cir. 2019) ..... *passim*

Thales Visionix Inc. v. United States,
850 F.3d 1343 (Fed. Cir. 2017) 6

Trinity Info Media, LLC v. Covalent, Inc.,
72 F.4th 1355 (Fed. Cir. 2023) 12

Turner v. Pleasant,
663 F.3d 770 (5th Cir. 2011) 5

Ubiquitous Connectivity, LP v. City of San Antonio,
No. SA-18-cv-718, 2019 WL 4696421 (W.D. Tex. Sept. 26, 2019) 20

Uniloc USA, Inc. v. LG Elecs. USA, Inc.,
957 F.3d 1303 (Fed. Cir. 2020) 11

Vervain, LLC v. Micron Tech., Inc.,
No. 6:21-cv-00487, 2022 WL 23469 (W.D. Tex. Jan. 3, 2022) 18

Visual Memory LLC v. NVIDIA Corp.,
867 F.3d 1253 (Fed. Cir. 2017) 14

Weisner v. Google LLC,
51 F.4th 1073 (Fed. Cir. 2022) 15

STATUTES

35 U.S.C. § 101 ..... *passim*

RULES

FED. R. CIV. P. 15(a)(2) 20

FED. R. CIV. P. 12(b)(6) 5, 6

I. INTRODUCTION

Plaintiff GoSecure, Inc. ("GoSecure") alleges that Defendants CrowdStrike, Inc. and CrowdStrike Holdings, Inc.'s (collectively, "CrowdStrike") infringe U.S. Pat. Nos. 9,954,872 and 9,106,697 ("Asserted Patents"). CrowdStrike moves to dismiss (D.I. 21) on three grounds. Each fails.

First, CrowdStrike argues that the Asserted Patents' claims amount to nothing more than an abstract idea—"collecting, storing, and sharing information"—not a technological improvement warranting patent protection under 35 U.S.C. § 101. CrowdStrike is incorrect. The Asserted Patents claim inventions that improve computer security using unconventional techniques and data structures to address specific technical problems involved in endpoint detection and response. The Federal Circuit has repeatedly found such claims eligible under § 101 as a matter of law. *See*, *e.g.*, *SRI Int'l, Inc. v. Cisco Sys., Inc.*, 930 F.3d 1295, 1304 (Fed. Cir. 2019) (improved network security claims); *Finjan, Inc. v. Blue Coat Sys., Inc.*, 879 F.3d 1299, 1303-04 (Fed. Cir. 2018) (improved behavior-based virus monitoring claims); *CosmoKey Sols. GmbH & Co. KG v. Duo Sec. LLC*, 15 F.4th 1091, 1097-98 (Fed. Cir. 2021) (improved authentication claims). The same conclusion follows here. At minimum, GoSecure's claims are plausibly eligible and raise factual issues that preclude dismissal at this stage.

Second, CrowdStrike contends that GoSecure failed to plead facts sufficient to make infringement plausible. But GoSecure provided a limitation-by-limitation analysis, based primarily on descriptions of the accused functionality provided in CrowdStrike's own publicly available documents, readily satisfying the pleading standard.

Third, CrowdStrike argues that the Complaint fails to allege pre-suit knowledge, but the Complaint includes facts that, at minimum, raise a plausible inference of willful blindness.

II. BACKGROUND

The Asserted Patents, each entitled "System and method for identifying unauthorized activities on a computer system using a data structure model," are directed to improved technology for

"protecting computer networks." '872 patent at 1:44-48.[1] Stemming from a non-provisional application filed in 2011, which in turn claims priority to a provisional application filed in 2010, the '697 patent issued in 2015 and the '872 patent issued as a continuation in 2018.

A. Technological Problems With Existing Computer Network Security Systems

"[N]etworked computers are … vulnerable to attacks, unwanted intrusions, and unauthorized access" by malicious computer programs such as malware. '872 patent at 1:53-57. The specification explains that prior anti-malware and network security systems—such as firewalls—suffered significant drawbacks because they focused on stopping known threats by matching "low-level IP data packets" against a preexisting database of "malware fingerprints." *Id.* at 1:58-2:8. But those conventional systems remained vulnerable to unknown threats: "A critical threat to computer networks is the so-called zero-day attack that exploits security vulnerabilities previously unknown …." *Id.* at 2:9-11. Likewise, because they relied on "match[ing]" fingerprints, conventional systems were vulnerable to slight modifications in malicious code, which would not be recognized. *Id.* at 2:5-8. GoSecure, therefore, saw "a great need for efficient methods of identifying fingerprint data for previously unknown types of malicious and/or unauthorized activities." *Id.* at 2:20-23. However, "identifying the fingerprints of malicious activities in the middle of numerous other non-malicious processes is not a trivial task." *Id.* at 2:17-19.

B. The Patentee's Specific Technological Solution

The patentee solved that technological problem with specific techniques to prevent unauthorized activities by "monitoring and identifying associations between activity sources and activity targets without using pre-determined fingerprints" and propagating that information across the network to protect other devices. '872 patent at 3:11-16; D.I. 1 ¶¶ 39-44.

[1] The patents share a common specification; parallel citations are omitted for brevity.

The '872 patent describes a series of inventive steps to that end. First, the invention monitors activity directly on the computer system (e.g., an endpoint device such as a laptop, desktop, or server) using a module that is integrated with the operating system. *Id.* at 4:15-21, 6:35-43, cl. 2 ("monitoring all activity on the first computer system"). The invention thereby shifts the focus of malware detection away from relying on libraries of fixed signatures (used by conventional systems) to monitoring activity directly on endpoint devices. *Id.* at 10:8-11. Second, the invention identifies activities based on "an activity source, an activity target, and an association between the activity source and the activity target." *Id.* at 15:25-33. By focusing on significant events and chains of activities (defined by associations between respective activity sources and activity targets), the invention takes a dynamic behavior-based approach to addressing threats, as opposed to the conventional approach of comparing in-bound data packets to fixed signatures. *Id.* at 1:58-2:31, 19:24-30. Third, the invention stores the activity in a specific, particularized data structure that identifies the activity sources, the activity targets, and the associations. *Id.* at 13:65-14:20. In doing so, the invention provides inventive techniques for processing and utilizing the vast amounts of data generated by monitoring all activity at a computer system. *Id.* at 16:5-7 ("time or sequence-based filters"). Fourth, the invention shares the newly-created security information with other computer systems "to prevent future attacks on the computer system or other computer systems, by blocking activity sources that match a pattern of unauthorized activities." *Id.* at 14:43-50.

Both patents claim these improvements. For example, claim 1 of the '872 patent recites:

> **1.** A computer implemented method of identifying unauthorized activities on a first computer system attached to a computer network, wherein the first computer system comprises one or more processors and memory, the method comprising:
>
> monitoring activity on the first computer system;
>
> identifying a plurality of activities being performed at the first computer system, wherein each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target;

> storing in the memory a data structure that identifies the activity sources, the activity targets, and the associations for the plurality of activities; and
>
> transmitting to one or more computer systems other than the first computer system information identifying one or more of the activity sources, the activity targets, and the associations for preventing future attacks, to the one or more computer systems, associated with the one or more of the activity sources, the activity targets, and the associations.

Other embodiments further disclose a computer system with a "virtual machine" to "lure[]" an attacker into revealing itself. '872 patent at 9:14-56. By using a separate "virtual machine monitor" to monitor the activity occurring on the virtual machine, the invention makes it "difficult for an attacker … to determine whether [it] is being monitored." *Id.* at 6:53-57. The '697 patent claims these additional improvements. For example, claim 1 provides:

> **1.** A computer implemented method of identifying unauthorized activities on a decoy computer system attached to a computer network, wherein the decoy system comprises:
>
> one or more processors; and
>
> memory storing:
>
> a virtual machine; and
>
> a virtual machine monitor supervising the virtual machine, the method comprising, at the virtual machine monitor:
>
> monitoring activity on the virtual machine;
>
> identifying a plurality of activities being performed at the virtual machine, wherein each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target;
>
> storing in the memory the activity sources, activity targets, and associations;
>
> creating, from the stored activities, a fingerprint indicative of the activity on the virtual machine; and
>
> transmitting the fingerprint to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint.

The independent claims are not representative of the *dependent* claims, which provide additional material structural limitations. *See* '872 patent cls. 2-19; '697 patent cls. 2-18, 21-23; D.I. 1 ¶¶ 42, 44; *infra* at 16.

III. LEGAL STANDARDS

A. Motions To Dismiss Under Rule 12(b)(6)

"To survive a Rule 12(b)(6) motion to dismiss, a complaint does not need detailed factual allegations, but must provide the plaintiff's grounds for entitlement to relief—including factual allegations that when assumed to be true raise a right to relief above the speculative level." *Cuvillier v. Taylor*, 503 F.3d 397, 401 (5th Cir. 2007).[2] In deciding a 12(b)(6) motion, a "court accepts all well-pleaded facts as true, viewing them in the light most favorable to the plaintiff." *In re Katrina Canal Breaches Litig.*, 495 F.3d 191, 205 (5th Cir. 2007). "The court's task is to determine whether the plaintiff has stated a legally cognizable claim that is plausible, not to evaluate the plaintiff's likelihood of success." *Lone Star Fund V (U.S.), L.P. v. Barclays Bank PLC*, 594 F.3d 383, 387 (5th Cir. 2010). Thus, a complaint need only "contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (cleaned up). "[A] motion to dismiss under 12(b)(6) is viewed with disfavor and is rarely granted." *Turner v. Pleasant*, 663 F.3d 770, 775 (5th Cir. 2011) (cleaned up).

B. Patent-Eligibility Under 35 U.S.C. § 101

Section 101 of the Patent Act provides that "[w]hoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title." 35 U.S.C. § 101. Section 101 includes an implicit exception for abstract ideas, but claims that "purport to improve the functioning of the computer itself" or "effect an improvement" in "technology or [a] technical field" are eligible under § 101. *Alice Corp. v. CLS Bank Int'l*, 573 U.S. 208, 225 (2014). The two-part *Alice* framework governs eligibility. *Id.* at 217-18.

---

[2] All emphasis added and internal quotations omitted unless otherwise noted.

At *Alice* step one, the Court determines whether the patent's "claimed advance" is "directed to an abstract idea" or instead focuses on a "specific asserted improvement" in technology. *Finjan*, 879 F.3d at 1303 (cleaned up); *see Alice*, 573 U.S. at 218. This step is a "meaningful one": "a substantial class of claims are not directed to a patent-ineligible concept." *Enfish, LLC, v. Microsoft Corp.*, 822 F.3d 1327, 1335 (Fed. Cir. 2016). Importantly, the Court must not "describ[e] the claims at such a high level of abstraction and untethered from the language of the claims" lest "the exceptions to § 101 swallow the rule." *Id.* at 1337. The Court must "articulate what the claims are directed to with enough specificity to ensure the step one inquiry is meaningful." *Thales Visionix Inc. v. United States*, 850 F.3d 1343, 1347 (Fed. Cir. 2017). If the claims are not abstract at step one, the inquiry ends and the claims are eligible. *See, e.g.*, *SRI*, 930 F.3d at 1304.

At *Alice* step two, even if the claims are directed to an abstract idea, they are eligible if their elements individually or in combination add an "inventive concept," such as technology that is not well-understood, routine, or conventional at the time of the invention. *Alice*, 573 U.S. at 218 n.3; *Bascom Global Internet Servs. v. AT&T Mobility*, 827 F.3d 1341, 1352 (Fed. Cir. 2016). "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," which CrowdStrike must "prove[] by clear and convincing evidence." *Berkheimer v. HP Inc.*, 881 F.3d 1360, 1368 (Fed. Cir. 2018). Thus, plausible allegations about those facts must be accepted as true at this stage, and "prevent dismissal pursuant to Rule 12(b)(6)." *Aatrix Software, Inc. v. Green Shades Software, Inc.*, 882 F.3d 1121, 1130 (Fed. Cir. 2018).

Applying *Alice*, the Federal Circuit routinely holds eligible claims that improve network and computer security technology. *See*, *e.g.*, *SRI*, 930 F.3d at 1303-04 (network monitoring); *Finjan*, 879 F.3d at 1303 (behavior-based virus monitoring); *CosmoKey*, 15 F.4th at 1097-98 (authentication technology).

IV. THE PATENTS CLAIM ELIGIBLE SUBJECT MATTER UNDER 35 U.S.C. § 101

The Asserted Claims are directed to a specific technological improvement in computer security, which is non-abstract and eligible at *Alice* step one. They separately add something inventive and, thus, are also eligible at *Alice* step two. At minimum, factual issues preclude dismissal because, with the facts construed in GoSecure's favor, the Asserted Claims are at least plausibly patent-eligible.

A. *Alice* Step 1: The Independent Claims Recite Improved Network Technology

At *Alice* step one, the inquiry turns on "whether the claims focus on 'the specific asserted improvement in computer capabilities ... or, instead, on a process that qualifies as an abstract idea for which computers are invoked merely as a tool.'" *Finjan*, 879 F.3d at 1303 (quoting *Enfish,* 822 F.3d at 1336).

1. The Claims Solve A Technological Problem With A Specific Improvement In Computer Security Technology

GoSecure's patent claims are eligible at step one, not abstract, because they address a technological problem—security vulnerabilities in conventional systems—with a specific technological solution. *Supra* at 2-4. Conventional systems were vulnerable because they relied on components, such as firewalls, that identified threats by matching computer activities against a predetermined database of known malware fingerprints. '872 patent at 1:57-2:8. Those conventional approaches were ineffective against previously *unknown* malware—so-called "zero-day" attacks. *Id.* at 2:9-11. Moreover, reliance on "match[ing]" fixed signatures left conventional systems blind to threats that were able to react and evade such relatively rudimentary security techniques. *Id.* at 2:20-23. The Asserted Patents address that technological problem by departing from the traditional approach and instead performing behavioral analysis on the fly using a series of specific steps on an endpoint device. *Id.* at 19:31-37.

For example, claim 1 of '872 patent recites an improved way of "identifying unauthorized activities" by: (1) monitoring activity directly on the network-connected "computer system" (an

endpoint device), thereby shifting the focus of malware detection away from relying on libraries of fixed signatures (as in conventional systems); (2) identifying activities based on "an activity source, an activity target, and an association between the activity source and the activity target," thereby taking a behavior-based approach that, again, does not rely on matching attacks to fixed signatures; (3) storing information about the activities in a particular "data structure"; and (4) transmitting that information to other computers on the network to "prevent[] future attacks." '872 patent, cl. 1; *see supra* at 3; D.I. 1 ¶¶ 39-44.

Claim 1 of the '697 patent recites those same improvements, but goes further. *Supra* at 4. That claim recites a system with a "virtual machine" and a "virtual machine monitor" that identifies threats using the techniques described. *See* '697 patent, cl. 1. This additional detail provides two more security benefits, per the specification. First, the invention can "lure[]" an attacker into revealing itself: although the virtual machine behaves like a normal, fully-functional operating system, it is monitoring the attacker's behavior and generating a new fingerprint on the fly. '872 patent at 9:14-56. Second, the use of a "virtual machine monitor" makes it "difficult for an attacker accessing the decoy operating system to determine whether [it] is being monitored." *Id.* at 7:43-58. These additional departures from traditional approaches provide additional technological solutions to the security vulnerabilities in conventional systems. *See supra* at 2-4; D.I. 1 ¶¶ 39-44. Consequently, all claims of the Asserted Patents are directed to patent-eligible improvements in technology, not abstract ideas.

2. The Claims Are Patentably Indistinguishable From The Claims The Federal Circuit Held Eligible In *SRI* And Other Cases

The Federal Circuit routinely holds that claims providing improved network technology and computer security are non-abstract (and thus eligible) at *Alice* step one. GoSecure's claims fall in that eligible subject matter bucket. In *SRI*, technological problem for example, the claims improved network security using "network monitors" to "detect[] … suspicious network activity based on analysis of network traffic data"; "generat[e] … reports of said suspicious activity"; and "receiv[e] and

integrat[e] the reports of suspicious activity." 930 F.3d at 1301; *see* Ex. 1 (eligible claim in *SRI*). The Federal Circuit held that the claims were non-abstract because they "are directed to using a specific technique—using a plurality of network monitors that each analyze specific types of data on the network and integrating reports from the monitors—to solve a technological problem arising in computer networks: identifying hackers or potential intruders into the network." *Id.* at 1303. That is, "[t]he 'focus of the claims is on the specific asserted improvement in computer capabilities'"—"providing a network defense system that monitors network traffic in real-time to automatically detect large-scale attacks." *Id.* In reaching that conclusion, the court relied on the specification's discussion of vulnerabilities in conventional networks and the claims' provision of a "framework" to improve network security. *Id.*

The claims here are eligible at step one for the same reasons. Like in *SRI*, GoSecure's claims seek to address a "technological problem" in computer system security, as the specification confirms. *Id.*; *see* '872 patent at 1:44-48. Like in *SRI*, the claims recite a "specific asserted improvement in computer capabilities" (there, using multiple network monitors to detect large scale attacks; here, monitoring activity on a network computer to detect previously-unknown attacks). 930 F.3d at 1303. And like in *SRI*, the claims here recite a series of steps to accomplish that goal (there, monitoring certain information to detect suspicious activity, generating reports, and receiving reports across the network; here, monitoring certain information about activity sources and targets, generating associations between activity and targets, storing that information in data structures, and propagating the information across the network). *Id.* Therefore, for the same reasons as in *SRI*, the claims here are eligible at *Alice* step one.

The Federal Circuit's decision in *Finjan* is also very close on the facts. 879 F.3d at 1303-05. There, the claims were brief, reciting:

> **1**. A method comprising:
> receiving by an inspector a Downloadable;

> generating by the inspector a first Downloadable security profile that identifies suspicious code in the received Downloadable; and
>
> linking by the inspector the first Downloadable security profile to the Downloadable before a web server makes the Downloadable available to web clients.

Id. at 1303; *see* Ex. 1. The court held the *Finjan* claims eligible because they sought to improve computer security with a particular "behavior-based" approach to identifying threats, rather than the conventional approach of matching against known threats. 879 F.3d at 1303-04. As the court explained, "traditional, 'code-matching' virus scans [were] limited to recognizing the presence of previously-identified viruses, typically by comparing the code … to a database of known suspicious code." *Id.* at 1304. In contrast, the patented invention "provid[ed] computer security by scanning a downloadable and attaching the results of that scan to the downloadable itself in the form of a 'security profile'"—"a new kind of file that enables a computer security system to do things it could not do before." *Id.* at 1304-05. And this improved technique "can be used to protect against previously unknown viruses as well as 'obfuscated code'—known viruses that have been cosmetically modified to avoid detection by code-matching virus scans." *Id.* at 1305. Therefore, the claims were eligible.

Similarly, the claims here depart from the "traditional" approach of "matching" against "previously-identified" malware in a database of "known" fingerprints, instead reciting a "behavior-based" approach to identify unknown or modified threats. *Id.* at 1303-05. Also, like the "security profile" in *Finjan*, the claims here monitor, store, and distribute particular information about potential threats ("an activity source, an activity target, and an association between the activity source and the activity target," *e.g.*, '872 patent cl. 1). That information "enables a computer security system to do things it could not do before." *Finjan*, 879 F.3d at 1305. As in *Finjan*, this allows for "more flexible and nuanced" detection of computer threats. *Id.* at 1304. Therefore, the claims here are just as eligible as—indeed, more detailed than—the claims in *Finjan*.

Ancora Techs., Inc. v. HTC America, Inc., 908 F.3d 1343, 1348 (Fed. Cir. 2018), is also instructive. There, the claims were eligible at step one because they sought to "[i]mprov[e] security … against a computer's unauthorized use of a program" with "a specific technique that departs from earlier approaches." *Id.* at 1348. The *Ancora* claims "addresse[d] a technological problem with computers: vulnerability of license-authorization software to hacking" by verifying authorization using "a structure containing a license record [that] is stored in a particular, modifiable, non-volatile portion of the computer's BIOS," unlike prior systems. *Id.* at 1348-49. Similarly, the claims here "depart[] from earlier approaches," *id.*, shifting away from fixed signatures by identifying and storing particular activity information on endpoint devices. *Supra* at 7-8. Also, as discussed, the '697 patent claims further recite a particular structure (a virtual machine and a virtual machine monitor) that enhances security by ensnaring attackers in a way that makes it more difficult for attackers to know they are being watched. *Supra* at 8. Like in *Ancora*, therefore, the security-enhancing techniques claimed here are eligible at *Alice* step one.

Other Federal Circuit decisions confirm that claims aimed at improving security or network communication technology were eligible at *Alice* step one. In *Packet Intelligence LLC v. NetScout Sys., Inc.*, 965 F.3d 1299, 1309-10 (Fed. Cir. 2020), the eligible claims "purport[ed] to meet a challenge unique to computer networks"—"disjointed connection flows in a network environment"—and "solve[d] [that] technological problem" by identifying and associating conversation flows. This allowed "more granular, nuanced, and useful classification of network traffic," which improved the ability to "diagnose network congestion" and "identify intrusions and malicious attacks." *Id.* at 1308-10. In *Uniloc USA, Inc. v. LG Elecs. USA, Inc.*, 957 F.3d 1303, 1305-06 (Fed. Cir. 2020), the claims were eligible because they "improve[d] conventional communication systems" by including an additional data field in the communication activation process. And in *Koninklijke KPN N.V. v. Gemalto M2M GmbH*, 942 F.3d 1143, 1151 (Fed. Cir. 2019), the claims were eligible because they "employ[ed]

new way of generating check data that enables the detection of persistent systematic errors in data transmissions that prior art systems were previously not equipped to detect." The claims here are similarly non-abstract and eligible at *Alice* step one.

3. CrowdStrike's Step One Arguments Are Untethered From The Claim Language And Contrary To Federal Circuit Precedent

CrowdStrike ignores this substantial, dispositive body of binding precedent. Instead CrowdStrike argues that the claims are directed to the abstract idea of "collecting, storing, and sharing information." Mot. 5-11. But that improperly describes the invention at "a high level of abstraction and untethered from the language of the claims." *Enfish*, 822 F.3d at 1337. In particular, CrowdStrike makes four arguments at step one; each fails.

First, CrowdStrike principally argues that claim 1 of the '872 patent is analogous to the claims in *Electric Power Grp., LLC v. Alstom S.A.*, 830 F.3d 1350 (Fed. Cir. 2016), and recites generic steps for collecting and processing data. Mot. at 5-7. Not so. In *Electric Power*, the claims did not purport to provide any "improvement in computers" themselves, and instead sought to provide "'humanly comprehensible' … information useful for users." 830 F.3d at 1354-55.[3] In fact, the Federal Circuit in *SRI* rejected the same argument CrowdStrike makes here: "the *Electric Power* claims were drawn to using computers as tools to solve a power grid problem, rather than improving the functionality of computers and computer networks themselves" like the *SRI* claims. *SRI*, 930 F.3d at 1304. The *SRI* claims "prevent[ed] the normal, expected operation of a conventional computer network" using specific techniques for monitoring, identifying, and propagating security threat information in a way that improved network functionality. So too here. *Supra* at 7-8.

---

[3] Likewise, in the other cases CrowdStrike cites, the claims did not improve computer technology but instead used computers as tools to perform abstract concepts, such as collecting and displaying data or otherwise automating human-performable activities. *See, e.g.*, *Trinity Info Media, LLC v. Covalent, Inc.*, 72 F.4th 1355, 1364 (Fed. Cir. 2023); *Int'l Bus. Machines Corp. v. Zillow Grp., Inc.*, 50 F.4th 1371, 1378 (Fed. Cir. 2022); *In re Killian*, 45 F.4th 1373, 1382 (Fed. Cir. 2022); *PersonalWeb Techs. LLC v. Google LLC*, 8 F.4th 1310, 1316 (Fed. Cir. 2021); Mot. at 5-11.

Second, CrowdStrike argues that claim 1 of the '872 patent is "recited functionally, with no technical details" and notes that it "is less lengthy and less detailed" than the ineligible claim in *Electric Power*. Mot. at 8, 6 n.2 (citing Mot. Ex. C). That is a red herring. Claim 1 of the '872 patent is *more* detailed than the claims the Federal Circuit found eligible in cases such as *SRI*, *Finjan*, *Ancora*, and *Uniloc*. *See* Ex. 1. Claim 1 of the '697 patent is still more detailed. Just as the claims in those cases had sufficient detail, so too do the claims here. The § 101 analysis is not a word-counting exercise, but instead looks to the fundamental character of the claims. The claims in *Electric Power*, while verbose, were abstract because they sought to collect and present information to improve human user activities or used computers as mere tools. On the other hand, the shorter claims in cases such as *SRI*, *Finjan*, and others were eligible because they sought to improve network and computer technology itself with a sufficiently particular solution. GoSecure's claims are in the latter category.

Third, CrowdStrike argues that "monitoring" and the other claim steps "can be performed in the human mind or using a pencil and paper" and likens the claims to the ones found ineligible in *Intellectual Ventures I LLC v. Symantec Corp.*, 838 F.3d 1307 (Fed. Cir. 2016). Mot. at 7-8. *SRI* rejected that argument as well, because "the human mind is not equipped to detect suspicious activity by using network monitors and analyzing network packets as recited by the claims." *SRI*, 930 F.3d at 1305 (distinguishing *Symantec*). The same is true here.

Fourth, CrowdStrike argues that claim 1 of the '697 patent is not materially different from claim 1 of the '872 patent. Mot. at 9-11. That is incorrect. As discussed, claim 1 of the '697 patent provides two additional security benefits: (1) the ability to "lure[]" an attacker to identify unauthorized access and generate a new fingerprint on the fly, and (2) using a "virtual machine monitor" (a distinct component that CrowdStrike does not address) to make it "difficult for an attacker accessing the decoy operating system to determine whether [it] is being monitored." '872 patent at 9:14-56, 7:43-58; *see supra* at 8; D.I. 1 ¶¶ 39-44. The specification explains that these limitations provide additional

technological improvements, confirming that claim 1 of the '697 patent is non-abstract at step one. *See Ancora*, 908 F.3d at 1348-49 (holding claims non-abstract at step one based on unconventional use of computer memory to enhance computer security); *Visual Memory LLC v. NVIDIA Corp.*, 867 F.3d 1253 (Fed. Cir. 2017). Because the claims are not directed to an abstract idea at step one, the inquiry ends and the Court need not address step two. *See, e.g.*, *SRI*, 930 F.3d at 1304.

B. *Alice* Step 2: The Independent Claims Add An Inventive Concept

Even if the claims were directed to CrowdStrike's proposed abstract idea of "collecting, storing, and sharing information" at step one (they are not), they are eligible at step two because the limitations provide an inventive concept both "in the recited components individually as well as in their arrangement and interaction with one another as a system." *Amdocs (Israel) Ltd. v. Openet Telecom, Inc.*, 841 F.3d 1288, 1299-1301, 1318 (Fed. Cir. 2016); *see* D.I. 1 ¶¶ 39-44.

CrowdStrike contends the claims recite only the abstract idea itself and conventional activity. Mot. at 11-15. That is incorrect. Apart from data collection, storage, and sharing, the claims use techniques that the specification explains are unconventional. ***First***, the claims recite monitoring activity directly on an endpoint computer, instead of the conventional approach of relying on libraries of fixed signatures. The specification teaches that is a non-conventional technological technique. '872 patent at 1:44-2:31, 3:11-16, 6:35-43. ***Second***, the claims monitor associations between activity sources and activity targets, which was an unconventional approach that allowed for activity to be monitored over time or across multiple operating systems (*id.* at 16:5-7, 19:24-30). ***Third***, the invention propagates that dynamically-identified behavioral information to other devices to enhance device security. *Id.* at 14:5-16. ***Fourth***, the '697 patent claims recite additional structure—a virtual machine and separate virtual machine monitor—that provides additional security benefits. *Supra* at 8. Regardless, even if all of those were individually well-known, routine, and conventional (the specification makes plain they are not), there is an inventive concept in the combination of elements.

As the specification explains, the claimed system improves security technology using this series of steps and components, departing sharply from conventional systems' use of databases with already-known signatures. *Supra* at 2-4. There is no evidence—let alone clear and convincing evidence—that these features or combinations for improving security are "well-understood, routine, conventional activities previously known to the industry." *CosmoKey*, 15 F.4th at 1097.

The claims are similar to others the Federal Circuit has found eligible at *Alice* step two. For example, in *CosmoKey*, the Federal Circuit held that the claimed authentication techniques were inventive because they recited using two separate channels and activating the authentication function only when necessary. *Id.* at 1097-99. The court explained that "the specification describes how the particular arrangement of steps … provides a technical improvement over conventional authentication methods" by reducing the "complexity of the authentication function." *Id.* at 1099. And, in *Bascom*, the Federal Circuit found an inventive concept in the combined elements even though the individual components were known. 827 F.3d at 1349-50. Prior art systems were either dependent on local processing or confined to an inflexible one-size-fits-all scheme. *Id.* But the inventors identified a particular arrangement of elements that broke that mold, thereby confirming eligibility of the claims. *Id.* Similarly, here, rather than the inflexibility of the prior art scheme—relying on already-known signatures—the invention allows for increased flexibility by dynamically identifying threats using a behavior-based approach, using the associations between activity sources and activity targets. *Id.; see also DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245 (Fed. Cir. 2014) (claims eligible at step two because "the computer network" does not "operat[e] in its normal, expected manner"); *Amdocs*, 841 F.3d at 1300-01 (claims eligible at step two because they provide "an unconventional technological solution … to a technological [security] problem," despite "requir[ing] arguably generic components"); *Weisner v. Google LLC*, 51 F.4th 1073, 1088 (Fed. Cir. 2022). As in *CosmoKey*, *Bascom*, and those other cases, the claims here include an inventive concept, and are therefore additionally eligible at step two.

At minimum, allegations in the specification and the Complaint raise plausible factual disputes precluding granting a motion to dismiss. D.I. 1 ¶¶ 39-44. *Aatrix* is instructive. 882 F.3d at 1129. There, the patentee described how the claims provided an advance in computer technology—"an improvement in the importation of data from third-party software applications"—that was not well-understood, routine, or conventional. *Id.* The Federal Circuit held that there was "no proper basis for rejecting those allegations as a factual matter" because "nothing in the specification describes this importation of data as conventional." *Id.* at 1128-29. Thus, the Federal Circuit found that those allegations precluded the district court from finding that "the claimed elements were well-understood, routine, or conventional" on a motion to dismiss. *Id.* at 1128 (vacating dismissal).[4] There is at least a fact issue here too because the claims "provide[] methods for performing behavioral analysis directly on an endpoint device, using locally-monitored data, to detect, identify, and prevent malicious activities in a way that existing systems could not." D.I. 1. ¶ 41. And "nothing in the specification describes this … as conventional." *Aatrix*, 882 F.3d at 1128-29.

C. The Dependent Claims Provide Additional Details Supporting Eligibility

CrowdStrike asserts that "claim 1 of each patent is representative" of all dependent claims. Mot. at 15. But "[t]he patent challenger who identifies a claim as representative of a group of claims bears the initial burden to make a *prima facie* showing that [they] are 'substantially similar and linked to the same' ineligible concept." *Mobile Acuity Ltd. v. Blippar Ltd.*, --- F.4th ----, 2024 WL 3659127, at *6 (Fed. Cir. 2024). CrowdStrike does not attempt to make that showing.

The dependent claims include additional details that confirm eligibility distinct from the independent claims. For example, various dependent claims recite: (1) techniques for monitoring

[4] *See also Cooperative Entertainment, Inc. v. Kollective Tech., Inc.*, 50 F.4th 127, 131 (Fed. Cir. 2022) (claims plausibly added two inventive concepts for improving networks at step two); *Cellspin Soft, Inc. v. Fitbit, Inc.*, 927 F.3d 1306, 1316 (Fed. Cir. 2019) (claims plausibly added an inventive concept at step two: the patentee "alleged that it was unconventional to separate the steps of capturing and publishing data so that each step would be performed by a different device linked via a wireless, paired connection").

chains of activities on a host computing device by tracking associations between an activity source and an activity target, which then becomes the source for another target, and tracking such associations over time, '872 patent cls. 10, 11; '697 patent cls. 11, 12; and (2) identifying activities that attempt to access "a portion of memory that is set as non-executable" or "underprivileged instructions," '872 patent cls. 13, 14; '697 patent cls. 14, 15. Such techniques provide additional technological details and flexibility over conventional fingerprint-based detection. These additional technical details further underscore the dependent claims' eligibility. *See CardioNet, LLC v. InfoBionic, Inc*, 955 F.3d 1358, 1369 (Fed. Cir. 2020). CrowdStrike's Motion should be denied.

V. GOSECURE'S COMPLAINT PLAUSIBLY ALLEGES INFRINGEMENT

The Court should deny CrowdStrike's motion to dismiss GoSecure's infringement claims because GoSecure "allege[s] facts giving rise to a plausible inference and fair notice of infringement by identifying the accused products and alleging that the accused products meet each and every element of at least one claim of the asserted patents." *Repairify, Inc. v. Keystone Auto. Indus., Inc.*, 610 F. Supp. 3d 897, 905 (W.D. Tex. 2022). That is enough. *See id.*; *Bot M8 LLC v. Sony Corp. of Am.*, 4 F.4th 1342, 1352 (Fed. Cir. 2021) ("It is enough that a complaint place the alleged infringer on notice of what activity ... is being accused of infringement.") (cleaned up); *Nalco Co. v. Chem-Mod, LLC*, 883 F.3d 1337, 1350 (Fed. Cir. 2018). GoSecure's Complaint contains a limitation-by-limitation analysis—using screenshots from CrowdStrike's own documents—explaining how the Accused Products infringe the claims of the Asserted Patents. *See, e.g.*, D.I. 1 ¶ 64 ("constantly monitoring and recording endpoint activity"), ¶ 67 ("all data is recorded on the endpoint from an activity perspective"), ¶¶ 69, 70. Those factual allegations, based on CrowdStrike's ***own*** statements regarding the operation of its ***own*** products, warrant denial under the flexible pleading standard prescribed in *Bot M8*.

As to the '872 patent, CrowdStrike argues that it must "guess how these screenshots might relate to the claim language." Mot. at 17. Not so, for two reasons. First, GoSecure mapped the

screenshots to the claims on a limitation-by-limitation basis, so no guesswork is necessary. D.I. 1 ¶¶ 61-76, 89-105. Second, "[a]llegations to the level of detail contained in infringement contentions are not required at the pleading stage." *MAZ Encryption Techs. LLC v. BlackBerry Ltd.*, No. 6:15-CV-1167, 2016 WL 9275008, at *3 (E.D. Tex. June 7, 2016), *report and recomm'n adopted*, 2016 WL 9275397 (June 27, 2016). GoSecure has plausibly alleged infringement based on publicly-available information, and GoSecure is entitled to an inference that a product that monitors "all data … on the endpoint from an activity perspective" (D.I. 1 ¶ 64) identifies activity sources, targets, and associations as claimed. *Pederson v. Zoho Corp.* No. 1:23-cv-71-DII, 2023 WL 3612333, at *2 (W.D. Tex. May 23, 2023) (plaintiff "entitled to all inferences in [its] favor on [its] theory that [the claim language] is broad enough to encompass [defendant's] software" at motion to dismiss stage).

As to the '697 patent, CrowdStrike adds on that the Complaint "alleges no facts" regarding how the claimed "fingerprints" are generated or shared. Mot. at 17-18. CrowdStrike is wrong. GoSecure specifically alleged (quoting CrowdStrike's documents) that the Accused Products generate "indicators of attack" and "indicators of misconfiguration" as fingerprints and share those indicators "to respond faster and stop breaches." D.I. 1 ¶¶ 98-101. Again, there is nothing implausible about inferring that a product that performs "high-fidelity telemetry on trillions of security events across endpoints" (*id.* ¶ 70) generates and share fingerprints. As the Federal Circuit has explained, "patentees need not prove their case at the pleading stage." *Bot M8*, 4 F.4th at 1346.

CrowdStrike's cited cases are inapt. *R2 Invs. LDC v. Phillips* involved alleged securities fraud, where pleading standards are "enhanced." 401 F.3d 638, 641 (5th Cir. 2005). And *Vervain, LLC v. Micron Tech., Inc.* is also distinguishable: there, the plaintiff alleged that the defendant infringed because it practiced "conventional" techniques, which the court found was not a "reasonable inference." No. 6:21-cv-00487, 2022 WL 23469, at *6 (W.D. Tex. Jan. 3, 2022). GoSecure, by contrast, is not alleging that CrowdStrike infringes because it uses "conventional" techniques. The other cases CrowdStrike

cites without analysis (Mot. at 4) are similarly inapposite. Those courts dismissed the complaints because the plaintiffs, for example, offered infringement theories that were "incompatible with" the claim language or that omitted claim limitations entirely. *See, e.g.*, *Contiguity, LLC v. Conduent Bus. Servs., LLC*, No. 23-cv-00038-XR, 2024 WL 252068, at *3 (W.D. Tex. Jan. 22, 2024).

VI. GOSECURE'S COMPLAINT PLAUSIBLY ALLEGES PRE-SUIT INDIRECT AND WILLFUL INFRINGEMENT

Finally, GoSecure's claims for pre-suit indirect and willful infringement survive because the factual allegations in the Complaint raise a plausible inference that CrowdStrike actually knew of the Asserted Patents or willfully blinded itself to their existence.

First, CrowdStrike argues that GoSecure did not identify facts sufficient to make CrowdStrike's actual knowledge of the Asserted Patents plausible. Mot. at 19-20. Not so. As alleged, CrowdStrike cited the published application of one of the Asserted Patents as a prior art reference in an IPR filed more than a year before GoSecure filed its Complaint (and over four years after both Asserted Patents had issued). *Id.* ¶ 38.[5] That factual allegation, which CrowdStrike ignores, warrants denial of its Motion. *Cf. Network Sys. Techs., LLC v. Qualcomm Inc.*, No. 1:22-cv-01331, 2023 WL 11833572, at *7 (W.D. Tex. July 21, 2023) (citation to a patent publication from after the patent had issued sufficed to "meet the pleading standards on a motion to dismiss").

Second, CrowdStrike argues that GoSecure failed to allege facts sufficient to make CrowdStrike's willful blindness plausible. Mot. at 20. Again, CrowdStrike is wrong. "[A] willfully blind defendant is one who takes deliberate actions to avoid confirming a high probability of wrongdoing and who can almost be said to have actually known the critical facts." *Global-Tech Appliances, Inc. v. SEB S.A.*, 563 U.S. 754, 769 (2011). GoSecure's Complaint alleges facts sufficient to

[5] As alleged in GoSecure's proposed First Amended Complaint, CrowdStrike's pre-suit knowledge is further evidenced by the fact that its subpoena to GoSecure in connection with this IPR specifically referenced the '872 patent. Ex. 2 ¶¶ 38-39.

support a reasonable inference that CrowdStrike took such "deliberate actions."

As alleged, Mr. Alperovitch—one of CrowdStrike's founders and its former CTO—learned about GoSecure's technology and efforts to obtain patent protection while serving on GoSecure's Board. *Id.* ¶¶ 29, 31, 33. Mr. Alperovitch then co-founded CrowdStrike, where he served as CTO for nearly a decade. *Id.* ¶¶ 25, 34-35. Those allegations, taken together, raise a plausible inference that CrowdStrike had pre-suit knowledge of the Asserted Patents. *Monolithic Power Sys., Inc. v. Silergy Corp.* is instructive. 127 F. Supp. 3d 1071 (N.D. Cal. 2015). The *Monolithic* complaint alleged pre-suit knowledge because one of the defendant's employees was "aware of [plaintiff's] entire patent pipeline due to his job responsibilities" while working for the plaintiff and because the parties had previously engaged in settlement negotiations relating to a separate breach of contract claim. *Id.* at 1074. The court found that those allegations, taken together, raised a plausible inference of pre-suit knowledge. *Id.* So too here. Mr. Alperovitch knew GoSecure had filed patent applications on its technology and attended Board meetings at which GoSecure's intellectual property strategy was discussed. D.I. 1 ¶¶ 29-33. If anything, the facts are even stronger here than in *Monolithic*, because CrowdStrike evaluated GoSecure's patent portfolio during a prior patent infringement suit. *Id.* ¶ 38. Thus, the Court should deny CrowdStrike's Motion in its entirety.

VII. IF NECESSARY, GOSECURE REQUESTS LEAVE TO AMEND

Alternatively, GoSecure requests leave to file a First Amended Complaint, attached as Ex. 2. The Court "should freely give leave [to amend] when justice so requires." FED. R. CIV. P. 15(a)(2). Because the proposed FAC includes additional details sufficient to obviate the issues raised in CrowdStrike's Motion, GoSecure submits that leave is warranted. *See Aatrix*, 882 F.3d at 1125 (district court erred in denying leave to amend when "factual allegations … in the proposed [] amended complaint" established eligibility); *Ubiquitous Connectivity, LP v. City of San Antonio*, 2019 WL 4696421 (W.D. Tex. Sept. 26, 2019) (denying motion to dismiss based on later-filed amended complaint).

Dated: August 22, 2024

Respectfully submitted,

By: */s/ Giri Pathmanaban*

S. Giri Pathmanaban (SBN: 24074865)
Daniel S. Todd (admitted *pro hac vice*)
LATHAM AND WATKINS LLP
300 Colorado Street, Suite 2400
Austin, TX 78701
Tel: (737) 910-7300
Fax: (737) 910-7301
Giri.Pathmanaban@lw.com
Daniel.Todd@lw.com

Maximilian A. Grant (SBN: 481610)
LATHAM AND WATKINS LLP
555 Eleventh Street, NW, Suite 1000
Washington, D.C. 20004
Tel: (202) 637-2200
Fax: (202) 637-2201
Max.Grant@lw.com

Clement Naples (admitted *pro hac vice*)
LATHAM AND WATKINS LLP
1271 Avenue of the Americas
New York, NY 10020
Tel: (212) 906-1200
Fax: (212) 751-4864
Clement.Naples@lw.com

Amit Makker (admitted *pro hac vice*)
LATHAM AND WATKINS LLP
505 Montgomery Street, Suite 2000
San Francisco, CA 94111
Tel: (415) 391-0600
Fax: (415) 395-8095
Amit.Makker@lw.com

ATTORNEYS FOR PLAINTIFF GOSECURE, INC.

CERTIFICATE OF SERVICE

Pursuant to the Federal Rules of Civil Procedure and Local Rule CV-5, I hereby certify that, on August 22, 2024, all counsel of record who have appeared in this case are being served with a copy of the foregoing via the Court's CM/ECF system.

/s/ Giri Pathmanaban
S. Giri Pathmanaban