UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

CASE NO.: 25-cv-60803-WPD

K.MIZRA LLC

Plaintiff,

vs.

CITRIX SYSTEMS, INC.,

Defendant.

ORDER DENYING DEFENDANT'S MOTION TO DISMISS

THIS CAUSE is before the Court on Defendant's Motion to Dismiss, filed herein on June 10, 2025. [DE 19] (the "Motion"). The Court has carefully considered the Motion, the Response and Reply thereto, filed June 24, 2025, and July 8, 2025, respectively, [DEs 22, 28], the arguments presented at the September 11, 2025 hearing, the language of the '705 Patent, and is otherwise fully advised. Upon close consideration, the Court denies Defendant's Motion.

I. BACKGROUND

This is an action for patent infringement, wherein Defendant challenges the validity of the Patent. Plaintiff, K.Mizra, is the owner by assignment of United States Patent No. 8,234,705 titled "Contagion Isolation and Inoculation" ("'705 Patent" or the "Patent"). [DE 1] ¶ 2. The U.S. Patent and Trademark Office ("USPTO") issued the Patent to inventors Dr. James A. Roskind and Mr. Aaron T. Emigh on July 31, 2012. *Id.* ¶ 18. The '705 Patent claims priority to U.S. Provisional Application No. 60/613,909, filed on September 27, 2004. *Id.* ¶ 19.

The '705 Patent explains the situation in computer security as then existing, as follows. "Hosts," such as laptop computers, pose a threat to "protected networks." [DE 1] ¶ 25 (quoting

’705 Patent, [DE 1-4] 1:14–31). Namely, by roaming the internet, laptops “may become infected by computer viruses.” *Id.* Or, the Patent explains, laptops could have “protective software removed without authorization.” *Id.* Then, an infected host “may infect . . . the protective network before measures can be taken to detect and prevent the spread of such infections.” *Id.*

The Patent steps in as a “way to ensure that a system does not infect or otherwise harm” the protected network. ’705 Patent, [DE 1-4] 1:39. Namely, the Patent claims a “multi-faceted network system” involving “interrelated software and hardware components” that “protect[s] a network from known and unknown threats.” [DE 1] ¶ 33. The claimed system “can direct an unclean computer attempting to connect to the secure network, known as the host computer, to a form of remediation, such as downloading a software patch or a software update, removing material from the host computer and/or enabling certain settings [] present on the host computer.” *Id.* (citing ’705 Patent, [DE 1-4] 1:14–41.) It was designed “to reduce the burdens of having to manually identify, connect to, isolate, and remove malicious software from an infected device.” [DE 1] ¶ 33.

The invention is an advance from the art in 2005. *Id.* It recites a system that automatically and dynamically detects an insecure condition by (1) contacting a trusted computing base, (2) receiving a response therefrom, (3) determining whether that response contains a valid identification of cleanliness, and (4) configuring and implementing a remediation action based on what is discovered about the state of an endpoint or “host” computer. *Id.* More specifically, the claims teach a system configured to communicate with a “trusted computing base” to determine when a response includes a valid digitally signed attestation of cleanliness, and to control access to the network accordingly. *Id.*

Plaintiff brought this action on April 24, 2025, asserting a single count of patent infringement under 35 U.S.C. § 271 against Citrix Systems, Inc. ("Citrix" or "Defendant"). *See* [DE 1] ¶¶ 42–58. Citrix is a computer security company. K.Mizra asserts Citrix has directly infringed, either literally or under the doctrine of equivalents, upon claim 19 of the '705 Patent by making, selling, using, and offering for sale computer network security products and services, specifically Citrix's Secure "Private Access" solution. *Id.* ¶ 39. Claim 19 recites as follows:

> [preamble] A computer program product for protecting a network, the computer program product being embodied in a non-transitory computer readable medium and comprising computer instructions for:
>
> [A] detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network,
>
> [B] wherein detecting the insecure condition includes:
>
> > [B1] contacting a trusted computing base associated with a trusted platform module within the first host,
> >
> > [B2] receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness,
>
> [C] wherein the valid digitally signed attestation of cleanliness includes at least one of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host;
>
> [D] when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network,

> [E] wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes
>
> > [E1] receiving a service request sent by the first host, serving a quarantine notification page to the first host when the service request comprises a web server request,
> >
> > [E2] and in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not
> >
> > associated with a remediation host configured to provide data usable to remedy the insecure condition; and
>
> [F] permitting the first host to communicate with the remediation host.

[DE 1-4] 22:14-49.

K.Mizra further reserves the right to assert additional claims of the Patent, including both independent and dependent claims. *Id.* ¶ 27. Defendant asserts the entire Patent can be invalidated based upon claim 19, which the Court should view as representative of all claims.[1]

[1] The specific allegations against Citrix with respect to infringement are not relevant at this stage because Citrix does not argue Plaintiff fails to state a claim for infringement based upon the elements of that claim. Instead, Citrix argues the '705 Patent is invalid under 35 U.S.C. § 101. Moreover, while the '705 Patent has a long history of litigation, both in Article III courts and at *inter partes* review at the Patent Trial and Appeal Board ("PTAB"), a review this past litigation is not pertinent here because neither party asserts collateral estoppel applies.

II. STANDARD OF LAW

The Federal Circuit has "repeatedly recognized that in many cases it is possible and proper to determine patent eligibility under 35 U.S.C. § 101 on a Rule 12(b)(6) motion." *Genetic Techs. Ltd. v. Merial L.L.C.,* 818 F.3d 1369, 1373 (Fed. Cir. 2016). This is because "[e]ligibility under 35 U.S.C. § 101 is a question of law, based on underlying facts." *SAP America, Inc. v. InvestPic, LLC*, 898 F.3d 1161, 1166 (Fed. Cir. 2018) (internal citations omitted). A motion to dismiss on grounds of patent ineligibility is properly granted "when there are no factual allegations that, taken as true, prevent resolving the eligibility question as a matter of law." *Aatrix Software, Inc. v. Green Shades Software, Inc.*, 882 F.3d 1121, 1125 (Fed. Cir. 2018).

A challenge to patent eligibility on § 101 grounds is an affirmative defense. *See Mobile Acuity Ltd. v. Blippar Ltd.*, 110 F.4th 1280, 1289 (Fed. Cir. 2024). But in the Eleventh Circuit, an affirmative defense may be raised on a motion to dismiss for failure to state a claim if the defense is apparent on face of complaint. *See Hudson Drydocks Inc. v. Wyatt Yachts Inc*., 760 F.2d 1144 (11th Cir. 1985). Here, the defense of invalidity is apparent on the face of the Complaint; the § 101 inquiry, therefore, is properly before the Court. *See, e.g. AR Design Innovations LLC v. City Furniture, Inc.,* No. 23-CV-20127, 2023 WL 3844917, at *6 (S.D. Fla. June 6, 2023) (considering a § 101 on a motion to dismiss); *PerDiemCo LLC v. NexTraq LLC*, 720 F. Supp. 3d 1365, 1371 (N.D. Ga. 2024) (same).

The 12(b)(6) standard is familiar and applies here. *See Aatrix*, 882 F.3d at 1121. A complaint survives a 12(b)(6) motion if it articulates "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). "A claim has facial plausibility when the pleaded factual content allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 129 S. Ct. 1937, 1949 (2009)

(citing *Twombly*, 550 U.S. at 556). When determining whether a claim has facial plausibility, "a court must view a complaint in the light most favorable to the plaintiff and accept all of the plaintiff's well-pleaded facts as true." *Am. United Life Ins. Co. v. Martinez*, 480 F.3d 1043, 1066 (11th Cir. 2007). However, the Court need not take allegations as true if they are merely "threadbare recitals of a cause of action's elements, supported by mere conclusory statements." *Iqbal*, 129 S. Ct. at 1949.

Patents granted by the Patent and Trademark Office are presumptively valid. *See Microsoft Corp. v. i4i Ltd. P'ship*, 564 U.S. 91 (2011) (citing 35 U.S.C. § 282).[2]

III. DISCUSSION

As an initial matter, at this juncture, Plaintiff has only asserted that Defendant infringed claim 19, but "reserves the right to assert additional claims of the Asserted Patent, including both independent and dependent claims." [DE 1] ¶ 27. Based upon Plaintiff's future reservation, Defendant invites this Court to view claim 19 as representative of all claims, and then invalidate the entire Patent based upon claim 19 alone. However, a plain reading of the Complaint reveals that Plaintiff only asserts infringement of claim 19; thus, there is no reason to determine whether claim 19 is representative of all claims. The Court therefore proceeds with an analysis of claim 19 based upon a plausible reading of the allegations in the Complaint.

a. Section 101

Section 101 of the Patent Act provides, "[w]hoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement

[2] Although "[a]ny fact . . . that is pertinent to the invalidity conclusion must be proven by clear and convincing evidence," *Berkheimer v. HP, Inc.*, 881 F.3d 1360, 1368 (Fed. Cir. 2018), the Court does not make any findings of fact right now; therefore, this burden does not meaningfully come into play.

thereof, may obtain a patent therefor. . . ." 35 U.S.C. § 101. This provision contains an "important implicit exception: Laws of nature, natural phenomena, and abstract ideas are not patentable." *Alice Corp. Pty. Ltd.*, 573 U.S. 208, 216 (2014) (quoting *Association for Molecular Pathology v. Myriad Genetics, Inc.,* 569 U.S. 576, 589 (2013)). *Alice* articulated a two-step framework to determine if this exception applies. The Court must ask, first, whether "the claims at issue are directed to one of those patent-ineligible concepts," and second, whether the claims present an "inventive concept" sufficient to ensure that the claim amounts to significantly more than a claim upon the abstract idea itself. *Alice*, 573 U.S. at 217.

i. Alice Step One

When considering § 101 eligibility under *Alice*, the Court must first determine "whether the claims at issue are directed to a patent-ineligible concept." *Alice*, 573 U.S. at 217 (citing *Mayo Collaborative Services v. Prometheus Laboratories, Inc.* 566 U.S. 66, 75 (2012)). This inquiry "cannot simply ask whether the claims *involve* a patent-ineligible concept, because essentially every routinely patent-eligible claim involving physical products and actions *involves* a law of nature and/or natural phenomenon." *Enfish, LLC v. Microsoft Corp*., 822 F.3d 1327, 1335 (Fed. Cir. 2016) (citing *Mayo,* 566 U.S. at 70). "Rather, the 'directed to' inquiry applies a stage-one filter to claims, considered in light of the specification, based on whether 'their character as a whole is directed to excluded subject matter.'" *Enfish*, 822 F.3d at 1335 (quoting *Internet Patents Corp. v. Active Network, Inc.,* 790 F.3d 1343, 1346 (Fed. Cir. 2015)). The Federal Circuit has cautioned against "describing the claims at such a high level of abstraction and untethered from the language of the claims," which "all but ensures that the exceptions to § 101 swallow the rule." *Enfish,* 822 F.3d at 1337.

In determining whether a patent is directed at an abstract idea, the Court may "consult the plain claim language, written description, and prosecution history" as well as the "intrinsic evidence and conclude that the claims are directed to improving the functionality of a computer or network." *CardioNet, LLC v. InfoBionic, Inc,* 955 F.3d 1358, 1373 (Fed. Cir. 2020). "The court need not consult the prior art to see if, in fact, the assertions of improvement in the patent's written description are true." *Id.*

Upon review of the briefing, arguments by counsels at the hearing, the relevant case law, and the Patent at issue, the Court finds claim 19 is not directed at an abstract idea. The Court will address each of Defendant's arguments, in turn.

A. Whether Claim 19 is Analogous to Patents Previously Found to be Ineligible

Defendant urges comparisons to "access control" patents previously found ineligible. Courts will sometimes "compare the claims at issue to those claims already found to be directed to an abstract idea in previous cases." *Enfish*, 822 F.3d at 1334. While analogous claims can be instructive, they are not decisive because "[u]ltimately, the § 101 inquiry must focus on the language of the [claims] themselves." *ChargePoint, Inc. v. SemaConnect, Inc.*, 920 F.3d 759, 769 (Fed. Cir. 2019). Defendant analogizes to several cases where patents were invalidated.

First, in *Prism Techs. LLC v. T-Mobile USA, Inc.*, 696 F. App'x 1014, 1017 (Fed. Cir. 2017)[3], the Federal Circuit found—after claim construction—that the asserted claims were

[3] The claim at issue in *Prism* recited:
1. A method for controlling access, by at least one authentication server, to protected computer resources provided via an Internet Protocol network, the method comprising:
receiving, at the at least one authentication server from at least one access server, identity data associated with at least one client computer device, the identity data forwarded to the at least one access server from the at least one client computer device with a request from the at least one client computer device for the protected computer resources;

directed to the abstract idea of "providing restricted access to resources." *Id.* The *Prism* claims were directed to a process that included "(1) receiving identity data from a device with a request for access to resources; (2) confirming the authenticity of the identity data associated with that device; (3) determining whether the device identified is authorized to access the resources requested; and (4) if authorized, permitting access to the requested resources." *Id.* The claims recited a "method for controlling access." *Id.* at 1016. Where plaintiff did not "proffer a persuasive argument in support of [its] conclusion" that the claims covered a "concrete, specific solution to a real world problem," the court found the claims were abstract. *Id.* at 1017. Moreover, the court agreed with defendant's analogies to "providing various pre-computer-age corollaries for which humans similarly restrict and provide access to resources." *Id.*

In *Ericsson Inc. v. TCL Commc'n Tech. Holdings Ltd.,* 955 F.3d 1317, 1326 (Fed. Cir. 2020),[4] the Federal Circuit likewise found, after claim construction, that the claims were "directed

---

authenticating, by the at least one authentication server, the identity data received from the at least one access server, the identity data being stored in the at least one authentication server;

authorizing, by the at least one authentication server, the at least one client computer device to receive at least a portion of the protected computer resources requested by the at least one client computer device, based on data associated with the requested protected computer resources stored in at least one database associated with the at least one authentication server; and

permitting access, by the at least one authentication server, to the at least the portion of the protected computer resources upon successfully authenticating the identity data and upon successfully authorizing the at least one client computer device.

[4] The claims at issue in *Ericsson* recited:

1. A system for controlling access to a platform, the system comprising:

a platform having a software services component and an interface component, the interface component having at least one interface for providing access to the software services component for enabling application domain software to be installed, loaded, and run in the platform;

an access controller for controlling access to the software services component by a requesting application domain software via the at least one interface, the access controller comprising:

an interception module for receiving a request from the requesting application domain software to access the software services component;

and a decision entity for determining if the request should be granted wherein the decision entity is a security access manager, the security access manager holding access and permission policies; and wherein the requesting application domain software is granted access to the software services component via the at least one interface if the request is granted.

to the abstract idea of controlling access to, or limiting permission to, resources." *Id.* at 1326. The claims discussed computer technology only in overbroad and generic terms. It taught a "system for controlling access to a platform" involving "software services component and interface component" an "interception model" and a "decision entity" and "security access manager." *Id.* The Federal Circuit determined that,

> "the security access manager / decision entity / interception module is the only claimed component of the "access controller," all four components collapse into simply "an access controller for controlling access" by "receiving a request" and then "determining if the request should be granted." That bare abstract idea, controlling access to resources by receiving a request and determining if the request for access should be granted, is at the core of claim 1.

Id. at 1326. The claims failed because the "recitation of functional computer components [did] not specify *how* the claim 'control[s] access to a platform,'" *Id.* (quoting the claim at issue) (emphasis added).

In *Digital Media Techs., Inc. v. Hulu, LLC*, No. 4:16CV245-MW/CAS, 2017 WL 4750705, at *5 (N.D. Fla. July 3, 2017), *aff'd sub nom. Digital Media Techs., Inc. v. Netflix, Inc.,* 742 F. App'x 510 (Fed. Cir. 2018),[5] the district court held that the claim was directed either to the abstract

---

Claim 5 further recites:
5. The system according to claim 1, wherein:
the security access manager has a record of requesting application domain software; and the security access manager determines if the request should be granted based on an identification stored in the record.

[5] The claim at issue in *Digital Media Technologies* recited:

A multimedia system, comprising:
an external control server configured to:
receive a request from a client device via a wide area network requesting protected content to be sent to the client device;
receive client device authentication information from the client device, the client device authentication information comprising at least information related to a user authentication and a device authorization;
validate the client device authentication information according to predetermined criteria; send protected content location information to the client device, the protected content location information being associated with a location of the protected content;

idea of "secured content-delivery," or, alternatively, "the abstract idea of delivering content secured with licenses and encryption." *Id.* at 5.

It appears to the Court at this juncture—before claim construction—that the '705 Patent differs from those above in two material respects.

First, unlike those claims discussed above, claim 19 articulates a "concrete assignment of specified functions among a computer's components to improve computer security." *Ancora Techs., Inc. v. HTC Am., Inc.*, 908 F.3d 1343, 1344 (Fed. Cir. 2018), *as amended* (Nov. 20, 2018).[6] That is, claim 19 not only teaches a "result" but outlines a specific "way of achieving it." *SAP Am., Inc. v. InvestPic, LLC,* 898 F.3d 1161, 1167 (Fed. Cir. 2018). Claim 19 articulates a system by which the protected network reaches into a trusted computer base—a piece of hardware that is immune from software infections—in the first host. The trusted computer base then responds with

---

encrypt, in response to receiving a request for a content license from the client device via the wide area network, the request comprising information related to a location of the content license and being based on a determination by the client device that the protected content is encrypted and requires a content license, the content license using a public key associated with the client device, the content license comprising a content key which the client device uses to decrypt the protected content and usage parameters specifying the terms under which the protected content can be consumed; and

send the encrypted content license to the client device, the client device using a private key associated with the client device to decrypt the content license and using the content key to decrypt the protected content for use according to usage parameters specified by the content license; and

an external content server configured to:

receive a request for the protected content from the client device, the request comprising the protected content location information provided by the external control server; and

send the protected content to the client device.

[6] The claim at issue in *Ancora* recited:

1. A method of restricting software operation within a license for use with a computer including an erasable, non-volatile memory area of a BIOS of the computer, and a volatile memory area; the method comprising the steps of:

selecting a program residing in the volatile memory,

using an agent to set up a verification structure in the erasable, non-volatile memory of the BIOS, the verification structure accommodating data that includes at least one license record,

verifying the program using at least the verification structure from the erasable non-volatile memory of the BIOS, and

acting on the program according to the verification.

a "valid digitally signed attestation of cleanliness." If there is no digitally signed attestation of cleanliness, the laptop will be "quarantined," and will not be allowed to send data to other hosts on the network. Claim 19 goes on to discuss the remediation step, namely, how to fix an infected host. The host is served with a quarantine notification page (if the host had made an internet-based request) or, IP address of a quarantine server configured to serve the quarantine notification page (if the service request includes a DNS query), permitting the first host to communicate with the remediation host. This degree of specificity in claim 19's articulation of how to improve security is an "improvement in computer functionality is eligible for patenting." *Ancora*, 908 F.3d at 1344.

Second, whereas the claimed inventions in the analogized patents only claimed systems of "access control," claim 19 of the '705 Patent provides a mechanism for tailored *remediation* in the same process. The "quarantine" patents in *Ericcsson, Prism,* and *Digital Media* did not contain any such secondary step. The two-step invention here that provides a fix just as it identifies a problem can be readily construed as "an improvement in the functioning of a networked system." from the "once-necessary human intervention from a fundamentally mechanical process." [DE 1] ¶ 32. The Court has no "basis for disputing" this claimed improvement. *Ancora*, 908 F.3d at 1349.

B. Whether the Patent Recites Generalized Steps to be Performed Using Conventional Computer Activity and Components

Defendant next argues many elements recited in the claims of the '705 Patent are plainly generic, such as a "computer program," "protected network," "host," and "software component." Defendant asserts these components are used only to perform conventional activities in the context of the claims:

> The patent confirms, for example, it did not invent "contacting a trusted computing base within a computer"; rather, the '705 patent discloses examples that had already been invented. '705 patent at 14:1-7. The '705 patent also explains its reference to contacting a trusted computing base is for a conventional purpose, "for example

> execut[ing] antivirus scans of the remainder of the computer" or "digitally sign[ing] assertions about the cleanliness (e.g. infestation status) and/or state of their computers." *Id.* at 14:7-12.

[DE 19] at p. 15.

The Court disagrees. "[w]hile generalized steps to be performed on a computer using conventional computer activity are abstract, not all claims in all software patents are necessarily directed to an abstract idea." *RecogniCorp, LLC v. Nintendo Co*., 855 F.3d 1322, 1326 (Fed. Cir. 2017) (cleaned up). Instead, "[s]oftware patent claims satisfy *Alice* step one when they are 'directed to a specific implementation of a solution to a problem in the software arts,' such as an improvement in the functioning of a computer." *Id.* (quoting *Enfish*, 822 F.3d at 1338–39).

And here, claim 19 is directed not only to software but hardware. Plaintiff sufficiently alleges that the generic components improve overall computer security through improved hardware-software system interaction. The claimed system ensures network security by contacting the trusted computing base, a secure "tamperproof hardware" component installed on the host system, to reliably provide information about the security status of the host computer. This process of contacting to hardware is an improvement over prior art. Such hardware is less vulnerable to attack than software, which, the '705 Patent explains, could be "removed or altered without authorization." '705 Patent, [DE 1-4] 1. This improved, automated system confirms the real-time security status of the host upon each reconnection instead of relying on previously installed software security measures that may have been compromised between connection sessions. Claim 19 offers more than just generalized steps to be performed on a computer using conventional computer components.

C. Whether Claim 19 can be Analogized to Quarantine

Defendant next asserts claim 19 is directed at an idea that is pervasive in human activity: quarantine, or access control. It is true that claims directed at access control alone are patent ineligible. *Ericsson*, 955 F.3d at 1327 ("[c]ontrolling access to resources is exactly the sort of process that 'can be performed in the human mind, or by a human using a pen and paper,' which we have repeatedly found unpatentable." (quoting *CyberSource Corp. v. Retail Decisions, Inc.*, 654 F.3d 1366, 1372 (Fed. Cir. 2011)). But the Patent here can be read as directed at a comprehensive system for computer security through a *two*-step process: (1) quarantining the infected host, and then (2) *cleaning* the infected host by downloading protective software. Once "quarantined" (such that the first host cannot send data to hosts on the protected network), the Patent teaches a system of remediation tailored to the method by which the first host attempts to contact the protected network.[7] Quarantine does not encompass the idea of remediation. And even if it did, it would not encompass the multi-method process of remediation articulated in claim 19. Even if some portion of the claim 19 can be analogized to quarantine, an abstract idea that "long predates the [asserted patent] and is pervasive in human activity," the specifics in claim 19 preclude a finding that claim 19 "as a whole" is directed to this abstract idea. *See Data Engine Techs. LLC v. Google LLC*, 906 F.3d 999, 1011 (Fed. Cir. 2018) (citing *Alice*, 573 U.S. at 218 n.3).

[7] [E] wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes

[E1] receiving a service request sent by the first host, serving a quarantine notification page to the first host when the service request comprises a web server request,

[E2] and in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host configured to provide data usable to remedy the insecure condition;

Getting closer to the mark, Defendant also tries to analogize to school enrollment, wherein a student is turned away from enrollment if he does not have the required vaccinations. Citrix analogizes to a Florida 2004 immunization statute, which directs schools to require vaccinations of its students. *See* Fla. Stat. § 1003.22 (2004). If a student is not vaccinated, the statute directs the school to refuse admittance until certification of immunization is provided. Citrix draws parallels to the steps of claim 19, for example, differentiating between a student "arriving" sick at school, versus "calling in" sick, to account for the various methods of contacting the remediation host in claim 19. Citrix also likens remediation host in claim 19 to the Florida County Health Departments that provides vaccinations.

This analogy is not persuasive. A claim "is not abstract just because it can be analogized to something that can be done in the physical world." *Sec. First Innovations, LLC v. Google LLC*, No. 2:23-CV-97, 2023 WL 7726389, at *16 (E.D. Va. Nov. 15, 2023); *Data Engine Techs. Ltd. v. Google LLC*, 906 F.3d 999, 1011 (Fed. Cir. 2018). Here, "the steps embodied in the asserted claims are virtually nonsensical—or, at the very least, entirely impractical—*except* in the context of computers, which supports the proposition that the claims are directed to an improvement in computer functionality." *Id.*

Claim 19 of the '705 Patent presents a computer security solution that would otherwise require manual intervention. It teaches a method for detecting and isolating an infected host by contacting trusted immutable hardware rather than relying on software that is more prone to infection. It also simultaneously conducts remediation by directing the infected host to a remediation host. It so directs based upon the way in which the infected host contacted the protected network. Though Defendant would have this Court view the claim 19 from a thousand

feet up, the Court declines to do so where claim 19, when read as a whole, and drawing all inferences in favor of Plaintiff, leads to the conclusion that claim 19 is not abstract.

ii. Alice Step Two

"Because the claims are not directed to an abstract idea under step one of the *Alice* analysis," the Court does "not need to proceed to step two of that analysis." *Enfish*, 822 F.3d at 1339. Still, to the extent claim 19 is abstract, the Court finds claim 19 survives the *Alice* step two test.

At *Alice* step two, question is whether the claim presents any "inventive concept." *Bascom Glob. Internet Servs., Inc. v. AT&T Mobility LLC*, 827 F.3d 1341, 1349 (Fed. Cir. 2016). To be inventive, the claim limitations must consist of "more than 'well-understood, routine, conventional activity.'" *See Ultramercial, Inc. v. Hulu, LLC*, 772 F.3d 709, 715 (Fed. Cir. 2014) (quoting *Mayo*, 566 U.S. at 79). An inventive concept "may arise in one or more of the individual claim limitations or in the ordered combination of the limitations." *Bascom*, 827 F.3d at 1349. In the computer context, the inventive concept "can be found in the non-conventional and non-generic arrangement of known, conventional pieces." *Id.* at 1350.

"[P]atentees who adequately allege their claims contain inventive concepts survive a § 101 eligibility analysis under Rule 12(b)(6)." *Aatrix Software, Inc. v. Green Shades Software, Inc.,* 882 F.3d 1121, 1126–27 (Fed. Cir. 2018) (citation omitted). At this juncture Plaintiff has sufficiently alleged that the "inventions of the Asserted Claims are each tethered to these advances over the art in the 2005 time frame." [DE 1] ¶ 33. A determination to the contrary presents a factual issue inappropriate for resolution on a motion to dismiss.

iii. Whether Claim 19 is Representative of All Claims

Defendant asks this Court to find claim 19 representative of all claims in the ’705 Patent. To the extent Plaintiff seeks to add or amend its claims at any later stage, the Court finds that claim 19 is not representative of all claims. “In a § 101 analysis, courts may evaluate representative claims.” *Automated Tracking Sols., LLC v. Coca-Cola Co*., 723 F. App’x 989, 991 (Fed. Cir. 2018) (citation omitted). In determining whether a claim is representative of other claims, courts ask whether claims are “substantially similar and linked to the same abstract idea.” *Content Extraction & Transmission LLC v. Wells Fargo Bank, Nat. Ass'n,* 776 F.3d 1343, 1348 (Fed. Cir. 2014). Accordingly, this “representative” analysis will often overlap with the merits of the “abstractness” analysis. *See Caselas, LLC v. VeriFone, Inc*., 624 F. Supp. 3d 1328, 1334 (N.D. Ga. 2022), *aff'd*, No. 2023-1036, 2024 WL 2720092 (Fed. Cir. May 28, 2024) (observing that “whether a claim is linked to the ‘same abstract idea’ as another claim will often hinge on a determination about whether both claims are abstract. . .”).

As explored above, claim 19 is not directed at an abstract idea; therefore, claim 19 is not representative of all claims. The ’705 Patent comprises of nineteen total claims: three independent claims—claims 1, 12, and 19—and sixteen dependent claims. The main difference among the independent claims is the medium within which the described system is contained. Claim 1 is directed at a “method for protecting a network.” ’705 Patent, [DE 1-4] 19:57. Claim 12 is directed at a “system for protecting a network comprising a processor configured to:” *Id.* 12:1, and claim 19 is directed at a “computer program product for protecting a network… being embodied in a non-transitory computer readable medium and comprising computer instructions for:” *Id.* 22:14. Claim 1 has ten dependent claims; claim 12 has six dependent claims and claim 19 has no dependent claims. *See id.* pp. 1922.

Defendant would have this Court read out of existence those claims which, at some later juncture, may assist in explaining the claimed invention and making it concrete. Because the undersigned must determine whether the "character [of the claims] as a whole is directed to excluded subject matter" *Internet Patents Corp. v. Active Network, Inc.,* 790 F.3d 1343, 1346 (Fed. Cir. 2015)), and because the Court determines the claims are not directed to an abstract idea, the Court finds that claim 19 is not representative of all claims.

IV. CONCLUSION

Based upon the foregoing, it is **ORDERED AND ADJUDGED** that the Motion [DE 19] is **DENIED**. Defendant shall file an answer by October 13, 2025.

DONE AND ORDERED in Chambers at Fort Lauderdale, Florida, this 29th day of September, 2025.

WILLIAM P. DIMITROULEAS
United States District Judge

Copies to:

Counsel of record