

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

TREND MICRO, INC.,

Petitioner,

v.

TAASERA LICENSING LLC,

Patent Owner.

Patent No. 9,092,616

Filing Date: July 27, 2012

Issue Date: July 28, 2015

Inventors: Srinivas Kumar and Dennis Pollutro

Title: SYSTEMS AND METHODS FOR
THREAT IDENTIFICATION AND REMEDIATION

PATENT OWNER'S PRELIMINARY RESPONSE

Case No. IPR2023-00799

TABLE OF CONTENTS

	<u>Page(s)</u>
I. INTRODUCTION	1
II. THE '616 PATENT	2
III. THE ALLEGED PRIOR ART	8
A. Mukherjee	8
B. Miliefsky	9
C. Guo	10
IV. CLAIM CONSTRUCTION	11
V. LEVEL OF ORDINARY SKILL IN THE ART	13
VI. PETITIONER HAS NOT DEMONSTRATED A REASONABLE LIKELIHOOD OF SUCCESS FOR THE GROUNDS ADVANCED IN THE PETITION, AND THE PETITION SHOULD BE DENIED	14
A. Claim 1 is Not Obvious Over Mukherjee in Combination with Miliefsky	16
1. Mukherjee in Combination with Miliefsky Does Not Disclose “receiving, by the trust orchestration server, third party network endpoint assessments,” as Required by Claim 1	16
2. Mukherjee in Combination with Miliefsky Does Not Disclose “generating, by the trust orchestration server, temporal events based at least in part on analyzing the third party network endpoint assessments,” as Required by Claim 1	19
3. Mukherjee in Combination with Miliefsky Does Not Disclose “correlating, by the trust orchestration server, the received endpoint events and the generated temporal events,” as Required by Claim 1	21
B. Dependent Claims 2-7	22

VII.	THE PETITION SHOULD BE DENIED IN THE DISCRETION OF THE DIRECTOR UNDER 35 U.S.C. § 314(A)	22
A.	The Parallel District Court Proceeding and the Petition Involve the Same Parties	24
B.	The District Court Litigation Involves Substantially the Same Claims.....	25
C.	Proximity of the District Court’s Trial Date	25
D.	Significant Investment and Petitioner’s Delay in Filing the Petition.....	27
E.	No Stay of the Parallel District Court Litigation	27
F.	Other Factors Favor Discretionary Denial	29
VIII.	THE BOARD SHOULD REJECT ANY LATE SOTERA STIPULATION	29
IX.	CONCLUSION.....	31

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Apple Inc. v. Fintiv, Inc.</i> , IPR2020-00019, Paper 11 (P.T.A.B. Mar. 20, 2020)	23, 30
<i>Apple, Inc. v. Contentguard Holdings, Inc.</i> , IPR2015-00355, Paper 9 at 9-10 (P.T.A.B. June 26, 2015)	14
<i>Broadcom Corp. v. Emulex Corp.</i> , 732 F.3d 1325 (Fed. Cir. 2013)	15
<i>Cisco Sys., Inc. v. Ramot at Tel Aviv Univ. Ltd.</i> , IPR2020-00122, Paper 15 (P.T.A.B. May 15, 2020)	25, 26
<i>Edward LifeSciences Corp. v. Evalve, Inc.</i> , IPR2019-01479, Paper 7 (P.T.A.B. Feb. 26, 2020)	26
<i>Gen. Plastic Indus. Co., Ltd. v. Canon Kabushiki Kaisha</i> , IPR2016-01357, Paper 19 (P.T.A.B. Sept. 6, 2017)	24
<i>Graham v. John Deere Co. of Kansas City</i> , 383 U.S. 1 (1966)	15
<i>Innogenetics, N.V. v. Abbott Lab'ys.</i> , 512 F.3d 1363 (Fed. Cir. 2008)	17
<i>Intell. Ventures II v. FedEx Corp.</i> , No. 2:16-cv-00980-JRG, Dkt. 141 (E.D. Tex. Oct. 24, 2017)	32
<i>Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.</i> , 821 F.3d 1359 (Fed. Cir. 2016)	15
<i>KSR Int'l Co. v. Teleflex Inc.</i> , 550 U.S. 398 (2007)	14
<i>Lennon Image Techs., LLC v. Macy's Retail Holdings, Inc.</i> , 2:13-CV-00235-JRG, 2014 WL 4652117 (E.D. Tex. Sept. 18, 2014)	27

<i>Los Angeles Biomedical Rsch. Inst. at Harbor-UCLA Med. Ctr.</i> <i>v. Eli Lilly & Co.</i> , 849 F.3d 1049 (Fed. Cir. 2017).....	15
<i>Next Caller Inc. v. TrustID, Inc.</i> , IPR2019-00961, -00962, Paper 10, at 8-16 (P.T.A.B. Oct. 16, 2019)	26
<i>NHK Spring Co. v. Intri-Plex Techs., Inc.</i> , IPR2018-00752, Paper 8 (P.T.A.B. Sept. 12, 2018).....	24
<i>NXP USA, Inc. v Impinj, Inc.</i> , IPR2021-01556, Paper 12, 5-6 (P.T.A.B. Aug. 25, 2022); <i>see also</i> <i>id.</i> , IPR2021-01556, Paper 13, 3-4 (P.T.A.B. Sept. 7, 2022)	30
<i>Pers. Web Techs., LLC v. Apple, Inc.</i> , 848 F.3d 987 (Fed. Cir. 2017)	15
<i>Samsung Elecs. Am., Inc. v. Uniloc 2017 LLC</i> , IPR2019-01218, Paper 7 (P.T.A.B. Jan. 7, 2020)	26
<i>Sotera Wireless, Inc. v. Masimo Corp.</i> , IPR2020-01019, Paper 12, 13-14 (P.T.A.B. Dec. 1, 2020) (designated Dec. 17, 2020)	29
<i>Stratoflex, Inc. v. Aeroquip Corp.</i> , 713 F.2d 1530 (Fed. Cir. 1983)	14
<i>Supercell Oy v. Gree, Inc.</i> , IPR2020-00513, Paper 11 (P.T.A.B. June 24, 2020)	26
<i>Trend Micro, Inc., v. Taasera Licensing LLC</i> , IPR2023-00801, Paper 3 (P.T.A.B. April 27, 2023)	24
<i>In re: Taasera Licensing LLC, Patent Litigation</i> , No. 2:22-md-03042-JRG (E.D. Tex. Aug. 3, 2022).....	<i>passim</i>
<i>In re Van Os</i> , 844 F.3d 1359 (Fed. Cir. 2017)	15
Statutes	
35 U.S.C. § 314(a)	<i>passim</i>

35 U.S.C. § 314(b)(1).....25

35 U.S.C. § 316(a)(11).....25

Other Authorities

37 C.F.R. § 42.1(b) 30

LIST OF EXHIBITS

Exhibit No.	Description of Document
2001	Eighth Amended Docket Control Order, Dkt. 278, <i>In re: Taasera Licensing LLC, Patent Litigation</i> , No. 2:22-md-03042-JRG (E.D. Tex. Sept. 7, 2023)
2002	Defendants' Joint Patent L.R. 3-3 Invalidity Contentions and Subject Matter Ineligibility Contentions, <i>In re: Taasera Licensing LLC, Patent Litigation</i> , No. 2:22-md-03042-JRG, served March 28, 2023
2003	Joint Patent L.R. 4-5 Joint Claim Construction Chart, Dkt. No. 276-1, <i>In re: Taasera Licensing LLC, Patent Litigation</i> , No. 2:22-md-03042-JRG, filed September 1, 2023

I. INTRODUCTION

On April 5, 2023, Trend Micro, Inc. (“Petitioner”) submitted a petition (Paper 2, “Petition” or “Pet.”) to institute *inter partes* review (“IPR”) of U.S. Patent No. 9,092,616 (Ex. 1001, the “’616 Patent”), challenging claims 1-7 (the “Challenged Claims”). The Petition asserts that the Challenged Claims 1-6 are obvious over “Network Intrusion Detection” by Biswanath Mukherjee, L. Todd Heberlein, and Karl N. Levitt (“Mukherjee”) in combination with U.S. Patent Application Publication US 2007/0192867 to Miliefsky (“Miliefsky”) and that Challenged Claim 7 is obvious over Mukherjee in combination with Miliefsky and U.S. Patent 8,104,089 to Guo, et al. (“Guo”). Pet. at 2. However, the Board should deny the Petition for at least two reasons: (1) the Petitioner fails to identify how certain elements of the Challenged Claims are obvious over Mukherjee in combination with Miliefsky and Guo; and (2) the Board should exercise its discretion to deny the Petition under 35 U.S.C. § 314(a).

Petitioner fails to show that Mukherjee’s NSM services are *endpoint* assessments, as required by the claim language, because Mukherjee describes that network connections are assessed rather than endpoints. Petitioner’s cited portions of Miliefsky are silent with respect to endpoint assessments. Miliefsky, like Mukherjee, focuses on assessing the network and the connections between equipment and the network, but does not assess the endpoint. Petitioner’s argument

is unclear because Petitioner does not disclose how Mukherjee's alleged endpoint events and generated temporal events are correlated.

Petitioner also does not explain why a POSITA would be motivated to combine Mukherjee with Miliefsky to compare an event to descriptions of locations and protocols of network based assets, when Petitioner's cited portion of Mukherjee clearly describes comparing two events for their proximity in time.

The Board should exercise its discretion to deny this Petition for at least the following reasons: (i) there exists a parallel District Court proceeding between the same parties regarding the same subject patent (the '616 Patent); (ii) the Petition is co-extensive with invalidity arguments that Petitioner has already raised in the District Court Litigation; (iii) the District Court's trial will be almost *seven months before* the projected statutory deadline; (iv) the parties have heavily invested in the District Court proceeding since claim construction briefing is complete, fact discovery closes in approximately three months on November 6, 2023, and a trial date is set for April 15, 2024, which is only about seven months away; and (v) there is no stay of the parallel District Court Litigation.

II. THE '616 PATENT

The '616 Patent "relates to the field of data center virtualization and, more particularly, to systems and methods for providing dynamic operational integrity

attestation of application security and a user reputation at runtime.” ’616 Patent, 1:15-18.

The ’616 Patent addresses several problems in existing attestation systems:

Existing attestation systems are often narrowly focused and generally aimed at specific use-cases limited to system components such as hardware and applications and therefore typically lack flexibility to dynamically address more general attestation problems. Further, existing definitions of attestation focus primarily on describing specific, narrow, and particular properties desirable in specific use-cases. Additionally, current attestation systems are created to work with one particular measurement system targeting one particular system of interest without considering the reputations of users or operators of the system of interest.

Id. at 3:62-4:5.

The claimed invention of the ’616 Patent provides several benefits that address the problems described above:

Accordingly, what the present inventors have identified as desirable are technology based attestation architectures, systems, and methods that perform a calculus of risk to determine a level of trust of systems that are not necessarily monolithic and can be made up of diverse hardware and software platforms and can be accessed by users with varying credentials and reputations. Accordingly, what the inventors have identified as being desirable are attestation architectures, systems, and methods that can be flexible enough to accommodate varying concepts of attestation, including taking the reputation of users that access targeted systems into account. What the present inventors also see as desirable are attestation systems and architectures that can

dynamically handle complex attestation scenarios and provide more complete runtime attestation than is currently achievable. What the present inventors additionally see as desirable are methods and systems for performing evidence based automated application binary analysis.

Id. at 4:6-24.

The '616 Patent describes that network endpoint assessments refer to assessments made of endpoints on a given network.

In an embodiment, the network endpoint assessment 1001 comprises performing a security scan of network endpoints for vulnerability, configuration, compliance, and patch management and use the results of these scans to generate a security assessment report 1026. As shown in FIG. 10, an endpoint collator 1002 is configured to receive the generated security assessment report 1026. In embodiments depicted in FIG. 10, at this point, the endpoint collator 1002 can then sort the security assessment report 1026 by endpoint address and/or geo-location to produce categorized reports 1027.

Id. at 22:43-52.

FIG. 4 illustrates data flows used to configure an attestation system. In particular, ***FIG. 4 depicts a data flow for consolidating and normalizing network endpoint assessments*** as part of a configuration for an exemplary attestation system 400.

Referring to FIG. 4, the exemplary attestation system 400 includes a trust orchestrator 430, a trust broker 407 configured to receive integrity reports 406 published by ***endpoint assessment services*** 401.

Id. at 11:8-15 (emphasis added).

With continued reference to FIG.4, the trust broker 407 can be configured to receive sensory data feeds that represent the configuration state of the system based on a remotely administered scan of a device, such as device 560 described with reference to FIG. 5 below, by *endpoint assessment services* 401.

Id. at 11:17-22 (emphasis added).

In embodiments, the integrity report 406 is generated by third party *endpoint assessment services* at platform- and application-level granularities.

Id. at 11:28-30 (emphasis added).

The '616 Patent describes the endpoint assessment analysis further, noting that “temporal events” “annotate the state of the endpoints (devices) at scan time”:

The trust broker 407 can also be configured to parse, normalize and collate received integrity reports 406. In accordance with embodiments, the parsing, normalizing, and/or collating can be based on one or more object identifiers. Exemplary object identifiers can include, but are not limited to, machine hostnames, IP addresses, application names, and package names. This parsing, normalization, and collation (collectively, processing) generates temporal events 409 that annotate the state of the endpoints (devices) at scan time. Additional embodiments of the trust broker are described with reference to FIGS. 5, 9, and 11 below. . . .

With continued reference to FIG. 4, the temporal events 409 can be an annotation (e.g., an XML representation) of the configuration state of the system (including device, application and package) and include trust and severity scores as generated by third party security vendors based

on integrity measurement and verification, in accordance with standards established by organizations. . . .

[T]emporal events can be assertions about operational parameters expressed in the Open Vulnerability and Assessment Language (OVAL) to convey system details representing configuration information and a system/machine state including vulnerability, configuration, patch level, etc. Alternatively, the system details can be conveyed using the SCAP protocol. According to embodiments, the state representation includes schema attributes to measure configuration, vulnerability (exposures), compliance, and patch level based on severity.

Id. at 11:40-12:9.

The generated temporal events of the claimed invention are based at least in part on analyzing the third party network endpoint assessments, which “are agnostic to runtime aspects of the system including applications thereon.”

With continued reference to FIG. 4, the trust broker 407 can be configured to receive sensory data feeds that represent the configuration state of the system based on a remotely administered scan of a device, such as device 560 described with reference to FIG. 5 below, by endpoint assessment services 401. These scans provide a snapshot in time of the state of the system and are agnostic to runtime aspects of the system including applications thereon.

Id. at 11:17-24.

The '616 Patent explains that integrity profiles for a system are formed based on correlation, which is determining a relationship between two separate types of events (*i.e.*, the received endpoint events and the generated temporal events):

According to embodiments, the system event correlator 410 shown in FIG. 5 can be ***configured to receive temporal events 409 generated by the trust broker 407 that measure the integrity of the system at last scan, and endpoint events 520 from the endpoint trust agent 510 that measure the runtime execution state of applications.*** The system event correlator 410 can be further configured to map the events to a cell in the risk correlation matrix 411 grid and processes the triggered system warnings to evaluate threats by category (or vectors). In one embodiment, the categories include at least resource utilization, system configuration, and application integrity. Each category is assigned a metric that is an indicator of the level of runtime operational integrity that may be asserted based on the system warnings and threat classification produced by the risk correlation matrix 411. The system event correlator 410 can also be configured to generate an integrity profile 420 for the device 560 that describes the security risks and threats posed by the measured execution state of running applications on the device 560.

Id. at 14:54-15:5 (emphasis added).

The '616 Patent describes that “the integrity profile 420 represents an aggregation of system warnings (threats such as malware) identified based on the received temporal 409 and endpoint 520 events.” *Id.* at 12:41-44.

III. THE ALLEGED PRIOR ART

A. Mukherjee

In Mukherjee, “several host-based and network-based IDSs are surveyed, and the characteristics of the corresponding systems are identified. The host-based systems employ the host operating system’s audit trails as the main source of input to detect intrusive activity, while most of the network-based IDSs build their detection mechanism on monitored network traffic, and some employ host audit trails as well. An outline of a statistical anomaly detection algorithm employed in a typical IDS is also included.” Ex. 1005, 1.

The disclosure of Mukherjee confirms that its NSM (Network Security Monitor) services do not assess an endpoint. For example, “[t]he NSM analyzes traffic on a broadcast LAN to detect intrusive behavior.” *Id.* at 8. Mukherjee further describes that network connections are assessed rather than endpoints: “During a particular two-month test period, the NSM analyzed more than 111,000 connections on the Computer Science LAN segment at UC Davis, and it correctly identified more than 300 of these connections as intrusive.” *Id.* at 11. Therefore, Mukherjee’s NSM (*network security* monitoring) services monitor and assess a network to determine whether there is intrusive behavior on that network.

B. Miliefsky

Miliefsky “relates to computer security, and more particularly to a micro-appliance for use in defending against common vulnerabilities and exploits.” Ex. 1006, [0004], Figs. 5-7 (“Automated Vulnerability Assessment Scanning Engine”).

Miliefsky focuses on assessing the network and the connections between equipment and the network, but does not assess the endpoint:

[T]he invention provides a security method that can be executed on a wired and/or wireless network. As part of the security method, in a first step *the network is scanned* and/or probed for any and all attached equipment and related assets, herein referred to as “network based” assets. The method will dynamically *detect and map changes* to LAN and WAN connected equipment including searching for equipment which may be deemed as rogue and creating a network-based assets list, wherein the list contains *information as to the location* of the network-based assets.

Id. at [0040] (emphasis added).

In a further step, the method audits one or more of the network-based assets for common vulnerabilities and exposures (CVEs).

Id. at [0043].

The method defines a true risk profile *for the computer-based network environment*, and uses the knowledge of external and internal CVEs as well as how to manage and remediate against these CVEs, to provide more robust and proactive security.

Id. at [0045] (emphasis added). As shown above, assets or endpoints are only monitored to the extent that Miliefsky can assess vulnerabilities and exposures and provide a risk profile (*i.e.*, create an assessment) ***for the network***, not the endpoint. Miliefsky's description of "network-based assets list" also refers to metrics of location and the structure of the network:

The list may contain information as to the Internet Protocol (IP) address of said network-based assets, and the list may contain information as to the open Ports of said network-based assets and related application, session, transport, sockets and other internet protocol (IP) related information. The list may contain other information such as the Media Access Control (MAC) address of said network based assets, whether the connection is Wired or Wireless of said network-based assets and other information about the structure of the network and its component devices.

Id. at [0041].

C. Guo

Guo "relates generally to antivirus software for detecting malicious code, and in particular to preventing packers from evading the scanning of their dynamically created malicious code." Ex. 1011, 1:15-18.

The invention of Guo is indicated by the graphic below:

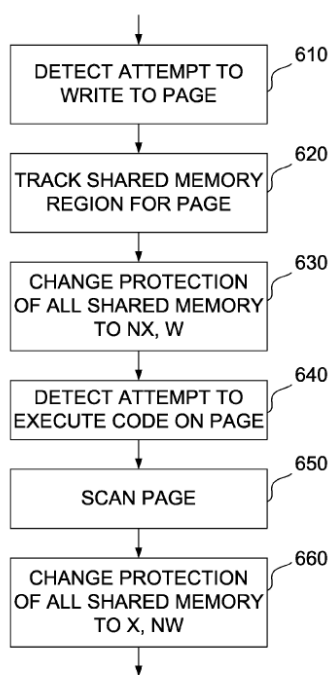


FIGURE 6

Id. at Fig. 6.

IV. CLAIM CONSTRUCTION

For the purposes of this Preliminary Response only, Patent Owner believes that claim construction is not required to resolve any issues. Petitioner also notes that it believes that claim construction is not otherwise warranted. Pet. at 10-11. However, there are several terms that both Petitioner and Patent Owner have proposed constructions for in the District Court Litigation, as noted below:

<u>Claim Term</u>	<u>Patent Owner's Proposed Construction</u>	<u>Petitioner's Proposed Construction</u>
"third party network endpoint assessments"	"at least two assessments of a	"at least two assessments of a

<u>Claim Term</u>	<u>Patent Owner's Proposed Construction</u>	<u>Petitioner's Proposed Construction</u>
'616 Patent Claims 1, 2, and 4	network endpoint provided by one or more third parties"	network endpoint provided by one or more third parties"
"attestation" '441 Patent Claims 1, 2, 3, 5, and 7 '616 Patent Claim 1	verification	verifying/verifies the identity of an application
"runtime" '616 Patent Claim 1	the time the system or device is running	the time the application being monitored is running.
"at runtime" '616 Patent Claim 1	at the time the system or device is running	Preamble limiting, at least as to "at runtime"; meaning: "at the time the application being monitored is running."
"a computing platform comprising a network trust agent" '616 Patent Claim 1	Plain and ordinary meaning	Limiting preamble; indefinite

Ex. 2003 at 39-45, 56-62. This, in addition to the plethora of other outstanding issues

that affect validity, weighs in favor of the Board using its discretion to deny institution of this Petition so that all validity issues could be resolved in the District Court Litigation.

V. LEVEL OF ORDINARY SKILL IN THE ART

For the purposes of this Preliminary Response only, Patent Owner utilizes Petitioner's proposed level of skill in the art: "a bachelor's degree in computer science, or a related field, or an equivalent technical degree or equivalent work experience, and an additional one to two years of education or experience in the field of computer security topics. More education can supplement practical experience and vice versa." Pet. at 10 (citations omitted).

**VI. PETITIONER HAS NOT DEMONSTRATED A REASONABLE
LIKELIHOOD OF SUCCESS FOR THE GROUNDS
ADVANCED IN THE PETITION, AND THE PETITION
SHOULD BE DENIED**

The question of obviousness is resolved on the basis of underlying factual determinations, including: (1) the scope and content of the prior art, (2) any differences between the claimed subject matter and the prior art, (3) the level of skill in the art, and (4) so-called secondary considerations where in evidence. *Graham v. John Deere Co. of Kansas City*, 383 U.S. 1, 17-18 (1966); *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question is not whether the differences themselves would have been obvious, but whether the claimed invention as a whole would have been obvious. *Stratoflex, Inc. v. Aeroquip Corp.*, 713 F.2d 1530, 1537 (Fed. Cir. 1983).

The Board has held that a failure to identify the differences between the claimed subject matter and the prior art is fatal to an obviousness challenge. *See, Apple, Inc. v. Contentguard Holdings, Inc.*, IPR2015-00355, Decision Denying Institution of *Inter Partes* Review, Paper 9 at 9-10 (P.T.A.B. June 26, 2015) (denying institution for failure to identify the differences between the claimed subject matter and the prior art).

In arriving at an obviousness determination, the Board must sufficiently explain and support the conclusions that the prior-art references disclose all the

elements recited in the Challenged Claims and a relevant, skilled artisan not only could have made, but would have been motivated to combine all the prior art references in the way the patent claims and reasonably expected success. *Pers. Web Techs., LLC v. Apple, Inc.*, 848 F.3d 987, 994 (Fed. Cir. 2017). That is, even if all the claim elements are found across a number of references, an obviousness determination must consider whether a person of ordinary skill in the art would have the motivation to combine those references. *Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1368 (Fed. Cir. 2016); *Los Angeles Biomedical Rsch. Inst. at Harbor-UCLA Med. Ctr. v. Eli Lilly & Co.*, 849 F.3d 1049, 1067 (Fed. Cir. 2017) (vacating and remanding an obviousness determination, in part, because the Board did not make factual finding as to whether there was an apparent reason to combine all three prior art references to achieve the claimed invention and whether a person of skill in the art would have had a reasonable expectation of success from such a combination). This combinability determination, as supported by an articulated motivation to combine, requires a plausible rationale as to why those prior art references would have worked together. *Broadcom Corp. v. Emulex Corp.*, 732 F.3d 1325, 1335 (Fed. Cir. 2013). Absent some articulated rationale, a “common sense” finding is no different than the conclusory statement “would have been obvious.” *In re Van Os*, 844 F.3d 1359, 1361 (Fed. Cir. 2017). Of additional importance, “knowledge of a problem and motivation to solve it are entirely different

from motivation to combine particular references. . . .” *Innogenetics, N.V. v. Abbott Lab’ys.*, 512 F.3d 1363, 1373 (Fed. Cir. 2008).

A. Claim 1 is Not Obvious Over Mukherjee in Combination with Miliefsky

1. Mukherjee in Combination with Miliefsky Does Not Disclose “receiving, by the trust orchestration server, third party network endpoint assessments,” as Required by Claim 1

Claim 1 of the ’616 Patent recites “receiving, by the trust orchestration server, third party network endpoint assessments.” Mukherjee in combination with Miliefsky does not render this claim limitation obvious, as Petitioner incorrectly asserts. Pet. at 38-43.

Petitioner argues that Mukherjee’s NSM (Network Security Monitor) services disclose the claimed “third party network endpoint assessments.” But despite stating that Mukherjee’s “‘NSM services’ provide *network* assessment to clients,” (Pet. at 38) and that Mukherjee’s “NSM services provide network assessments regarding the hosts or device” (Pet. at 39), Petitioner fails to show that NSM services are *endpoint* assessments, as required by the claim language. The disclosure of Mukherjee confirms that NSM services do not assess an endpoint. For example, “[t]he NSM analyzes traffic on a broadcast LAN to detect intrusive behavior.” Ex. 1005, 8. Mukherjee further describes that network connections are assessed rather than endpoints: “During a particular two-month test period, the NSM analyzed more than

111,000 connections on the Computer Science LAN segment at UC Davis, and it correctly identified more than 300 of these connections as intrusive.” *Id.* at 11. Therefore, NSM (**network security** monitoring) services merely monitor and assess a network to determine whether there is intrusive behavior on that network. But monitoring network traffic or network connections is not monitoring or assessing an endpoint.

Miliefsky does not cure the deficiencies of Mukherjee, and Petitioner’s cited portions of Miliefsky are silent with respect to endpoint assessments. The only assessments described in those portions of the Petition describe only vulnerability assessments. *See* Pet. at 40 (“Miliefsky discloses that the security appliance collects a wide range of data including vulnerability assessments.”); *see also* Ex. 1006, Figs. 5-7 (“Automated Vulnerability Assessment Scanning Engine”). Miliefsky, like Mukherjee, focuses on assessing the network and the connections between equipment and the network, but does not assess the endpoint:

[T]he invention provides a security method that can be executed on a wired and/or wireless network. As part of the security method, in a first step **the network is scanned** and/or probed for any and all attached equipment and related assets, herein referred to as “network based” assets. The method will dynamically **detect and map changes** to LAN and WAN connected equipment including searching for equipment which may be deemed as rogue and creating a network-based assets list, wherein the list contains **information as to the location** of the network-based assets.

Ex. 1006, [0040] (emphasis added).

In a further step, the method audits one or more of the network-based assets for common vulnerabilities and exposures (CVEs).

Id. at [0043].

The method defines a true risk profile *for the computer-based network environment*, and uses the knowledge of external and internal CVEs as well as how to manage and remediate against these CVEs, to provide more robust and proactive security.

Id. at [0045] (emphasis added). Assets or endpoints are only monitored to the extent that Miliefsky can assess vulnerabilities and exposures and provide a risk profile (*i.e.*, create an assessment) *for the network*, not the endpoint.

Petitioner's stated motivation to combine Mukherjee and Miliefsky to form an Intrusion Detection System is also misguided because the '616 Patent explicitly distinguishes IDS systems, such as the one proposed by Petitioner's combination of Mukherjee and Miliefsky:

The current predominant security paradigm is based on a hard edge and softcore architecture. Security appliances such as network firewalls and intrusion detection/prevention systems deploy at the edge (perimeter). Antivirus and network based integrity measurement and verification services scan and audit the soft-core that comprises business critical systems, services and high value data silos. Once the edge is breached, defensive methods are largely ineffective in protecting vulnerable or compromised systems. In this paradigm, the

hard edge does not generally provide any level of assurance of the runtime operational integrity of the soft core.

'616 Patent, 2:24-34. The combination of Mukherjee and Miliefsky forms an IDS like the prior art description of the '616 Patent that is also “deploy[ed] at the edge” because both Mukherjee and Miliefsky ultimately only assess the network and its connections, but not the endpoint as the claim requires.

Mukherjee in combination with Miliefsky does not render obvious this claim limitation.

2. Mukherjee in Combination with Miliefsky Does Not Disclose “generating, by the trust orchestration server, temporal events based at least in part on analyzing the third party network endpoint assessments,” as Required by Claim 1

Claim 1 of the '616 Patent recites “generating, by the trust orchestration server, temporal events based at least in part on analyzing the third party network endpoint assessments.” Mukherjee in combination with Miliefsky does not render this claim limitation obvious, as Petitioner incorrectly asserts. Pet. at 43-44.

Since Petitioner fails to show how Mukherjee in combination with Miliefsky discloses, teaches, or suggests the claimed “third party network endpoint assessments,” it cannot now disclose, teach, or suggest “generating, by the trust orchestration server, temporal events *based at least in part on analyzing the third party network endpoint assessments.*” See *supra* Section VI.A.1.

Petitioner’s argument that Miliefsky’s “network based assets list” corresponds to the claimed “temporal events,” Pet. at 43-44, should be rejected. Miliefsky’s description of “network-based assets list” only refers to metrics of location and the structure of the network:

The list may contain information as to the Internet Protocol (IP) address of said network-based assets, and the list may contain information as to the open Ports of said network-based assets and related application, session, transport, sockets and other internet protocol (IP) related information. The list may contain other information such as the Media Access Control (MAC) address of said network based assets, whether the connection is Wired or Wireless of said network-based assets and other information about the structure of the network and its component devices.

Ex. 1006, [0041]. Miliefsky’s description of network based lists is completely devoid of “analyzing [] third party network endpoint assessments” as the claim requires.

Petitioner’s argument that the claimed temporal events are disclosed by combining “configuration data collected or processed” with “vulnerability assessment data” or “internal assessments” combined with “external assessments” is incorrect. Pet. at 44. Combinations of two existing data presupposes that both exist at a given time and, therefore one set of data cannot be based on the other. The claim language recites “generating . . . temporal events based at least in part on analyzing

the third party network endpoint assessments,” which is not met by the disclosure of Miliefsky.

Therefore, Mukherjee in combination with Miliefsky does not render obvious this claim limitation.

3. Mukherjee in Combination with Miliefsky Does Not Disclose “correlating, by the trust orchestration server, the received endpoint events and the generated temporal events,” as Required by Claim 1

Claim 1 of the '616 Patent recites “correlating, by the trust orchestration server, the received endpoint events and the generated temporal events.” Mukherjee in combination with Miliefsky does not render this claim limitation obvious, as Petitioner asserts. Pet. at 45-47.

Since Petitioner fails to show how Mukherjee in combination with Miliefsky discloses, teaches, or suggests the claimed “generated temporal events,” it cannot now disclose, teach, or suggest “correlating, by the trust orchestration server, the received endpoint events and the generated temporal events.” *See supra* Section VI.A.2.

Petitioner’s argument is unclear because Petitioner does not disclose how Mukherjee’s alleged endpoint events and generated temporal events are correlated. The only description of correlation in Petitioner’s cited portion of Mukherjee refers to how “the expert system uses time windows to correlate events occurring in

temporal proximity.” Pet. at 45-46 (citing Ex. 1005, 13). Mukherjee further describes how that temporal proximity is a related pattern of behavior or attack signature. *Id.* None of Mukherjee’s “correlate[d] events” are the temporal events (*i.e.*, network based asset lists) described by Petitioner with respect to the previous claim.

Petitioner does not explain why a POSITA would be motivated to combine Mukherjee with Miliefsky to compare an event to descriptions of locations and protocols of network based assets, when Petitioner’s cited portion of Mukherjee clearly describes comparing two events for their proximity in time.

Therefore, Mukherjee in combination with Miliefsky does not render obvious this claim limitation.

B. Dependent Claims 2-7

Claims 2-7 are dependent on Claim 1. Therefore, Claims 2-7 are not rendered obvious by any combination of Mukherjee, Miliefsky, and Guo for at least the same reasons as Claim 1.

VII. THE PETITION SHOULD BE DENIED IN THE DISCRETION OF THE DIRECTOR UNDER 35 U.S.C. § 314(A)

Based on Petitioner’s reasons regarding § 314(a), the Board should exercise its discretion to deny this Petition.

The circumstances of the parallel District Court Litigation necessitate denial of the Petition under the Board’s precedent, as every factor considered in relation to

efficiency, fairness, and the merits supports denial. *See Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11, at 6 (P.T.A.B. Mar. 20, 2020) (precedential) (considering (a) “whether the petitioner and the defendant in the parallel proceeding are the same party”; (b) “overlap between issues raised in the petition and in the parallel proceeding” (c) “proximity of the court’s trial date to the Board’s projected statutory deadline for a final written decision”; (d) “investment in the parallel proceeding by the court and the parties”; (e) “whether the court granted a stay or evidence exists that one may be granted if a proceeding is instituted”; and (f) “other circumstances that impact the Board’s exercise of discretion, including the merits.”).

As set forth below, these factors collectively demonstrate that efficiency and integrity of the AIA are best served by denying review. First, the Petitioner is the Defendant in the parallel proceeding. *See infra* Section VII.A. Second, the asserted claims in the District Court Litigation are all at issue in the Petition. *See infra* Section II.B. Third, trial in the District Court Litigation is set for April 15, 2024, eight months earlier than the projected statutory deadline for a Final Written Decision of this Petition in December 16, 2024. *See infra* Section VII.C. Fourth, the parties (and Patent Owner in particular) have invested significant resources on developing legal and factual issues of validity and infringement in the District Court Litigation and will have invested substantially more resources before any decision on this Petition. *See infra* Section VII.D. Fifth, the Court has neither granted nor denied a stay

pending this Petition. *See infra* Section VII.E. Finally, no other factors favor institution. *See infra* Section VII.F.

Accordingly, the Board should exercise its discretion under § 314(a) and deny the Petition because institution of this proceeding would not be consistent with the objective of the AIA to “provide an effective and efficient alternative to District Court litigation.” *NHK Spring Co. v. Intri-Plex Techs., Inc.*, IPR2018-00752, Paper 8, at 20 (P.T.A.B. Sept. 12, 2018) (quoting *Gen. Plastic Indus. Co., Ltd. v. Canon Kabushiki Kaisha*, IPR2016-01357, Paper 19, at 16–17 (P.T.A.B. Sept. 6, 2017) (precedential)).

A. The Parallel District Court Proceeding and the Petition Involve the Same Parties

As noted in Patent Owner’s Mandatory Notice, there exists a parallel District Court Litigation between the same parties regarding the same subject patent (the ’616 Patent). *Trend Micro, Inc., v. Taasera Licensing LLC*, IPR2023-00799, Paper 3 at 2-3 (P.T.A.B. April 26, 2023); Pet. at 63-64. Petitioner is a party to the District Court Litigation captioned as *In re: Taasera Licensing LLC, Patent Litigation*, No. 2:22-md-03042-JRG (E.D. Tex. Aug. 3, 2022) (the “District Court Litigation”). Accordingly, this factor weighs in favor of discretionary denial.

B. The District Court Litigation Involves Substantially the Same Claims

The asserted claims in the District Court Litigation are all at issue in the Petition since this Petition involves all of the '616 Patent's claims. "In at least these ways, the parallel proceedings would duplicate effort. This is an inefficient use of Board, party, and judicial resources and raises the possibility of conflicting decisions." *Cisco Sys., Inc. v. Ramot at Tel Aviv Univ. Ltd.*, IPR2020-00122, Paper 15 at 10 (P.T.A.B. May 15, 2020). Accordingly, this fact weighs in favor of discretionary denial.

C. Proximity of the District Court's Trial Date

The proximity of the District Court Litigation's trial date to the Board's projected statutory deadline for a Final Written Decision strongly weighs in favor of discretionary denial.

The parties' trial is scheduled for April 15, 2024. Exhibit 2001 (Eighth Amended Docket Control Order, Dkt. 278, *In re: Taasera Licensing LLC, Patent Litigation*, No. 2:22-md-03042-JRG (E.D. Tex. September 7, 2023)). Pursuant to 35 U.S.C. §§ 314(b)(1) and 316(a)(11), the projected statutory deadline for a Final Written Decision of this Petition is December 16, 2024.¹ As the District Court's trial

¹ The statutory deadline for institution is December 14, 2023, "three months after receiving a preliminary response to the petition under section 313." *See* 35 U.S.C. § 314(b)(1). If instituted, the statutory deadline for Final Written Decision is

will be almost *eight months before* the projected statutory deadline, this factor weighs strongly in favor of denying institution. *See Supercell Oy v. Gree, Inc.*, IPR2020-00513, Paper 11 at 10-12 (P.T.A.B. June 24, 2020) (denying institution where the jury trial was scheduled to conclude approximately ten months before the statutory deadline); *Edward LifeSciences Corp. v. Evalve, Inc.*, IPR2019-01479, Paper 7, at 6-13 (P.T.A.B. Feb. 26, 2020) (denying institution where jury trial would conclude more than nine months before a final decision would be due); *Samsung Elecs. Am., Inc. v. Uniloc 2017 LLC*, IPR2019-01218, Paper 7, at 7-10 (P.T.A.B. Jan. 7, 2020) (denying institution where jury selection was scheduled for approximately six months before trial in the Board proceeding would conclude); *Next Caller Inc. v. TrustID, Inc.*, IPR2019-00961, -00962, Paper 10, at 8-16 (P.T.A.B. Oct. 16, 2019) (denying institution where trial was scheduled to conclude “several months,” before a final decision would be due); *Cisco Sys., Inc.*, IPR2020-00122, Paper 15 at 8 (“Because the trial date is substantially earlier than the projected statutory deadline for the Board’s final decision, this factor weighs in favor of discretionary denial.”).

Petitioner does not contest that the proximity of the trial favors denial of institution. Thus, this factor also weighs in favor of discretionary denial.

December 16, 2024, “not later than 1 year after the date on which the Director notices the institution of a review,” because December 14, 2024 falls on a Saturday.

D. Significant Investment and Petitioner's Delay in Filing the Petition

The parties' investment in the parallel proceeding weighs in favor of discretionary denial. In the District Court Litigation, the Court has already entered nine Docket Control Orders (Dkts. 8, 15, 46, 84, 209, 225, 239, 257, 278), Discovery Order (Dkt. 137), Protective Order (Dkt. 162), and E-Discovery Order (Dkt. 195). Discovery is also well under way. The parties have already exchanged claim construction briefing, infringement contentions pursuant to P.R. 3-1, and invalidity contentions pursuant to P.R. 3-3, fact discovery closes in less than three months on November 6, 2023, and a trial date is set for April 15, 2024, which is less than seven months away. Ex. 2001. Thus, the parties' and Court's substantial investment in this proceeding weighs in favor of denial of institution under this factor.

E. No Stay of the Parallel District Court Litigation

There is no stay of the parallel District Court Litigation. Even if the Petition were instituted and Petitioner filed a motion to stay the District Court Litigation, prejudice, tactical disadvantage to Taasera, the late stage of the litigation, and the lack of potential simplification would weigh strongly against such a motion. *See Lennon Image Techs., LLC v. Macy's Retail Holdings, Inc.*, 2:13-CV-00235-JRG, 2014 WL 4652117, at *1 (E.D. Tex. Sept. 18, 2014). The statutory deadline for institution is not until after the district court's claim construction hearing and the

deadline to complete fact discovery,² placing any motion for a stay close to trial. Ex. 2001; *see Intell. Ventures II v. FedEx Corp.*, No. 2:16-cv-00980-JRG, Dkt. 141 at 5 (E.D. Tex. Oct. 24, 2017) (“The Court agrees that the Parties have already invested substantial effort and resources during discovery and in preparing claim construction briefing. . . . These circumstances weigh against staying this case”).

Moreover, a stay would not decrease the burden on the Court and the parties since any instituted IPR would not cover any of the references that Petitioner raised in the District Court Litigation for both anticipation or any of the combinations of obviousness, and do not include Petitioner’s challenges under § 112 or § 101. *See* generally Ex. 2002, at 28-31, 35, 69-70, 199-222, 290-292, and 380-382. *Intell. Ventures II*, No. 2:16-cv-00980-JRG, Dkt. 141 at 3-4 (“[T]he instituted IPRs only cover a narrow slice of the invalidity arguments Defendants have raised in this case. For example, Defendants have argued that the ’715 Patent is invalid under § 102 with respect to at least eight references . . . under § 103 with respect to at least twenty-six combinations . . . under § 112 [], and under § 101.”).

Accordingly, it would be unlikely for the Court to hold that a stay would streamline the litigation and this factor supports denial of institution.

² As noted above, the statutory deadline for institution is December 14, 2023. *See supra* n. 1. Per Ex. 2001, the claim construction hearing is October 11, 2023, and the deadline to complete fact discovery is November 6, 2023.

F. Other Factors Favor Discretionary Denial

Petitioner does not present a strong case on the merits, further supporting denial of institution. *See supra* Section VI. Petitioner also does not identify any other factors which weigh against discretionary denial. Pet. at 61-63.

Thus, when viewing the factors together, the Petition should be denied in the Director's discretion under 35 U.S.C. § 314(a).

VIII. THE BOARD SHOULD REJECT ANY LATE SOTERA STIPULATION

Petitioner has not made a *Sotera*-style stipulation that “if IPR is instituted, [Petitioner] will not pursue in the District Court Litigation any ground raised or that could have been reasonably raised in an IPR” in its Petition, which weighs further in favor of discretionarily denying institution. *See Sotera Wireless, Inc. v. Masimo Corp.*, IPR2020-01019, Paper 12, 13-14 (P.T.A.B. Dec. 1, 2020) (designated Dec. 17, 2020).

The Board should not accept any late *Sotera* stipulation after this Patent Owner Preliminary Response. Petitioner has known about the related District Court Litigation since Patent Owner filed a Complaint asserting infringement of the '616 Patent against Trend Micro Incorporated (November 30, 2021) approximately 16 months before this Petition (April 5, 2023) and has had several docket control orders for the District Court Litigation, which originally anticipated a trial date for October

30, 2023. Docket Control Order, Dkt. 17, *Taasera Licensing LLC v. Trend Micro Incorporated*, No. 2:21-cv-00441-JRG (E.D. Tex. August 3, 2022). Any withholding of the *Sotera* stipulation in its Petition is gamesmanship and prejudicial to Patent Owner in this proceeding, and is inconsistent with 37 C.F.R. § 42.1(b)'s mandate to "secure the just, speedy, and inexpensive resolution of every proceeding."

Both the Board and Director are abundantly clear that Petitioner cannot wait until after the Board renders its Institution Decision to address the issue of *Fintiv*, the Board's discretionary authority, and to submit a *Sotera* stipulation. *NXP USA, Inc. v Impinj, Inc.*, IPR2021-01556, Paper 12, 5-6 (P.T.A.B. Aug. 25, 2022); *see also id.*, IPR2021-01556, Paper 13, 3-4 (P.T.A.B. Sept. 7, 2022) (resulting the Director finding "that the Board correctly determined that a stipulation, offered by a petitioner for the first time after a decision denying institution, is not a proper basis for granting rehearing of the decision on institution;" "[p]ermitting a petitioner to wait and see if the Board denies institution under *Fintiv*, and then offer such a stipulation for the first time on rehearing, frustrates these goals [of avoiding conflicting decisions] and would open the door to gamesmanship;" "***the only appropriate time for a petitioner to offer a stipulation related to the Fintiv factor 4 analysis is prior to the Board's decision of whether to institute review***") (emphasis added).

IX. CONCLUSION

For the foregoing reasons, Patent Owner respectfully requests that the Board deny institution of the Petition in its entirety.

Respectfully submitted,

Dated: September 14, 2023 By: / Peter Lambrianakos /
Peter Lambrianakos (Reg. No. 58,279)
Lead Counsel for Patent Owner
FABRICANT LLP
411 Theodore Fremd Avenue,
Suite 206 South
Rye, New York 10580
Tel. 212-257-5797
Fax. 212-257-5517
Email: plambrianakos@fabricantllp.com

Vincent J. Rubino, III (Reg. No. 68,594)
Alfred R. Fabricant (subject to motion to
appear *pro hac vice*)
Joseph M. Mercadante (Reg. No. 64,077)
Backup Counsel for Patent Owner
FABRICANT LLP
411 Theodore Fremd Avenue,
Suite 206 South
Rye, New York 10580
Tel. 212-257-5797
Fax.: 212-257-5517
Email: vrubino@fabricantllp.com
Email: ffabricant@fabricantllp.com
Email: jmercadante@fabricantllp.com

CERTIFICATE OF WORD COUNT

The undersigned hereby certifies that the portions of the above-captioned PATENT OWNER'S PRELIMINARY RESPONSE specified in 37 C.F.R. § 42.24 has 7,447 words in compliance with the 14,000 word limit set forth in 37 C.F.R. § 42.24. This word count was prepared using Microsoft Word for Office 365.

Respectfully Submitted,

September 14, 2023

By: / Peter Lambrianakos /
Peter Lambrianakos (Reg. No. 58,279)
Lead Counsel for Patent Owner
FABRICANT LLP
411 Theodore Fremd Avenue,
Suite 206 South
Rye, New York 10580
Tel. 212-257-5797
Fax. 212-257-5517

CERTIFICATE OF SERVICE

A copy of PATENT OWNER'S PRELIMINARY RESPONSE and EXHIBITS 2001 through 2003 have been served on Petitioner's counsel of record as follows:

Robert M. Hansen
Email: rhansen@marburylaw.com
Email: pat-docketng@marburylaw.com
Matthew J. Anderson
Email: manderson@marburylaw.com
Scott B. Amankwatia
Email: samankwatia@marburylaw.com
THE MARBURY LAW GROUP, PLLC
11800 Sunrise Valley Drive, 15th Floor
Reston, VA 20191

Attorneys for Trend Micro Inc.

September 14, 2023

By: / Peter Lambrianakos /
Peter Lambrianakos (Reg. No. 58,279)
Lead Counsel for Patent Owner
FABRICANT LLP
411 Theodore Fremd Avenue,
Suite 206 South
Rye, New York 10580
Tel. 212-257-5797
Fax. 212-257-5517