Trials@uspto.gov
Tel: 571-272-7822

Paper 35
Entered: October 21, 2015

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

INTERNATIONAL BUSINESS MACHINES CORPORATION,
Petitioner,

v.

INTELLECTUAL VENTURES II LLC,
Patent Owner.

Case IPR2014-00682
Patent 6,715,084 B2

Before KRISTEN L. DROESCH, JENNIFER S. BISK, and JUSTIN BUSCH, *Administrative Patent Judges.*

BISK, *Administrative Patent Judge*.

FINAL WRITTEN DECISION
35 U.S.C. § 318(a) and 37 C.F.R. § 42.73

INTRODUCTION

A. Background

Petitioner, International Business Machines Corporation, filed a Corrected Petition (Paper 4, "Petition" or "Pet.") requesting an *inter partes* review of claims 19, 20, and 22–33 of U.S. Patent No. 6,715,084 B2 (Ex. 1004, "the '084 patent"). On October 30, 2014, we instituted a review (Paper 11, "Decision to Institute" or "Dec.") based upon Petitioner's assertion that (1) claims 26, 28, and 30–33 are unpatentable, under 35 U.S.C. § 103(a), over the combination of Porras[1] and Cheswick,[2] and (2) claims 26 and 30–32 are unpatentable, under 35 U.S.C. § 102(b), as anticipated by NetRanger.[3] Dec. 22. Petitioner provides a Declaration from Dr. Steven M. Bellovin (Ex. 1001), and Patent Owner provides a Declaration from Dr. David Goldschlag (Ex. 2017).

This is a Final Written Decision under 35 U.S.C. § 318(a). Based on the record presented, we are persuaded that Petitioner has shown by a preponderance of the evidence that claims 26, 28, and 30–33 are unpatentable.

B. Related Matters

At the time of filing the Petition in this proceeding, IBM filed another petition for *inter partes* review in IPR2014-00681 challenging claims 1–9

---

[1] Phillip A. Porras & Alfonso Valdes, *Live Traffic Analysis of TCP/IP Gateways*, In Proceedings of the 1998 ISOC Symposium on Network and Distributed Sys. Security 1–13, (Dec. 12, 1997) (Ex. 1005) ("Porras").

[2] William R. Cheswick & Steven M. Bellovin, *Firewalls and Internet Security* 001–005, (1st ed. 1994) (Ex. 1008) ("Cheswick").

[3] NetRanger™ User's Guide Version 1.3.1, WheelGroup Corp. 001–327, (1997) (Ex. 1007) ("NetRanger").

and 12–18 of the ’084 patent. We denied institution in that proceeding and denied Petitioner’s subsequent request for rehearing. *See* IPR2014-00681, Papers 11, 14.

Subsequent to IBM’s filings, another petitioner also filed two petitions challenging claims of the ’084 patent in IPR2014-00793 and IPR2014-00801. We denied institution and a subsequent request for rehearing in IPR2014-00793. *See* IPR2014-00793, Papers 7, 9. We instituted *inter partes* review in IPR2014-00801 on December 1, 2015. IPR2014-00801, Paper 7 (final written decision being issued concurrently).

IBM indicates that the ’084 patent is the subject of concurrent proceedings in various district courts, none of which name IBM as a defendant. *See* Paper 32 (Petitioner’s Amended Mandatory Notices) 2–3; Paper 9 (Petitioner’s Amended Mandatory Notices) 2–3.

C. The ’084 Patent

The ’084 patent relates to network-based intrusion detection systems. Ex. 1004, 1:7–10. Intrusion detection systems are used to determine that a breach of computer security—access to computer resources by an unauthorized outsider—has occurred, is underway, or is beginning. *Id.* at 3:38–49. Conventional intrusion detection products and services are based on specialized equipment located on a customer’s premises and are directed to the analysis of a single customer’s data. *Id.* at 4:51–67. These systems may produce false alarms and are often unable to detect the earliest stages of network attacks. *Id.* In contrast, the broad-scope intrusion detection system disclosed in the ’084 patent analyzes the traffic coming into multiple hosts or other customers’ computers or sites, providing additional data for analysis, and, consequently, the ability to recognize intrusions that would

otherwise be difficult or impossible to diagnose. *Id.* at 5:44–56. Because the data collection and processing center gathers information from multiple network devices, including potentially multiple customers, it has access to a broader scope of network activity. *Id.* at 8:13–21. This additional data allows for the recognition of additional patterns of suspicious activity beyond those detectable with conventional systems. *Id.* at 8:21–22.

Figure 2 of the ’084 patent is reproduced below.

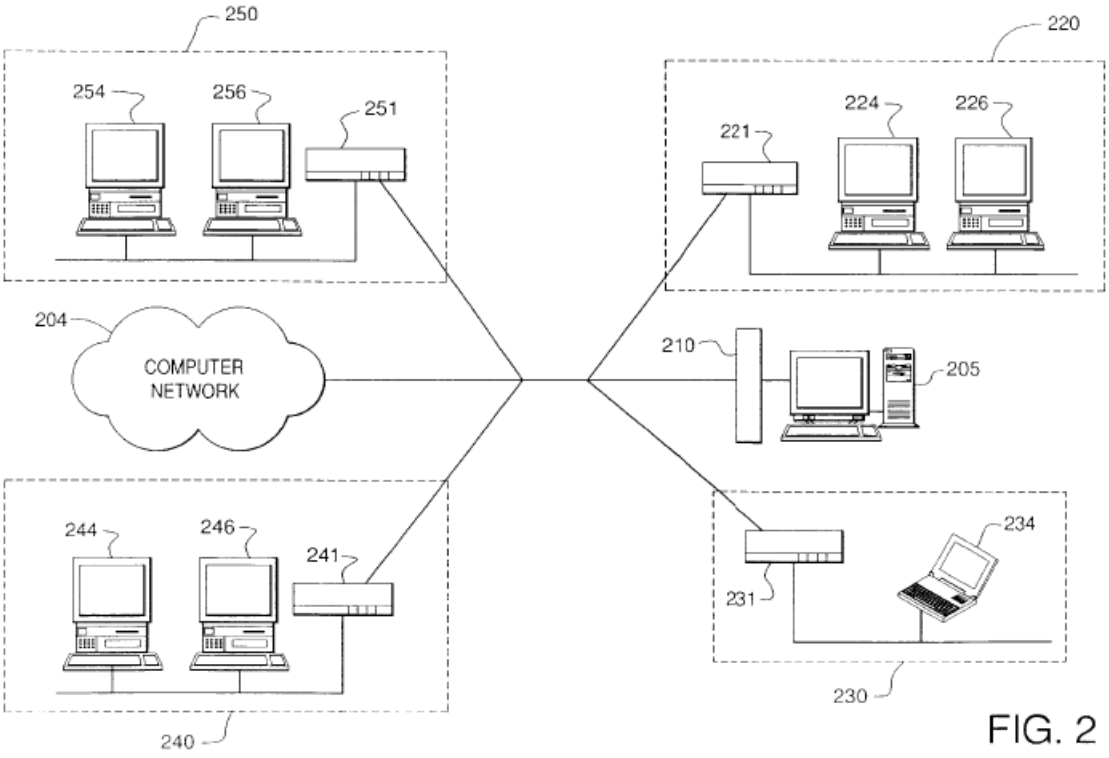


FIG. 2

Figure 2 shows a broad-scope intrusion detection system as described by the ’084 patent. *Id.* at 6:50–52. A separately maintained data collection and processing center, comprising computer or server 205 and firewall 210, is coupled to network 204. *Id.* at 7:18–20. The data collection and processing center receives information from the various network devices coupled to network 204. *Id.* at 7:33–36. “For example, all communications sent to each host 220, 230, 240, 250 are forwarded to, or otherwise captured by, the

data collection and processing center." *Id.* at 7:36–39. The '084 patent also discloses that "certain devices can be used as sensors to sense data traffic and pass their findings on to the data collection and processing center." *Id.* at 7:45–47.

To detect intrusions, the '084 patent describes a "multi-stage technique" of collecting suspicious network traffic events, forwarding those events to a central database and analysis engine, and then using pattern correlations to determine suspected intrusion-oriented activity. Ex. 1004, 8:23–31. Upon detection of suspected malicious activity, adjustments to devices such as firewalls can be made to focus sensitivity on attacks from suspected sources or against suspected targets. *Id.* at 8:31–35, 10:49–67. In addition, if any intrusions or attempted intrusions have been detected, appropriate alerts or notifications can be transmitted to pertinent devices. *Id.* at 10:62–65.

D. Claims at Issue

Of the claims at issue, claim 26 is independent. Claims 28, 30, 31, and 33 depend from claim 26. Claim 32 depends from claim 31. Claim 26 recites:

> 26. A data collection and processing center comprising a computer with a firewall coupled to a computer network, the data collection and processing center monitoring data communicated to the network, and detecting an anomaly in the network using network-based intrusion detection techniques comprising analyzing data entering into a plurality of hosts, servers, and computer sites in the networked computer system.

ANALYSIS

A. Claim Construction

For purposes of the Decision to Institute we expressly construed the terms "anomaly" and "determining which . . . are anticipated to be affected by the anomaly." Dec. 6–8. In its response, Patent Owner does not address explicitly the construction of any claim terms, including the two discussed in the Decision to Institute. Paper 23 ("PO Resp."). Petitioner also does not address explicitly the constructions adopted by the Decision to Institute. Petitioner, however, characterizes Patent Owner's response brief as being "premised upon its improperly narrow construction of the term 'data' as recited in claim 26 of the '084 patent." Paper 27 ("Reply"), 1.

We construe all claim terms using the broadest reasonable construction in light of the '084 patent specification. 37 C.F.R. § 42.100(b). Based on the record, and to properly resolve the issues presented in this proceeding, we address explicitly only the terms below.

1. "anomaly"

In the Decision to Institute, we construed the term "anomaly" as "a departure from the usual or expected; an abnormality or irregularity." Dec. 6. Specifically, we agreed with Patent Owner's assertion that this is the plain meaning of the term and is consistent with the specification of the '084 patent. *Id.* at 7. For example, the '084 patent states that "[a]nomaly detection systems look for statistically anomalous behavior . . . [s]tatistical scenarios can be implemented for user, dataset, and program usage to detect 'exceptional' use of the system." *Id.* (citing Ex. 1004, 3:54–57). Neither party contests this construction. We see no reason to deviate from this construction of "anomaly."

2. "data / data communicated to the network / data entering into a plurality of hosts"

Although Patent Owner never proposes expressly a claim construction for the term "data" in its response, Patent Owner, at least arguably, implies that the term requires construction by emphasizing it throughout much of its brief.[4] In the claims, the term "data," however, never stands on its own. Thus, based on the context, we understand the term being discussed to be two phrases in which data is used in the claims—"data communicated to the network" and "data entering into a plurality of hosts" ("the data limitations").

For example, in the section entitled "Summary of Response," Patent Owner states that Petitioner "ignored that the claimed data collection and processing center must detect anomalies by analyzing the *data* entering computers in the network," and instead pointed to references, "at best, describ[ing] a central unit that performs a meta-analysis of analysis *results* reported by distributed devices." PO Resp. 1 (emphases added by Patent Owner); *see also id.* at 3 (same emphasis added to the word data). Further, Patent Owner states that "surveillance modules . . . send anomaly and signature *reports—not data—*. . ." *Id.* at 6 (emphases added). Patent Owner, thus, argues that the data limitations are not equivalent to reports about such data being sent by a computer. *See also id.* at 1–2 ("As its name suggests, the data collection and processing center of claim 26 is a central

[4] During oral argument, Patent Owner stated that "the dispute here isn't over what does 'data' mean." Tr. 32. It is difficult to harmonize this statement with the briefing in this case. Regardless of whether Patent Owner intends its arguments to relate to claim construction, we address the issue in order to provide a complete analysis of both parties' arguments.

unit that collects and processes data to detect anomalies rather than merely receiving reports of detected anomalies.").

Patent Owner reinforces the understanding that they are arguing for a limited interpretation of the data limitations by emphasizing that "IBM and its expert repeatedly and correctly contended that Porras' gateway surveillance modules send *anomaly reports rather than the raw data* to the enterprise-lawyer monitor, and that the enterprise-layer monitor *correlates those results rather than* detecting anomalies by *analyzing the data*." PO Resp. 11 (emphases added). To support its assertion that "the claims do not read on merely analyzing anomaly reports received from remote modules," Patent Owner points to the following language from the '084 patent:

> [For example,] all communications sent to each host 220, 230, 240, 250 are forwarded to, or otherwise captured by, the data collection and processing center. Thus, the data collection and processing center receives all communications (i.e., the data) originating from a user on the computer network 204 and flowing to host 220 (and vice versa), for example, as well as all communications originating from the computer network 204 and flowing to all other hosts (and vice versa).

PO Resp. 2–3 (quoting Ex. 1004, 7:37–44). Taken together, Patent Owner's arguments appear to propose a construction of the data limitations that excludes "anomaly reports" or "analysis results" sent to a central collection and processing center.

Petitioner similarly interprets Patent Owner's arguments to be a proposed construction of the claim term "data." Reply 1–4. Based on this understanding, Petitioner argues that Patent Owner's proposed construction is improperly narrow, requiring the data collection and processing center to monitor and analyze "data" "firsthand." *Id.* at 2. Petitioner points out that

the language quoted above, relied upon by Patent Owner for the proposition that the claims do not read on analyzing anomaly reports, is immediately followed by language stating that "[i]t should be noted that certain devices can be used as sensors to sense data traffic and pass their findings on to the data collection and processing center . . . ." *Id.* at 2–3 (quoting Ex. 1004, 7:44–51).

According to Petitioner, this language shows that the '084 patent contemplates that the data collection and processing center may not necessarily look at "data traffic communicated to the network" firsthand. Reply 3. Instead, this language indicates that the '084 patent also considers monitoring and analysis of "findings" based on sensed data traffic to be within the scope of the subject matter at issue. *Id.* Further, Petitioner points out that the '084 patent describes an example in which "[d]ata from existing customer's conventional intrusion detection system is provided to the central database and then analyzed" where "[d]ata records comprise, for example, a time-stamp, a description of the activity, and the source of the probe." *Id.* (quoting Ex. 1004, 9:4–8). Petitioner explains that the construction of the term "data" must be broad enough to encompass all of the listed types of data. *Id.*

We agree with Petitioner that the data limitations do not necessarily exclude anomaly reports or analysis results sent to a central collection and processing center. Instead, we are persuaded that, as used by the '084 patent, the plain and ordinary meaning of these terms governs. The plain and ordinary meaning of "data" allows for transfer between entities without losing acquired characteristics, such as where the item came from. In other words, "data communicated to the network" qualifies as such when it is

initially intercepted by a computer on the network, after it is placed in a report or other record (whether or not that record contains further analysis or additional data items), and after it has been forwarded to another computer. Thus, without an express description to the contrary, we presume that "data communicated to the network" and "data entering into a plurality of hosts," as recited in claim 26, retains the plain and ordinary meaning of those phrases before, during, and after initial interception by a computer or computers. Patent Owner does not point to persuasive evidence to the contrary.

B. Obviousness over Porras and Cheswick

Petitioner asserts that claims 26, 28, and 30–33 would have been obvious over a combination of Porras and Cheswick. Pet. 13–24, 27–28. In the Decision to Institute, we determined that Petitioner had shown a reasonable likelihood of prevailing on this proposed ground of unpatentability. Dec. 10–12. In particular, we determined that Petitioner was likely to prevail on its assertions that the combination of Porras and Cheswick disclosed every limitation of claims 26, 28, and 30–33.[5] *Id.* We also found reasonable Petitioner's asserted rationale that a person of ordinary skill would have combined the teachings of Porras and the teaching of firewalls from Cheswick because it was conventional, for security purposes, to include firewalls on internal domains within secured networks.

[5] As part of this analysis, on page 12 of the Decision to Institute, we stated that "[f]urther, Figure 1 of Porras shows that the surveillance modules are part of the enterprise-layer monitor." Dec. 12 (citing Pet. 14). Both parties agree that this statement is incorrect and the surveillance modules are *not* part of the enterprise-layer monitor. PO Resp. 5–11; Reply 5; Tr. 6, 39–40, 56. We acknowledge the statement to be incorrect and, to the extent necessary, we retract that statement from the Decision to Institute.

Id. at 10 (citing Ex. 1001, ¶¶ 91–93; Ex. 1008, 004; *KSR Int'l v. Teleflex Inc.*, 550 U.S. 398, 418 (2007) (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006))).

We have reviewed Petitioner's obviousness arguments and supporting evidence, including Porras's disclosure, Cheswick's disclosure, the detailed claim chart appearing on pages 18–24 of the Petition (Petitioner cites to the claim chart of claim elements 19[d]–[h] for claim 26), and the testimony of Dr. Bellovin. Despite the counter-arguments in Patent Owner's Response, and the evidence cited therein, which we also have considered, Petitioner has shown, by a preponderance of the evidence, that each of claims 26, 28, and 30–33 is unpatentable under 35 U.S.C. § 103 as obvious over the combination of Porras and Cheswick.

1. Overview of Porras

Porras is an article describing "Live Traffic Analysis of TCP/IP Gateways." Ex. 1005. The article discloses "a variety of ways to extend both statistical and signature-based intrusion-detection analysis techniques to monitor network traffic." *Id.* at Abstract. According to Porras, "there have been various developments in recent years in passive surveillance mechanisms to monitor network traffic for signs of malicious or anomalous (e.g., potentially erroneous) activity." *Id.* at 1.

Porras describes a system called EMERALD (Event Monitoring Enabling Responses to Anomalous Live Disturbances), which applies intrusion-detection methods to the analysis of network activity. Ex. 1005, 2. Porras describes multiple distributed devices (surveillance modules) that monitor traffic at specific points on a network. *Id.* at 8. These surveillance monitors develop analysis results that are then directed up to a centralized

monitor (enterprise-layer monitor) that correlates the reports produced by all the surveillance monitors. *Id.*

Figure 1 of Porras is reproduced below.[6]

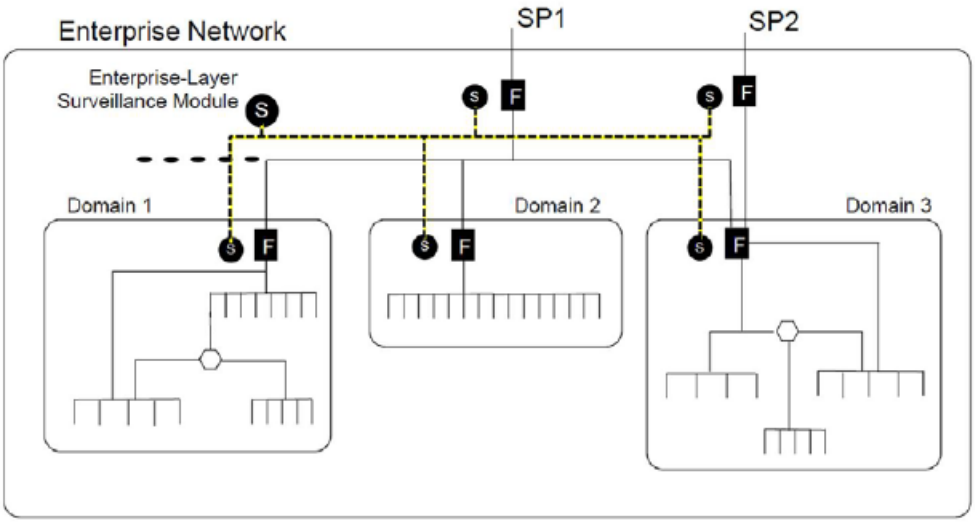


Figure 1 depicts an example enterprise network consisting of interconnected local network domains—Domains 1, 2, and 3. *Id.* at 8. Connectivity with the external world is provided through one or more service providers—SP1 and SP2. *Id.* Each local domain maintains a traffic filtering control—F-boxes—over its own subnetworks. The S-circles (the five smaller black circles containing an "s" that are pictured near an F-box, but not the large "S" labeled "Enterprise-Layer Surveillance Module") represent EMERALD surveillance monitors that are deployed to the various entry points of the enterprise and domains. *Id.* The surveillance monitors "develop analysis results that are then directed up to an enterprise-layer monitor [in Figure 1,

[6] This is a copy of a clearer version of Porras' Figure 1 found both in Patent Owner's Brief (PO Resp. 6) and http://www.csl.sri.com/projects/emerald/live-traffic.html (last visited on September 23, 2015). The dotted black line was added by Patent Owner for readability. PO Resp. 6.

the large "S" labeled "Enterprise-Layer Surveillance Module"], which correlates the distributed results into a meta-event stream." *Id.* "The enterprise monitor employs both statistical anomaly detection and signature analyses to further analyze the results produced by the distributed gateway surveillance modules, searching for commonalities or trends in the distributed analysis results." *Id.* at 8–9.

EMERALD maintains and updates a profile, which is a description of network traffic with respect to measures determined by statistical algorithms. *Id.* at 4. The profile has both short- and long-term elements. *Id.* The short-term profile has an aging mechanism that "accumulates values between updates, and exponentially ages values for comparison to the long-term profile." *Id.* The long-term profile is also slowly aged to adapt to changes in network activity. *Id.* Both the short- and long-term profiles are used to detect anomalous events based on a "subject-specific score threshold." *Id.* at 5.

2. Overview of Cheswick

Cheswick is an excerpt of a book titled "Firewalls and Internet Security." Ex. 1008. The excerpt includes several pages from a chapter called "Firewalls," which defines the term firewall and describes how and why they are used. *Id.* at 003–005. Petitioner relies on Cheswick only for the firewall element of the challenged claims. Pet. 14.

3. Claim 26

Petitioner asserts that Porras discloses each of the limitations of claim 26 except the firewall. Specifically, Petitioner relies on Porras's enterprise-layer monitor as teaching the claimed data collection and processing center. Pet. 18, 27. According to Petitioner, Porras discloses that the enterprise-

layer monitor "monitor[s] data communicated to the network" by correlating the distributed results reported from the surveillance monitors. *Id.* at 19–20 (quoting Ex. 1005, 8–9). Similarly, Petitioner asserts that Porras discloses that the enterprise-layer monitor "detect[s] an anomaly in the network using network-based intrusion detection techniques comprising analyzing data entering into a plurality of hosts, servers, and computer sites in the networked computer system" because it "employs both statistical anomaly detection and signature analyses to further analyze the results produced by the distributed gateway surveillance modules, searching for commonalities or trends in the distributed analysis results." *Id.* at 20–21 (quoting Ex. 1005, 8–9). As mentioned above, Petitioner relies on Cheswick solely for the firewall element of the challenged claims. *Id.* at 14.

Patent Owner argues that Petitioner has not shown that the enterprise-layer monitor analyzes data as required by the claims. PO Resp. 3–12. According to Patent Owner, because the enterprise-layer monitor analyzes *results* rather than *data* as it initially enters the surveillance monitors, it does not "analyz[e] data entering into a plurality of hosts, servers, and computer sites" in the networked computer system as required. *Id.* at 4. Patent Owner, instead, refers to the enterprise-level monitor's analysis of reports as "meta-analysis." *Id.* at 5. Further, as discussed in more detail above, Patent Owner states that the anomaly reports are "not data." *Id.* at 6. Patent Owner, thus, concludes that "[u]nlike the claimed data collection and processing center, Porras' enterprise-layer monitor does not monitor the data firsthand, and does not detect anomalies by analyzing data. Rather it receives reports of detected anomalies and looks for commonalities and trends in the reports." *Id.* at 7 (citing Ex. 1005, 8–9, Ex. 2017 ¶¶ 36–37). In

other words, Patent Owner contends that the enterprise-layer monitor must directly analyze the data from the network as opposed to indirectly analyzing that data after it has already been partially analyzed by another entity. Paper 34 (Transcript of Oral Hearing ("Tr.")), 39; *see also* Ex. 2017 ¶ 38 ("Porras' enterprise-layer monitor does not monitor the network traffic first hand, and it does not analyze data entering a plurality of hosts, servers, and computer sites.").

As explained above, we do not agree with Patent Owner that the broadest reasonable interpretation of the term "data" or the data limitations excludes "anomaly reports" or "analysis results" sent to a central collection and processing center. Moreover, we are not persuaded that the claimed data collection and processing center must monitor and analyze data "firsthand" as Patent Owner contends. PO Resp. 1–3, 7. In its Response, Patent Owner bases its narrow reading of the scope of claim 26 on the description in the '084 patent that "all communications sent to each host 220, 230, 240, 250 are forwarded to, or otherwise captured by, the data collection and processing center" and "[t]hus, the data collection and processing center receives all communications (i.e., the data) originating from a user on the computer network 204 and flowing to . . . all . . . hosts (and vice versa)." *Id.* at 2–3 (quoting Ex. 1004, 7:37–44). Nothing in this language, however, limits the data collection and processing center to receiving communications that *directly* originate from a user. In other words, nothing in this language prevents a device from intercepting the communications, doing some data manipulation or analysis, and then forwarding the resulting product on to the data collection and processing center. In fact, the language itself seems to contemplate that scenario—"all

communications . . . are *forwarded to*, or otherwise captured by, the data collection and processing center." Ex. 1004, 7:36–37 (emphasis added). We are not persuaded to the contrary by Dr. Goldschlag's testimony, which simply recites the claim language and concludes that "[m]onitoring and analyzing reports based on such data does not satisfy the claim language." Ex. 2017 ¶¶ 21–23.

Moreover, Patent Owner does not address, in its brief, the very next sentence of the '084 patent, which describes a situation similar to that described by Porras, where the data collection and processing center does *not* monitor the data "firsthand." Ex. 1004, 7:45–47 ("It should be noted that certain devices can be used as sensors to sense data traffic and pass their *findings* on to the data collection and processing center.") (emphasis added). During oral argument, Patent Owner suggested that this language reflects an embodiment with functionality not encompassed by claim 26.[7] Tr. 34 ("The specification contemplates additional embodiments that are not claimed here, and this claim does not prevent taking additional information, such as reports from the sensors, and using that information further."). We are persuaded, however, that the correct reading of this language, in context, is that the '084 patent contemplates network devices that may implement various amounts of processing of incoming data prior to forwarding that data on to the central data collection and processing center. At the very least, the '084 patent does not clearly restrict that amount of data manipulation and processing.

We are persuaded that Petitioner has shown by a preponderance of the evidence that Porras discloses an enterprise-layer monitor that "analyz[es]

[7] Petitioner objects to this argument as improper new argument. Tr. 49.

data entering into a plurality of hosts, servers, and computer sites in the networked computer system" as required. *See* Pet. 16, 19–21; Ex. 1001 ¶¶ 95–101; *see also* Ex. 1041, 48:6–17 (Dr. Goldschlag stating that "analysis, reports, metadata, data, may be sent up to the enterprise-layer surveillance module, which does analysis of that analysis . . ."). Thus, we are persuaded that Petitioner has shown by a preponderance of the evidence that claim 26 would have been obvious over Porras and Cheswick.

4. Claim 28

Claim 28 depends from claim 26, adding that "the data collection and processing center further determines which of a plurality of devices that are connected to the network have been affected by the anomaly and alerts the devices." Petitioner asserts that Porras discloses this additional limitation because it discusses "identify[ing] devices with user-installed network services on unregistered ports or detect[ing] devices impacted by a worm or fault" and "actively terminating a channel session or tun[ing] or point[ing] out mistakes in filtering rules." Pet. 22–24 (citing Ex. 1005, 8–12; Ex. 1001 ¶¶ 113–119).

Patent Owner argues that Petitioner does not show either determining which devices have been affected by an anomaly or alerting those devices.[8] PO Resp. 13 (citing Ex. 2017 ¶ 51). In the Decision to Institute, agreeing with statements in Patent Owner's Preliminary Response, we found that

[8] Both parties agree that "and alerts *the devices*" recited in claim 28 refers to "devices that . . . have been affected by the anomaly," as opposed to referring to all of the "plurality of devices." PO Resp. 12–13; Tr. 58–59. Although we note the claim may be unclear in this respect, applying the prior art in this case would result in the same conclusion under either reading.

Porras discloses sending warnings to domains that have not yet experienced an anomaly. Dec. 9 (citing Paper 10 ("Prelim. Resp."), 25 ("[T]he cited portion of Porras expressly states that there is a need to warn the domains that have not yet experienced the anomaly to combat 'spreading attacks.")). Indeed, Porras discloses that the reports from surveillance modules "could lead to enterprise-layer responses or warnings to other domains that have not yet experienced or reported the session anomalies." Ex. 1005, 10. To warn domains that have not yet experienced an anomaly, Porras must necessarily determine which domains *have* experienced the anomaly. Patent Owner does not address this disclosure of Porras in its response brief. Thus, we continue to be persuaded that Porras discloses the enterprise-layer monitor "determin[ing] which of a plurality of devices that are connected to the network have been affected by the anomaly."

We also are persuaded that Petitioner has shown sufficiently that Porras discloses alerting those devices that have been determined to be affected. Petitioner relies on the following activities described by Porras for the disclosure of this limitation: "actively terminate a channel session," "perform . . . (re)configuration of logging facilities within network components," and "tune or point out mistakes in filtering rules." Pet. 22–23 (citing Ex. 1005, 9–11); Reply 8–9. We agree, and Patent Owner does not appear to dispute, that all of these activities involve methods of alerting a device or set of devices of an anomaly. *See* Ex. 1005 ¶ 118; PO Resp. 12–15. Patent Owner instead argues that nothing in the language Petitioner quotes from Porras ties that alert to a specific device that has been detected to have an anomaly. PO Resp. 12–15. Patent Owner, however, does concede that Porras discusses alerting *all devices*. *Id.* at 14 ("(Porras 10–11)

discusses reconfiguring devices, but does not discuss determining which devices were affected and alerting those devices (as opposed to all devices).”). We agree that Porras discloses alerting *all devices*. *See* Ex. 1001 ¶ 116 (“Porras also teaches that the enterprise-layer monitor caused an ‘enterprise-wide response’ if it determined that ‘exceptional network activity’ had affected network devices.”). Because alerting *all devices* necessarily includes alerting those devices determined to have been affected by an anomaly, a subset of all devices on the network, we are persuaded that Porras discloses this limitation.

Thus, we are persuaded that Petitioner has shown by a preponderance of the evidence that claim 28 would have been obvious over Porras and Cheswick.

5. Claim 30

Claim 30 depends from claim 26, adding that “the anomaly comprises one of an intrusion, an intrusion attempt, and reconnaissance activity.” Petitioner asserts that Porras discloses this additional limitation because it discusses “attacks using corruption or forgery of legitimate traffic in an attempt to negatively affect routing services, application-layer services, or other network controls,” “attempts to subvert or bypass internal network services,” and “intelligence gathering activities, including finger, echo, or mail alias expansion.” Pet. 24 (citing Ex. 1005, 1, 3, 9, 11; Ex. 1001 ¶¶ 122–126), 28.

Patent Owner does not separately argue that Porras does not teach the limitation of claim 30. We are persuaded that Petitioner has shown by a preponderance of the evidence that claim 30 would have been obvious over Porras and Cheswick.

6. Claims 31 and 32

Claim 31 depends from claim 26, adding that "the data collection and processing center detects the anomaly by analyzing a plurality of data packets with respect to predetermined patterns." Claim 32 depends from claim 31, adding that "the data collection and processing center analyzes data packets that have been received by at least two devices that are connected to the network."

Petitioner asserts that Porras discloses the additional limitation of claim 31 because it discusses the surveillance monitors analyzing TCP/IP packet streams searching for "signs of malicious activity, nonmalicious failures, and other exceptional events" with examples of exceptional events including "[h]igh volumes of discarded packets," "scanning of [UDP] ports or IP address scanning," and "occurrence of a SYN-attack." Pet. 25 (citing Ex. 1005, 1, 6–9; Ex. 1001 ¶¶ 129–131), 28. For claim 32's additional limitation, Petitioner relies on Porras's disclosure that the enterprise-layer monitor correlates analysis results for multiple domains throughout the enterprise. *Id.* at 25–26 (citing Ex. 1005, 8–9; Ex. 1001 ¶¶ 134–136).

Like its arguments with respect to claim 26, Patent Owner argues that Petitioner does not show that the enterprise-layer monitor performs this function, as opposed to the surveillance monitors. PO Resp. 15–16 (citing Ex. 2017 ¶ 52). For claim 32, Patent Owner relies on the arguments it makes for claims 26 and 31. *Id.* at 17–18 (citing Ex. 2017 ¶¶ 37, 53). Petitioner responds that claim 31 does not require the data collection and processing center to analyze the data packets firsthand or directly. Reply 10. Instead, Petitioner argues that claim 31 encompasses situations where the

data collection and processing center analyzes information about data packets it receives from sensor devices. *Id.*

For the reasons discussed above with respect to claim 26, we agree that claims 31 and 32 are broad enough to encompass the situation described by Porras where surveillance monitors analyze a plurality of data packets with respect to predetermined patterns, create reports based on those packets, and forward the reports to the enterprise-layer monitor for further analysis. Thus, we are persuaded that Petitioner has shown by a preponderance of the evidence that claims 31 and 32 would have been obvious over Porras and Cheswick.

7. Claim 33

Claim 33 depends from claim 26, adding that "the data collection and processing center adjusts anomaly detection sensitivity and alarm thresholds based on the detected anomaly." Petitioner asserts that Porras discloses this additional limitation because it discusses "ag[ing] the short-term and long-term profiles" and "adapt[ing] the subject-specific score threshold." Pet. 26–27 (citing Ex. 1005, 4, 5, 8–9; Ex. 1001 ¶¶ 140–143), 28.

Patent Owner argues that none of the portions of Porras that Petitioner relies on show adjusting anomaly detection sensitivity and alarm thresholds. PO Resp. 19–20 (citing Ex. 2017 ¶ 54). Specifically, Patent Owner asserts that Porras does not disclose that the aging mechanism is performed by the enterprise-layer monitor. *Id.* at 19. Dr. Bellovin states that "[o]ne having ordinary skill in the art would have understood Porras to teach the enterprise-layer monitor maintaining and 'aging' anomaly detection sensitivity because Porras expressly states that the adjustments were performed by a 'statistical algorithm'" and it is "the enterprise-layer monitor

[that] used 'statistical anomaly detection' in its analysis." Ex. 1001 ¶ 141. We find this testimony persuasive. Although this portion of Porras does not explicitly state that it is the enterprise-layer monitor that is doing the aging, we agree that a person of ordinary skill in the art would understand this to be the case. Porras makes it clear that it is the enterprise-layer monitor that generally does enterprise-wide analysis in the disclosed system. Ex. 1005, 8–9, Fig. 1. Moreover, Porras discloses that profiles and statistical analysis can be created based on a specific network gateway (surveillance monitor) by itself or on a combination of gateways such as "satellite offices" and "rest of world." *Id.* at 4. This disclosure indicates that the enterprise-layer monitor, at a level above the gateways, must have the ability to create and maintain profiles.

Thus, we are persuaded that Petitioner has shown by a preponderance of the evidence that claim 33 would have been obvious over Porras and Cheswick.

C. Anticipation by NetRanger

Petitioner asserts that claims 26 and 30–32 are anticipated by NetRanger. Pet. 48–52, 56–59. In the Decision to Institute, we determined that Petitioner had shown a reasonable likelihood of prevailing on this proposed ground of unpatentability. Dec. 18–20.

We have reviewed Petitioner's anticipation argument and supporting evidence, including NetRanger's disclosure, the detailed claim chart appearing on pages 48–52 of the Petition (Petitioner cites to the claim chart of claim elements 19[d]–[h] for claim 26), and the testimony of Dr. Bellovin. We are, however, persuaded by the counter-arguments in Patent Owner's Response, and the evidence cited therein, that Petitioner does not provide

sufficient evidence that NetRanger discloses each and every element of the claims. Thus, as described below, we conclude that Petitioner has not met its burden to show, by a preponderance of the evidence, as required by 35 U.S.C. § 316(e), that claims 26 and 30–32 are anticipated by NetRanger.

1. Overview of NetRanger

NetRanger is a user guide for a product of the same name—"a real-time network security management system that detects, analyzes, responds to, and deters unauthorized network activity." Ex. 1007, 019. NetRanger uses "centralized monitoring and management of remote dynamic packet filtering devices that plug into TCP/IP networks." *Id.* The NetRanger System includes the "NSX," which is the "sensing and management component." *Id.* at 020–021. The NSX, in turn, communicates with one or more "Director[s]," which provide monitoring and analysis. *Id.*

2. Analysis

Petitioner asserts that NetRanger discloses claim 26's limitation of "a computer with a firewall coupled to a computer network." Pet. 48 (citing Ex. 1007, 041; Ex. 1001 ¶¶ 233–34). Specifically, Petitioner asserts that NetRanger's Director teaches the claimed data collection and processing center. *Id.* There is no dispute that NetRanger discloses the Director comprising a computer. To support the firewall portion of this limitation, Petitioner relies solely on the following language from NetRanger in a section titled "How Existing Firewalls Affect NetRanger Installation":

> *The NetRanger NSX can work in conjunction with existing firewalls* as long as they are appropriately placed within your network. Ideally, the NetRanger NSX should be located in front of the existing firewall. If the NetRanger NSX packet filter is placed behind a firewall, intrusion detection will be limited to traffic that has been allowed through the firewall, and

> it will not generate alarms on reconnaissance or failed malicious activity. In cases where there is no need for address translation or other proxy services, *NetRanger can replace firewalls*. If there is no need for address translation or other proxy services, NetRanger works best without a firewall and has less impact on network performance.

Id. (quoting Ex. 1007, 041) (emphases added); Reply 13. According to Dr. Bellovin, "[o]ne having ordinary skill in the art would have understood that, since NetRanger could 'replace firewalls,' NetRanger was a firewall itself." Ex. 1001 ¶ 233.

Patent Owner argues that Petitioner doesn't identify a single disclosed embodiment where NetRanger's *Director* comprises a computer with a firewall coupled to a network as required by the claims. PO Resp. 22. Instead, Petitioner states that the NetRanger system, generically, may replace a firewall, or can work in conjunction with a firewall. Pet. 48 (citing Ex. 1007, 041; Ex. 1001 ¶¶ 233–34). In its reply, Petitioner states that it "provided a block quote in support of the fact that NetRanger teaches that the Director was a computer with a firewall" referring to a portion of the paragraph reproduced above. Reply 13 (citing Pet. 48; Ex. 1007, 041). Nonetheless, Petitioner does not explain, and it is not clear on its face, how the cited language supports a teaching that the *Director* can replace a firewall, as opposed to, for example, the entire NetRanger system or NetRanger's NSX component replacing the firewall. Thus, Petitioner has not shown persuasively that NetRanger discloses this limitation.

We conclude, therefore, that Petitioner has not met its burden to show, by a preponderance of the evidence, that NetRanger anticipates independent claim 26. For the same reasons, we conclude that Petitioner has not met its

burden with regard to claims 30–32, which depend, either directly or indirectly, from claim 26.

ORDER

Accordingly, it is:

ORDERED that claims 26, 28, and 30–33 of the ’084 patent are determined to be *unpatentable*; and

FURTHER ORDERED that, because this is a Final Written Decision, parties to the proceeding seeking judicial review of the decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

PETITIONER:

Kenneth Adamo
Eugene Goryunov
KIRKLAND & ELLIS LLP
kenneth.adamo@kirkland.com
eugene.goryunov@kirkland.com

PATENT OWNER:

Jonathan Strang
Lori Gordon
STERNE, KESSLER, GOLDSTEIN & FOX
jstrang-PTAB@skgf.com
lgordon-PTAB@skgf.com

Donald J. Coulman
Tim Seeley
INTELLECTUAL VENTURES
dcoulman@intven.com
tim@intven.com