IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

BRITISH TELECOMMUNICATIONS PLC and BT AMERICAS, INC.,	)	
Plaintiffs,	)	C.A. No. 22-_____
v.	)	**JURY TRIAL DEMANDED**
PALO ALTO NETWORKS, INC.,	)	
Defendant.	)	

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiffs British Telecommunications plc and BT Americas, Inc. (collectively, "BT") file this Complaint for Patent Infringement against Defendant Palo Alto Networks, Inc., ("PAN"), and allege as follows:

NATURE OF THIS ACTION

1. This is a patent infringement action brought by BT against PAN based on PAN's continued willful infringement of U.S. Patent No. 7,159,237 (entitled "Method and system for dynamic network intrusion monitoring, detection and response") ("the '237 Patent") and U.S. Patent No. 7,895,641 (entitled "Method and system for dynamic network intrusion monitoring, detection and response") ("the '641 Patent") (collectively, the "Schneier Patents").

2. A true and correct copy of the '237 Patent is attached as Ex. A.

3. A true and correct copy of the '641 Patent is attached as Ex. B.

PARTIES

4. Plaintiff British Telecommunications plc is a corporation organized under the laws of England and Wales, and has a principal place of business at 1 Braham Street, London E1 8EE, United Kingdom.

5. Plaintiff BT Americas, Inc. is a Delaware corporation, and has a principal place of business at 8951 Cypress Waters Blvd, Suite 200, Dallas TX 75019.

6. Upon information and belief, Defendant Palo Alto Networks, Inc. is a Delaware corporation, and has a principal place of business at 3000 Tannery Way, Santa Clara, CA 95054. PAN can be served through its registered agent, Corporation Service Company, 251 Little Falls Drive, Wilmington, Delaware 19808.

JURISDICTION AND VENUE

7. This is an action for patent infringement arising under the United States patent statutes, 35 U.S.C. § 100, et seq.

8. This Court has subject matter jurisdiction over this action under 28 U.S.C. §§ 1331 and 1338(a).

9. This Court has personal jurisdiction over Defendant PAN because PAN is incorporated in Delaware and has continuous and systematic contacts with the State of Delaware, including, inter alia, continuous contacts with, and sales to, customers in Delaware. Further, PAN has committed acts within the District of Delaware giving rise to this action, directly and through subsidiaries or intermediaries, including distributing, offering for sale, selling, using, importing and/or advertising products and services that infringe the claims of the Schneier Patents in the State of Delaware.

10. PAN is incorporated in Delaware and venue is proper in this District under 28 U.S.C. §§ 1391(b), 1391(c), and/or 1400(b).

FACTUAL BACKGROUND

British Telecommunications plc., BT Americas, Inc. and Counterpane

11. BT is the oldest telecommunications company in the world, tracing its origins back to the Electric Telegraph Company, which was incorporated in England in 1846. Today, BT

provides communications services in 180 countries and employs more than 100,000 people worldwide.

12. From early on, BT has been on the forefront of research and innovation in the world of communications, starting with its adaption in the nineteenth century of leading-edge telegraphy technology, including the world's first commercial telegraph service.

13. In 1975, BT opened its renowned research facility at Adastral Park, near Ipswich in the county of Suffolk, England. Adastral Park has housed some of the leading technology researchers and engineers in the world. Their inventive efforts have led to the issuance of more than 10,000 patents by the turn of the century.

14. BT, directly or through its subsidiaries, has continued to maintain its longstanding commitment to research and innovation, and spends over £600,000,000 (six hundred million pounds sterling) annually on research and development, with over 13,000 scientists and technologists worldwide. As part of its strategy to develop global professional services capabilities and—with the proliferation of and sophistication of cyberattacks—to enhance Internet and infrastructure security, BT has acquired various companies throughout the years.

15. Specifically, in 2006, BT acquired Counterpane Internet Security, Inc. ("Counterpane"), an Internet security company founded by Dr. Bruce Schneier—one of the most famous names in security. As part of that acquisition, BT Americas, Inc. obtained all rights, title and interest in Counterpane's patent portfolio, including the Schneier Patents which name Dr. Schneier as an inventor.

16. Among other things, Counterpane was the first to create a remote, 24/7 security service that monitored network operations of customers from a secure operations center ("SOC"). Counterpane leveraged a novel security system architecture to enable it to operate its

security service effectively, "including the analysis of residual status data to identify potential security events for further analysis." Ex. C. (Declaration of Bruce Schneier in Support of BT Americas Inc.'s Preliminary Response Under 35 U.S.C. §313 and 37.C.F.R. §42.107(a), dated August 26, 2019 ("Schneier Decl.")). This architecture, claimed by the Schneier Patents, allows for the detection of previously unknown attacks or security events by filtering and analyzing status data. It enables a dynamic response to these attacks by transmitting information about the identified events to analysts or analyst systems and allowing for feedback to be provided at its probes, which dynamically improve the system's detection capabilities. The benefits provided by this architecture led to its adoption by the major providers of enterprise-grade security, and eventually gave rise to the security monitoring market segment that BT and Palo Alto, among many others, now occupy.

Palo Alto Networks

17. Upon information and belief, PAN is a cybersecurity company that offers a broad range of products and services which incorporate technologies invented by BT and Counterpane. These include, *inter alia*, PAN's security appliances (*e.g.*, PA-Series, CN-Series, VM-Series, and Prisma Access).

18. As early as June 28, 2018, PAN had knowledge of the Schneier Patents and its infringement of those patents. As detailed below, BT informed PAN of its infringement and also requested that PAN enter into discussions with BT to address it, *e.g.*, through a licensing arrangement.

19. Specifically, on June 28, 2018, the chief counsel for Intellectual Property Rights of BT ("BT's IP Counsel") sent a letter to PAN identifying, in relevant part, the Schneier Patents and providing clear notice that PAN infringed them. The June 28, 2018 letter identified representative

products and also included detailed claim charts showing how the representative products infringed the Schneier Patents. Accordingly, BT proposed that PAN take a license.

20. Although PAN responded that it would investigate BT's assertions and contact BT after completing the investigation, PAN did not follow-up with BT.

21. On January 14, 2020, BT followed up with PAN by sending another letter advising PAN of its infringement. This letter also informed PAN that a third party—Fortinet, Inc. ("Fortinet")—had filed petitions for *inter partes* review ("IPR") on patents previously identified in BT's June 28, 2018 letter and that the IPR petitions for the Schneier Patents had been rejected by the United States Patent and Trademark Office ("USPTO").[1] Again, BT encouraged PAN to take a license for its infringement of the Schneier Patents.

22. Hearing no response from PAN, on August 27, 2021, BT sent yet another follow-up letter to PAN. This time, BT also shared a recent claim construction order from this District construing various terms of the Schneier Patents. In light of this new development, BT again offered PAN the opportunity to enter into licensing discussions with BT to address its continued infringement of the Schneier Patents. PAN never responded despite its continued use of the inventions of the Schneier Patents.

23. On January 20, 2022, BT sent yet another letter to PAN—this time informing PAN that its competitor—Fortinet—had already agreed to a confidential settlement. BT re-emphasized the favorable claim construction order rendered in the Fortinet litigation and the denial of the IPR petitions by the USPTO, and once again offered to license the Schneier Patents to PAN.

[1] BT sent PAN another update on January 22, 2020, informing PAN that all of Fortinet's IPR petitions had been denied.

24. On February 19, 2022, PAN responded to BT by letter, finally agreeing to discuss the matter with BT. Though BT engaged PAN in confidential discussions over the course of several months, the parties did not reach agreement.

25. PAN has derived and will continue to derive substantial value from its products and services that incorporate the technologies of the Schneier Patents. PAN failed to provide meaningful responses to BT's correspondences and chose instead to continue infringing the Schneier Patents, both willfully and wantonly.

26. Despite BT's repeated attempts to reach an amicable resolution with PAN, PAN has continued to infringe willfully and wantonly. BT brings this action to recover the just compensation it is owed for PAN's past infringement, and to prevent PAN from continuing to benefit from the patented inventions in the future without authorization or compensation to BT.

PAN Infringes the Schneier Patents

27. The USPTO issued the '237 Patent (U.S. Patent No. 7,159,237) on January 2, 2007. BT Americas, Inc. is the lawful owner by assignment of all rights, title and interest in the '237 Patent, including the right to sue for patent infringement and damages, including past damages.

28. The USPTO issued the '641 Patent (U.S. Patent No. 7,895,641) on February 22, 2011. The '641 patent is a continuation of the application that issued as the '237 patent. BT Americas, Inc. is the lawful owner by assignment of all rights, title and interest in the '641 Patent, including the right to sue for patent infringement and damages, including past damages.

29. The Schneier Patents represent important advances in the field of cybersecurity and disclose an architecture for unearthing and addressing network intrusions. This architecture has now been widely adopted throughout the cybersecurity industry, including by PAN.

30. Dr. Bruce Schneier is an internationally renowned cryptographer and security expert who has been called a "security guru" by The Economist. He is the author of several

books on computer security and cryptography—having written the definitive book on cryptography—as well as other books, including, but not limited to 1) Applied Cryptography, 2) Cryptography Engineering, 3) Secrets and Lies, and 4) Schneier on Security.[2] He teaches the subject at Harvard's Kennedy School of Government, has testified before Congress numerous times, published hundreds of articles, holds dozens of patents, and hosts a widely followed cybersecurity blog. Dr. Schneier is sufficiently famous that he rated mention in the De Vinci Code—and is often referred to as the "Chuck Norris of Security."

31. In 1999, Dr. Schneier attended an RSA Conference and was struck by the obvious inadequacies of the security solutions being offered. Believing he could do better, he formed Counterpane to solve these issues and immediately hired additional exceptional talent, including Jon Callas and Andrew Gross.

32. Jon Callas, a named inventor of the Schneier Patents, is also an internationally renowned security expert. Mr. Callas has served as the Chief Technology Officer of Entrust and worked on Apple's core security technology over the years, including Mac and iOS.[3] He has since founded several companies and won major innovation awards for security product designs, including an award from the Wall Street Journal.

33. Andrew Gross, another named inventor, was previously the head of security research at San Diego Supercomputer Center, which was funded by the NSA. He was hired as the chief architect for Counterpane Internet Security. On information and belief, he now (or previously) works at Oracle and holds responsibility for the security of JAVA.

---

[2] See, *e.g.*, Bruce Schneier, Wikipedia (available at https://en.wikipedia.org/wiki/Bruce_Schneier) (last accessed 11/22/2022).

[3] See, *e.g.*, Jon Callas, Wikipedia (available at https://en.wikipedia.org/wiki/Jon_Callas) (last accessed 6/13/2018)

34. Following the creation of Counterpane, Dr. Schneier and his fellow inventors went to work and filed for patent applications, which described Counterpane's own novel security system design. In Dr. Schneier's own words, "Counterpane's successful implementation of technology described in the '237 and '641 patents spawned an entirely new product category—called Managed Security Monitoring—which has since come to be a very large commercial space." Ex. C (Schneier Decl.).

35. The Schneier Patents relate generally to a method and system for dynamic network intrusion monitoring that monitors network activity using a probe that collects status data from monitored components, filters that status data positively and negatively, while analyzing the "residue" status data to identify potential security events. Information about these events are then transmitted to an analyst and feedback can be provided to the probe, which allows the probe to dynamically modify its detection capabilities based on that feedback.

36. Prior art solutions—the conventional approach—consisted of anti-virus (and other anti-malware) software at the edge of the network that would be updated periodically with newly discovered viruses or malware. Prior art solutions were focused on prevention as opposed to monitoring, detection and response. *See* '641 Patent Col 1:24-33; '237 Patent Col 1:12-22. Decisions on whether traffic was bad, good or indeterminate were typically made immediately at the interface of the network based primarily on the presence or absence of patterns matching the viruses (or malware) that had been previously identified as opposed to analyzing status data. However, prior art solutions had limited ability to address newer (or previously unknown) forms of viruses (and malware) and detect intrusions quickly enough and to enable a response to prevent them from doing a great deal of damage within a computer network.

37. The inventions of the Schneier Patents are remarkable improvements in computer networks and technology that address these problems in the prior art. They take a far more flexible and dynamic approach to identify and remedy previously undetected malware and potential network attacks. To achieve the benefit of identifying and addressing unknown attacks while generating less—or no—false alerts, which would otherwise impair the performance of the network, the Schneier patents take an approach that differs greatly from the conventional approach at the time. For example, the Schneier patents analyze residual status data. Probes comprised of network sensors extract status data, which is analyzed—in part—by running the data through a filtering subsystem. The filtering subsystem filters that status data and determines what is interesting and what is not. Instead of stopping there, the residual status data, which is neither selected nor discarded, is further analyzed to identify other potential security events. Moreover, information about the identified events is then transmitted to a secure operations center ("SOC") where analysts can further analyze the information—using the empirical data to provide feedback at the probes (*e.g.*, by comparing status data collected from other probes situated at other locations). Thereafter, feedback is provided at the probe—which improves its security dynamically, without needing to go offline.

38. This novel and unconventional architecture allows the security system to dynamically respond and protect against new and constantly evolving attacks. Other benefits include that the architecture makes it possible for contextual information from various probes to be correlated and for empirical data to be used to improve the security of the overall system. The architecture and methodology was a significant improvement to existing computer security technology at the time. In contrast, previous conventional security systems were constrained to pattern matching at a single point in the network. *See, e.g.*, Patent App. No. 09/766,343 (issued as

’237 Patent), Notice of Allowability at 4 (noting in “Networking and Security, all data is filtered by intrusion detection, firewall, gateway, proxy, sensor, probe, or sentry, or some other type of device” such that “if an attack occurs the data is transmitted for further analysis” but “[a]ll other data is usually blocked or discarded”). Not only were prior art systems incapable of dynamically detecting new threats with just pattern matching, but such prior art systems did not provide an architecture that allowed the system to dynamically respond to new threats the way the Schneier patents do.

39. As described in detail in Counts I and II below, PAN offers a series of products and services that infringe the Schneier Patents. For example, PAN’s “Strata” network security platform consists of several products and services, including various PAN security appliances (*e.g.*, PA-Series, CN-Series, VM-Series, and Prisma Access). Furthermore, PAN’s WildFire service—also a part of Strata—receives and analyzes residual status data to determine whether it might represent an unknown attack or security-related event. Information about these events is then transmitted to analysts, such as PAN’s Unit 42 and/or those using PAN’s Cortex platform.

COUNT I
(INFRINGEMENT OF U.S. PATENT NO. 7,159,237)

40. BT repeats and re-alleges the allegations contained in Paragraphs 1 through 399 above as if fully set forth herein.

41. PAN has directly infringed and continues to directly infringe, literally or under the doctrine of equivalents, one or more claims of the ’237 Patent in violation of 35 U.S.C. §271(a) by making, using, offering to sell, selling (directly or through intermediaries), and/or importing, in this District and elsewhere in the United States, various PAN products and services including, but not limited to, Strata, the PA/CN/VM Series security appliances, Prisma Access, and WildFire.

42. For example, PAN infringes claim 1 of the ’237 Patent, which provides as follows:

A method of operating a probe as part of a security monitoring system for a computer network, comprising:

a) collecting status data from at least one monitored component of said network;

b) analyzing status data to identify potentially security-related events represented in the status data, wherein the analysis includes filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering;

c) transmitting information about said identified events to an analyst associated with said security monitoring system;

d) receiving feedback at the probe based on empirically-derived information reflecting operation of said security monitoring system; and

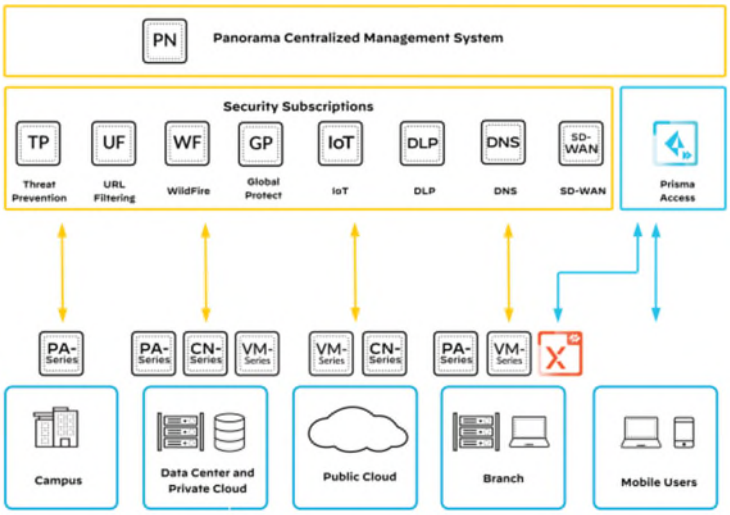
e) dynamically modifying an analysis capability of said probe during operation thereof based on said received feedback.

43. PAN performs each and every step of claim 1, among other claims, and was placed squarely on notice of its infringement of the ’237 Patent at least by June 28, 2018 and in various correspondence detailing its infringement (*e.g.*, BT’s letters of January 14, 2020, August 27, 2021, and January 20, 2022).

44. By way of example, PAN provides and operates a series of products that individually and collectively provide security services (“a security monitoring system”) for networks that belong to PAN’s customers. PAN refers to this system as “Strata,” and it is a network security platform that provides security management, cloud-delivered security services, and next generation firewalls, while utilizing machine learning and analytics.

45. The following figure provides a detailed overview of the Strata platform:

Figure 2 Strata network security platform overview



Palo Alto Networks, *Network Security Overview* at 12, PALOALTONETWORKS.COM, Dec. 2020, https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/guides/network-security-overview (last accessed 9/29/2022).

46. As seen in the figure above, PAN operates a variety of probes as part of its security monitoring system. Namely, PAN's next generation firewalls ("PAN NGFs")—including the PA-Series, CN-Series, VM-Series, and Prisma Access—are probes that monitor and process network traffic to identify malicious, benign, and suspicious network traffic. These probes all leverage a common operating system—PAN-OS—and can be deployed as physical appliances (PA-Series), virtualized appliances (VM-Series), container form factors (CN-Series), and as a cloud-hosted service (Prisma Access). *See Network Security Overview* at 13.

47. PAN NGFs collect status data from at least one monitored component of the network. PAN NGFs are composed of multiple special purpose sensors. A sensor includes at least the portion of the PAN NGFs that receives network traffic destined for or originating from a monitored component of the network, and processes that traffic to collect information relevant to the state or condition of the network, network traffic, or the monitored component.

48. The status data is informative as to the status of the network and its components. Status data may also include both information extracted from the underlying network traffic (such as the IP addresses of the originating and/or destination computers) and information determined from the underlying network traffic (such as the frequency of messages, sensor IP address, message count, and associated time stamps or the duration of an event). Other status data collected might provide context for other status data should it be subsequently desirable to correlate status data across multiple sensors to enhance the detection and response capabilities of the system.

49. By way of example, PAN NGFs collects status data related to attributes of a data packet. For example, IP address status data is collected by PAN's probes as seen below.

- **Source IP**—Forward the source IP address that sent the unknown file.
- **Source Port**—Forward the source port that sent the unknown file.
- **Destination IP**—Forward the destination IP address for the unknown file.
- **Destination Port**—Forward the destination port for the unknown file.
- **Virtual System**—Forward the virtual system that detected the unknown file.
- **Application**—Forward the user application that transmitted the unknown file.
- **User**—Forward the targeted user.
- **URL**—Forward the URL associated with the unknown file.
- **Filename**—Forward the name of the unknown file.
- **Email sender**—Forward the sender of an unknown email link (the name of the email sender also appears in WildFire logs and reports).
- **Email recipient**—Forward the recipient of an unknown email link (the name of the email recipient also appears in WildFire logs and reports).
- **Email subject**—Forward the subject of an unknown email link (the email subject also appears in WildFire logs and reports).

Palo Alto Networks, *WildFire Administrator's Guide Version 8.0 (EoL)* at 11, PaloAltoNetworks.com, https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/wildfire/8-0/wildfire-admin/wildfire-admin.pdf (last revised, Oct. 31, 2019) ("WildFire Guide 8.0"); *see also* Palo Alto Networks, *WildFire Administrator's Guide Version 10.1*, Version 10.1, PALOALTONETWORKS.COM, https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/

pdf/wildfire/10-1/wildfire-admin/wildfire-admin.pdf (last revised, May 21, 2021) ("WildFire Guide 10.1").

50. PAN's NGFs perform filtering and analysis of the status data to identify security related events that represent suspicious and/or malicious activity ("to identify potentially security-related events represented in the status data"). They analyze status data to identify potentially security-related events represented in the status data and that analysis includes filtering followed by an analysis of post-filtering residue.

51. For example, once the network traffic data has been processed and status data relating to it is under consideration, the PAN NGFs can then make one of three choices. The first two choices involve the application of the filter to determine what is good or bad (which includes what is suspicious). Here, based upon analysis of related status data, the traffic that is good can be allowed and the traffic that is known to be bad (or suspicious) can be blocked. For example, the PAN NGFs may use "white listing" and "black listing" techniques or similar but more advanced processes to allow or block traffic based on a generated alert or the absence of a generated alert.

52. In white listing, the PAN NGFs determine from the status data that there is no need for an alert as the status data does not appear to represent a security event (i.e., the PAN NGFs determine that the status data represents normal expected traffic). White listing could be applied, for example, by filtering based on an IP address extracted by the sensor during the collection of status information. The PAN NGFs support white listing using a variety of different status data. *See, e.g.*, WildFire Guide 8.0 at 512 ("If you find that certain critical applications trigger protocol anomaly signatures, you can then exclude those applications from protocol anomaly enforcement. To do this, add another rule to the Vulnerability Protection

Profile that whitelists protocol anomalies and attach the profile to the security policy rule that enforces traffic to and from the critical applications."); *see also, Id.* at 930 ("The initial rulebase you create will have the following types of rules:…Whitelist rules for the applications you officially sanction and deploy….Whitelist rules for safely enabling access to general types of applications you want to allow per your acceptable use policy.").

53. In black listing, the PAN NGFs determine from the status data that there is a sufficiently high likelihood that it represents a security related event (*e.g.*, bad or suspicious), allowing for the generation of an appropriate alert. The PAN NGFs can use the alert to automatically block the underlying network traffic to which the derived status data/alert relates. Black listing could be applied, for example, by filtering based on an IP address extracted by the sensor during the collection of status information. *See, e.g.*, WildFire Guide 8.0 at 944 ("you must create rules that explicitly blacklist applications designed to evade or bypass security or that are commonly exploited by attackers, such as public DNS and SMTP, encrypted tunnels, remote access, and non-sanctioned file-sharing applications."); *see also, Id.* at 930 ("The initial rulebase you create will have the following types of rules:… Blacklist rules that block applications that have no legitimate use case.").

54. After the positive and negative filtering performed by the PAN NGFs, the status data that was neither selected by positive filtering nor discarded by negative filtering is sent to the Wildfire service for further analysis. "WildFire is a cloud-based virtual environment that analyzes and executes unknown samples . . . and determines the samples to be malicious, phishing, grayware, or benign." *See* Palo Alto Networks, *PAN-OS® Administrator's Guide*, Version 10.1, PALOALTONETWORKS.COM, https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/getting-started/enable-basic-wildfire-forwarding (last updated, Sep. 13, 2022) ("PAN-

OS Admin Guide"). PAN NGFs "can forward unknown samples to WildFire for analysis." *Id*. Additionally, PAN NGFs forward "information about the network session for a sample." WildFire Guide 10.1 at 10. This includes status information such as source IP or destination IP, among others. *Id*. at 10-11.

55. During this phase, the post-filtering residue status data undergoes further analysis to determine whether it might represent an unknown attack. Unknown attacks are sometimes referred to as "zero day" attacks because they represent zero days for the vendor to apply a fix. This includes attacks where the adversary's exploit is known but where there is no public solution or patch available. As the attack is unknown, there is no known signature that would indicate the attack. "Samples submitted for WildFire analysis receive a verdict [along with] a detailed analysis report [] generated for each sample." WildFire Guide 10.1 at 41.

56. The Wildfire service then transmits information about these identified events to an analyst associated with the PAN security system. For example, "WildFire signatures and verdicts are [] shared globally." WildFire Guide 10.1 at 19. The PAN "threat research team uses the threat intelligence gathered from malware variants to block malicious IP addresses, domains, and URLs." PAN-OS Admin Guide.

57. PAN provides analysts as well as analyst systems for receiving the transmitted information. For example, PAN provides the Cortex XDR platform, which can "consume[] WildFire threat intelligence." *See* Palo Alto Networks, *Cortex XDR Pro Administrator's Guide 3.4* at 458, PALOALTONETWORKS.COM, https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/cortex/cortex-xdr/cortex-xdr-pro-admin/cortex-xdr-pro-admin.pdf (last revised, Aug. 21, 2022) ("Cortex Guide"). WildFire transmits the WildFire report through Cortex XDR to analysts. *Id*.

58. PAN also provides PAN analysts through a managed detection and response service. *See* Palo Alto Networks, *Unit 42 Managed Detection and Response Service*, PALOALTONETWORKS.COM, https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/datasheets/unit42-managed-detection-and-response.pdf (last accessed, Oct. 27, 2022). These analysts utilize PAN's Cortex XDR platform. *Id*. Thus PAN transmits information about identified events from its analysis of status data to a variety of analysts.

59. PAN also receives feedback at the PAN NGFs based on empirically-derived information reflecting operation of the system. "Each WildFire cloud . . . analyzes samples and generates malware signatures independently." WildFire Guide 10.1 at 16. These "signatures are shared globally, enabling WildFire users worldwide to benefit from malware coverage regardless of the location in which the malware was first detected." *Id*.

60. PAN dynamically modifies the analysis capability of the PAN NGFs during operation such that the methods of analysis are improved based on then-current intelligence. Specifically, PAN is able to push up-to-date security intelligence to PAN NGFs during operation—rather than offline—delivering timely protection against new and emerging threats. For example, the WildFire service provides a Real-Time Update feature allowing retrieval of "signatures for newly-discovered malware as soon as the WildFire public cloud can generate them." WildFire Guide 10.1 at 25 ("Select **Device > Dynamic Updates** and enable the firewall to get the latest WildFire signatures in real-time.").

61. PAN infringes the '237 Patent, both literally and through the doctrine of equivalents, and/or induces its customers in the examples given above and in other ways and with other products that operate in the same or similar manner. The examples of PAN's

infringement are not exhaustive and PAN's infringement is not limited only to those products or implementations.

62. Despite BT's written notice to PAN of PAN's infringement of the '237 Patent, PAN has not stopped its infringement. Rather, PAN continues to make, use, and offer its products and services in a manner which infringes the '237 Patent.

63. PAN's infringement of the '237 Patent has been and is willful because PAN has known of the '237 Patent, known that its products and services infringe the '237 Patent, and still continues to offer them in an infringing manner in disregard of BT's patent rights. Following BT's notice, PAN has continued to infringe by supplying infringing equipment, using the claimed methods to service its clients, and continuing to encourage infringement.

64. PAN also actively induces infringement under 35 U.S.C. § 271(b) by instructing its customers through manuals and other training materials to configure and operate the Palo Alto products in an infringing manner. Palo Alto provides, for example, administrator guides, technical notes, data sheets, and white papers—among other materials—to its customers. These materials instruct, enable, and otherwise cause customers to use various products and services in ways that infringe the '237 Patent. PAN provides these materials knowing that its customers' use of PAN's products in the manner instructed by PAN gives rise to infringement. PAN also contributorily infringes under 35 U.S.C. § 271(c) by selling its products, while knowing and—even encouraging—use of those products in an infringing manner.

65. PAN does not have a license or permission to use the claimed subject matter.

66. BT has been damaged and continues to be damaged by PAN's infringement.

67. BT is entitled to recover from PAN the damages sustained by BT as a result of PAN's wrongful acts in an amount to be determined at trial and up to three times its actual damages due to PAN's willful infringement.

68. BT is suffering and will continue to suffer irreparable harm for which there is no adequate remedy at law as a result of PAN's infringement of the '237 Patent. By way of example, PAN's infringing products and/or services compete with those of BT Americas. Unless enjoined, PAN will continue its infringing conduct.

COUNT II
(INFRINGEMENT OF U.S. PATENT NO. 7,895,641)

69. BT repeats and re-alleges the allegations contained in Paragraphs 1 through 39 above as if fully set forth herein.

70. PAN has directly infringed and continues to directly infringe, literally or under the doctrine of equivalents, one or more claims of the '641 Patent in violation of 35 U.S.C. §271(a) by making, using, offering to sell, selling (directly or through intermediaries), and/or importing, in this District and elsewhere in the United States, various PAN products and services including, but not limited to, Strata, the PA/CN/VM Series security appliances, Prisma Access, and WildFire.

71. For example, PAN infringes claim 1 of the '641 Patent, which provides as follows:

> A system for operating a probe as part of a security monitoring system for a computer network, the system comprising:
>
> a) a sensor coupled to collect status data from at least one monitored component of the network;
>
> b) a filtering subsystem coupled to analyze status data to identify potentially security-related events represented in the status data, wherein the analysis includes filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering;
>
> c) a communications system coupled to transmit information about the identified events to an analyst system associated with the security monitoring system;

d) a receiver for receiving feedback at the probe based on empirically- derived information reflecting operation of the security monitoring system; and

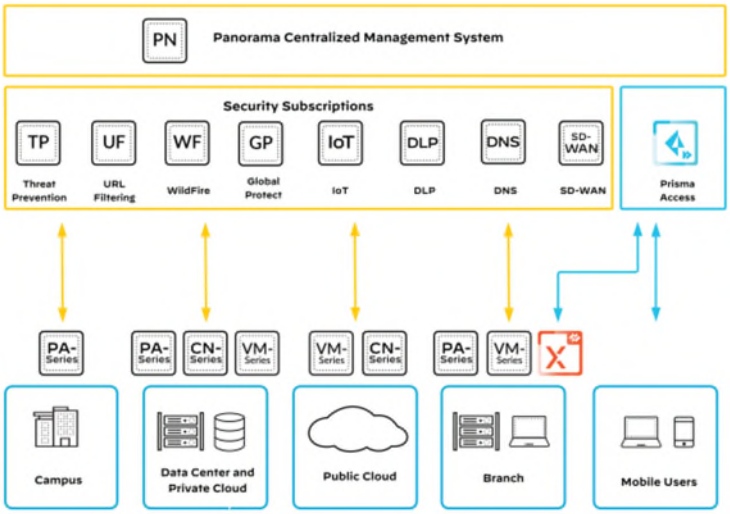
e) a modification control system for dynamically modifying an analysis capability of the probe during operation thereof based on the received feedback.

72. PAN offers and operates a series of products that individually and/or collectively infringe claim 1, among other claims, and was placed squarely on notice of its infringement of the ’641 Patent at least by June 28, 2018 and in various correspondence detailing its infringement (*e.g.*, BT’s letters of January 14, 2020, August 27, 2021, and January 20, 2022).

73. By way of example, PAN offers a series of products that individually and collectively provide security services (“a security monitoring system”) for networks that belong to PAN’s customers. PAN refers to this system as “Strata,” and it is a network security platform that provides security management, cloud-delivered security services, and next generation firewalls, while utilizing machine learning and analytics.

74. The following figure provides a detailed overview of the Strata platform:

Figure 2 Strata network security platform overview



Network Security Overview at 12.

75. PAN's next generation firewalls ("PAN NGFs")—including the PA-Series, CN-Series, VM-Series, and Prisma Access—are composed of multiple special purpose sensors. These sensors are coupled to collect status data from at least one monitored component of the network. These probes all leverage a common operating system—PAN-OS—and can be deployed as physical appliances (PA-Series), virtualized appliances (VM-Series), container form factors (CN-Series), and as a cloud-hosted service (Prisma Access). *See Network Security Overview* at 13. A sensor includes at least the portion of the PAN NGFs that receives network traffic destined for or originating from a monitored component of the network, and processes that traffic to collect information relevant to the state or condition of the network, network traffic, or the monitored component.

76. The status data is informative as to the status of the network and its components. Status data may also include both information extracted from the underlying network traffic (such as the IP addresses of the originating and/or destination computers) and information determined from the underlying network traffic (such as the frequency of messages, sensor IP address, message count, and associated time stamps or the duration of an event). Collected status data might provide context for other status data should it be subsequently desirable to correlate status data across multiple sensors to enhance the detection and response capabilities of the system.

77. By way of example, PAN NGFs collect status data related to attributes of a data packet. For example, IP Address status data is collected by PAN's probes as seen below.

- **Source IP**—Forward the source IP address that sent the unknown file.
- **Source Port**—Forward the source port that sent the unknown file.
- **Destination IP**—Forward the destination IP address for the unknown file.
- **Destination Port**—Forward the destination port for the unknown file.
- **Virtual System**—Forward the virtual system that detected the unknown file.
- **Application**—Forward the user application that transmitted the unknown file.
- **User**—Forward the targeted user.
- **URL**—Forward the URL associated with the unknown file.
- **Filename**—Forward the name of the unknown file.
- **Email sender**—Forward the sender of an unknown email link (the name of the email sender also appears in WildFire logs and reports).
- **Email recipient**—Forward the recipient of an unknown email link (the name of the email recipient also appears in WildFire logs and reports).
- **Email subject**—Forward the subject of an unknown email link (the email subject also appears in WildFire logs and reports).

WildFire Guide 8.0 at 11; *see also* WildFire Guide 10.1 at 11.

78. The PAN NGFs are composed of various sub-systems that perform filtering and analysis. The filtering sub-system is operatively coupled to analyze status data to identify potentially security-related events represented in the status data and connected to the sensor such that the collected status information can be received and processed. This analysis includes filtering followed by analysis of post-filtering residue. For example, the Threat Prevention feature for PAN NGFs "scans, inspects, classifies, and blocks threats in a single pass." *Network Security Overview* at 35. By analyzing status data present in network traffic, PAN's products have the ability to identify security related events that represent suspicious and/or malicious activity ("to identify potentially security-related events represented in the status data").

79. The PAN NGFs will subject the status data to further processing (i.e., "filtering") in order to determine whether the status data is actually indicative of an event that requires one or more network packets to be blocked. The PAN NGFs can then make one of three choices. The first two choices involve the application of the filter to determine what is good or bad (which includes what is suspicious). Here, based upon analysis of related status data, the traffic that is

known to be good can be allowed and the traffic that is known to be bad (or suspicious) can be blocked. For example, the PAN NGFs may use "white listing" and "black listing" techniques or similar, but more advanced processes to allow or block traffic based on a generated alert or the absence of a generated alert.

80. In white listing, the PAN NGFs determine from the status data that there is no need for an alert as the status data does not appear to represent a security event (i.e., the PAN NGFs determine that the status data represents normal expected traffic). White listing could be applied, for example, by filtering based on an IP address extracted by the sensor during the collection of status information. The PAN NGFs support white listing using a variety of different status data. *See, e.g.*, WildFire Guide 8.0 at 512 ("If you find that certain critical applications trigger protocol anomaly signatures, you can then exclude those applications from protocol anomaly enforcement. To do this, add another rule to the Vulnerability Protection Profile that whitelists protocol anomalies and attach the profile to the security policy rule that enforces traffic to and from the critical applications."); *see also, Id.* at 930 ("The initial rulebase you create will have the following types of rules:…Whitelist rules for the applications you officially sanction and deploy….Whitelist rules for safely enabling access to general types of applications you want to allow per your acceptable use policy.").

81. In black listing, the PAN NGFs determine from the status data that there is a sufficiently high likelihood that it represents a security related event (*e.g.*, bad or suspicious), allowing for the generation of an appropriate alert. The PAN NGFs can use the alert to automatically block the underlying network traffic to which the derived status data/alert relates. Black listing could be applied, for example, by filtering based on an IP address extracted by the sensor during the collection of status information. *See, e.g.*, WildFire Guide 8.0 at 944 ("you must

create rules that explicitly blacklist applications designed to evade or bypass security or that are commonly exploited by attackers, such as public DNS and SMTP, encrypted tunnels, remote access, and non-sanctioned file-sharing applications."; *see also*, *Id*. at 930 ("The initial rulebase you create will have the following types of rules:… Blacklist rules that block applications that have no legitimate use case.").

82. Data neither discarded nor selected by filtering represents status data that is indeterminate in that it has not been selected or discarded by the initial analysis. This status data is sent to the Wildfire service for further analysis. "WildFire is a cloud-based virtual environment that analyzes and executes unknown samples . . . and determines the samples to be malicious, phishing, grayware, or benign." *See* PAN-OS Admin Guide. PAN NGFs "can forward unknown samples to WildFire for analysis." *Id*. The PAN NGFs deliver to WildFire the indeterminate status data in order to determine whether it might represent an unknown attack. For example, PAN NGFs forward "information about the network session for a sample." WildFire Guide 10.1 at 10. This includes status information such as source IP or destination IP, among others. *Id*. at 10-11.

83. During this phase, the post-filtering residue status data undergoes further analysis to determine whether it might represent an unknown attack. Unknown attacks are sometimes referred to as "zero day" attacks because they represent zero days for the vendor to apply a fix. This includes attacks where the adversary's exploit is known but where there is no public solution or patch available. As the attack is unknown, there is no known signature that would indicate the attack. "Samples submitted for WildFire analysis receive a verdict [along with] a detailed analysis report [] generated for each sample." WildFire Guide 10.1 at 41.

84. The analysis of the status data by WildFire is transmitted by a communications system to an "analyst system" associated with the PAN security monitoring system. For example,

"WildFire signatures and verdicts are [] shared globally." WildFire Guide 10.1 at 19. The PAN "threat research team uses the threat intelligence gathered from malware variants to block malicious IP addresses, domains, and URLs." PAN-OS Admin Guide.

85. PAN provides analysts as well as analyst systems for receiving the transmitted information. For example, PAN provides the Cortex XDR platform, which can "consume[] WildFire threat intelligence." *See* Cortex Guide at 458. WildFire transmits the WildFire report through Cortex XDR to analysts. *Id.*

86. PAN also provides PAN analysts through a managed detection and response service. *See Unit 42 Managed Detection and Response Service*. These analysts utilize PAN's Cortex XDR platform. *Id.* Thus PAN transmits information about identified events from its analysis of status data to a variety of analysts.

87. The PAN NGFs receive feedback at the probe based on empirically-derived information. "Each WildFire cloud . . . analyzes samples and generates malware signatures independently." WildFire Guide 10.1 at 16. These "signatures are shared globally, enabling WildFire users worldwide to benefit from malware coverage regardless of the location in which the malware was first detected." *Id.*

88. The PAN NGFs' modification control system dynamically modifies its analysis capability during operation based on that feedback such that the methods of analysis are improved based on then-current intelligence. Specifically, PAN NGFs can retrieve up-to-date security intelligence during operation—rather than offline—delivering timely protection against new and emerging threats. For example, the WildFire service provides a Real-Time Update feature allowing retrieval of "signatures for newly-discovered malware as soon as the WildFire public

cloud can generate them." WildFire Guide 10.1 at 25 ("Select **Device** > **Dynamic Updates** and enable the firewall to get the latest WildFire signatures in real-time.").

89. PAN infringes the '641 Patent, both literally and through the doctrine of equivalents, and induces its customers to infringe, in the examples given above and in other ways and with other products that operate in the same or similar manner. The examples of PAN's infringement above are not exhaustive and PAN's infringement is not limited only to those products or implementations.

90. Despite BT's written notice to PAN of PAN's infringement of the '641 Patent, PAN has not stopped its infringement. Rather, PAN continues to make, use, and offer its products and services in a manner which infringes the '641 Patent.

91. PAN's infringement of the '641 Patent has been and is willful because PAN has known of the '641 Patent, known that its products and services infringe the '641 Patent, and still continues to offer them in an infringing manner in disregard of BT's patent rights. Following BT's notice, PAN has continued to infringe by supplying infringing equipment, using the claimed method to service its clients, and continuing to encourage infringement.

92. PAN also actively induces infringement under 35 U.S.C. § 271(b) by instructing its customers through manuals and other training materials to configure and operate the Palo Alto products in an infringing manner. Palo Alto provides, for example, administrator guides, technical notes, data sheets, and white papers—among other materials—to its customers instructing, enabling, and otherwise causing customers to use various products and services in ways infringing the '641 Patent and with knowledge that the customer's use gives rise to infringement. PAN also contributorily infringes under 35 U.S.C. § 271(c) by selling its products, while knowing and—even encouraging—use of those products in an infringing manner.

93. PAN does not have a license or permission to use the claimed subject matter.

94. BT has been damaged and continues to be damaged by PAN's infringement.

95. BT is entitled to recover from PAN the damages sustained by BT as a result of PAN's wrongful acts in an amount to be determined at trial and up to three times its actual damages due to PAN's willful infringement.

96. BT is suffering and will continue to suffer irreparable harm for which there is no adequate remedy at law as a result of PAN's infringement of the '641 Patent. By way of example, PAN's infringing products and/or services compete with those of BT Americas. Unless enjoined, PAN will continue its infringing conduct.

PRAYER FOR RELIEF

WHEREFORE, BT respectfully requests that this Court enter judgment against PAN, granting BT the following relief:

A. A judgment holding PAN liable for direct infringement of the Schneier Patents;

B. A judgment holding PAN liable for inducing infringement of the Schneier Patents;

C. A judgment holding PAN liable for contributory infringement of the Schneier Patents;

D. All damages available under 35 U.S.C. § 284 resulting from PAN's infringement of the Schneier Patents in an amount to be proven at trial, but no less than a reasonable royalty, together with pre-judgment interest and post-judgment interest;

E. An order and judgment permanently enjoining PAN from further acts of infringement of the Schneier Patents;

F. A judgment holding PAN's infringement of the Schneier Patents to be willful and deliberate, and a trebling of damages pursuant to 35 U.S.C. § 284;

G. A judgment holding this to be an exceptional case, and an award to BT for its attorneys' fees, costs and expenses incurred prosecuting this action pursuant to 35 U.S.C. § 285; and

H. Such other and further relief as the Court deems just and equitable.

DEMAND FOR JURY TRIAL

BT demands a trial by jury of all issues so triable.

POTTER ANDERSON & CORROON LLP

By: */s/ Philip A. Rovner*
Philip A. Rovner (#3215)
Jonathan A. Choa (#5319)
Hercules Plaza
P.O. Box 951
Wilmington, DE 19899
(302) 984-6000
provner@potteranderson.com
jchoa@potteranderson.com

Attorneys for Plaintiff British Telecommunications plc and BT Americas, Inc.

OF COUNSEL:

Bart H. Williams
PROSKAUER ROSE LLP
2029 Century Park East
Suite 2400
Los Angeles, California 90067
310-557-2900
bwilliams@proskauer.com

Baldassare Vinti
Nolan M. Goldberg
PROSKAUER ROSE LLP
Eleven Times Square
New York, New York 10036
212-969-3000
bvinti@proskauer.com
ngoldberg@proskauer.com

Edward Wang
PROSKAUER ROSE LLP
1001 Pennsylvania Avenue NW
Suite 600
Washington, DC 20004
202-416-6800
ewang@proskauer.com

Dated: November 28, 2022