**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION**

TREND MICRO INCORPORATED,	)	
	)	
Plaintiff,	)	Case No. 2:23-cv-00459
	)	
v.	)	
	)	
OPEN TEXT, INC. and OPEN TEXT	)	
CORP.,	)	JURY TRIAL DEMANDED
	)	
Defendants.	)	
	)	
	)	

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Trend Micro Incorporated ("Trend Micro" or "Plaintiff") files this Complaint for Patent Infringement and requests a Jury Trial against Defendants Open Text, Inc. ("OTI") and Open Text Corp. ("OTC") (collectively, "Open Text" or "Defendants"). Trend Micro alleges as follows:

1. Trend Micro is a leading cyber security software company that protects businesses and individuals against various cyber threats. Trend Micro operates a portfolio of products and services that allow people to use their computers, mobile phones, tablets, and various other electronic devices safely and securely. Trend Micro developed many innovative products, including those that are cloud-based and utilize machine learning and artificial intelligence technologies, to provide top-of-the-line security to its customers. Some of these innovations include those covered by U.S. Patent Nos. 8,161,548, 8,505,094 and 8,045,808 (collectively, the "Asserted Patents").

2. Trend Micro seeks to enjoin infringement and obtain damages resulting from Defendants' unauthorized making, using, offering for sale, selling and/or importing software and/or services that implement the patented technologies in the Asserted Patents.

NATURE OF THE CASE

3. Plaintiff brings claims under the patent laws of the United States, 35 U.S.C. § 1, *et seq.*, for infringement of the Asserted Patents. Defendants have infringed and continue to infringe each of the Asserted Patents under at least 35 U.S.C. §§ 271(a), 271(b) and 271(c).

THE PARTIES

4. Trend Micro Inc. is a corporation organized and existing under the laws of the State of California, with its principal place of business at 225 East John Carpenter Freeway, Suite 1500 Irving, Texas 75062. Among other activities, it is in the business of providing cyber security software to protect individuals and businesses against malware, spam, and other cyber threats. Trend Micro has customers throughout the United States, the State of Texas, and in this judicial District.

5. Open Text, Inc. is a corporation organized and existing under the laws of Delaware, with its principal place of business at Suites 301 & 302, 2440 Sand Hill Road, Menlo Park, CA 94025.

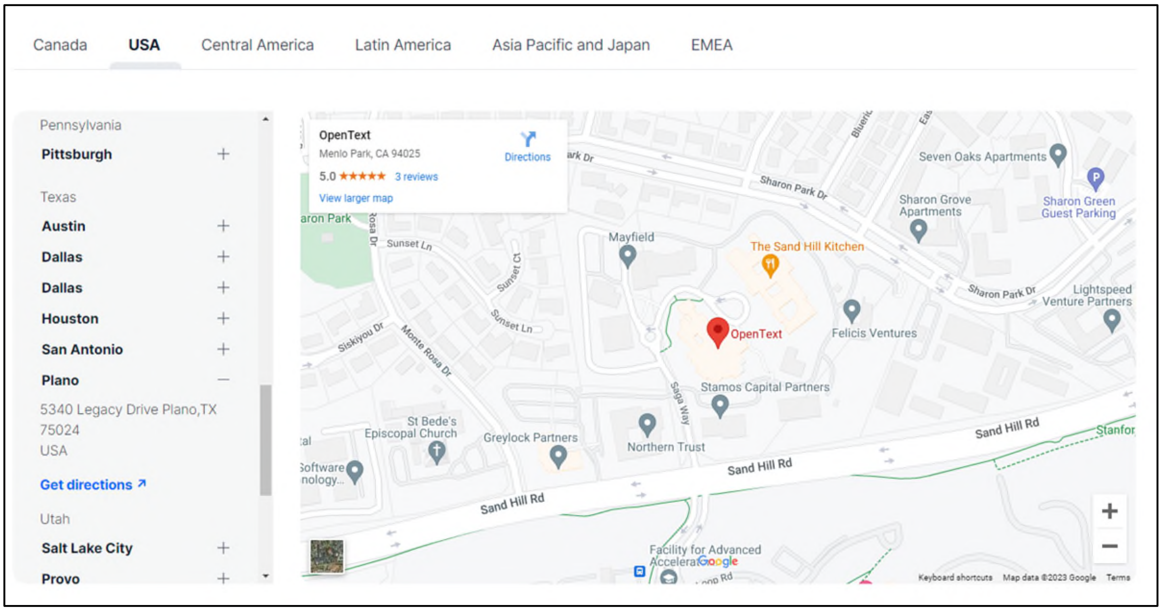
6. Open Text Corp. is a corporation organized and existing under the laws of Ontario, Canada, with its principal place of business at 275 Frank Tompa Dr. Waterloo ON, N2L 0A1.

JURISDICTION AND VENUE

7. This action arises under the Patent Laws of the United States, 35 U.S.C. § 1, *et seq*. Accordingly, this Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

8. This Court has personal jurisdiction over OTI and OTC, which it may exercise under the Texas Long Arm Statute. Exercise of such personal jurisdiction is proper and comports with due process because this Court, among other reasons, has specific personal jurisdiction over OTI and OTC.

9. Specific personal jurisdiction exists over Defendants because, according to Open Text's website (shown below), Open Text maintains numerous offices in the United States, including at least six offices in the State of Texas, at least one of which is located in the Eastern District of Texas :



Canada USA Central America Latin America Asia Pacific and Japan EMEA

Pennsylvania
Pittsburgh +

Texas
Austin +
Dallas +
Dallas +
Houston +
San Antonio +
Plano –

5340 Legacy Drive Plano,TX
75024
USA

Get directions ↗

Utah
Salt Lake City +
Provo +

OpenText
Menlo Park, CA 94025
5.0 ★★★★★ 3 reviews
View larger map
Directions

https://www.opentext.com/about/office-locations

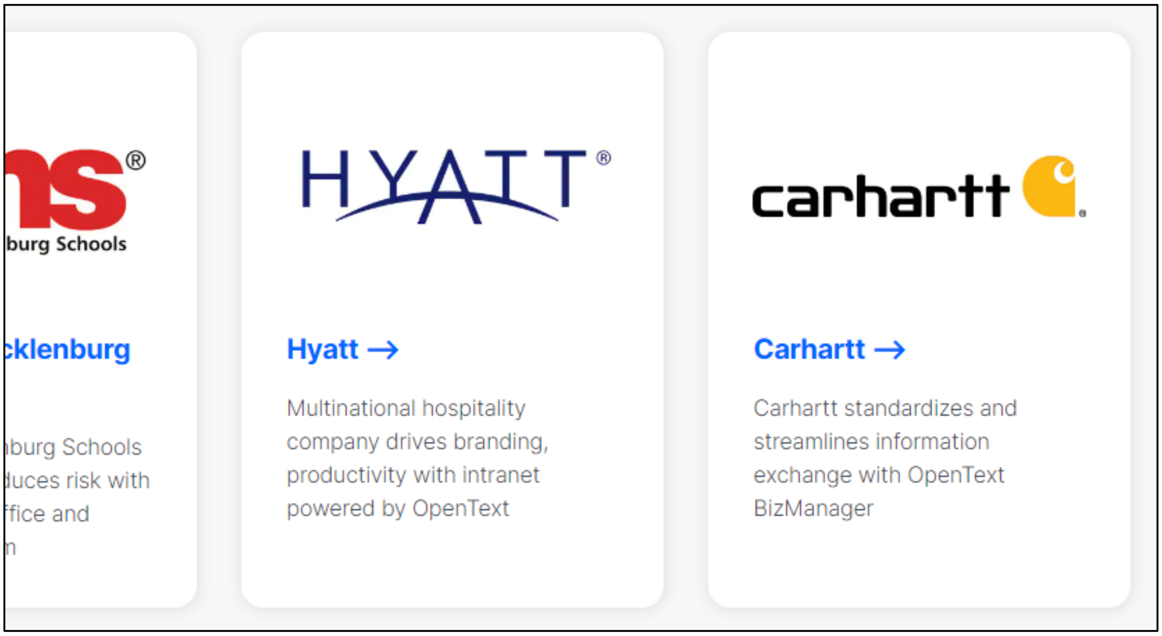
10. This Court also has specific personal jurisdiction over OTI and OTC because, on information and belief, OTI and OTC have purposefully and voluntarily placed

one or more infringing products into the stream of commerce with the expectation that they will be purchased and/or used by residents of this judicial District. Additionally, each Defendant has purposefully availed itself of the privileges of conducting business in the State of Texas and in the Eastern District of Texas; each Defendant has sought protection and benefit from the laws of the State of Texas; each Defendant regularly conducts business within the State of Texas and within the Eastern District of Texas; and Plaintiff's causes of action arise directly from Defendants' business contacts and other activities in the State of Texas and in the Eastern District of Texas.

11. In particular, OTI and OTC have committed acts of infringement within the United States, the State of Texas and this judicial District by, *inter alia*, directly and/or indirectly through intermediaries shipping, distributing, advertising, selling, offering for sale, importing, and/or using products that infringe one or more claims of Trend Micro's patents asserted herein. Upon information and belief, each Defendant has committed patent infringement in the State of Texas and in the Eastern District of Texas, has contributed to patent infringement in the State of Texas and in the Eastern District of Texas, and/or has induced others to commit patent infringement in the State of Texas and in the Eastern District of Texas.

12. Open Text also solicits customers in the State of Texas and in the Eastern District of Texas, and has many paying customers who are residents of the State of Texas and the Eastern District of Texas and who use Open Text products and services in the State of Texas and in the Eastern District of Texas. *See Trend Micro Incorporated v. Open Text, Inc.*, *et al.*, No. 1-22-cv-1063, Dkt. No. 47 at 4 (E.D. Va. Sept. 29, 2023) ("OTI sells products in Texas and 'makes all of its products and services available in Texas ….'"

(citation omitted)). For example, some of Open Text's largest customers are either located in and/or have locations in this District, including Hyatt (Allen, TX), AAA The Auto Club Group (Allen, TX), Lids (Tyler, TX) and Carhartt (Tyler, TX).



cklenburg

burg Schools
duces risk with
ffice and
n

Hyatt →

Multinational hospitality company drives branding, productivity with intranet powered by OpenText

Carhartt →

Carhartt standardizes and streamlines information exchange with OpenText BizManager

See, e.g., https://www.opentext.com/customers

13. Additionally, OTC has purchased multiple companies either headquartered in or with offices located in the State of Texas. For example, on November 23, 2015, OTC acquired Daegis Inc., a global information governance, data migration solutions and development company, based in Texas, United States, for $23.3 million. On July 13, 2011, OTC acquired Global 360 Holding Corp. (Global 360), a software company based in Dallas, Texas, United States, for $256.6 million. *See* https://www.sec.gov/Archives/edgar/data/1002638/000100263816000080/a10-kq4x16.htm. OTC also purchased a company called Actuate, which on information and belief had facilities located in Allen, Texas, located in this District.

14. OTC and OTI have also initiated multiple actions for patent infringement in the State of Texas. *See Open Text Corp. v. Alfresco Software, Ltd. et al.*, Case No. 6:20-cv-920 (W.D. Tex. Oct. 5, 2020); *Open Text Corp. et al. v. Alfresco Software, Ltd. et al.*, Case No. 6:20-cv-928 (W.D. Tex. Oct. 7, 2020); *Open Text Corp. et al. v. Alfresco Software, Ltd. et al.*, Case No. 6:20-cv-941 (W.D. Tex. Oct. 9, 2020); *Open Text Inc. et al. v. AO Kaspersky Labs., Case No.* 6:22-cv-00243 (W.D. Tex. Mar. 4, 2022); *Open Text Inc. et al. v. CrowdStrike Holdings, Inc. et al.*, Case No. 6:22-cv-241 (W.D. Tex. Mar. 4, 2022); *Open Text Inc. et al. v. Sophos Ltd.*, Case No. 6:22-cv-240 (W.D. Tex. Mar. 4, 2022); *Open Text Inc. et al. v. Trend Micro, Inc.*, Case No. 6:22-cv-239 (W.D. Tex. Mar. 4, 2022); *Open Text Inc. et al. v. Forecpoint LLC,* Case No. 6:22-cv-342 (W.D. Tex. Mar. 4, 2022).

15. Additionally, Defendants, directly or through intermediaries, including its subsidiaries, maintain control over websites accessible to residents of the State of Texas and this judicial District, through which Defendants promote and facilitate sales of the infringing products. For example, the website https://www.opentext.com directs consumers in the United States, including those in the State of Texas and this judicial District, to purchase Defendants' infringing products.

16. Additionally, OTI is registered to do business in the State of Texas, and maintains a registered agent at 211 E. 7th St., Suite 620, Austin, TX 78701-3218. OTI's registration with the State of Texas lists Muhi Majzoub as a Vice President of OTI. Mr. Majzoub is also the Executive Vice President and Chief Product Officer for OTC. OTI also lists Madhu Ranganathan as its President and Director. Ms. Ranganathan is an Executive Vice President and Chief Financial Officer of OTC. OTI also lists Simon Harrison as a Vice President. Mr. Harrison is an Executive Vice President for Enterprise

Sales at OTC. Thus a number of the senior executives of OTI, who direct OTI's business in the State of Texas and this District, are also officers and directors of OTC. OTC also prepares consolidated financial reports on behalf of both OTC and OTI.

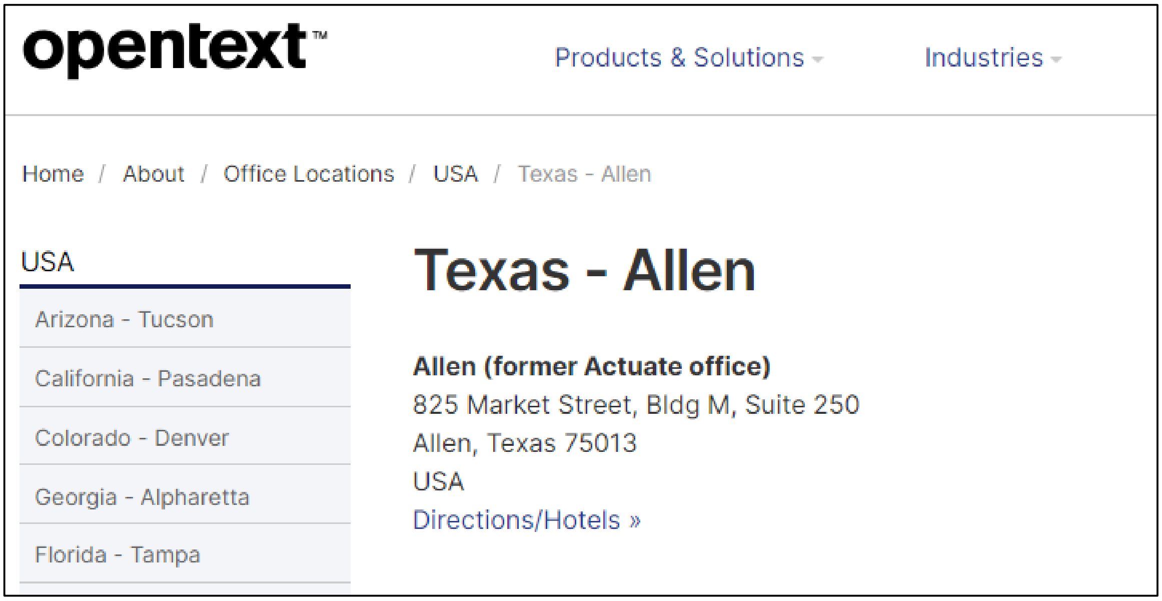
17. Thus, Defendants have established minimum contacts with the State of Texas and the exercise of jurisdiction would not offend traditional notions of fair play and substantial justice.

18. Additionally, or alternatively, personal jurisdiction exists over OTC at least by virtue of Federal Rule of Civil Procedure 4(k)(2). For the same reasons discussed previously, OTC has sufficient contacts with the U.S. as a whole to satisfy due process and justify application of federal law. *See also Open Text S.A. v. Box, Inc.*, No. 2:13-cv-00319, Dkt. No. 1 (Complaint) ¶ 7 (E.D. Va. June 5, 2013) ("Open Text Corporation distributes software products and provides customer support and professional services through a number of subsidiaries, including Open Text, Inc., which sells Open [] Text software and services in the United States."); *Open Text Corp. v. Hyland UK Operations Ltd.*, No. 2:21-cv-9101, Dkt. No. 1 (Complaint) ¶ 2 (W.D. Tex.); *Open Text Corp. v. Hyland Software, Inc.*, No. 8:20-cv-2123, Dkt. No. 2 (Complaint) ¶ 2 (C.D. Cal.); *Touchcom, Inc. v. Bereskin & Parr*, 574 F.3d 1403, 1416 (Fed. Cir. 2009) ("Rule 4(k)(2) contemplates a defendant's contacts with the entire United States, as opposed to the state in which the district court sits."). Further demonstrating its contacts with the United States, Open Text sponsored "OpenText World 2022" in Las Vegas, Nevada on October 4-6, 2022, featuring a "keynote" speech by OTC Chief Executive Officer & Chief Technology Officer, Mark J. Barrenechea, and OTC Executive Vice President & Chief Product Officer, Muhi S. Majzoub. On information and belief, this event occurs annually.

19. Venue is proper for both Defendants in this judicial District pursuant to 28 U.S.C. §§ 1391(b), (c) and 1400(b).

20. Venue is proper for OTC because venue for foreign entities in a patent infringement action is governed by the general venue statute, 28 U.S.C. § 1391, which provides that "a Defendant not resident in the United States may be sued in any judicial district." 28 U.S.C. § 1391(c)(3).

21. Venue is proper for OTI because, on information and belief, OTI has committed acts of infringement and maintains regular and established places of business in this District. For example, screen shots below show that OTI has a branch registration and maintains an office in Allen in the State of Texas, which is located in this judicial District.

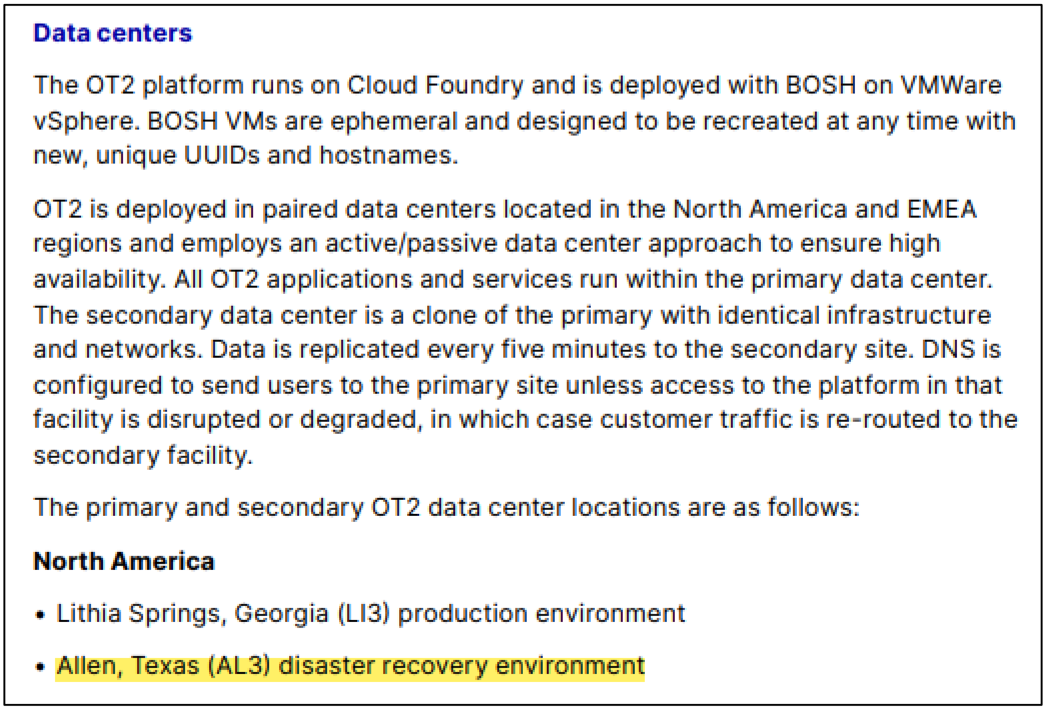


Texas - Allen

Allen (former Actuate office)
825 Market Street, Bldg M, Suite 250
Allen, Texas 75013
USA
Directions/Hotels »

https://www.opentext.co.uk/about/office-locations/usa/texas-allen

22. Additionally, on information and belief, OTI maintains a regular and established presence in Allen where it owns and operates data centers.



Data centers

The OT2 platform runs on Cloud Foundry and is deployed with BOSH on VMWare vSphere. BOSH VMs are ephemeral and designed to be recreated at any time with new, unique UUIDs and hostnames.

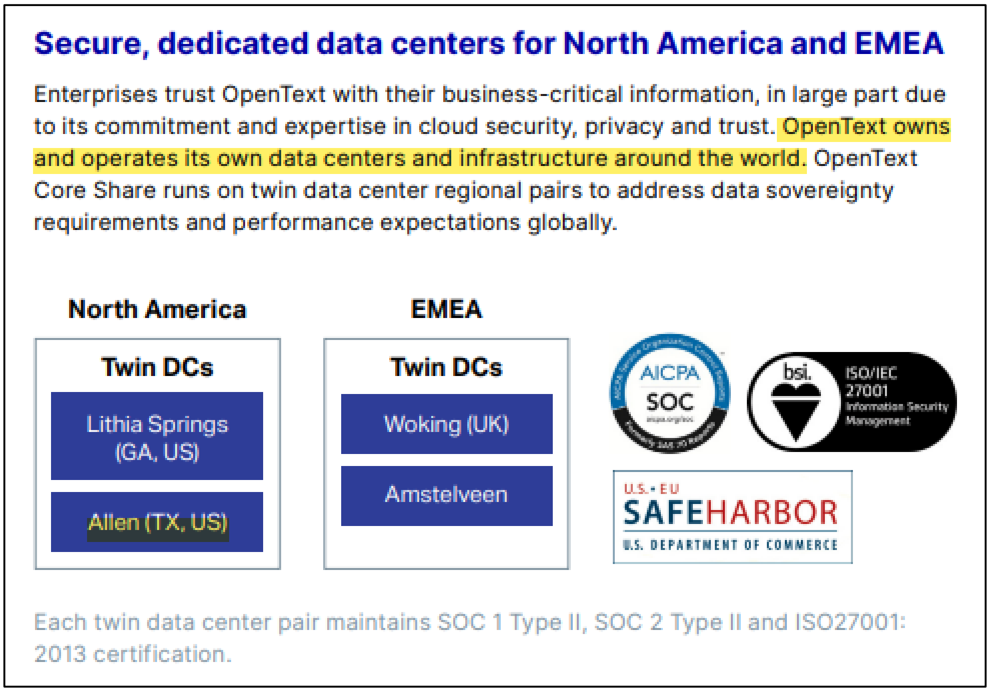
OT2 is deployed in paired data centers located in the North America and EMEA regions and employs an active/passive data center approach to ensure high availability. All OT2 applications and services run within the primary data center. The secondary data center is a clone of the primary with identical infrastructure and networks. Data is replicated every five minutes to the secondary site. DNS is configured to send users to the primary site unless access to the platform in that facility is disrupted or degraded, in which case customer traffic is re-routed to the secondary facility.

The primary and secondary OT2 data center locations are as follows:

North America

- Lithia Springs, Georgia (LI3) production environment
- Allen, Texas (AL3) disaster recovery environment

https://www.opentext.com/file_source/OpenText/en_US/PDF/opentext-wp-overview-of-ot2-platform-en.pdf



Secure, dedicated data centers for North America and EMEA

Enterprises trust OpenText with their business-critical information, in large part due to its commitment and expertise in cloud security, privacy and trust. OpenText owns and operates its own data centers and infrastructure around the world. OpenText Core Share runs on twin data center regional pairs to address data sovereignty requirements and performance expectations globally.

North America

Twin DCs

Lithia Springs (GA, US)

Allen (TX, US)

EMEA

Twin DCs

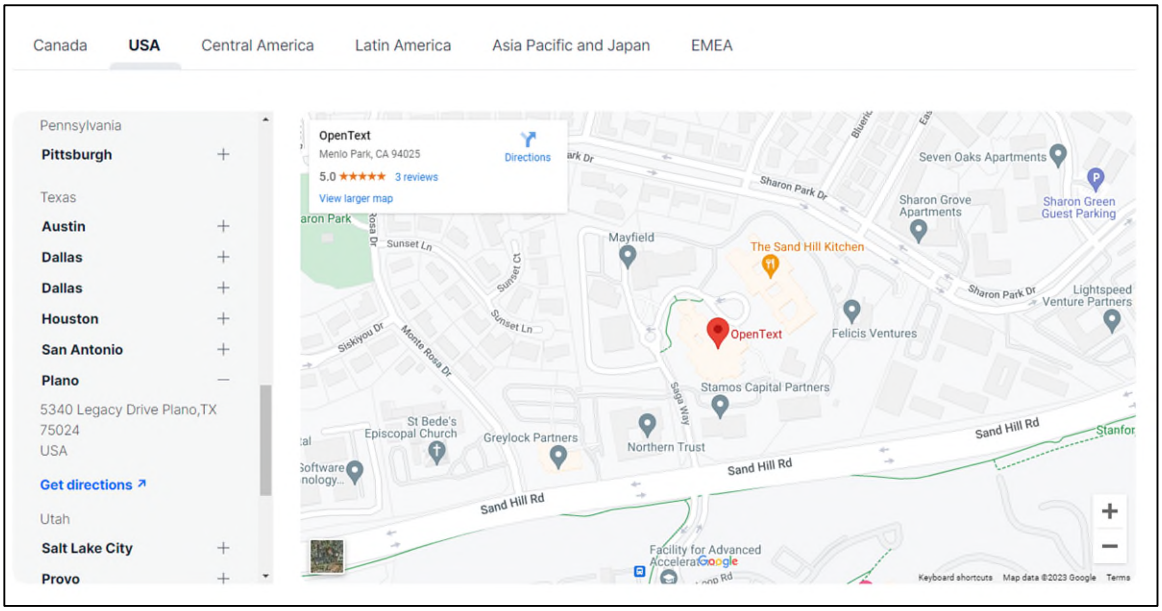
Woking (UK)

Amstelveen

Each twin data center pair maintains SOC 1 Type II, SOC 2 Type II and ISO27001: 2013 certification.

https://www.opentext.com/file_source/OpenText/en_US/PDF/opentext-wp-secure-file-sharing-and-collaboration-in-the-opentext-cloud-en.pdf

23. Additionally, Defendants' website lists an office in Plano, Texas, which is located in this judicial District:



Pennsylvania

Pittsburgh +

Texas

Austin +

Dallas +

Dallas +

Houston +

San Antonio +

Plano –

5340 Legacy Drive Plano,TX
75024
USA

Get directions ↗

Utah

Salt Lake City +

Provo +

OpenText
Menlo Park, CA 94025
5.0 ★★★★★ 3 reviews
View larger map

https://www.opentext.com/about/office-locations

24. Moreover, on April 5, 2019, OTI admitted this district is a proper forum for venue. *See UnoWeb Virtual, LLC v. Open Text Inc.*, No. 2:19-cv-8-JRG, Dkt. No. 19 (Answer), at 8 (E.D. Tex. Apr. 5, 2019).

PLAINTIFF'S PATENTS

United States Patent No. 8,161,548

25. On April 17, 2012, the United States Patent & Trademark Office (USPTO) issued United States Patent No. 8,161,548 ("the '548 Patent"), titled "Malware Detection Using Pattern Classification." Trend Micro is the lawful owner of all right, title, and interest in the '548 Patent. A true and correct copy of the '548 Patent is attached as Exhibit A to this Complaint.

26. The '548 Patent improves upon conventional methods of computer-based malware detection and classification. At the time of filing of the '548 Patent, "it [was]

common for malicious software such as computer viruses, worms, spyware, etc. to affect a computer," causing files to be deleted, clogging e-mail accounts, stealing confidential information, causing computer crashes, allowing unauthorized access and generally performing other undesirable actions. Exhibit A at 1:14-21. At the time, users were able to create backups of their computer systems and files in the event of catastrophic failure, such as a power loss, hard drive crash, or a system operation failure. *Id*. at 1:22-29. But backup restoration techniques were not effective when dealing with infection by malicious software. *Id*. at 1:29-31. For example, if a backup restoration point were set to a time when the malware was still present on the computer system but had not been detected, then restoring the backup would not solve the problem as the malware would still be on the system and another catastrophic failure would be imminent. Thus, it was important to be able to detect unknown malware when it first became present in a computer system or before it could even be transferred to a user's computer. *Id*. at 1:31-33.

27. Conventional malware detection techniques were inadequate for solving the problem as they either were unable to detect unknown malware at all, or they were costly and time consuming and thus could not realistically address unknown threats when they first became present, and they also could not achieve both a high detection rate and a low false-positive rate. Specifically, "[p]rior art techniques [were] able to detect known malware us[ing] a predefined pattern database that compares a known pattern with suspected malware." Exhibit A at 1:34-36. Such techniques, however, had the problem of not being able to "handle new, unknown malware." *Id.* at 1:36-37. Other techniques "use[d] predefined rules or heuristics to detect unknown malware." *Id.* at 1:37-38. Such techniques, however, had the problem of requiring the predefined rules to be written down manually,

which were hard to maintain and time consuming. *Id.* at 1:39-43. Because the number of predefined rules had to be limited, the techniques could not "achieve both a high detection rate and a low false-positive rate." *Id.* at 1:43-46.

28. Moreover, at the time, there was a multitude of different types of malware that could infect a computer system, such as viruses, Trojan horse programs, worms, exploits, root kits, and more. *Id*. at 2:65-4:19. Thus, a malware detection system had to be sufficiently flexible to detect a wide variety of different types of malware in order to effectively detect unknown types of malware.

29. The '548 Patent solved these problems by claiming specific and significant improvements over the conventional malware detection and classification methods. The '548 Patent describes and claims techniques that train and employ a machine learning classifier to determine whether or not a software program is a particular type of malware. Conventional technology attempted to detect malware based on specific malicious behavior, which malware such as worms could avoid such as by creating processes with different names on different machines, making its behavior difficult to track. *Id.* at 4:66-5:7. But the inventors of the '548 Patent discovered that "each type of malware exhibits a certain pattern which is different from that of benign computer software," such that a classifier configured with a pattern classification algorithm could be used to detect the malware. *Id*. at 5:8-26. The claimed techniques of the '548 Patent took pattern classification algorithms that had previously been used in different applications, and applied them to a specific computer security application using an unconventional and particular configuration and tuning of the classifier in order to detect particular types of malware, thereby improving ability of a computer to detect unknown malware in ways that

conventional malware detection systems could not. For example, the claimed techniques employ an unconventional configuration of the classifier that utilizes specific features such as "characteristics of said type of malware, DLL names and function names executed by said type of malware, and alphanumeric strings used by said type of malware" to improve the ability of the classifier to detect a particular type of malware. The "resulting trained model is tuned to specifically detect" the particular type of malware. *Id*. at 5:38-41. "By providing these features and their values to the classifier, the classifier is better able to identify a particular type of malware." *Id*. at Abstract, 2:7-9.

30. During prosecution, the Applicant further explained how the '548 Patent claims are directed to specific technological solutions to a problem rooted in computer functionality:

> Further, independent claims 1, 8 and 14 have all been amended to require that the first and second groups of features are <u>combined</u> into one feature set in the feature definition file. Support for this limitation may be found, for example in the paragraph spanning pages 9 and 10 the present Specification. The advantage of using two feature sets, and combining these sets of features into a single larger feature set, is that a training model can be produced to identify at least two different kinds of malware (in the case of claim 1), and that a classification algorithm can identify at least two different kinds of malware (in the case of claims 8 and 14). If the feature sets are not combined, then one must either use two training models, or use two different classification algorithms in order to identify different types of malware.

'548 Patent Prosecution History, Sept. 30, 2011 Applicant Arguments/Remarks at 8. By specifically tuning the claimed training model to utilize the combined feature sets, which further involves combining the logic of the classification functions for detecting the different malware types, *id*. at 5:42-51, this unconventional configuration avoids the need to train two separate classifiers that would have otherwise been costly and time-consuming and would have otherwise resulted in a lower detection rate and higher false-positive rate. And the unconventional combining of features for different types of malware makes the ’548 Patent’s improved malware detection technology “suitable for use with a wide variety of types and formats of malware,” which as explained above was critical to detecting unknown malware. *Id*. at 4:20-21.

31. The claims of the ’548 Patent are thus directed to a specific improvement necessarily rooted in computer technology by employing a machine learning classifier tuned with a specific combination of features for detecting different types of malware. This unconventional approach allows a computer security system to detect unknown malware, ensuring that threats are identified before they reach a user’s computer with a high detection rate and low false-positive rate, unlike conventional approaches to malware detection.

32. The unconventional claimed elements, individually and in combination, that form the ’548 Patent’s innovative malware detection technology “provides the ability to detect a high percentage of unknown malware with a very low false-positive rate,” as confirmed by exemplary test results disclosed in the patent, something conventional techniques could not achieve at the time. *Id*. at 1:56-58, 10:45-11:34. And in addition to reducing error rates and false positives, the ’548 Patent provides numerous other technical advantages over conventional malware detection, including enhanced security protection such as through automatic detection of threats, the ability to quickly adapt to detect new threats and unknown malware, efficient detection of malware, and improved usability for users by eliminating the need to continuously check for threats.

United States Patent No. 8,505,094

33. On January 13, 2010, the United States Patent & Trademark Office (USPTO) issued United States Patent No. 8,50s5,094 (“the ’094 Patent”), titled “Detection

of Malicious URLs in a Webpage." Trend Micro is the lawful owner of all right, title, and interest in the '094 Patent. A true and correct copy of the '094 Patent is attached as Exhibit B to this Complaint.

34. The '094 Patent improves upon conventional methods of detecting malicious URLs. At the time of filing of the '094 Patent, computer users were not only being exposed to malware attached to e-mail messages, but they were also facing malicious software threats from the World Wide Web. Exhibit B at 1:12-14. Even legitimate sites were being hijacked by hackers who would inject malicious URLs into the webpages of that site that redirected innocent users to a site containing malware, which was downloaded to the user's computer. *Id.* at 1:16-48.

35. At the time, there were no solutions that sufficiently addressed the problem. Google had created a Safe Browsing project providing a diagnostic page for various websites to reflect the security of the site, but while the project diagnosed the problem, it did not propose any solutions. *Id.* at 1:49-64.

36. Conventional solutions for detecting malicious URLs were also inadequate. One proposed solution was to "crawl all Web sites in order to find malicious sites and uncover the various attack vectors located at these sites." *Id.* at 1:65-67. But in addition to the "sheer magnitude of sites that must be crawled, many malicious sites [were] sophisticated enough (or the hacker is) to detect if a crawler is from an antivirus company and may be able to take evasive action to avoid detection. *Id.* at 1:67-2:4. Furthermore, most malicious sites changed their domains frequently so the problem became "a moving target that [could not] be hit." *Id.* at 2:4-6.

37. Other approaches at the time were to "reference a blacklist that lists which URLs are suspicious of being malicious" or to use a "Simple RegExp match to identify an unknown malicious site." *Id.* at 2:7-10. Such techniques, however, had the problem of not being able to "identify new threats located at newly formed malicious Web sites." *Id.* at 2:10-12. Further, it was difficult to detect a malicious URL in a webpage because there was often not enough "direct information to make a positive identification, and, it [was] difficult to retrieve the contents of pages pointed to by these malicious URLs." *Id.* at 2:12-16.

38. Thus, "a new approach [was] desired to be able to detect malicious URLs in legitimate Web sites in order to prevent malware from being downloaded to a user computer." *Id*. at 2:17-20.

39. The '094 Patent solved these problems and provided the desired solution by claiming specific and significant improvements over the conventional methods of detecting malicious URLs. "[T]hrough extensive analysis," the inventors of the '094 Patent discovered that "the number of Web sites compromised by an injected malicious URL is on the order of hundreds of time more common than the number of malicious Web sites to which these malicious URLs link," such that "an approach that targets these compromised Web sites will have a dramatic impact." *Id*. at 3:18-24. The inventors also discovered that "most all malicious URLs on a legitimate Web page contain useless information except for the URL itself," and that "most all malicious URLs that have been injected into a Web page are not relevant to the page into which they have been inserted for many different reasons." *Id*. at 3:25-30. After extensive research, it was discovered "that most injected malicious URLs are not relevant to their host pages based upon various dimensions such as referring behavior, page layout and page content." *Id*. at 3:54-59.

40. Leveraging these discoveries borne from extensive research, the ’094 Patent describes and claims techniques that employ a machine learning classifier to determine whether or not a URL is malicious. For example, based on research performed on over 2.4 million external scripts and “iframes” from 1.1 million webpages, the inventors came to the conclusion that a URL linking to a page having a lower page rank than the present page is likely to be a malicious URL. The ’094 Patent thereby claims a machine learning classifier configured to utilize a “numerical referring vector” that is determined from the page rank of a parent webpage and the page rank of a child webpage identified by an embedded URL in the HTML code of the parent webpage in order to determine whether or not the URL is malicious. *See, e.g.*, ’094 Patent at claim 7.

41. Further research showed that over 83% of malicious “iframes” are located in isolated sections of their host pages compared to only 4% of normal “iframes,” and over 5% of malicious scripts are located in isolated sections compared to about 0.35% of normal scripts. *Id.* at 4:24-30. In other words, “a malicious script is 16 times more likely to be found in an isolated section of a Web page.” *Id.* at 4:30-32. The ’094 Patent thereby also claims a machine learning classifier configured to utilize a “numerical layout vector” that is determined from the layout features of an embedded URL on a webpage related to the layout of the embedded URL within the HTML code of the webpage in which it is embedded, such as whether the embedded URL is located within the header or the footer of the HTML code, in order to determine whether or not the URL is malicious. *See, e.g.*, *id.* at claim 1.

42. The inventors also discovered that “[m]ost normal links on a Web page point to content at another Web site concerning the same general subject,” whereas

"malicious iframes typically link to content that is irrelevant to the host page, and links from malicious scripts are loosely coupled with a host page." *Id*. at 4:35-44. The '094 Patent thereby also claims a machine learning classifier configured to utilize a "numerical relevancy vector" that is determined from the relevancy between the content of a parent webpage and the content of a child webpage identified by an embedded URL on the parent webpage, in order to determine whether or not the URL is malicious. *See*, *e.g.*, *id*. at claim 14.

43. Through its unconventional application of a machine learning classifier configured with parameters discovered through extensive research, the '094 Patent provides a technological solution to the problem of detecting malicious URLs hosted on legitimate websites, thereby preventing malware from being downloaded onto a user's computer. The '094 Patent addresses a problem that specifically arises in the realm of computer networks—the detection of malicious URLs embedded in legitimate websites—and claims solutions rooted in Internet technology.

44. The claims of the '094 patent are thus directed to a specific improvement necessarily rooted in computer technology by employing a machine learning classifier configured with a specific combination of parameters for detecting a malicious URL. This unconventional approach allows a computer security system to detect malicious URLs embedded in legitimate host websites, ensuring that even previously unknown URLs could be identified, including new threats located at newly formed malicious websites, thereby preventing malware from being downloaded to a user computer.

45. The unconventional claimed elements, individually and in combination, that form the '094 Patent's innovative malicious URL detection technology "provides an

effective way to detect malicious URLs either on the client side or at the back end." *Id*. at 2:25-27. The '094 Patent reduces error rates and false positives, enhances security protection such as through the automatic detection of threats, provides the ability to quickly adapt to detect new threats and malicious URLs, provides efficient detection of malicious URLs, and provides improved usability for users by eliminating the need to continuously check for malicious URLs.

United States Patent No. 8,045,808

46. On October 25, 2011, the United States Patent & Trademark Office (USPTO) issued United States Patent No. 8,045,808 ("the '808 Patent"), titled "Pure Adversarial Approach for Identifying Text Content in Images." Trend Micro is the lawful owner of all right, title, and interest in the '808 Patent. A true and correct copy of the '808 Patent is attached as Exhibit C to this Complaint.

47. The '808 Patent improves upon conventional methods of identifying text content in images. At the time of filing of the '808 Patent, email had become a relatively common means of communication, but its popularity also led to "spammers" sending mass quantities of unsolicited emails, or spam. Exhibit C at 1:23-37. Whereas spam had previously consisted of text and images linked to websites, at the time of the '808 Patent, spammers had started to embed inappropriate content in images. *Id*. at 1:38-41. Existing spam detectors that relied on "keyword and statistical filters" or comparing URLs in the spam to databases of known domains were unable to detect such spam emails because they did not contain obvious "spammy textual content" or a link or domain that can be looked up in a database of bad links or domains. *Id*. at 1:41-58.

48. Optical character recognition (OCR) was proposed as a potential solution because OCR can detect text in images. *Id*. at 1:59-62. Such OCR anti-spam applications

involved "performing OCR on an image to extract text from the image, scoring the extracted text, and comparing the score to a threshold to determine if the image contains spammy content." *Id.* at 1:63-2:1. Spammers, however, responded "with images deliberately designed with anti-OCR features" that could avoid detection by traditional OCR-based anti-spam applications. *Id.* at 2:1-3. For example, spammers utilized irregular backgrounds, fonts, and color schemes to confuse traditional OCR modules, which would make text extracted by a traditional OCR module largely unintelligible. *Id*. at FIGS. 1 and 2, 3:7-16, 8:3-31.

49. The '808 Patent solved these problems by providing "a novel and effective approach for identifying content in an image even when the image has anti-OCR features." *Id*. at 2:6-8. The '808 Patent describes and claims techniques that utilizes an adversarial OCR approach to identify text content within an image. "The adversarial approach allows for better accuracy in identifying inappropriate content in images by focusing its search for a particular expression, allowing for more accurate reading of text embedded in images" than traditional OCR. *Id*. at 4:19-22. Whereas traditional OCR requires identification of a particular character in each character block when extracting text from an image, the '808 Patent's claimed solution calculates the probability that a particular character block includes a character, making the '808 Patent's solution more robust than conventional OCR. *Id*. at 9:41-47. The '808 Patent then applies the unconventional step of identifying a candidate sequence of character blocks to compare to the search term to determine if the search term is present.

50. Because the '808 Patent's unconventional claimed approach "does not necessarily require establishment of which letter, digit, or symbol a character-block

contains," in contrast to conventional OCR, the '808 Patent's approach is able to "provide a more accurate identification of search terms compared to conventional OCR approaches." *Id*. at 11:9-18. Because traditional OCR requires determination of which letter, digit, or symbol is in a character block, it is vulnerable to anti-OCR features that use confusing and ambiguous letters, such as an upper case "I," a vertical bar, a lower case "l," and an exclamation point. *Id*. at 11:16-22. The '808 Patent's unconventional approach on the other hand, by utilizing the probabilities of particular characters in a character block and forming a candidate sequence to match against a search term, can match these aforementioned ambiguous characters to search terms without identifying a particular ambiguous character in a particular character block. *Id*. at 11:22-33. For example, in an image containing the word "symbol" with obfuscating features such as an irregular background, conventional OCR may detect the letter "l" as an exclamation point, resulting in the word being extracted as the text "symbo!" and a match against the search term "symbol" would (incorrectly) not be found. Whereas the '808 Patent, which does not require the detection of each individual character, applies an unconventional approach of using the probabilities for each character block to determine that the search term "symbol" appears with sufficient likelihood within the text, thereby resulting in a match.

51. During prosecution, the Applicant further explained how the adversarial approach claimed in the '808 Patent was an improvement over methods relying on conventional OCR methods:

> The plain language of claim [8] recites that the adversarial OCR module receives a search term and ***searches the image for the search term***. In marked contrast, Myers discloses the reverse approach of extracting extracted texts from an image, and the texts are then compared a library of spam-indicative terms. *See* '808 Patent

> Prosecution History, Dec. 16, 2010 Applicant Arguments/Remarks at 7 (emphasis in original).
>
> In Myers, an image is OCR processed to generate an OCR output (Myers, FIG. 2, step 210). The OCR output is then searched for spam-indicative words and phrases (Myers, FIG. 2, step 220). That is, instead of searching the image for a search term, Myers discloses extracting text from the image, and comparing the extracted text against spam-indicative words and phrases. *See* ’808 Patent Prosecution History, Dec. 16, 2010 Applicant Arguments/Remarks at 8.
>
> It is thus respectfully submitted that Myers does not teach or suggest an adversarial OCR module that searches an image for a search term. Instead, Myers discloses performing OCR to generate an output, and comparing the output against a list of known spam-indicative words. As explained in the Specification, such an approach is error prone. *See* ’808 Patent Prosecution History, Dec. 16, 2010 Applicant Arguments/Remarks at 9.
>
> The plain language of claim 1 recites that the candidate sequence of blocks formed from the plurality of blocks represents ***a candidate match for a search term***. It is respectfully submitted that Metois does not teach or suggest forming candidate sequence of blocks representing a candidate match for a search term. In Metois, a fingerprint is generated for a blob, and the fingerprint is then compared to other blob fingerprints. That is, Metois discloses comparison of an image to another image. Metois does not pertain to forming candidate sequence of blocks that represent a candidate match for a search term. *See* ’808 Patent Prosecution History, Dec. 16, 2010 Applicant Arguments/Remarks at 9-10 (emphasis in original).
>
> It is to be noted that claim 1 recites “determining if the search term is present in the candidate sequence of blocks,” which poses the question of whether a search term is present in the candidate sequence of blocks. This adversarial approach starts with the search term, and determines whether the search term is present in the candidate sequence of blocks. It is respectfully submitted that none of the references of record pertain to an adversarial approach. *See* ’808 Patent Prosecution History, Dec. 16, 2010 Applicant Arguments/Remarks at 11.

52. The ’808 Patent’s claimed solution provides benefits not only in the context of antispam, but provides a more robust solution to detecting text in images in general, allowing for search terms to be identified in images containing anti-OCR features, even if not deliberate such as in the case of a low-quality scanned document. *Id*. at 7:3-9.

53. The ’808 Patent is thus directed to a specific solution to a problem necessarily rooted in computer technology, specifically the identification of a search term in an image that may contain anti-OCR features that conventional OCR systems were unable to address. The ’808 Patent’s solution improves OCR technology, making it more robust and more accurate at detecting search terms within low-quality images, images with blurry backgrounds or messy handwriting, or images containing other anti-OCR features.

DEFENDANTS’ INFRINGING PRODUCTS AND ACTIVITIES

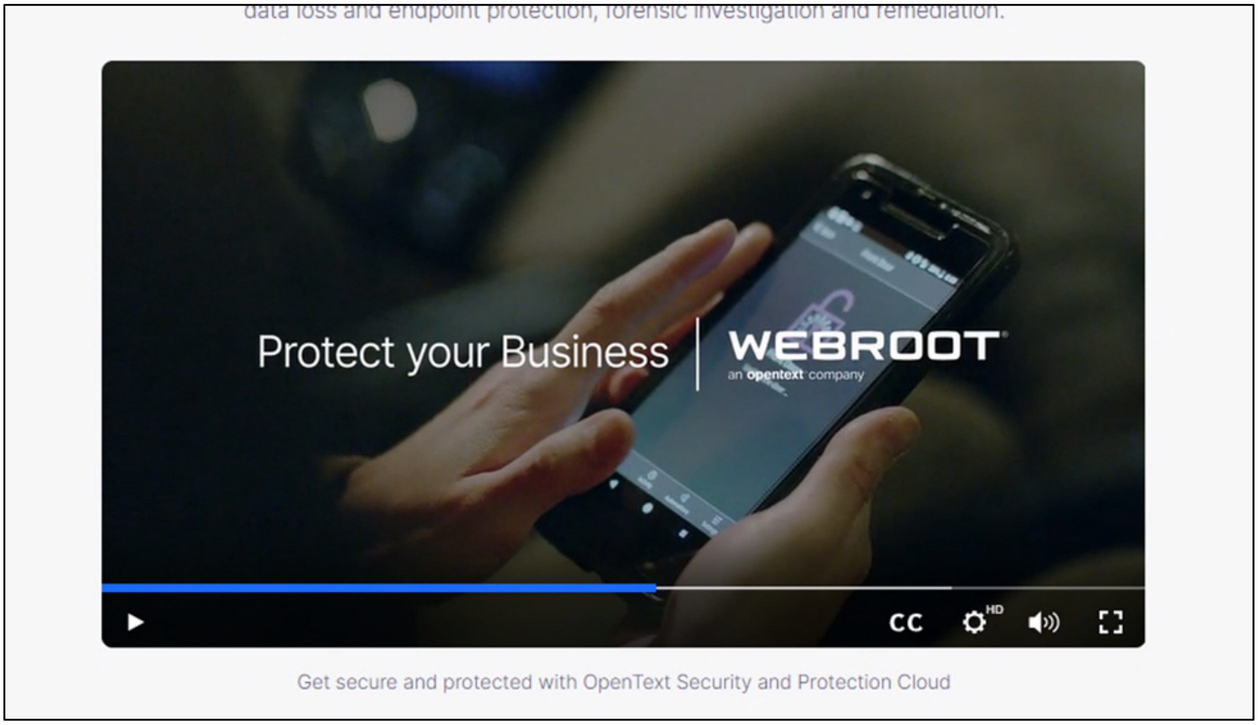
Accused Products for the ’548 Patent and ’094 Patent

54. Defendants offer several products that operate to provide various aspects of malware and malicious file/URL detection using machine learning. Open Text offers and sells (i) security products that implement Trend Micro’s patented technologies, such as, but not limited to, Open Text Security Solutions, Open Text Security & Protection Cloud and Open Text EnCase; and (ii) information and content management products that implement Trend Micro’s patented technologies, such as, but not limited to, Open Text Enterprise & Content Management, Open Text Business Network, Open Text AI & Analytics, Open Text Experience, Open Text Experience Cloud, Open Text Digital Process Automation, Open Text Discovery (“Open Text Products”). Additionally, Open Text offers and sells security software, systems, and services, such as, but not limited to, Webroot SecureAnywhere Business Endpoint Protection, Webroot SecureAnywhere Endpoint

Protection, Webroot DNS Protection, Webroot Wifi Security, and BrightCloud Threat Intelligence Services ("Webroot Products"). The Open Text Products and Webroot Products are collectively referred to as "'548 Patent Accused Products" and "'094 Patent Accused Products."

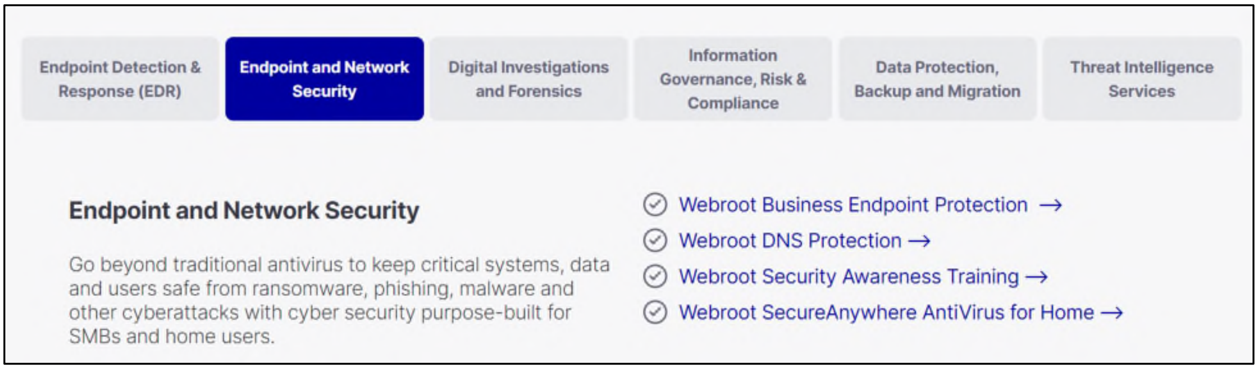
55. The fact that Open Text offers and sells Webroot Products is demonstrated by the fact that, for example, the "Contact Us" page for Webroot Products (https://www.webroot.com/us/en/about/contact-us) identifies Open Text e-mail addresses (wr-customersales@opentext.com and wr-enterprise@opentext.com) as the "SALES" contacts for purchasing the Webroot Products. The web page for BrightCloud (https://www.brightcloud.com/contact#BrightCloudForm) similarly lists an Open Text e-mail address (brightcloud-support@opentext.com) as the "Support" contact for BrightCloud products. Also, Open Text has represented that "Webroot currently has no employees or offices in the United States at all—its former employees have all been converted to OTI employees." *Open Text. Inc. et al. v. Trend Micro, Inc.*, Case No. 6:22-cv-239-ADA-DTG, Docket No. 87, p.16 (W.D. Tex. Feb. 16, 2023).

56. Further, on information and belief, OpenText packages Webroot Products with its security products. For example, OpenText Security & Protection Cloud lists Webroot Products as products with which it integrates.


data loss and endpoint protection, forensic investigation and remediation.

Get secure and protected with OpenText Security and Protection Cloud

https://www.opentext.com/products-and-solutions/products/opentext-cloud/opentext-security-cloud (The following screenshot is taken from a marketing video on the OpenText Security & Protection Cloud product webpage on Open Text's website and shows that Webroot's software, systems, and services are part of OpenText's Security & Protection Cloud)


Endpoint Detection & Response (EDR) | Endpoint and Network Security | Digital Investigations and Forensics | Information Governance, Risk & Compliance | Data Protection, Backup and Migration | Threat Intelligence Services

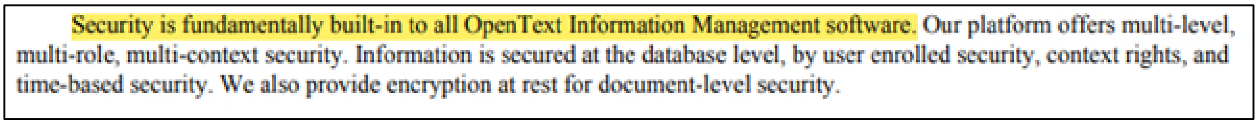
Endpoint and Network Security

Go beyond traditional antivirus to keep critical systems, data and users safe from ransomware, phishing, malware and other cyberattacks with cyber security purpose-built for SMBs and home users.

- ✓ Webroot Business Endpoint Protection →
- ✓ Webroot DNS Protection →
- ✓ Webroot Security Awareness Training →
- ✓ Webroot SecureAnywhere AntiVirus for Home →

https://www.opentext.com/products-and-solutions/products/opentext-cloud/opentext-security-cloud (This screenshot further shows that the Endpoint and Network Security of the Open Text Security & Protection Cloud comprises Webroot Security Services and Products).

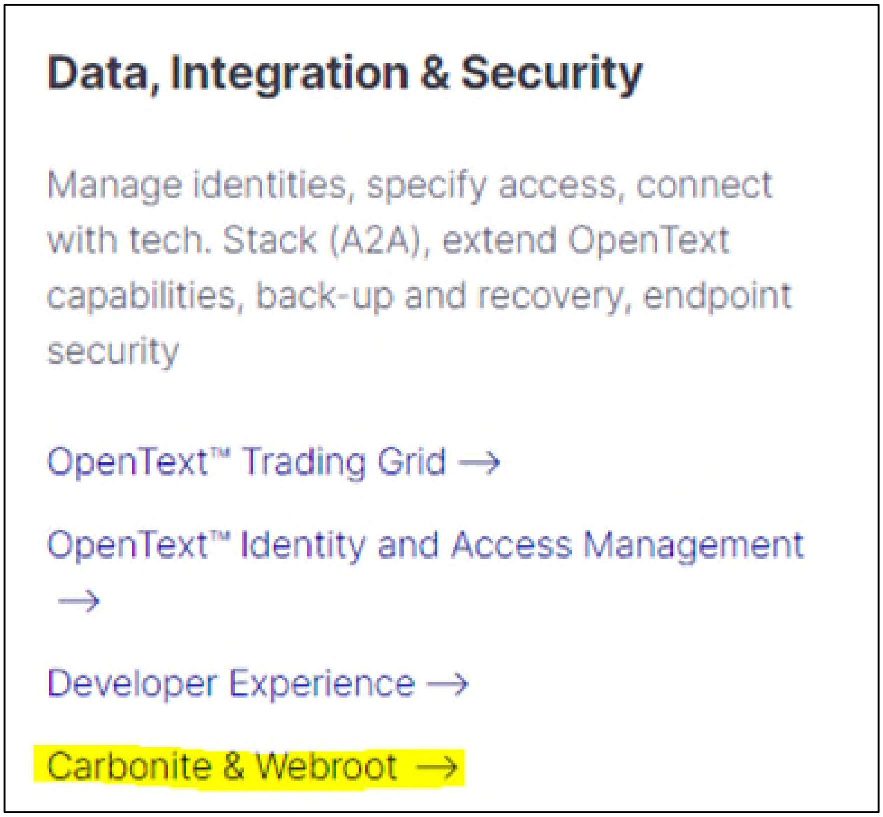
57. On information and belief, Open Text's security products, including, but not limited to, Open Text EnCase and Open Text Security Solutions, integrate with the rest of Open Text's product offerings, including its information and content management products. For example, Open Text states in its 2021 Annual Report that "[s]ecurity is fundamentally built-in to all Open [] Text Information Management software."



Security is fundamentally built-in to all OpenText Information Management software. Our platform offers multi-level, multi-role, multi-context security. Information is secured at the database level, by user enrolled security, context rights, and time-based security. We also provide encryption at rest for document-level security.

https://s23.q4cdn.com/197378439/files/doc_financials/2021/ar/OpenText-2021-Annual-Report.pdf at 8.

58. On information and belief, this "security" as referenced in Open Text's 2021 Annual Report also includes Webroot Products. For example, Open Text uses Webroot Products to provide security for its Open Text Experience Cloud.



Data, Integration & Security

Manage identities, specify access, connect with tech. Stack (A2A), extend OpenText capabilities, back-up and recovery, endpoint security

OpenText™ Trading Grid →

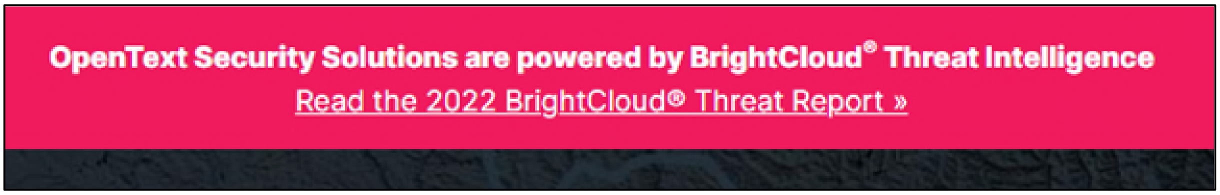
OpenText™ Identity and Access Management →

Developer Experience →

Carbonite & Webroot →

https://www.opentext.com/products-and-solutions/products/digital-experience.

59. Furthermore, Open Text's security products, such as Open Text Security Solutions, are powered by BrightCloud Threat Intelligence, one of the Webroot Products.



OpenText Security Solutions are powered by BrightCloud® Threat Intelligence

Read the 2022 BrightCloud® Threat Report »

https://www.brightcloud.com.

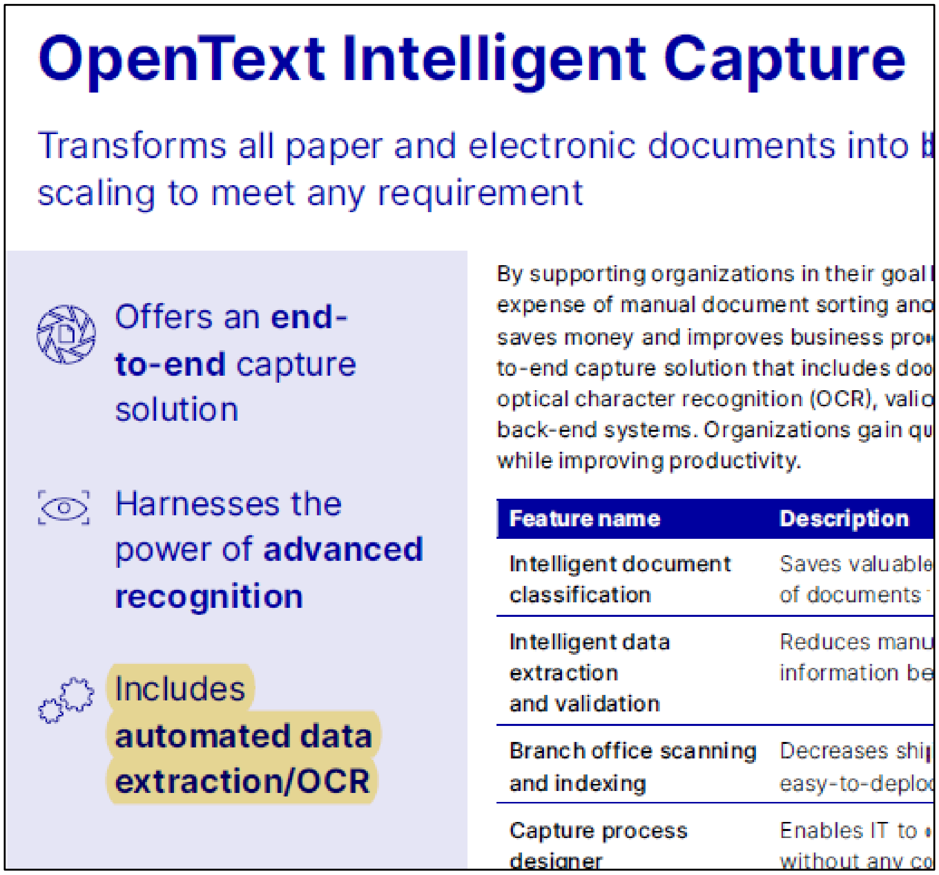
60. On information and belief, Open Text's security products are integrated with Webroot Products and Open Text's information and content management products are integrated with both Open Text's security products and Webroot Products.

61. Defendants, directly or through intermediaries, including its subsidiaries, make, use, sell, offer to sell within the United States and/or import into the United States and this District the ’548 Patent and ’094 Patent Accused Products.

Accused Products for the ’808 Patent

62. Defendants offer several products that operate to provide various aspects of document and character recognition by capturing the data stored in scanned images and faxes and interprets it using Optical Character Recognition methods (“OCR”). Open Text offers several products that implement Trend Micro’s patented technologies, such as, but not limited to, Open Text Intelligent Capture (previously Open Text Captiva), Open Text Capture Center, and Open Text Business Center Capture, Open Text Capture Full Page Reader and Open Text Capture Document Reader (collectively, the “’808 Patent Accused Products”).

63. Open Text Intelligent Capture is an end-to-end capture solution that includes document classification, data extraction/optical character recognition (OCR), validation and delivery to Open Text’s back-end systems. It utilizes both traditional techniques and “advanced recognition technology for automated classification and data extraction/OCR.” *See* https://www.opentext.com/file_source/OpenText/en_US/PDF/opentext-ds-opentext-intelligent-capture-en.pdf.



OpenText Intelligent Capture

Transforms all paper and electronic documents into b
scaling to meet any requirement

Offers an end-to-end capture solution

Harnesses the power of advanced recognition

Includes automated data extraction/OCR

By supporting organizations in their goal
expense of manual document sorting and
saves money and improves business pro
to-end capture solution that includes doc
optical character recognition (OCR), valid
back-end systems. Organizations gain qu
while improving productivity.

Feature name	Description
Intelligent document classification	Saves valuable of documents
Intelligent data extraction and validation	Reduces manu information be
Branch office scanning and indexing	Decreases shi easy-to-deplo
Capture process designer	Enables IT to without any co

https://www.opentext.com/file_source/OpenText/en_US/PDF/opentext-ds-opentext-intelligent-capture-en.pdf.

64. Open Text Capture Center is also a capture solution that automatically captures and interprets paper documents, scanned images, email, and faxes using sophisticated document and character recognition software. It captures and extracts business data from the "digital image using Optical Character Recognition (OCR), Intelligent Character Recognition (ICR), and Intelligent Document Recognition (IDR)." *See* https://www.opentext.com/products-and-solutions/products/enterprise-content-management/capture/opentext-capture-center.

65. Open Text Business Center Capture is "an OCR technology that automatically extracts and validates data from incoming documents." *See* https://www.revasolutions.com/sales-order-automation-with-opentext-bcc-and-sap/.

66. Open Text Capture Full Page Reader incorporates Open Text Capture Recognition Engine to recognize the different elements of a scanned image of a document. The product breaks down the text before applying optical character recognition. It utilizes advanced image processing and multi-engine voting techniques. *See* https://www.opentext.com/file_source/OpenText/en_US/PDF/opentext-so-capture-full-page-reader-en.pdf.

67. Open Text Capture Document Reader is a document analysis tool that offers auto-classification and metadata extraction, utilizing rule-based and self-learning technology. The product structures scanned images as documents and utilizes three recognition modules to locate and extract data. *See* https://www.opentext.com/file_source/OpenText/en_US/PDF/opentext-document-reader-product-overview.pdf.

68. Defendants, directly or through intermediaries, including its subsidiaries, make, use, sell, offer to sell within the United States and/or import into the United States and this District the '808 Patent Accused Products.

COUNT I
(Infringement of the '548 Patent pursuant to 35 U.S.C. § 271)

69. Trend Micro repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs.

70. Defendants have infringed and continues to infringe one or more claims of the '548 Patent, literally and/or under the doctrine of equivalents, in violation of 35 U.S.C.

§ 271(a) at least by, without authority, making, using, offering to sell, and/or selling the ’548 Patent Accused Products in this judicial District and elsewhere in the United States and will continue to do so unless enjoined by this Court.

71. The ’548 Patent Accused Products, when used for their ordinary and customary purposes, practice each element of at least Claim 1 of the ’548 Patent as demonstrated below.

72. For example, Claim 1 of the ’548 Patent recites:

> 1. A method of training a malware classifier, said method comprising:
>
> determining a classification label that represents a type of malware, said type of malware not including benign software;
>
> determining a classification label that represents a second type of malware;
>
> creating a feature definition file that includes first features relevant to the classification of said type of malware and that includes second features relevant to the classification of said second type of malware, wherein said first and second features are combined into one feature set in said feature definition file, wherein said features include characteristics of said type of malware, DLL names and function names executed by said type of malware, and alphanumeric strings used by said type of malware;
>
> selecting software training data including software of the same type as said type of malware and software that is benign;
>
> executing a training application on a computer associated with said malware classifier and inputting said feature definition file and said software training data into said training application; and
>
> outputting a training model associated with said malware classifier on said computer, whereby said training

model is arranged to assist in the identification of said type of malware and said second type of malware.

73. To the extent the preamble is construed to be limiting, Defendants perform *a method of training a malware classifier, said method comprising*. For example, BrightCloud Threat Intelligence Services, run by Open Text, classifies malware. using machine learning. *See* Exhibit D ("The Webroot Approach to Machine Learning Whitepaper") at 2, 3, 4.

74. Defendants perform the step of *determining a classification label that represents a type of malware, said type of malware not including benign software.* BrightCloud Threat Intelligence's algorithm classifies malware into different groups. *Id.* at 2 ("Webroot utilizes over 500 classifiers operating in parallel across URLs, IP's, files, multiple languages, etc…"). BrightCloud Threat Intelligence, which includes BrightCloud IP Reputation Service and BrightCloud File Reputation Service, detects various types of malware and determines a classification label that represents each different type, where the different types of malware are not benign software. *Id.* at 3;

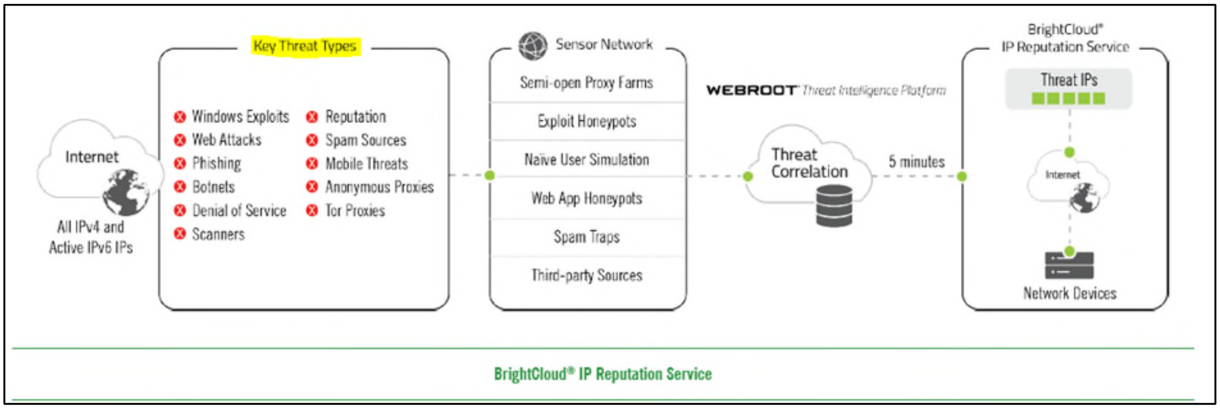


Exhibit E ("BrightCloud IP Reputation Service Datasheet") at 2;

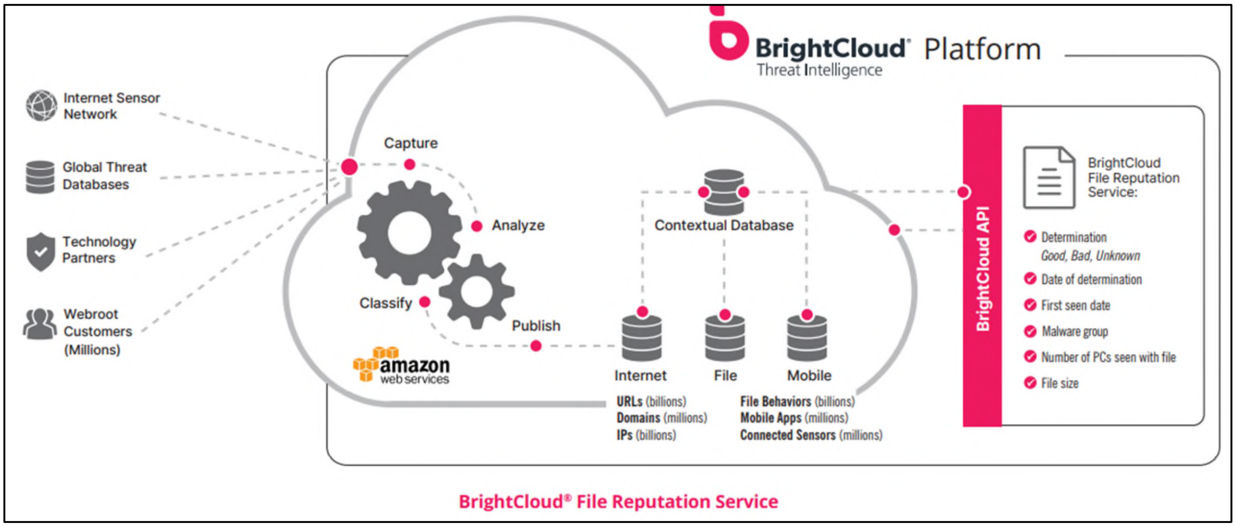


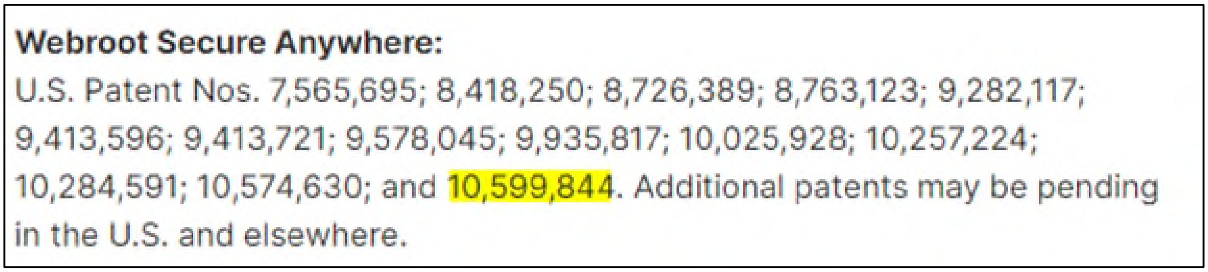
Exhibit F ("BrightCloud File Reputation Service Datasheet") at 2.

75. Defendants perform the step of *determining a classification label that represents a second type of malware*. As explained above, BrightCloud Threat Intelligence determines classification labels for at least two types of malware. Exhibit D at 2 ("Webroot utilizes over 500 classifiers operating in parallel across URLs, IP's, files, multiple languages, etc…"); Exhibit E at 2.

76. Defendants performs the step of *creating a feature definition file that includes first features relevant to the classification of said type of malware and that includes second features relevant to the classification of said second type of malware, wherein said first and second features are combined into one feature set in said feature definition file*. BrightCloud Threat Intelligence captures up to 10 million features in order to classify different types of malware, including features relevant to a first type of malware and features relevant to a second type of malware. Exhibit D at 2 ("For some of Webroot's machine learning applications, we have the ability to capture up to 10 million characteristics pertaining to a single object, and our machine learning automates the research and classification of millions of objects daily."), 4 ("The large number of

characteristics we collect, in conjunction with the large scale of our models, ensures that any information pertaining to malware on any of our endpoints, in any location of the world will be incorporated into our training models.”). The large number of features is stored in memory, and on information and belief, the features are combined into a feature definition file. See id. at 3-4.

77. Defendants perform the step of *wherein said features include characteristics of said type of malware, DLL names and function names executed by said type of malware, and alphanumeric strings used by said type of malware.* The 10 million features extracted by BrightCloud Threat Intelligence Service comprise characteristics of the type of malware, DLL names and function names executed by the type of malware, and alphanumeric strings used by the type of malware. *See id.* at 2 (“For some of Webroot’s machine learning applications, we have the ability to capture up to 10 million characteristics pertaining to a single object, and our machine learning automates the research and classification of millions of objects daily.”), 4 (“The large number of characteristics we collect, in conjunction with the large scale of our models, ensures that any information pertaining to malware on any of our endpoints, in any location of the world will be incorporated into our training models.”). Additionally, Open Text represents on its website that its products, including Webroot Endpoint Protection (SecureAnywhere), which integrates with BrightCloud Threat Intelligence, practice U.S. Patent No. 10,599,844 (the “’844 Patent”).



Webroot Secure Anywhere:
U.S. Patent Nos. 7,565,695; 8,418,250; 8,726,389; 8,763,123; 9,282,117; 9,413,596; 9,413,721; 9,578,045; 9,935,817; 10,025,928; 10,257,224; 10,284,591; 10,574,630; and 10,599,844. Additional patents may be pending in the U.S. and elsewhere.

https://www.opentext.com/about/copyright-information/opentext-patent-information

The '844 Patent discloses collecting a variety of different features to detect malware using a machine learning model, including characteristics of said type of malware, DLL names and function names executed by said type of malware, and alphanumeric strings used by said type of malware. *See* '844 Patent at 5:62-6:22.

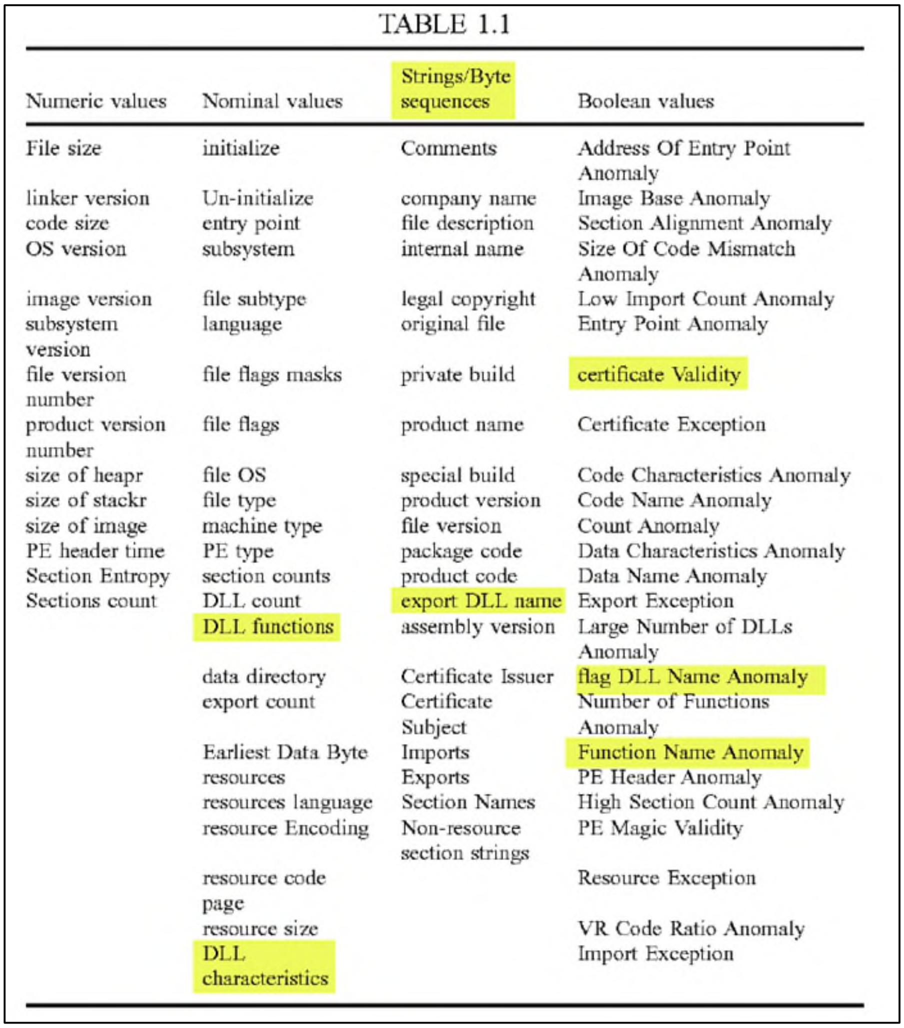
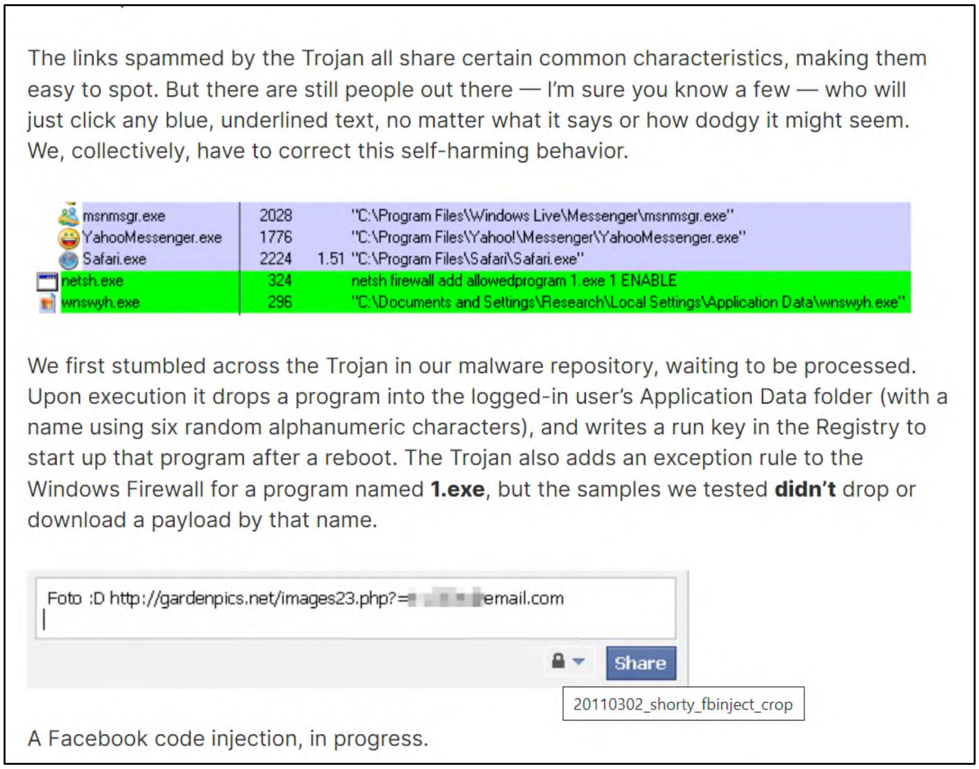


TABLE 1.1

Numeric values	Nominal values	Strings/Byte sequences	Boolean values
File size	initialize	Comments	Address Of Entry Point Anomaly
linker version	Un-initialize	company name	Image Base Anomaly
code size	entry point	file description	Section Alignment Anomaly
OS version	subsystem	internal name	Size Of Code Mismatch Anomaly
image version	file subtype	legal copyright	Low Import Count Anomaly
subsystem version	language	original file	Entry Point Anomaly
file version number	file flags masks	private build	certificate Validity
product version number	file flags	product name	Certificate Exception
size of heapr	file OS	special build	Code Characteristics Anomaly
size of stackr	file type	product version	Code Name Anomaly
size of image	machine type	file version	Count Anomaly
PE header time	PE type	package code	Data Characteristics Anomaly
Section Entropy	section counts	product code	Data Name Anomaly
Sections count	DLL count	export DLL name	Export Exception
	DLL functions	assembly version	Large Number of DLLs Anomaly
	data directory	Certificate Issuer	flag DLL Name Anomaly
	export count	Certificate Subject	Number of Functions Anomaly
	Earliest Data Byte	Imports	Function Name Anomaly
	resources	Exports	PE Header Anomaly
	resources language	Section Names	High Section Count Anomaly
	resource Encoding	Non-resource section strings	PE Magic Validity
	resource code page		Resource Exception
	resource size		VR Code Ratio Anomaly
	DLL characteristics		Import Exception

’844 Patent at 6:23-58. For example, one such feature is “certificate Validity,” and the ’844 Patent explains that “[c]ommercial software files tend to have a valid certificate, whereas malware in general do not have valid certificates.” ’844 Patent at 9:12-13. As another example, the BrightCloud Domain Reputation Service of BrightCloud Threat Intelligence references alphanumeric string such as a name using six random alphanumeric characters in detecting Trojan horse as publicized at its website.



The links spammed by the Trojan all share certain common characteristics, making them easy to spot. But there are still people out there — I’m sure you know a few — who will just click any blue, underlined text, no matter what it says or how dodgy it might seem. We, collectively, have to correct this self-harming behavior.

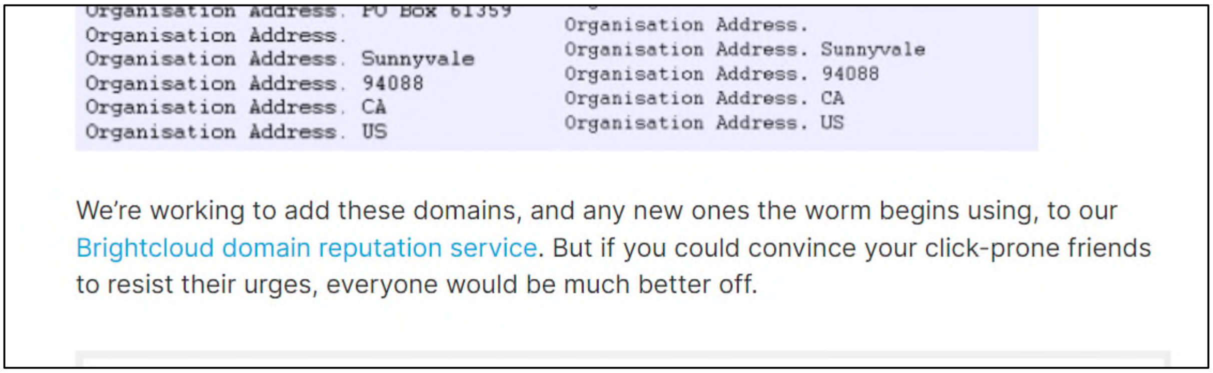
```
msnmsgr.exe           2028        "C:\Program Files\Windows Live\Messenger\msnmsgr.exe"
YahooMessenger.exe    1776        "C:\Program Files\Yahoo!\Messenger\YahooMessenger.exe"
Safari.exe            2224   1.51 "C:\Program Files\Safari\Safari.exe"
netsh.exe              324        netsh firewall add allowedprogram 1.exe 1 ENABLE
wnswyh.exe             296        "C:\Documents and Settings\Research\Local Settings\Application Data\wnswyh.exe"
```

We first stumbled across the Trojan in our malware repository, waiting to be processed. Upon execution it drops a program into the logged-in user’s Application Data folder (with a name using six random alphanumeric characters), and writes a run key in the Registry to start up that program after a reboot. The Trojan also adds an exception rule to the Windows Firewall for a program named **1.exe**, but the samples we tested **didn’t** drop or download a payload by that name.

Foto :D http://gardenpics.net/images23.php?=[redacted]email.com

A Facebook code injection, in progress.

https://www.webroot.com/blog/2011/03/04/shorty-worm-spams-links-hijacks-browsers/



```
Organisation Address. PO Box 61359        Organisation Address.
Organisation Address.                     Organisation Address. Sunnyvale
Organisation Address. Sunnyvale           Organisation Address. 94088
Organisation Address. 94088               Organisation Address. CA
Organisation Address. CA                  Organisation Address. US
Organisation Address. US
```

We’re working to add these domains, and any new ones the worm begins using, to our Brightcloud domain reputation service. But if you could convince your click-prone friends to resist their urges, everyone would be much better off.

https://www.webroot.com/blog/2011/03/04/shorty-worm-spams-links-hijacks-browsers/

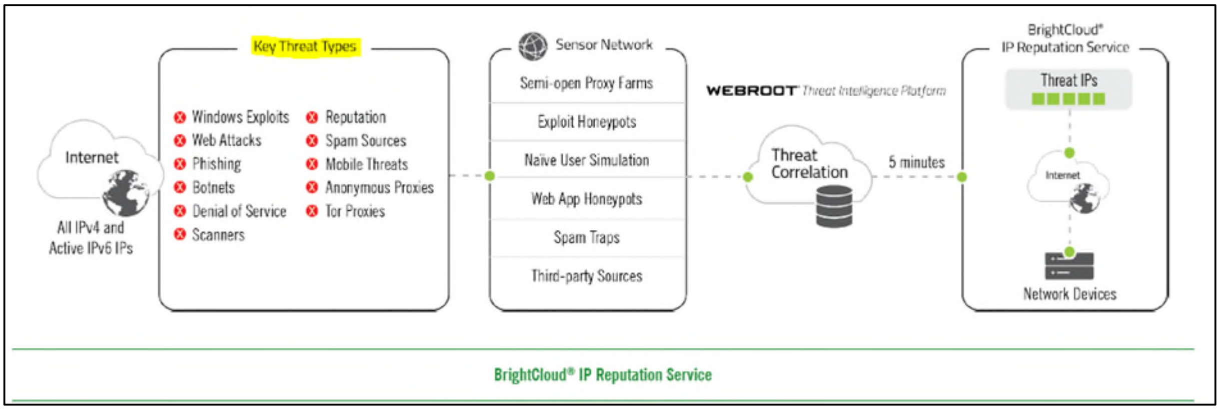
78. Defendants perform the step of *selecting software training data including software of the same type as said type of malware and software that is benign*. BrightCloud Threat Intelligence selects software training data including each type of malware as well as software that is benign. Exhibit D at 3 ("While training the model, the machine learning selects and fine tunes the model parameters (i.e. its weights) thus determining the mapping from input vector to determination (in the simplest instance of benign or malicious file). . . . At a minimum, training and refining our models typically relies on millions of data points (a data point is a specific instance of an internet object). . . . Currently, training a Webroot model utilizes approximately 10 million data points (10 million instances of input vectors) to determine 400 million model parameters.").

79. Defendants perform the step of *executing a training application on a computer associated with said malware classifier and inputting said feature definition file and said software training data into said training application*. For example, Webroot Endpoint Protection (SecureAnywhere) inputs a feature definition file and 10 million training samples into a training application on a computer associated with the malware classifier.

> "Currently, training a Webroot model utilizes approximately 10 million data points (10 million instances of input vectors) to determine 400 million model parameters. For efficiency and speed, the model parameters are kept in memory while training the model. To accomplish this, we leverage Amazon Web Services and the San Diego Supercomputer Center at the University of California, San Diego in La Jolla, CA. Our smaller training models use specially designed computer systems with 400–500 GB of RAM using multicore machines (around 20 nodes) for parallelization. Our larger training models will typically leverage instances with up to one terabyte of RAM and 64 nodes."

Id. at 4.

80. Defendants perform the step of *outputting a training model associated with said malware classifier on said computer, whereby said training model is arranged to assist in the identification of said type of malware and said second type of malware*. As explained above, BrightCloud Threat Intelligence trains a machine learning model to output a training model that classifies at least two or more types of malware. *See id.* at 4 ("Webroot acquires new information, runs a training model, and publishes new models every day that incorporate this new knowledge. We improve and publish models daily, repeating the process for files, URLs, IPs, phishing sites, mobile apps, etc.");



see also Exhibit E at 2.

81. Defendants have had actual knowledge of the '548 Patent since at least September 16, 2022, when Trend Micro filed a complaint asserting this patent against Defendants in the Eastern District of Virginia.

82. To the extent the marking requirement applies with respect to the '548 Patent, Trend Micro has a practice of marking at least its product manuals with the patents that the product practices.

83. Defendants and their partners, customers, and end users of the ’548 Patent Accused Products and corresponding systems and services, directly infringe at least Claim 1 of the ‘548 Patent, literally or under the doctrine of equivalents, at least by using the ’548 Patent Accused Products in the manner described above. On information and belief, the infringing actions of Defendants’ partners, customers, and end users of the ’548 Patent Accused Products are attributable to Defendants. For example, Defendants direct and control their partners by contractual agreement to operate, or to provide Defendants with the means to operate (e.g., servers), or otherwise distribute the ’548 Patent Accused Products in a manner that infringes the ’548 Patent. Defendants further condition receipt of benefit of the ’548 Patent Accused Products upon use of the patented features, such as performing steps of the methods claimed in the ’548 Patent.

84. In addition to Defendants’ direct infringement, Defendants have infringed and continue to infringe the ‘548 Patent indirectly, including by actively inducing others to directly infringe at least Claim 1 of the ’548 Patent in violation of 35 U.S.C. § 271(b). For example, Defendants knowingly, or with willful blindness, encourage and induce customers to use the ’548 Patent Accused Products in a manner that infringes at least Claim 1 of the ‘548 Patent by offering and providing software that performs a method that infringes Claim 1 when installed and operated by Defendants’ customers, and by activities related to selling, marketing, advertising, promotion, installation, support, and distribution of the ’548 Patent Accused Products.

85. Defendants encourage and induce third parties to use the ’548 Patent Accused Products in a manner that infringes the ’548 Patent as described above, including through advertising, marketing, customer support, user manuals, instructions, installation,

and distribution of the ’548 Patent Accused Products in the United States. For example, Defendants’ customers and end users test and/or operate BrightCloud Threat Intelligence in the United States in accordance with Defendants’ instructions contained in, for example, its user manuals, thereby also performing the claimed methods and infringing the asserted claims of the ’548 Patent reciting such operation. *See* Exhibit D; Exhibit E; Exhibit F; Exhibit G (“BrightCloud Threat Intelligence App for Splunk User Guide v1.5”).

86. Moreover, Defendants have infringed and continue to infringe the ‘548 Patent indirectly, including by contributing to direct infringement of at least Claim 1 of the ’548 Patent in violation of 35 U.S.C. § 271(c). Defendants contribute to infringement of the ’548 Patent by, among other activities, offering for sale, selling within the United States, and/or importing into the United States the ’548 Patent Accused Products with knowledge that such activities practice every element of one or more claims of the ’548 Patent, or being willfully blind to such activities practicing every element of one or more claims of the ’548 Patent. Defendants’ affirmative acts of offering for sale, selling, and/or importing into the United States the ’548 Patent Accused Products contribute to Defendants’ customers and end-users infringing of one or more claims of the ’548 Patent. The infringing software components of the ’548 Patent Accused Products are specially designed in a way that infringes one or more claims of the ’548 Patent and can be used only in a manner that infringes the ’548 Patent and thus have no substantial non-infringing uses.

87. The above description regarding Defendants’ infringement of the ’548 Patent is based on publicly available information and a reasonable investigation of the operation of the ’548 Patent Accused Products. Trend Micro reserves the right to modify

this description, including, for example, on the basis of information about the ’548 Patent Accused Products that it obtains during discovery.

88. Unless and until enjoined by this Court, Defendants will continue to infringe the ’548 Patent. Defendants’ infringement is causing and will continue to cause Trend Micro irreparable harm, for which there is no remedy at law.

89. Under 35 U.S.C. § 283, Trend Micro is entitled to a preliminary and permanent injunction against further infringement of the ’548 Patent.

90. Defendants’ infringement of the ’548 Patent has been knowing and willful since at least September 16, 2022.

91. Trend Micro has suffered and continues to suffer damages, including lost profits, as a result of Defendants’ infringement of the ‘548 Patent. Under 35 U.S.C. § 284, Trend Micro is entitled to damages adequate to compensate it for Defendants’ infringement, in no event less than a reasonable royalty for Defendants’ use of the inventions of the ’548 Patent, together with interest and costs as fixed by the Court.

COUNT II
(Infringement of the ’094 Patent pursuant to 35 U.S.C. § 271)

92. Trend Micro repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs.

93. Defendants have infringed and continue to infringe one or more claims of the ’094 Patent, literally and/or under the doctrine of equivalents, in violation of 35 U.S.C. § 271(a) at least by, without authority, making, using, offering to sell, and/or selling the Accused Products in this judicial District and elsewhere in the United States and will continue to do so unless enjoined by this Court.

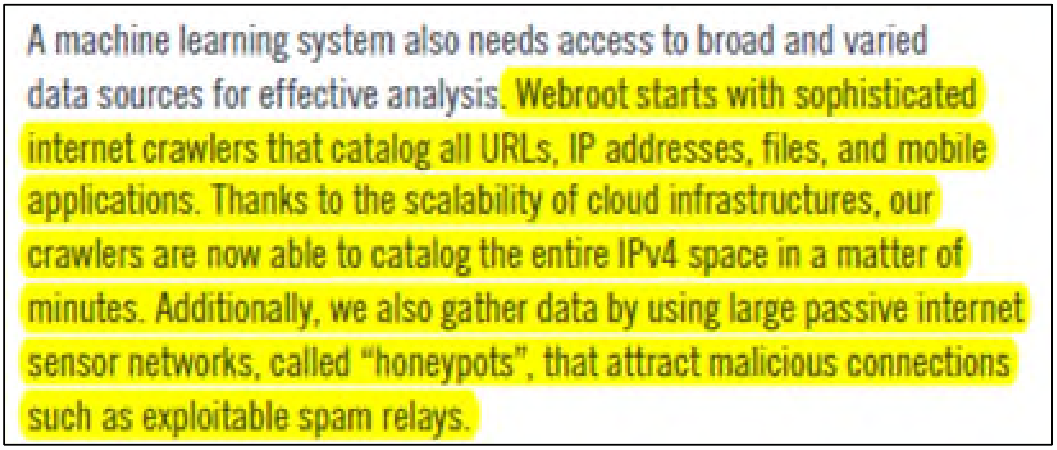
94. The’094 Patent Accused Products, when used for their ordinary and customary purposes, practice each element of at least Claim 1 of the ’094 Patent as demonstrated below.

95. For example, Claim 1 of the ’094 Patent recites:

> 1. A method of detecting a malicious URL, said method comprising:
>
> retrieving HTML code representing a Web page;
>
> scanning said HTML code and identifying at least one embedded URL of said HTML code;
>
> identifying layout features of said embedded URL related to the layout of said embedded URL within said HTML code, one of said layout features indicating that said embedded URL is located within the header or the footer of said HTML code;
>
> producing a numerical layout vector that indicates the presence of said layout features;
>
> processing said numerical layout vector using a classifier algorithm; and
>
> outputting a score from said classifier algorithm indicating the likelihood that said embedded URL of said HTML code is a malicious URL.

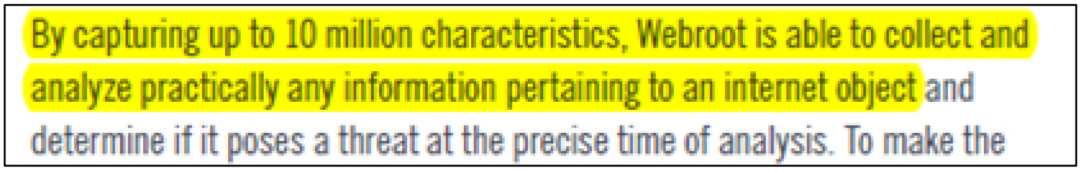
96. To the extent the preamble is construed to be limiting, Defendants perform *a method of detecting a malicious URL, said method comprising*. For example, the ’094 Patent Accused Products incorporate BrightCloud Threat Intelligence, which provides a method of detecting malicious URLs. *See* Exhibit D at 2 (“Webroot utilizes over 500 classifiers operating in parallel across URLs,…to recognize patterns, determine reputations and accurately categorize internet objects.”).

97. Defendants perform the step of *retrieving HTML code representing a Web page*. For example, BrightCloud Threat Intelligence utilizes internet crawlers that retrieves the HTML code representing a webpage associated with a URL.



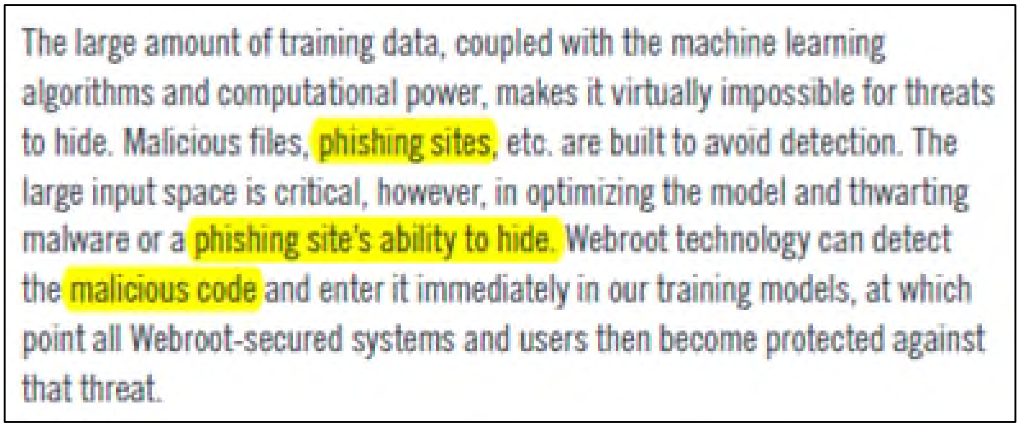
A machine learning system also needs access to broad and varied data sources for effective analysis. Webroot starts with sophisticated internet crawlers that catalog all URLs, IP addresses, files, and mobile applications. Thanks to the scalability of cloud infrastructures, our crawlers are now able to catalog the entire IPv4 space in a matter of minutes. Additionally, we also gather data by using large passive internet sensor networks, called "honeypots", that attract malicious connections such as exploitable spam relays.

Id. at 2 (highlight added);



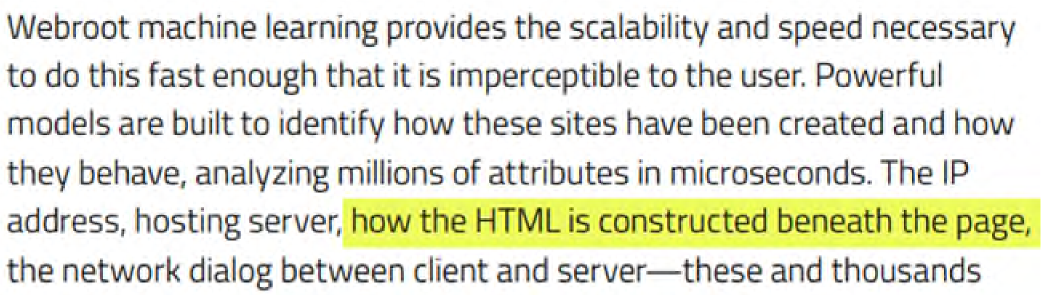
By capturing up to 10 million characteristics, Webroot is able to collect and analyze practically any information pertaining to an internet object and determine if it poses a threat at the precise time of analysis. To make the

id. (highlight added);



The large amount of training data, coupled with the machine learning algorithms and computational power, makes it virtually impossible for threats to hide. Malicious files, phishing sites, etc. are built to avoid detection. The large input space is critical, however, in optimizing the model and thwarting malware or a phishing site's ability to hide. Webroot technology can detect the malicious code and enter it immediately in our training models, at which point all Webroot-secured systems and users then become protected against that threat.

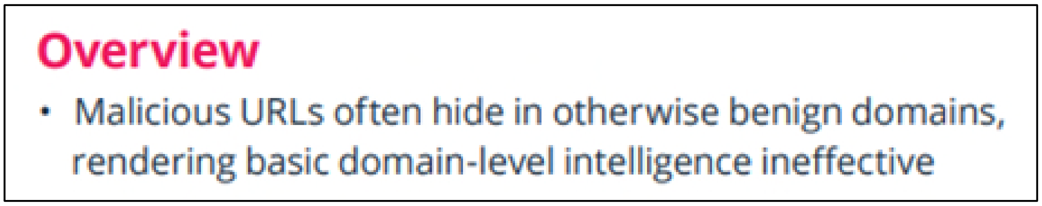
id. at 4 (highlight added);



Webroot machine learning provides the scalability and speed necessary to do this fast enough that it is imperceptible to the user. Powerful models are built to identify how these sites have been created and how they behave, analyzing millions of attributes in microseconds. The IP address, hosting server, how the HTML is constructed beneath the page, the network dialog between client and server—these and thousands

Exhibit H ("How to Harness Machine Learning – Tap into the Webroot DNA for Security at Scale") at 9 (highlighted added).

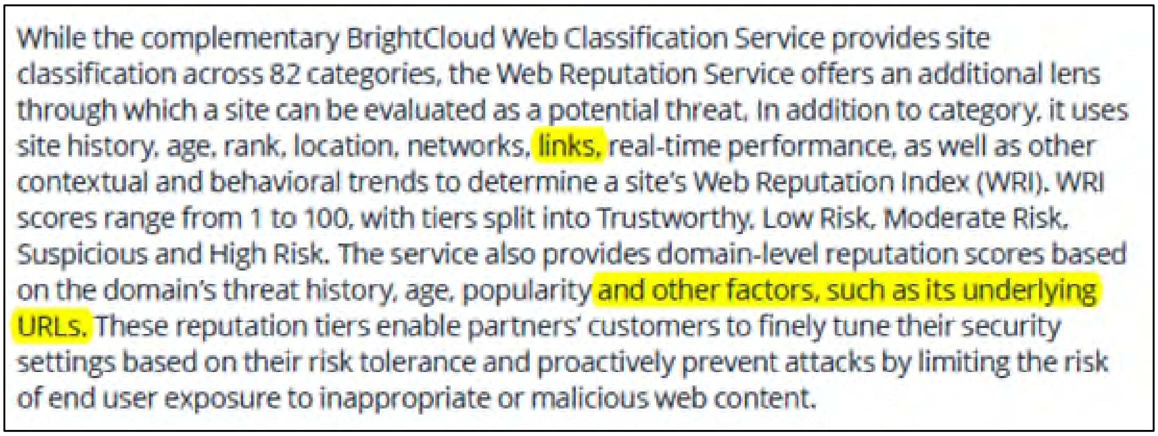
98. Defendants perform the step of *scanning said HTML code and identifying at least one embedded URL of said HTML code*. For example, BrightCloud Threat Intelligence dynamically crawls uncategorized sites, which includes scanning the HTML code and identifying embedded URLs. *See* Exhibit D at 2 ("Whenever a user visits an uncategorized site, it is dynamically crawled and scored.");



Overview

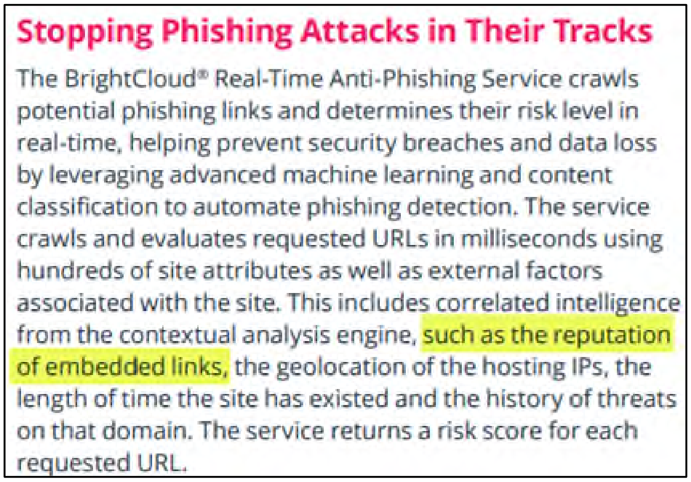
- Malicious URLs often hide in otherwise benign domains, rendering basic domain-level intelligence ineffective

Exhibit I ("BrightCloud Web Classification and Reputation Services") at 1;



While the complementary BrightCloud Web Classification Service provides site classification across 82 categories, the Web Reputation Service offers an additional lens through which a site can be evaluated as a potential threat. In addition to category, it uses site history, age, rank, location, networks, links, real-time performance, as well as other contextual and behavioral trends to determine a site's Web Reputation Index (WRI). WRI scores range from 1 to 100, with tiers split into Trustworthy, Low Risk, Moderate Risk, Suspicious and High Risk. The service also provides domain-level reputation scores based on the domain's threat history, age, popularity and other factors, such as its underlying URLs. These reputation tiers enable partners' customers to finely tune their security settings based on their risk tolerance and proactively prevent attacks by limiting the risk of end user exposure to inappropriate or malicious web content.

id. at 2;

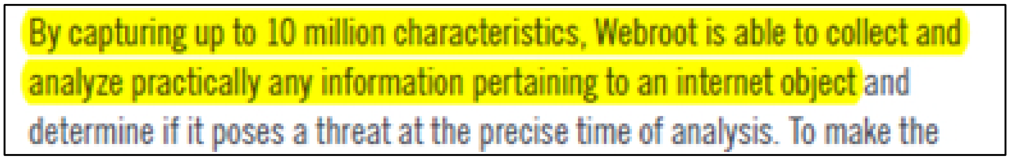


Stopping Phishing Attacks in Their Tracks

The BrightCloud® Real-Time Anti-Phishing Service crawls potential phishing links and determines their risk level in real-time, helping prevent security breaches and data loss by leveraging advanced machine learning and content classification to automate phishing detection. The service crawls and evaluates requested URLs in milliseconds using hundreds of site attributes as well as external factors associated with the site. This includes correlated intelligence from the contextual analysis engine, such as the reputation of embedded links, the geolocation of the hosting IPs, the length of time the site has existed and the history of threats on that domain. The service returns a risk score for each requested URL.

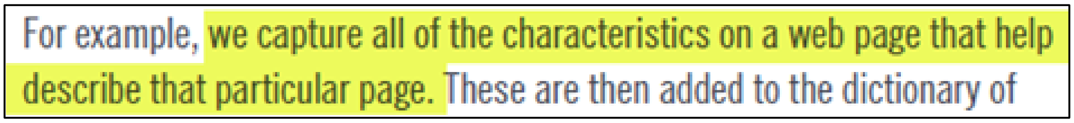
Exhibit J ("BrightCloud Real-Time Anti-Phishing Service") at 1.

99. Defendants perform the step of *identifying layout features of said embedded URL related to the layout of said embedded URL within said HTML code, one of said layout features indicating that said embedded URL is located within the header or the footer of said HTML code*. For example, BrightCloud Threat Intelligence identifies 10 million characteristics of a webpage associated with a URL, including the webpage's layout features.



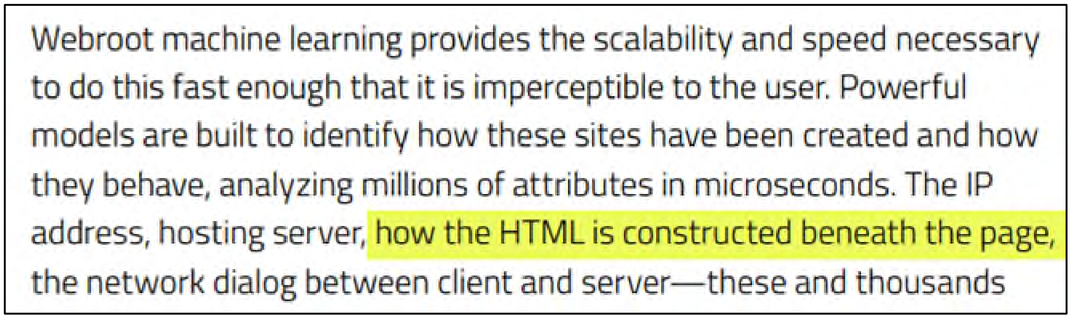
By capturing up to 10 million characteristics, Webroot is able to collect and analyze practically any information pertaining to an internet object and determine if it poses a threat at the precise time of analysis. To make the

Exhibit D at 2 (highlight added);



For example, we capture all of the characteristics on a web page that help describe that particular page. These are then added to the dictionary of

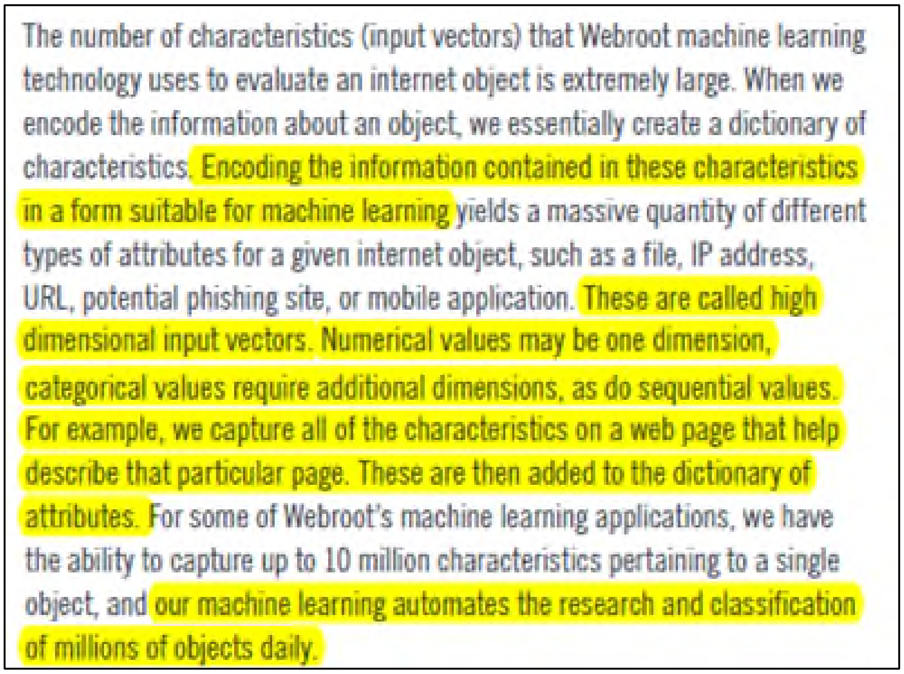
id. (highlight added);



Webroot machine learning provides the scalability and speed necessary to do this fast enough that it is imperceptible to the user. Powerful models are built to identify how these sites have been created and how they behave, analyzing millions of attributes in microseconds. The IP address, hosting server, how the HTML is constructed beneath the page, the network dialog between client and server—these and thousands

Exhibit H at 9 (highlighted added). On information and belief, the 10 million characteristics of the web page that are collected include layout features related to the layout of the embedded URL within the HTML code of the host webpage, including whether the embedded URL is located within the header or footer of the HTML code.

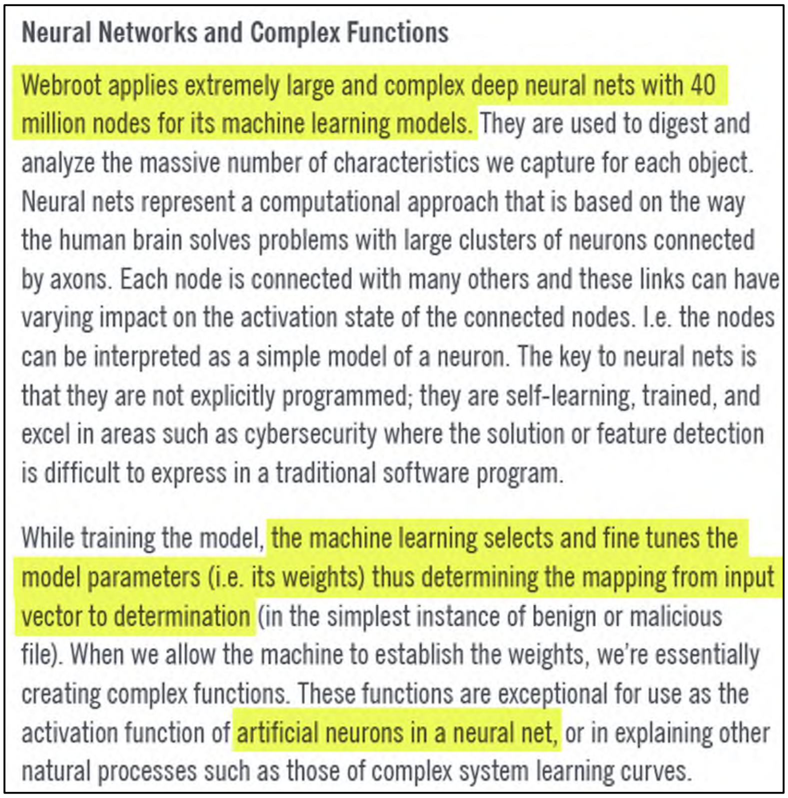
100. Defendants perform the step of *producing a numerical layout vector that indicates the presence of said layout features*. For example, BrightCloud Threat Intelligence produces numerical input vectors that indicate the characteristics that describe the web page, including the aforementioned layout features.



The number of characteristics (input vectors) that Webroot machine learning technology uses to evaluate an internet object is extremely large. When we encode the information about an object, we essentially create a dictionary of characteristics. Encoding the information contained in these characteristics in a form suitable for machine learning yields a massive quantity of different types of attributes for a given internet object, such as a file, IP address, URL, potential phishing site, or mobile application. These are called high dimensional input vectors. Numerical values may be one dimension, categorical values require additional dimensions, as do sequential values. For example, we capture all of the characteristics on a web page that help describe that particular page. These are then added to the dictionary of attributes. For some of Webroot's machine learning applications, we have the ability to capture up to 10 million characteristics pertaining to a single object, and our machine learning automates the research and classification of millions of objects daily.

Exhibit D at 2 (highlighted added).

97. Defendants perform the step of *processing said numerical layout vector using a classifier algorithm.* For example, BrightCloud Threat Intelligence processes the input vector using a classifier algorithm. *See id.* at 2. BrightCloud Threat Intelligence utilizes at least one or more of the following classifier algorithms: Bayesian classifier, Support Vector Machine, Maximum Entropy Discrimination and Artificial Neural Networks (ANNs) with Deep Learning.

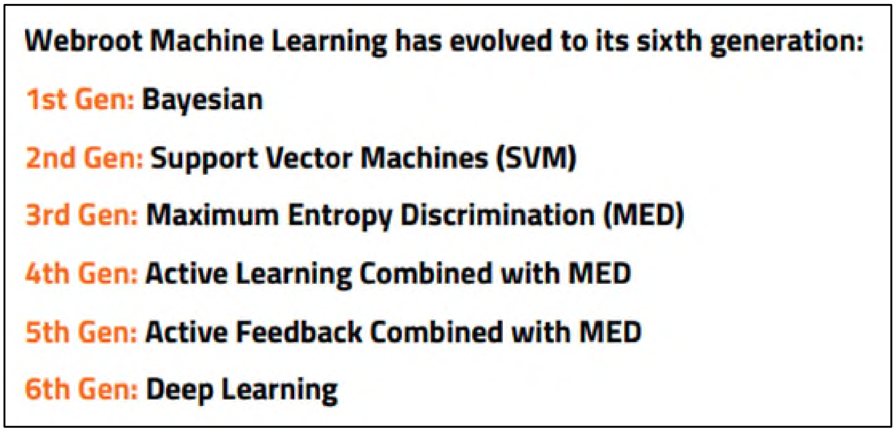


Neural Networks and Complex Functions

Webroot applies extremely large and complex deep neural nets with 40 million nodes for its machine learning models. They are used to digest and analyze the massive number of characteristics we capture for each object. Neural nets represent a computational approach that is based on the way the human brain solves problems with large clusters of neurons connected by axons. Each node is connected with many others and these links can have varying impact on the activation state of the connected nodes. I.e. the nodes can be interpreted as a simple model of a neuron. The key to neural nets is that they are not explicitly programmed; they are self-learning, trained, and excel in areas such as cybersecurity where the solution or feature detection is difficult to express in a traditional software program.

While training the model, the machine learning selects and fine tunes the model parameters (i.e. its weights) thus determining the mapping from input vector to determination (in the simplest instance of benign or malicious file). When we allow the machine to establish the weights, we're essentially creating complex functions. These functions are exceptional for use as the activation function of artificial neurons in a neural net, or in explaining other natural processes such as those of complex system learning curves.

Exhibit D at 2 (highlight added);



Webroot Machine Learning has evolved to its sixth generation:

1st Gen: Bayesian

2nd Gen: Support Vector Machines (SVM)

3rd Gen: Maximum Entropy Discrimination (MED)

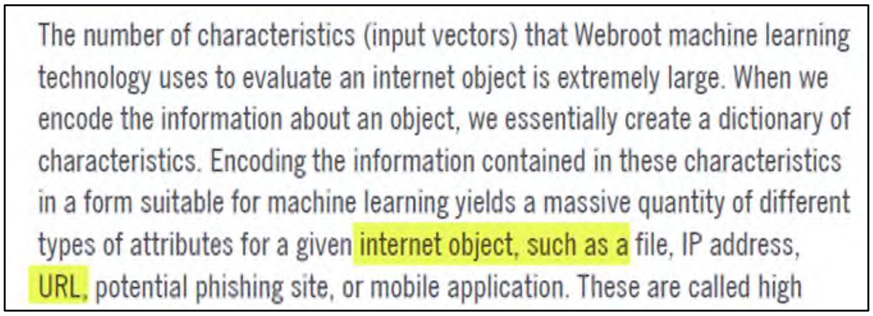
4th Gen: Active Learning Combined with MED

5th Gen: Active Feedback Combined with MED

6th Gen: Deep Learning

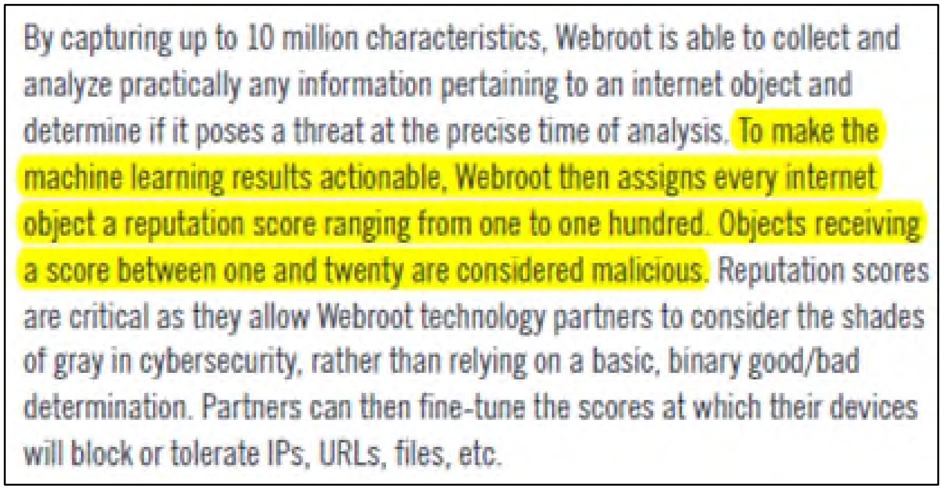
Exhibit H at 7.

101. Defendants perform the step of *outputting a score from said classifier algorithm indicating the likelihood that said embedded URL of said HTML code is a malicious URL*. For example, BrightCloud Threat Intelligence outputs a reputation score from its classifier algorithm that indicates the likelihood that an internet object such as an embedded URL is malicious.



The number of characteristics (input vectors) that Webroot machine learning technology uses to evaluate an internet object is extremely large. When we encode the information about an object, we essentially create a dictionary of characteristics. Encoding the information contained in these characteristics in a form suitable for machine learning yields a massive quantity of different types of attributes for a given internet object, such as a file, IP address, URL, potential phishing site, or mobile application. These are called high

Exhibit D at 2 (highlight added);



By capturing up to 10 million characteristics, Webroot is able to collect and analyze practically any information pertaining to an internet object and determine if it poses a threat at the precise time of analysis. To make the machine learning results actionable, Webroot then assigns every internet object a reputation score ranging from one to one hundred. Objects receiving a score between one and twenty are considered malicious. Reputation scores are critical as they allow Webroot technology partners to consider the shades of gray in cybersecurity, rather than relying on a basic, binary good/bad determination. Partners can then fine-tune the scores at which their devices will block or tolerate IPs, URLs, files, etc.

id. (highlight added).

102. Defendants have had actual knowledge of the ’094 Patent since at least September 16, 2022, when Trend Micro filed a complaint asserting this patent against Defendants in the Eastern District of Virginia.

103. To the extent the marking requirement applies with respect to the ’094 Patent, Trend Micro has a practice of marking at least its product manuals with the patents that the product practices.

104. Defendants and their partners, customers, and end users of their ’094 Patent Accused Products and corresponding systems and services, directly infringe at least Claim 1 of the ‘094 Patent, literally or under the doctrine of equivalents, at least by using the ’094 Patent Accused Products as described above. On information and belief, the infringing actions of Defendants’ partners, customers, and end users of the ’094 Patent Accused Products are attributable to Defendants. For example, Defendants direct and control their partners by contractual agreement to operate, or to provide Defendants with the means to operate (e.g., servers), or otherwise distribute the ’094 Patent Accused Products in a manner that infringes the ’094 Patent. Defendants further condition receipt of benefit of

the ’094 Patent Accused Products upon use of the patented features, such as performing steps of the methods claimed in the ’094 Patent.

105. In addition to Defendants’ direct infringement, Defendants have infringed and continue to infringe the ‘094 Patent indirectly, including by actively inducing others to directly infringe at least Claim 1 of the ’094 Patent in violation of 35 U.S.C. § 271(b). For example, Defendants knowingly, or with willful blindness, encourage and induce customers to use the ’094 Patent Accused Products in a manner that infringes at least Claim 1 of the ‘094 Patent by offering and providing software that performs a method that infringes Claim 1 when installed and operated by the customers, and by activities related to selling, marketing, advertising, promotion, installation, support, and distribution of the ’094 Patent Accused Products.

106. Defendants encourage and induce third parties to use the ’094 Patent Accused Products in a manner that infringes the ’094 Patent as described above, including through advertising, marketing, customer support, user manuals, instructions, installation, and distribution of the ’094 Patent Accused Products in the United States. For example, Defendants’ customers and end users test and/or operate BrightCloud Threat Intelligence in the United States in accordance with Defendants’ instructions contained in, for example, its user manuals, thereby also performing the claimed methods and infringing the asserted claims of the ’094 Patent reciting such operation. *See* Exhibit D; Exhibit E; Exhibit F; Exhibit G.

107. Moreover, Defendants have infringed and continue to infringe the ‘094 Patent indirectly, including by contributing to direct infringement of at least Claim 1 of the ’094 Patent in violation of 35 U.S.C. § 271(c). Defendants contribute to infringement of

the ’094 Patent by, among other activities, offering for sale, selling within the United States, and/or importing into the United States the ’094 Patent Accused Products with knowledge that such activities practice every element of one or more claims of the ’094 Patent, or being willfully blind to such activities practicing every element of one or more claims of the ’094 Patent. Defendants’ affirmative acts of offering for sale, selling, and/or importing into the United States the ’094 Patent Accused Products contribute to Defendants’ customers and end-users infringing of one or more claims of the ’094 Patent. The infringing software components of the ’094 Patent Accused Products are specially designed in a way that infringes one or more claims of the ’094 Patent and can be used only in a manner that infringes the ’094 Patent and thus have no substantial non-infringing uses.

108. The above description regarding Defendants’ infringement of the ’094 Patent is based on publicly available information and a reasonable investigation of the operation of the ’094 Patent Accused Products. Trend Micro reserves the right to modify this description, including, for example, on the basis of information about the ’094 Patent Accused Products that it obtains during discovery.

109. Unless and until enjoined by this Court, Defendants will continue to infringe the ’094 Patent. Defendants’ infringement is causing and will continue to cause Trend Micro irreparable harm, for which there is no remedy at law.

110. Under 35 U.S.C. § 283, Trend Micro is entitled to a preliminary and permanent injunction against further infringement of the ’094 Patent.

111. Defendants’ infringement of the ’094 Patent has been knowing and willful since at least September 16, 2022.

112. Trend Micro has suffered and continues to suffer damages, including lost profits, as a result of Defendants' infringement of the '094 Patent. Under 35 U.S.C. § 284, Trend Micro is entitled to damages adequate to compensate it for Defendants' infringement, in no event less than a reasonable royalty for Defendants' use of the inventions of the ’094 Patent, together with interest and costs as fixed by the Court.

COUNT III
(Infringement of the ’808 Patent pursuant to 35 U.S.C. § 271)

113. Trend Micro repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs.

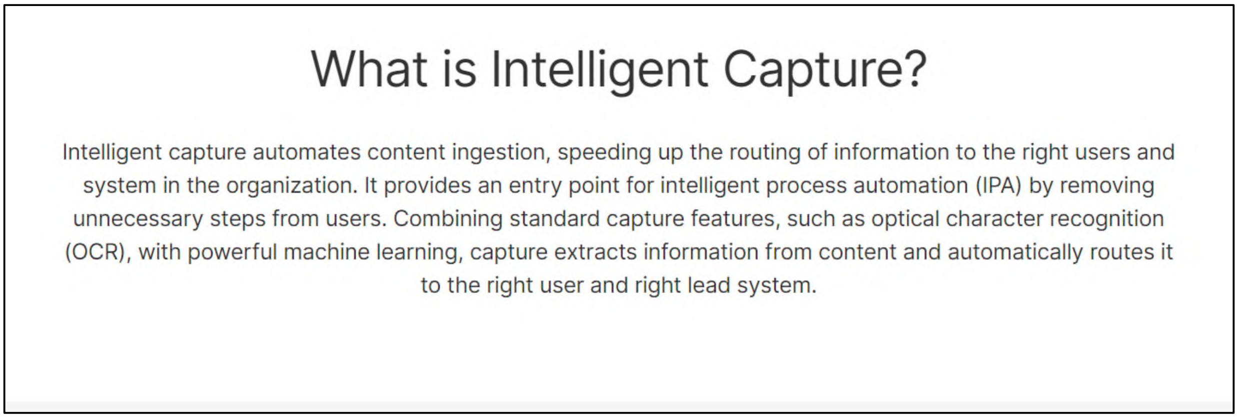
114. Open Text has infringed and continues to infringe one or more claims of the ’808 Patent, literally and/or under the doctrine of equivalents, in violation of 35 U.S.C. § 271(a) at least by, without authority, making, using, offering to sell, and/or selling the ’808 Patent Accused Products in this judicial District and elsewhere in the United States and will continue to do so unless enjoined by this Court. The ’808 Patent Accused Products, when used for their ordinary and customary purposes, practice each element of at least Claim 1 of the ’808 Patent as demonstrated below.

115. For example, Claim 1 of the ’808 Patent recites:

> 1. A computer-implemented method of identifying text content in images, the method comprising:
>
> receiving an input image;
>
> splitting the image into a plurality of character blocks, each character block in the plurality of character blocks containing pixel information that may represent one or more characters;
>
> calculating a probability that a character block in the plurality of character blocks includes a character;

> forming a candidate sequence of character blocks from the plurality of character blocks, the candidate sequence of character blocks representing a candidate match for a search term; and
>
> comparing the candidate sequence of character blocks to the search term to determine if the search term is present in the candidate sequence of character blocks.

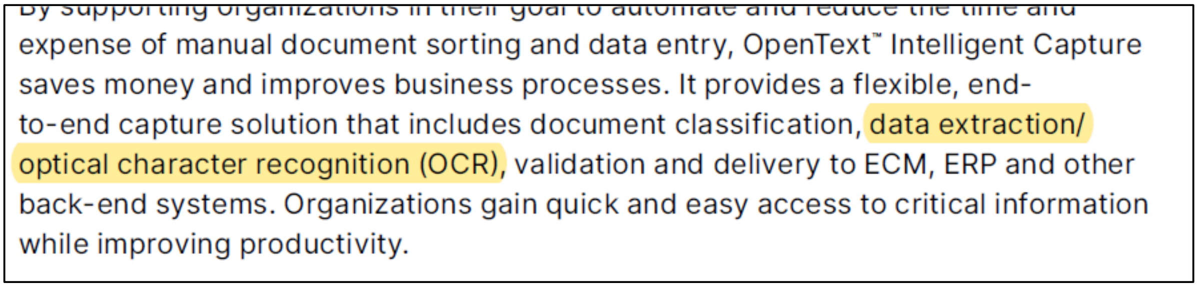
116. To the extent the preamble is limiting, Open Text performs *a method of identifying text content in images, the method comprising*. For example, Open Text Intelligent Capture extracts data, such as keywords from scanned documents. *See* Exhibit K (Open Text Intelligent Capture Datasheet) at 1.



What is Intelligent Capture?

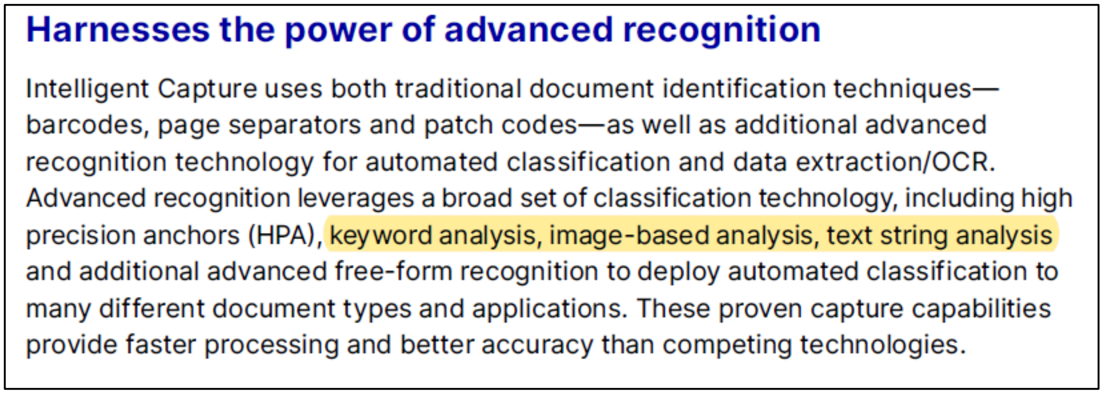
Intelligent capture automates content ingestion, speeding up the routing of information to the right users and system in the organization. It provides an entry point for intelligent process automation (IPA) by removing unnecessary steps from users. Combining standard capture features, such as optical character recognition (OCR), with powerful machine learning, capture extracts information from content and automatically routes it to the right user and right lead system.

https://www.opentext.com/products-and-solutions/products/enterprise-content-management/intelligent-capture



By supporting organizations in their goal to automate and reduce the time and expense of manual document sorting and data entry, OpenText™ Intelligent Capture saves money and improves business processes. It provides a flexible, end-to-end capture solution that includes document classification, data extraction/ optical character recognition (OCR), validation and delivery to ECM, ERP and other back-end systems. Organizations gain quick and easy access to critical information while improving productivity.

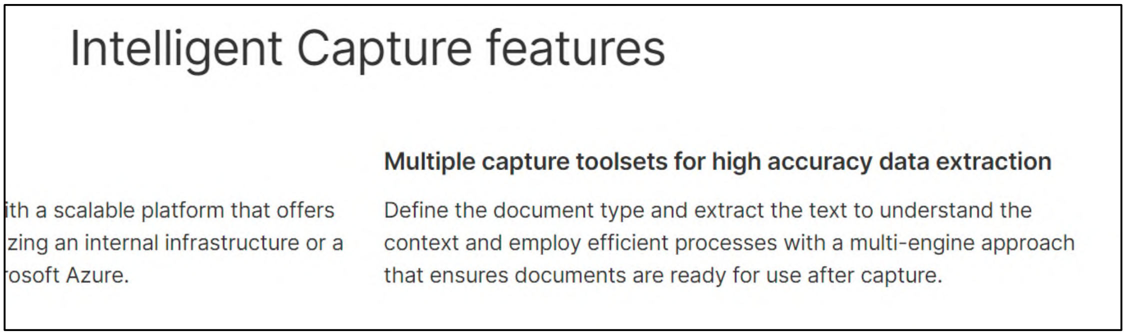
Exhibit K at 1;



Harnesses the power of advanced recognition

Intelligent Capture uses both traditional document identification techniques—barcodes, page separators and patch codes—as well as additional advanced recognition technology for automated classification and data extraction/OCR. Advanced recognition leverages a broad set of classification technology, including high precision anchors (HPA), keyword analysis, image-based analysis, text string analysis and additional advanced free-form recognition to deploy automated classification to many different document types and applications. These proven capture capabilities provide faster processing and better accuracy than competing technologies.

id. at 2;



Intelligent Capture features

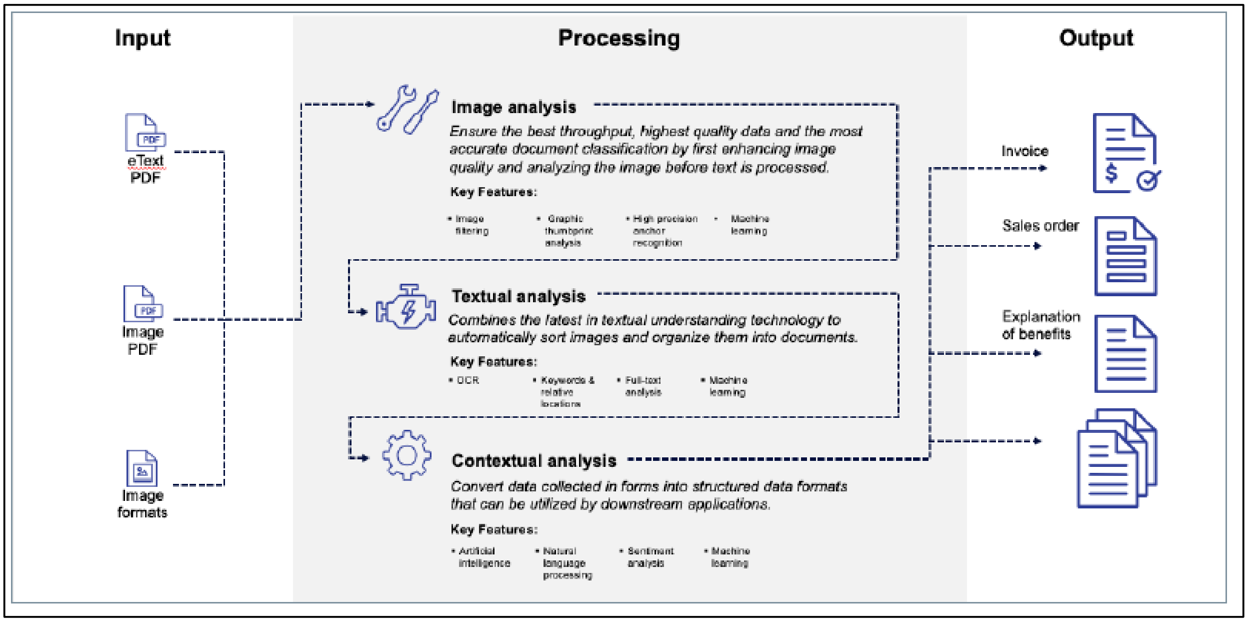
ith a scalable platform that offers zing an internal infrastructure or a osoft Azure.

Multiple capture toolsets for high accuracy data extraction

Define the document type and extract the text to understand the context and employ efficient processes with a multi-engine approach that ensures documents are ready for use after capture.

https://www.opentext.com/products-and-solutions/products/enterprise-content-management/intelligent-capture.

117. Defendants perform a method that includes *receiving an input image*. For example, as explained above, Open Text Intelligent Capture takes static document images, such as scanned documents as inputs.



Processing

Image analysis

Ensure the best throughput, highest quality data and the most accurate document classification by first enhancing image quality and analyzing the image before text is processed.

Key Features:

- Image filtering
- Graphic thumbprint analysis
- High precision anchor recognition
- Machine learning

Textual analysis

Combines the latest in textual understanding technology to automatically sort images and organize them into documents.

Key Features:

- OCR
- Keywords & relative locations
- Full-text analysis
- Machine learning

Contextual analysis

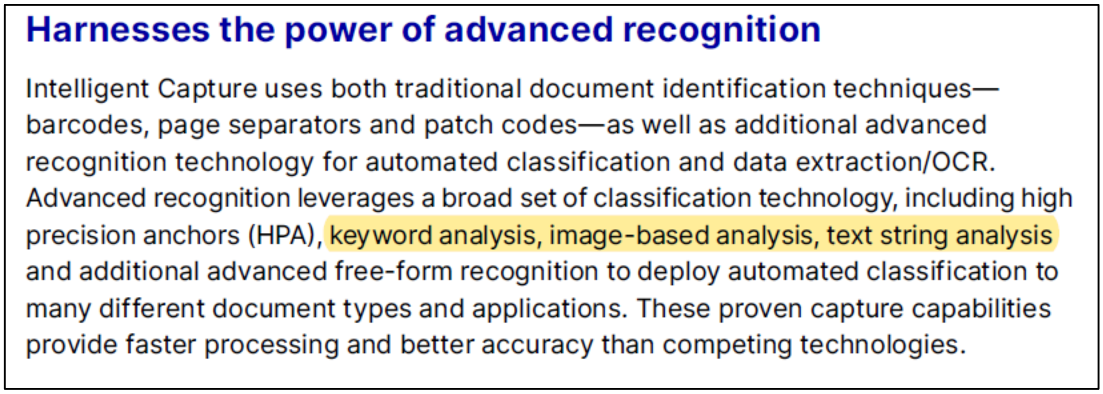
Convert data collected in forms into structured data formats that can be utilized by downstream applications.

Key Features:

- Artificial intelligence
- Natural language processing
- Sentiment analysis
- Machine learning

Exhibit K at 3.

118. Defendants perform a method that includes *splitting the image into a plurality of character blocks, each character block in the plurality of character blocks containing pixel information that may represent one or more characters*. For example, Open Text Intelligent Capture's advanced recognition technology includes keyword analysis, which extracts keywords from static document images, as well as image-based analysis and text string analysis. On information and belief, these processes split the image into character blocks containing pixel information.

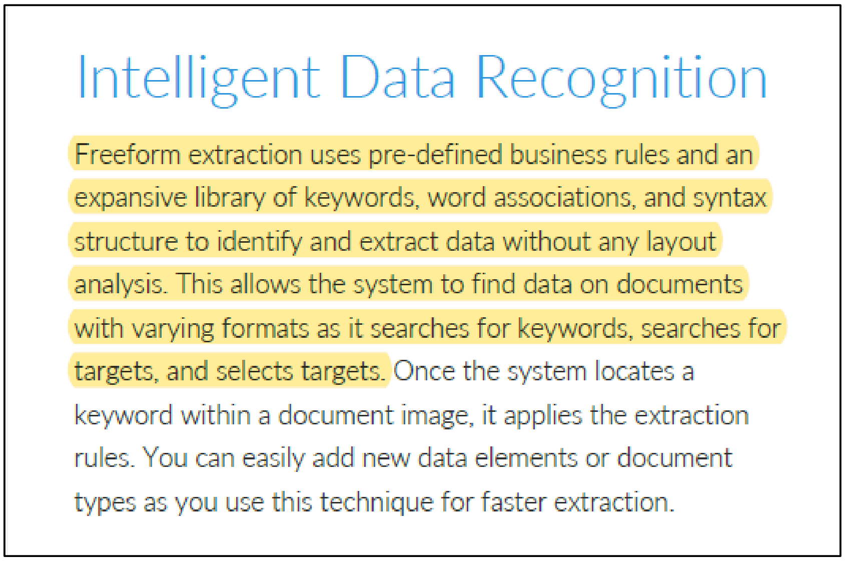


Harnesses the power of advanced recognition

Intelligent Capture uses both traditional document identification techniques—barcodes, page separators and patch codes—as well as additional advanced recognition technology for automated classification and data extraction/OCR. Advanced recognition leverages a broad set of classification technology, including high precision anchors (HPA), keyword analysis, image-based analysis, text string analysis and additional advanced free-form recognition to deploy automated classification to many different document types and applications. These proven capture capabilities provide faster processing and better accuracy than competing technologies.

Id. at 2.

119. The ’808 Accused Products perform a method that includes *calculating a probability that a character block in the plurality of character blocks includes a character*. On information and belief, Open Text Intelligent Capture calculates the probability that a character block contains a character using word associations and syntax structure. On information and belief, using word associations and syntax structure require at least some calculation of the likelihood of the selected pixel block containing a character.

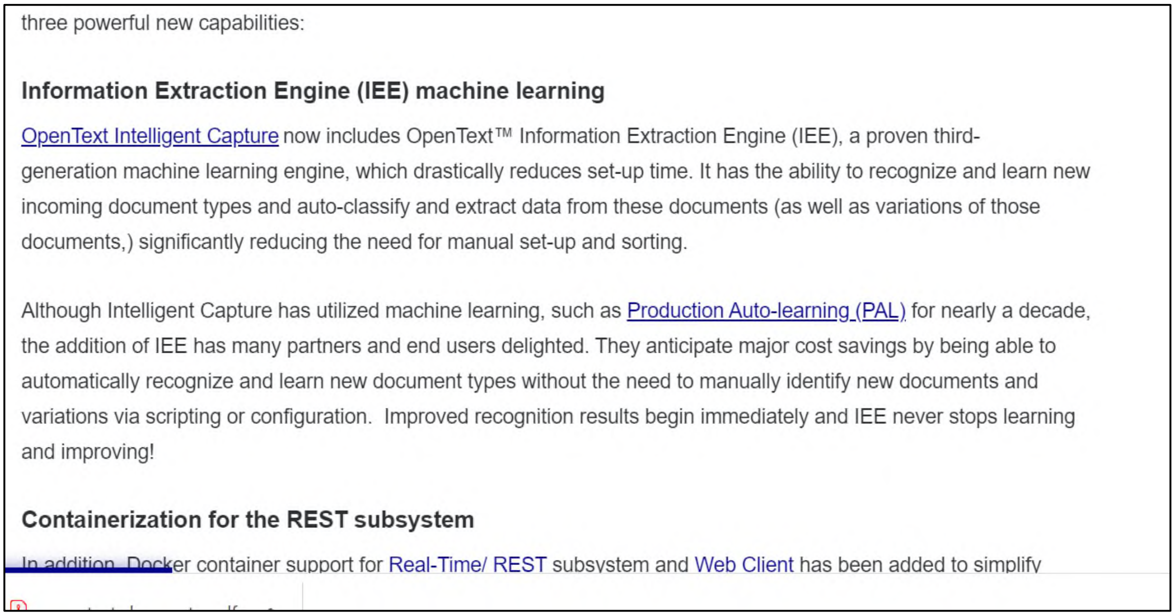


Intelligent Data Recognition

Freeform extraction uses pre-defined business rules and an expansive library of keywords, word associations, and syntax structure to identify and extract data without any layout analysis. This allows the system to find data on documents with varying formats as it searches for keywords, searches for targets, and selects targets. Once the system locates a keyword within a document image, it applies the extraction rules. You can easily add new data elements or document types as you use this technique for faster extraction.

Exhibit L (Open Text Captiva Product Guide) at 18

In addition, Open Text Intelligent Capture utilizes AI, machine learning, and natural language processing techniques to recognize a character based on a probabilistic model. Screenshots below show that Open Text Intelligent Capture incorporates machine learning.



three powerful new capabilities:

Information Extraction Engine (IEE) machine learning

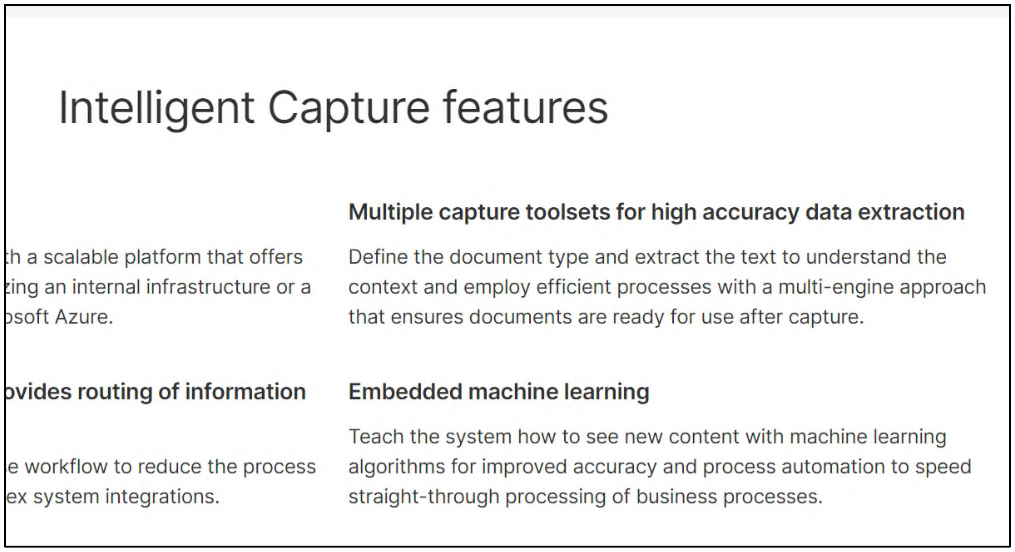
OpenText Intelligent Capture now includes OpenText™ Information Extraction Engine (IEE), a proven third-generation machine learning engine, which drastically reduces set-up time. It has the ability to recognize and learn new incoming document types and auto-classify and extract data from these documents (as well as variations of those documents,) significantly reducing the need for manual set-up and sorting.

Although Intelligent Capture has utilized machine learning, such as Production Auto-learning (PAL) for nearly a decade, the addition of IEE has many partners and end users delighted. They anticipate major cost savings by being able to automatically recognize and learn new document types without the need to manually identify new documents and variations via scripting or configuration. Improved recognition results begin immediately and IEE never stops learning and improving!

Containerization for the REST subsystem

In addition, Docker container support for Real-Time/ REST subsystem and Web Client has been added to simplify

https://blogs.opentext.com/whats-new-in-opentext-intelligent-capture-2/?_ga=2.240896704.274546278.1657137672-1283720118.1656174271



Intelligent Capture features

th a scalable platform that offers
zing an internal infrastructure or a
osoft Azure.

ovides routing of information

e workflow to reduce the process
ex system integrations.

Multiple capture toolsets for high accuracy data extraction

Define the document type and extract the text to understand the context and employ efficient processes with a multi-engine approach that ensures documents are ready for use after capture.

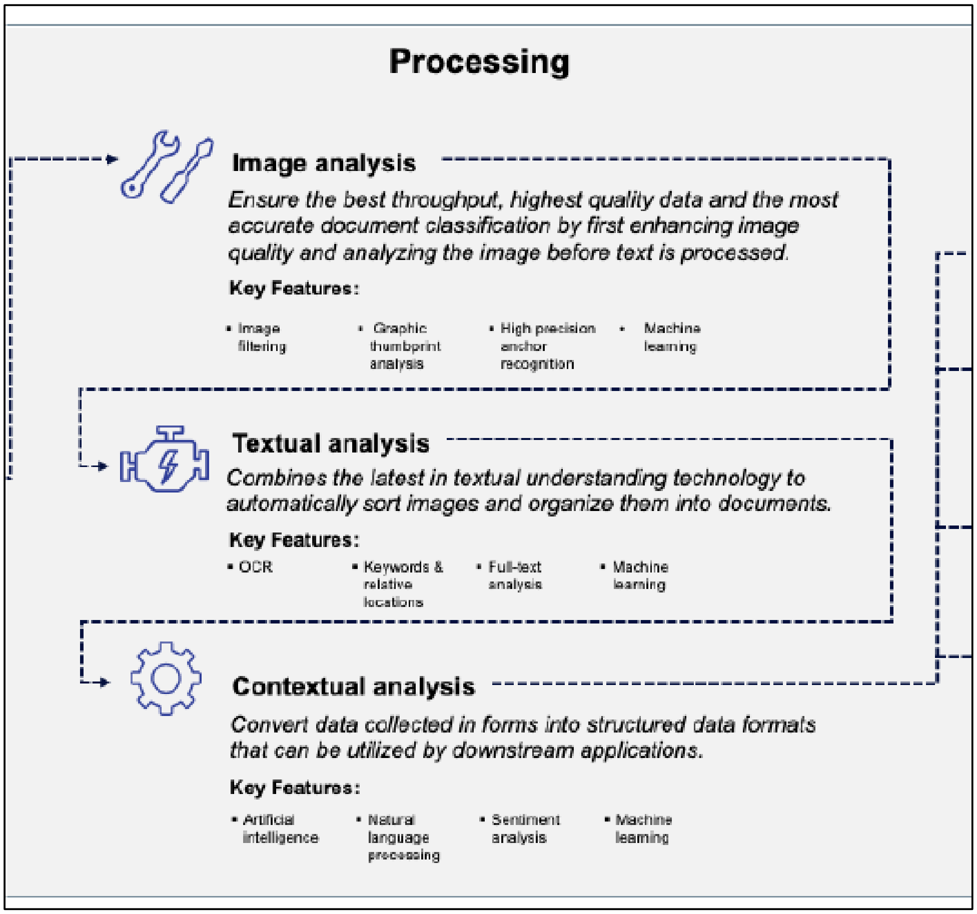
Embedded machine learning

Teach the system how to see new content with machine learning algorithms for improved accuracy and process automation to speed straight-through processing of business processes.

https://www.opentext.com/products-and-solutions/products/enterprise-content-management/intelligent-capture

120. The ’808 Accused Products perform a method that includes *forming a candidate sequence of character blocks from the plurality of character blocks, the candidate sequence of character blocks representing a candidate match for a search term.*

For example, Open Text Intelligent Capture provides three steps in processing the image input. As explained above, on information and belief, Open Text Intelligent Capture splits the image into plurality of character blocks and calculates a probability that a character block in the plurality of character blocks includes a character. On information and belief, in the textual analysis step, Open Text Intelligent Capture creates a candidate sequence of character blocks representing a candidate match for a search term. The screenshot below shows that the candidate sequence of character blocks is subsequently validated using techniques such as "Keywords & relative locations," "Full-text analysis," "Natural language processing," and "Sentiment analysis." Exhibit K at 3.



Processing

Image analysis

Ensure the best throughput, highest quality data and the most accurate document classification by first enhancing image quality and analyzing the image before text is processed.

Key Features:

- Image filtering
- Graphic thumbprint analysis
- High precision anchor recognition
- Machine learning

Textual analysis

Combines the latest in textual understanding technology to automatically sort images and organize them into documents.

Key Features:

- OCR
- Keywords & relative locations
- Full-text analysis
- Machine learning

Contextual analysis

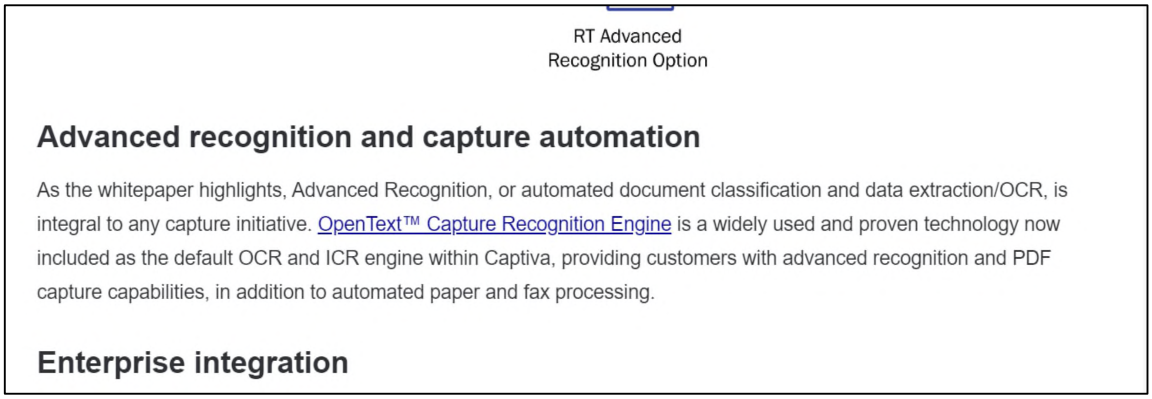
Convert data collected in forms into structured data formats that can be utilized by downstream applications.

Key Features:

- Artificial intelligence
- Natural language processing
- Sentiment analysis
- Machine learning

Id.

121. The ’808 Accused Products perform a method that includes *comparing the candidate sequence of character blocks to the search term to determine if the search term is present in the candidate sequence of character blocks*. For example, on information and belief, Open Text Intelligent Capture compares numerous candidates to the search term to select the one with the highest confidence level. *See* Exhibit M (Open Text Capture Recognition Engine Product Overview) at 2. Open Text Intelligent Capture (formerly Captiva) incorporates Open Text Capture Recognition Engine.



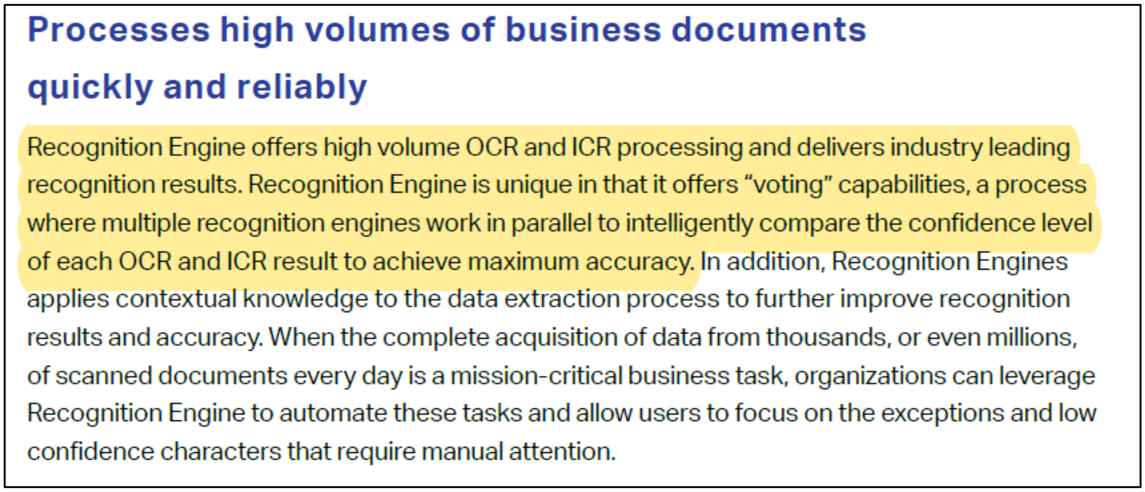
RT Advanced
Recognition Option

Advanced recognition and capture automation

As the whitepaper highlights, Advanced Recognition, or automated document classification and data extraction/OCR, is integral to any capture initiative. OpenText™ Capture Recognition Engine is a widely used and proven technology now included as the default OCR and ICR engine within Captiva, providing customers with advanced recognition and PDF capture capabilities, in addition to automated paper and fax processing.

Enterprise integration

https://blogs.opentext.com/opentext-captiva-intelligent-capture-continues-to-set-the-industry-benchmark/. Open Text Capture Recognition Engine uses a voting capability, which involves multiple Engines working simultaneous to provide multiple candidates. On information and belief, the candidates are compared to the search term and the candidate with the highest confidence level is selected.



Processes high volumes of business documents quickly and reliably

Recognition Engine offers high volume OCR and ICR processing and delivers industry leading recognition results. Recognition Engine is unique in that it offers “voting” capabilities, a process where multiple recognition engines work in parallel to intelligently compare the confidence level of each OCR and ICR result to achieve maximum accuracy. In addition, Recognition Engines applies contextual knowledge to the data extraction process to further improve recognition results and accuracy. When the complete acquisition of data from thousands, or even millions, of scanned documents every day is a mission-critical business task, organizations can leverage Recognition Engine to automate these tasks and allow users to focus on the exceptions and low confidence characters that require manual attention.

Exhibit M at 2.

122. Open Text has had actual knowledge of the ’808 Patent since at least September 16, 2022, when Trend Micro filed a complaint asserting this patent against Defendants in the Eastern District of Virginia.

123. To the extent the marking requirement applies with respect to the ’808 Patent, Trend Micro has a practice of marking at least its product manuals with the patents that the product practices.

124. Open Text and its partners, customers, and end users of its ’808 Patent Accused Products and corresponding systems and services, directly infringe at least Claim 1 of the ’808 Patent, literally or under the doctrine of equivalents, at least by using the ’808 Patent Accused Products as described above. On information and belief, the infringing actions of Open Text’s partners, customers, and end users of the ’808 Patent Accused Products are attributable to Open Text. For example, Open Text direct and control their partners by contractual agreement to operate, or to provide Open Text with the means to operate (e.g., servers), or otherwise distribute the ’808 Patent Accused Products in a manner that infringes the ’808 Patent. Open Text further conditions receipt of benefit of

the ’808 Patent Accused Products upon use of the patented features, such as performing steps of the methods claimed in the ’808 Patent.

125. In addition to Open Text’s direct infringement, Open Text has infringed and continues to infringe the ‘808 Patent indirectly, including by actively inducing others to directly infringe at least Claim 1 of the ’808 Patent in violation of 35 U.S.C. § 271(b). For example, Open Text knowingly, or with willful blindness, encourages and induces customers to use the ’808 Patent Accused Products in a manner that infringes at least Claim 1 of the ‘808 Patent by offering and providing software that performs a method that infringes Claim 1 when installed and operated by the customers, and by activities related to selling, marketing, advertising, promotion, installation, support, and distribution of the ’808 Patent Accused Products.

126. Open Text encourages and induces third parties to use the ’808 Patent Accused Products in a manner that infringes the ’808 Patent as described above, including through advertising, marketing, customer support, user manuals, instructions, installation, and distribution of the ’808 Patent Accused Products in the United States. For example, Open Text’s customers and end users test and/or operate Open Text Intelligent Capture in the United States in accordance with Open Text’s instructions contained in, for example, its user manuals, thereby also performing the claimed methods and infringing the asserted claims of the ’808 Patent reciting such operation. *See* Exhibit K; Exhibit L; Exhibit M; Exhibit N (“Captiva Capture Installation Guide”).

127. Moreover, Open Text has infringed and continues to infringe the ‘808 Patent indirectly, including by contributing to direct infringement of at least Claim 1 of the ’808 Patent in violation of 35 U.S.C. § 271(c). Open Text contributes to infringement of

the ’808 Patent by, among other activities, offering for sale, selling within the United States, and/or importing into the United States the ’808 Patent Accused Products with knowledge that such activities practice every element of one or more claims of the ’808 Patent, or being willfully blind to such activities practicing every element of one or more claims of the ’808 Patent. Open Text’s affirmative acts of offering for sale, selling, and/or importing into the United States the ’808 Patent Accused Products contribute to Open Text’s customers and end-users infringing of one or more claims of the ’808 Patent. The infringing software components of the ’808 Patent Accused Products are specially designed in a way that infringes one or more claims of the ’808 Patent and can be used only in a manner that infringes the ’808 Patent and thus have no substantial non-infringing uses.

128. The above description regarding Open Text’s infringement of the ’808 Patent is based on publicly available information and a reasonable investigation of the operation of the ’808 Patent Accused Products. Trend Micro reserves the right to modify this description, including, for example, on the basis of information about the ’808 Patent Accused Products that it obtains during discovery.

129. Unless and until enjoined by this Court, Open Text will continue to infringe the ’808 Patent. Open Text’s infringement is causing and will continue to cause Trend Micro irreparable harm, for which there is no remedy at law.

130. Under 35 U.S.C. § 283, Trend Micro is entitled to a preliminary and permanent injunction against further infringement of the ’808 Patent.

131. Open Text’s infringement of the ’808 Patent has been knowing and willful since at least September 16, 2022.

132. Trend Micro has suffered and continues to suffer damages, including lost profits, as a result of Open Text's infringement of the '808 Patent. Under 35 U.S.C. § 284, Trend Micro is entitled to damages adequate to compensate it for Open Text's infringement, in no event less than a reasonable royalty for Open Text's use of the inventions of the '808 Patent, together with interest and costs as fixed by the Court.

JURY TRIAL DEMAND

Trend Micro hereby demands trial by jury on all issues so triable pursuant to Rule 38 of the Federal Rules of Civil Procedure.

PRAYER FOR RELIEF

WHEREFORE, Trend Micro respectfully requests the following relief from this Court:

(A) A judgement that Defendants have infringed one or more claims of each of the Asserted Patents;

(B) A judgment that Defendants have willfully infringed one or more claims of each of the Asserted Patents;

(C) A judgment that Defendants have indirectly infringed by inducing the infringement of one or more claims of each of the Asserted Patents;

(D) A judgment that Defendants have indirectly infringed by contributing to the infringement of one or more claims of each of the Asserted Patents;

(E) A judgment that each of the Asserted Patents is valid and enforceable;

(F) A judgment awarding Trend Micro its damages resulting from Defendants' infringement of each of the Asserted Patents, and in no event less than a reasonable royalty;

(G) A judgment requiring Defendants to pay Trend Micro's costs, expenses, and pre-judgment and post-judgment interest for Defendants' infringement of each of the Asserted Patents;

(H) An order and judgment permanently enjoining Defendants and their officers, directors, agents, servants, employees, affiliates, attorneys, and all others acting in privity or in concert with them, and their parents, subsidiaries, divisions, successors and assigns from further acts of infringement of the Asserted Patents or, to the extent an injunction is not entered, a judgment requiring Defendants to pay Trend Micro an ongoing royalty for Defendants' continuing acts of infringement;

(I) A judgment finding that this is an exceptional case and awarding Trend Micro its reasonable attorneys' fees incurred pursuant to 35 U.S.C. § 285; and

(J) Such other relief as the Court deems proper and just.

Dated: October 2, 2023

Respectfully Submitted,

By: /s/ *Jonathan Lamberson*
Jonathan Lamberson

WHITE & CASE LLP
Yar R. Chaikovsky
yar.chaikovsky@whitecase.com
Philip Ou
philip.ou@whitecase.com
Jonathan Lamberson
jonathan.lamberson@whitecase.com
Radhesh Devendran
radhesh.devendran@whitecase.com
Michael Costello-Caulkins
Michael.costello-caulkins@whitecase.com
3000 El Camino Real
2 Palo Alto Square, Suite 900
Palo Alto, CA 94306-2109
Telephone: (650) 213-0300
Facsimile: (650) 213-8158

THE DACUS FIRM
Deron Dacus
TX Bar No. 00790553
ddacus@dacusfirm.com
821 ESE Loop 323, Suite 430
Tyler, TX 75701
Telephone: (903) 705-1117
Facsimile: (903) 581-2543

Attorneys for
Plaintiff Trend Micro Inc.