Talent Development & Excellence
Vol.12, No. 1, 2020, 4755—4771

Taxonomy of Network Security Software According to Features and Attributes

Evon Abu-Taieh[1] , Issam AlHadid[1], Auhood Alfaries[3], Hanan A. Mengash[2], Mai Alduailij[2], Omer Rana[4], Sufian AlKhawaldeh[1], Manal A. Alohaly[2]
[1]The University of Jordan, [2]Princess Norah Bin Abdulrahman University, [3]King Saud University, [4]Cardiff University.

Abstract

The cyber world reinvented a need for an age-old quest of safety. This research discussed 211 network security software environment according to 12 features. The paper first presented related research conducted on this topic. Next, the paper presented the 12 suggested features: Anti-Spam, Anti-Virus, Email Attachment Protection, Event Tracking, Internet Usage Monitoring, Intrusion Detection System, IP Protection, Spyware Removal, Two-Factor Authentication, Vulnerability Scanning, Web Threat Management, Web Traffic Reporting. Following, the paper showed the most popular features according to network security software. Afterward, the paper presented the top 6 network security software out of 211 that comply with at least 10 features.

Keywords: Network Security Software, cyber security, web threat, protection.

I. INTRODUCTION

The needs of security are an old quest of the human being. In this day and age of the virtual world, the need for security is even more. Hackers are stealing keystrokes, emails, chat-room dialogs, websites visited (browser history), programs run, Social Security numbers , credit card information, websites downloads, system login credentials, and sundry critical passwords, log files, system information, documents, spreadsheets, system credentials with no remorse, shame, or repentance of the destruction left behind. The mindless, senseless and despicable act of stealing is left unpunished because of the frailty of the information systems being used. Hence, the need for tools and techniques for protection from this absurdity.

Computer security is to protect the computer system and information from harm, theft, and unauthorized access. Network security is only one part of computer security. Abu-Taieh [1] stated that "Since technology is advancing expeditiously, it is not only challenging, but it is also imperative to pre-determine the process of security". Abu-Taieh [2] stated, "Cybersecurity encompasses physical and non-physical security of data, software, and hardware, from harm by both authorized and non-authorized access, whether access is internal or external".

In this research 211, network security software environment were researched according to 12 features. Although this research was conducted on 280 network security software environment, still 211 announced the 12 features on their websites. The 12 features are Anti-

ISSN 1869-0459 (print)/ISSN 1869-2885 (online)
© 2020 International Research Association for Talent Development and Excellence

Spam, Anti-Virus, Email Attachment Protection, Event Tracking, Internet Usage Monitoring, Intrusion Detection System, IP Protection, Spyware Removal, Two-Factor Authentication, Vulnerability Scanning, Web Threat Management, Web Traffic Reporting. The goal of this survey is to provide an overview of the main ideas, challenges, and solutions developed in the area, distilling them for a broad audience. Decision-makers, practitioners, scholars, and academicians are in need of such a study that put in a nutshell for them the scope for network security software and the different features that can be used to compare apples and oranges of network security software.

II. RELATED STUDIES

A great number of researchers attempted to survey the security software among them [3], [4], and [5]. Network Vulnerability scanning tools were reviewed in [6]. The authors classified the scanning tools according to types, capabilities, and functioning. Hence, the researchers classified the tools into two classes: Automatic scanning with publicly shared results and personal interaction-based scanning with results reported only to the user. The first class included tools like Shdan, Thingful, ZoomEye, Censys, PunkSPIDER. The second class included tools like Nesses, Vega, skipfish, Acunetix, Vulners, IVRE. The research gave a brief about each software and summarized the pros and cons of each software.

Another survey was conducted in [7] on server-side approaches to securing web applications. To secure web applications many techniques were developed according to web application lifecycle: development, review, auditing to deployment. The researchers categorized the techniques into three classes: Secure Construction of New Web Applications, Security Analysis/Testing of Legacy Web Applications, Runtime Protection of Legacy Web Applications. The researchers classify the techniques with two properties: 1) "the security vulnerabilities that they address and the attacks they aim to defeat" [7]; the second property "is the design objectives they bear and the phases during which they can be carried out" [7].

A survey of 18 Anti-Virus was conducted by [8] to study their security weaknesses. The research found that 12 of the 18 Anti-viruses had security weaknesses that can be utilized by their proposed Anti-Virus. The research of [9] discusses Intrusion Detection Systems (IDSs) and Collaborative IDSs (CIDSs) giving a detailed survey and comparison of specific CIDS approaches. And presenting a comprehensive analysis for the framework of requirements, building blocks, and attacks.

The research [10] states that "Collaborative security is an abstract concept that applies to a wide variety of systems and has been used to solve security issues inherent in distributed environments". The research studies 6 systems: technologies, standards, frameworks, strengths, and weaknesses. Furthermore, "present a comprehensive study with respect to their analysis target, timeliness of analysis, architecture, network infrastructure, initiative, shared information and interoperability" [10].

The research conducted by [11] gave a review of the general basic concepts related to Intrusion Detection Systems including taxonomies, attacks, data collection, modeling, evaluation metrics, and commonly used methods.

III. FEATURES

In this section, the paper presents 12 features used to categorize the Network Security Software, namely: Anti-Spam, Anti-Virus, Email Attachment Protection, Event Tracking, Internet Usage Monitoring, Intrusion Detection System, IP Protection, Spyware Removal, Two-Factor Authentication, Vulnerability Scanning, Web Threat Management, Web Traffic Reporting. The 12 features each will be discussed and explained.

Anti-Spam

Unwanted email sent by a range of senders from e-commerce, business, individuals to email users. Spam is so annoying that the USA set a law called CAN-SPAM ACT (Controlling the Assault of Non-Solicited Pornography and Marketing Act) in 2003. The email receiver has the right to stop unwanted emails hence opt-in and opt-out options. Many Network Security Software has this feature, out of the 211 software studied in this research there are 51 software claimed to have this feature. Spam emails can be advertising, malware and unwanted and disruptive information. Others define the concept “Spams are unwanted activities such as when marketers send members unwanted advertisements, post fake reviews, or steal user information by directing users to malicious external pages” [12]. Researchers in [13] opted to Evaluate social spammer detection systems. According to [14] there are two spam strategies link-based Web spam and content spamming.

Anti-Virus

Anti-Virus is a computer program that “cures” computers from malicious programs such as worms, viruses, Trojan horses. The curing process is to find, remove and fix the ill effects of the malicious programs. The term “Anti-Virus” is adopted from the medical term. Such programs are very essential for computer users since an infected computer can spread malicious programs throughout a computer network. Hence, one of the jobs of Anti-Virus is to prevent infections. Some well-known Anti-Virus software are: Bitdefender, Kaspersky, McAfee, Norton. In this research 68 security software claimed to have such property. In this research 68 network security software claimed to have such property.

Email Attachment Protection

Some malicious programs can exist in the attachment in the email. Hence, the email itself is clean and not infected while the attachment is contaminated. Software that can detect such a scenario has such property. In this research 49 network security software claimed to have such property.

Event Tracking

Event tracking is a method in JAVA library ga.js that record all user interactions with a web page. "Event Tracking employs an object-oriented model that you can use to collect and classify different types of interaction with your web page objects" [15]. In this research 73 network security software claimed to have such property.

Internet Usage Monitoring

As the name may suggest, this property is to monitor the use of the internet by the employee for the benefit of the employer. The end result of such activity is a Brows Report that reflects the different websites visited by the employee using the organization internet bandwidth. Furthermore, an organization must watch the promised performance and level of service by the ISP [16]. In this research 44, network security software claimed to have such property.

Intrusion Detection System

"Intrusion detection systems are the 'burglar alarms' (or rather 'intrusion alarms') of the computer security field" [17]. The same source, although old, still the paper gives a great insight into IDS. Axelsson [17], categorized IDS according to 3 Detection Principle: *anomaly, signature,* and *signature* inspired. The detection principle anomaly is further broken into two subclasses: *self-learning* and *programmed.* In turn *self-learning* subclass is broken into *time series* and *non-time series*; on the other hand, the *programmed* subclass is broken into *descriptive* and *default deny*. The *signature* class has one sub-class dubbed also programmed which is broken to sub-sub-class: *state-modeling, expert-system, string-matching,* and *simple rule-based*. The third class is *signature* inspired which is *self-learning* further classified as *automatic feature selection*. In this research 57, network security software claimed to have such property.

IP Protection

An IP address is like a Social security number or driving license number must be kept private. Internet Assigned Numbers Authority (IANA) a division of the Internet Corporation for Assigned Names and Numbers (ICANN) grants the IP address. The IP address "discerns your physical location" allowing "advertisers and adversaries track you online" [18]. The same sources suggest the cure is hiding the IP number using VPN. In this research 79, network security software environments out of 211 claimed to protect IP address.

Spyware Removal

Spyware are malicious software that steals information from the victim's computer and uses such information against the victim. The spyware steals information like keystrokes, emails, chat-room dialogs, websites visited (browser history), programs run, Social Security numbers, credit card information, website downloads, system login credentials, and sundry critical passwords, log files, system information, documents, spreadsheets, system credentials. [19] and [20]) categorized spyware into two categories: first category, according to spyware function according to [19], which are: Password Stealers, Banking Trojans, Infostealer, Kelogger. The second category is offered by [20] according to tactics, which are: Adware, Trojan, Tracking cookies, and system monitors. *Spyware Removal* is a property that Network Security Software used since 2000, after the term used back in 1996 according to [19]. In this research 32 network security software claimed to have such property.

Two-Factor Authentication

Two-factor authentication is, known as 2FA, the second level of authentication to log-in level. In the log-in a user enters username and password, in 2FA the user is required to have one of the three following credentials: Something you know (password), Something you have(ATM card) and Something you are (biometric) [21], [22], [23]. In this research 41, network security software claimed to have such property.

Vulnerability Scanning

Vulnerability scanning is inspecting, scrutinizing, examining, exploring, and probing of the potential points of exploit on a computer or network to identify security holes. A vulnerability scan detects and classifies system weaknesses in computers, networks, and communications equipment and predicts the effectiveness of countermeasures. There are two approaches to vulnerability scanning, authenticated and unauthenticated scans. For example TripWire SecureScan [24], [25], [26]. In this research 79, network security software claimed to have such property.

Web Traffic Reporting

Web Traffic Reporting is a property in Web Traffic Reporting that allows the organization to know who is visiting an organization website. [27] lists a number of information that can be provided to the organization by using their tool: keyword page ranking searched keywords relative to business, unique visitors, traffic sources, social media activity, advertising performance, etc. In this research 58, network security software claimed to have such property.

Table 1. Features offered by Network Security Software

Feature	**Number of Software offered this feature**
Web Threat Management	83
IP Protection	79
Vulnerability Scanning	79
Event Tracking	73
Anti-Virus	68
Web Traffic Reporting	58

Intrusion Detection System	57
Anti-Spam	51
Email Attachment Protection	49
Internet Usage Monitoring	44
Two-Factor Authentication	41
Spyware Removal	32

Web Threat Management

According to [28] Cyber Threat Management (CTM) is “an advanced management program enabling early identification of threats, data-driven situational awareness, accurate decision-making, and timely threat mitigating actions”. The CTM, according to the same source, includes :

- *Manual and automated intelligence gathering and threat analytics*
- *A comprehensive methodology for real-time monitoring including advanced techniques such as behavioral modeling*
- *Use of advanced analytics to optimize intelligence, generate security intelligence, and provide Situational Awareness*
- *Technology and skilled people leveraging situational awareness to enable rapid decisions and automated or manual actions*

In this research 83 security software claimed to have Web Threat Management property.

Table 2. Top 6 Network Security Software that included features

	Anti-Spam	Anti-Virus	Email Attachment Protection	Event Tracking	Internet Usage Monitoring	Intrusion Detection System	IP Protection	Spyware Removal	Two-Factor Authentication	Vulnerability Scanning	Web Threat Management	Web Traffic Reporting	**Count**
WebTitan	x	x	x	x	x		x		x	x	x	x	10

Sophos UTM	x	x	x	x	x	x		x	x		x	x	10
SiteLock	x	x		x	x	x	x		x	x	x	x	10
iPrism Web Security	x	x	x		x	x	x	x		x	x	x	10
AtomOS Kwick Key	x	x	x	x	x	x	x		x	x	x	x	11
B@mbu cloud	x	x	x	x	x	x	x	x	x	x	x		11
Violet	x	x	x	x	x	x	x	x	x	x	x	x	12

IV. THE TOP FEATURES

The top features offered by the 211 Network Security Software is *Web Threat Management* offered by 83 Network Security Software. Next *IP Protection* and *Vulnerability Scanning* both offered by 79 Network Security Software. After, *Event Tracking property* offered by 73 Network Security Software, followed by *Anti-Virus* and *Web Traffic Reporting* offered by 68 and 58 respectively Network Security Software. *Intrusion Detection System* was offered by 57 Network Security Software. *Anti-Spam* and *Email Attachment Protection* features were offered by 51 and 49 Network Security Software. *Internet Usage Monitoring* and *Two-Factor Authentication* ranked in 11th and 12th place when 44 and 41 Network Security Software offered them as features. The least mentioned feature is *Spyware Removal* feature offered by only 32 Network Security Software. The results are reflected in Table 1:

V. TOP SIX NETWORK SECURITY SOFTWARE

There are 6 Network Security Software that covered more than 10 properties as shown in table 2. *WebTitan* is a “DNS Based Web content filter and web security layer that blocks malware, *ransomware* and phishing attempts as well as providing web content control” [29]. WebTitan covered 10 features and did not cover the Intrusion Detection System & Spyware Removal. There were 163 reviews with 4.5 starts evaluation[30]. WebTitatn is developed by TitanHQ established in the USA in 1995.

Sophos UTM has 10 features except for *IP Protection* and *Vulnerability Scanning*. According to [30] 13 reviewers gave the software 4.5 stars. The developed Sophos was founded in 1985 in the USA. SiteLock has 10 Network Security features except for *Email Attachment Protection* and *Spyware Removal*. According to [30] 11 reviewers gave the software 4 stars. *iPrism Web Security* has 10 Network Security features except *Event Tracking* and *Two-Factor Authentication*. According to [30] 11 reviewers gave the software 4 stars.

AtomOS Kwick Key was created in 2005 has 11 Network Security features except for *Spyware Removal*. Still, according to [31]) it has many more features. B@mbu cloud was created in 2005 has 11 Network Security features except Web Traffic Reporting. Still, according to [32] has many more features. Violet was created in 2014 has 12 Network Security features. Still, according to [32] has many more features.

VI. APPLICATIONS

Any decision-maker is faced with protecting the different assets of the organization. Some assets that pertain to information technology are of at most importance. Although no one denies the importance of protecting data, still; there is a price for the protection procedure. Paying too much or too little money for protection is also important as it is considered an investment in the organization's reputation and assets. This research is will help decision-makers, as well as, users, researchers, practitioners, and academicians. In making a basic comparison of the different Network Security Software.

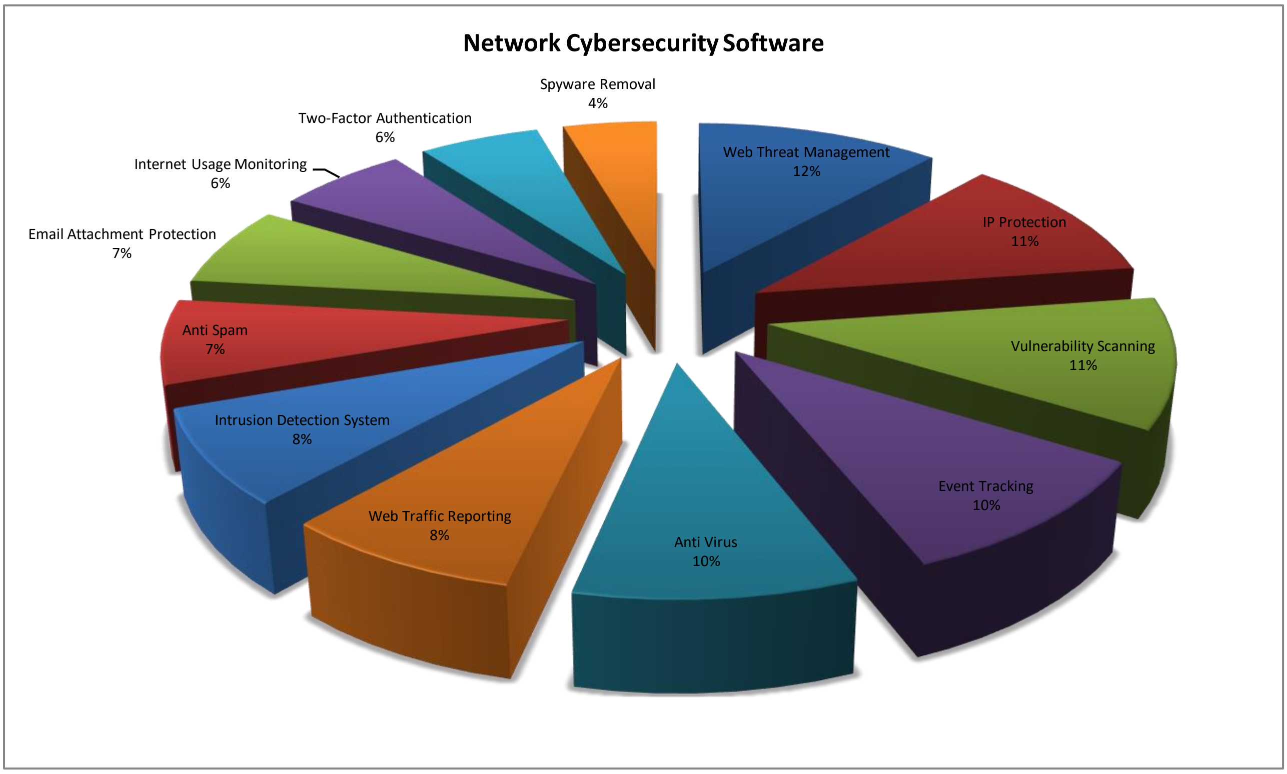

Figure. 1. The 12 features and Network Security Software using them.

VII. CONCLUSION AND FUTURE RESEARCH DIRECTIONS

This research paper presented 211 network security software according to 12 known features. The paper first out lied related work where researchers surveyed network security software. Then the paper discussed the 12 features in detail. Next, the paper discussed the top features according to the study. The study ranked the features according to their popularity in Network Security Software. Next, the paper presented the top six Network Security Software who covered more than 10 features.

In later research, one may search for the techniques used in each software. Such an endeavor may face the problem of divulging trade secrets and Intellectual property issues. Furthermore, many of the software environments discussed in this paper may not be divulging such essential trade secrets for their work.

ACKNOWLEDGMENT

This research was funded by the Deanship of Scientific Research at Princess Nourah bint Abdulrahman University through the Fast-track Research Funding Program.

REFERENCES

[1]. E. Abu-Taieh, "Cyber Security body of knowledge", IEEE SC2-2017. The 7th IEEE International Symposium on Cloud and Service Computing. Kanazawa, Japan, November 22-25, 2017. DOI: 10.1109/SC2.2017.23. URL: https://ieeexplore.ieee.org/document/8315363/?part=1

[2] E. Abu-Taieh, A. Alfaries, S. T. Alotaibi, "Cyber Security Body of Knowledge and Curricula Development". Reimagining New Approaches in Teacher Professional Development. 2018. ISBN 978-953-51-6129-5. Book edited by:Prof. Vimbi Mahlangu. Intech. London. UK.

[3]. C. Cadar and K. Sen, "Symbolic Execution for Software Testing: Three Decades Later". Commun. ACM 56, 2 (2013), 82–90. https://doi.org/10.1145/2408776.2408795

[4]. C. S. Pasareanu and W. Visser. 2009. "A Survey of New Trends in Symbolic Execution for Software Testing and Analysis". Int. Journal on Software Tools for Technology Transfer 11, 4 (2009), 339–353. https://doi.org/10.1007/ s10009-009-0118-1

[5]. R. Baldoni, E. Coppa, D. Cono D'elia, C. Demetrescu, and I. Finocchi. 2018. "A Survey of Symbolic Execution Techniques". ACM Comput. Surv. 51, 3, Article 50 (May 2018), 39 pages. DOI: https://doi.org/10.1145/3182657

[6]. A. Tundis, W. Mazurczyk, and M. Mühlhäuser. 2018. "A review of network vulnerabilities scanning tools: types, capabilities and functioning". In Proceedings of the 13th International Conference on Availability, Reliability and Security (ARES 2018). ACM, New York, NY, USA, Article 65, 10 pages. DOI: https://doi.org/10.1145/3230833.3233287

[7]. X. Li and Y. Xue. 2014. "A survey on server-side approaches to securing web applications". ACM Comput. Surv. 46, 4, Article 54 (March 2014), 29 pages. DOI: https://doi.org/10.1145/2541315

[8]. B. Min and V. Varadharajan. 2015. "Design, implementation and evaluation of a novel anti-virus parasitic malware". In Proceedings of the 30th Annual ACM Symposium on Applied Computing (SAC '15). ACM, New York, NY, USA, 2127-2133. DOI: https://doi.org/10.1145/2695664.2695683

[9]. E. Vasilomanolakis, S. Karuppayah, M. Mühlhäuser, and M. Fischer. 2015. "Taxonomy and Survey of Collaborative Intrusion Detection". ACM Comput. Surv. 47, 4, Article 55 (May 2015), 33 pages. DOI: https://doi.org/10.1145/2716260

[10]. G. Meng, Y. Liu, J. Zhang, A. Pokluda, and R. Boutaba. 2015. "Collaborative Security: A Survey and Taxonomy". ACM Comput. Surv. 48, 1, Article 1 (July 2015), 42 pages. DOI: https://doi.org/10.1145/2785733

[11]. P. Angelo A. Resende and A. C. Drummond. 2018. "A Survey of Random Forest Based Methods for Intrusion Detection Systems". ACM Comput. Surv. 51, 3, Article 48 (May 2018), 36 pages. DOI: https://doi.org/10.1145/3178582.

[12]. A. Lupher, C. Engle, , R. Xin,: "Feature Selection and Classification of Spam on Social Networking Sites". Available online: bid.berkeley.edu/cs294-1-spring12/images/archive/6/6a/20120515031244!Spam-lupher-engle-xin.pdf, (2012)

[13]. K. Ho, V. Liesaputra, S. Yongchareon, and M. Mohaghegh. 2018. "Evaluating social spammer detection systems". In Proceedings of the Australasian Computer Science Week Multiconference (ACSW '18). ACM, New York, NY, USA, Article 18, 7 pages. DOI: https://doi.org/10.1145/3167918.3167936

[14]. C. Wei, Y. Liu, M. Zhang, S. Ma, L. Ru, and K. Zhang. 2012. "Fighting against web spam: a novel propagation method based on click-through data". In Proceedings of the 35th international ACM SIGIR conference on Research and development in information retrieval (SIGIR '12). ACM, New York, NY, USA, 395-404. DOI: https://doi.org/10.1145/2348283.2348338

[15]. GoogleDeveloper, 2018. https://developers.google.com/analytics/devguides/collection/gajs/eventTrackerGuide. (Accessed 20- oct 2018)

[16]. E. Geier. JUL 11, 2017. "How to monitor, measure, and manage your broadband consumption". PCWorld From IDG. https://www.pcworld.com/article/3072638/home-networking/how-to-measure-monitor-and-manage-your-broadband-consumption.html

[17]. S. Axelsson, (2000). "Intrusion detection systems: A survey and taxonomy" (Vol. 99). Technical report.. http://neuro.bstu.by/ai/To-dom/My_research/Paper-0-again/For-research/D-mining/Anomaly-D/Intrusion-detection/taxonomy.pdf. (Accessed 20- oct 2018)

[18]. M. Eddy . (Jan. 2018)."How to Hide Your IP Address". PCMAG DIGITAL EDITION. https://www.pcmag.com/article/343394/how-to-hide-your-ip-address

[19]. Malwarebytes, 2018. https://www.malwarebytes.com/spyware/. Accessed 15 Oct 2018

[20]. Norton. 2018. https://us.norton.com/internetsecurity-how-to-catch-spyware-before-it-snags-you.html

[21]. M. Khamis, R. Hasholzner, A. Bulling, and F. Alt. 2017. "GTmoPass: two-factor authentication on public displays using gaze-touch passwords and personal mobile devices". In Proceedings of the 6th ACM International Symposium on Pervasive Displays (PerDis '17). ACM, New York, NY, USA, Article 8, 9 pages. DOI: https://doi.org/10.1145/3078810.3078815.

[22]. T. Petsas, G. Tsirantonakis, E. Athanasopoulos, and S. Ioannidis. 2015. "Two-factor authentication: is the world ready?: quantifying 2FA adoption". In Proceedings of the Eighth European Workshop on System Security (EuroSec '15). ACM, New York, NY, USA, Article 4, 7 pages. DOI: https://doi.org/10.1145/2751323.2751327.

[23]. M. Azimpourkivi, U. Topkara, and B. Carbunar. 2017. "Camera Based Two Factor Authentication Through Mobile and Wearable Devices". Proc. ACM Interact. Mob. Wearable

Ubiquitous Technol. 1, 3, Article 35 (September 2017), 37 pages. DOI: https://doi.org/10.1145/3131904

[24]. H. Holm. 2012. “Performance of automated network vulnerability scanning at remediating security issues”. Comput. Secur. 31, 2 (March 2012), 164-175. DOI: http://dx.doi.org/10.1016/j.cose.2011.12.014

[25]. M. Rouse , M. Haughn. “network vulnerability scanning”. https://searchsecurity.techtarget.com/definition/vulnerability-scanning. Accessed 15 Oct 2018

[26]. I. Pomeranz. 2017. “Generation of Transparent-Scan Sequences for Diagnosis of Scan Chain Faults”. ACM Trans. Des. Autom. Electron. Syst. 22, 3, Article 43 (May 2017), 17 pages. DOI: https://doi.org/10.1145/3007207

[27]. Google, 2018. https://webmarketsonline.com/Analytics. Accessed 15 Oct 2018

[28]. IOCTM. 2018. What is Cyber Threat Management?, https://www.ioctm.org/What-is-Cyber-Threat-Management. Accessed 15 Oct 2018

[29]. TitanHQ. 2018. https://www.titanhq.com/. Accessed 15 Oct 2018

[30]. Capterra. 2018. WebTitan. https://www.capterra.com/p/146034/WebTitan/. Accessed 15 Oct 2018

[31]. Atomampd. 2018. http://www.atomampd.com/atomos.html. Accessed 15 Oct 2018

[32]. Bambucloud. 2018. https://www.bambucloud.net/. Accessed 15 Oct 2018

Appendix (1)

	Anti Spam	Anti Virus	Email	Event Tracking	Internet Usage	Intrusion	IP Protection	Spyware	Two-Factor	Vulnerability	Web Threat	Web Traffic	**count**
Acunetix				x	x	x				x	x	x	**6**
ManageEngine Firewall Analyzer													**0**
WebTitan	x	x	x	x	x		x		x	x	x	x	**10**
Avatier Identity Anywhere									x				**1**
AVG Antivirus Business Edition	x	x	x					x					**4**
EventLog Analyzer				x			x			x	x	x	**5**
Log360				x							x	x	**3**
Avast Business Antivirus Pro	x	x			x		x	x					**5**
Norton Security	x	x	x					x			x		**5**
Spiceworks Network Monitor				x	x							x	**3**
Cloudflare				x			x		x		x	x	**5**
NordVPN							x				x		**2**
TunnelBear	x						x						**2**
bitdefender GravityZone	x	x	x				x				x		**5**
Black Duck Hub										x	x		**2**
DNSFilter		x			x						x	x	**4**
OpenVPN Access Server							x		x				**2**
PureVPN	x			x		x	x				x		**5**
Centrify Infrastructure Sevices				x			x		x		x	x	**5**
CylancePROTECT		x											**1**
RMail			x										**1**
Webroot SecureAnywhere DNS protection		x									x	x	**3**
Reve Antivirus	x	x	x					x		x			**5**
Smart protection	x					x		x		x			**4**
EventTracker				x		x	x	x		x	x		**6**
MailWasher	x		x					x					**3**
McAfee Preventsys Risk Analyzer													**0**
SUPERAntiSpyware		x						x					**2**
Aguard	x			x				x			x		**4**
Indeni				x									**1**
Sophos UTM	x	x	x	x	x	x	x		x	x		x	**10**
SPAMfighter	x	x	x										**3**
AlienVault USM						x				x	x		**3**
Fusion	x	x								x	x		**4**

ISSN 1869-0459 (print)/ISSN 1869-2885 (online)
© 2020 International Research Association for Talent Development and Excellence

SiteLock	x	x		x	x	x	x		x	x	x	x	**10**
The Email Laundry	x	x	x		x								**4**
Bot Mitigation and Management	x			x	x						x	x	**5**
PracticeProtect				x		x	x		x	x			**5**
ZoneAlarm Pro		x			x	x	x	x			x		**6**
F-Secure Anti-Virus		x	x			x		x		x	x		**6**
GFI LanGuard										x			**1**
NANO Antivirus		x	x					x		x	x		**5**
Unified Threat Management													**0**
Astra Security	x			x		x	x			x	x	x	**7**
CryptoPhoto	x	x			x	x	x		x		x		**7**
PhishingBox			x			x				x			**3**
STOPzilla Antivirus		x						x					**2**
Firewall-1							x						**1**
ForeScout CounterACT Edge		x								x			**2**
RansomFree		x											**1**
KerioControl	x	x				x	x		x			x	**6**
Saint Security Suite		x								x	x		**3**
X-VPN - Change and Hide IP	x						x	x					**3**
SpyHunter	x	x						x					**3**
wildfire		x		x									**2**
Active Shield		x						x					**2**
AVDS										x			**1**
Bot Detection and Mitigation by Distil Networks				x								x	**2**
SPIRION DLP Suite			x	x			x						**3**
modusCloud	x	x	x	x			x			x			**6**
NetSpective Content Filter				x	x							x	**3**
PerfectMail	x	x	x										**3**
PerfectMail Antispam	x	x								x			**3**
Privatoria			x				x						**2**
Privileged Account Security Solution			x						x	x	x		**4**
QualysGuard Enterprise										x			**1**
Blesk				x	x	x	x			x		x	**6**
Dome9										x			**1**
iSecurity		x	x	x		x			x	x			**6**
Lynis Enterprise						x				x			**2**
Netskope Cloud Security Platform			x	x		x	x		x	x	x	x	**8**
NG Firewall		x											**1**
RedSeal										x			**1**
Cloudmark Authority	x												**1**

ISSN 1869-0459 (print)/ISSN 1869-2885 (online)
© 2020 International Research Association for Talent Development and Excellence

Flextivity	x												**1**
SecurenceMail	x	x	x				x		x				**5**
Cloudmark Authority		x											**1**
Flextivity		x											**1**
SecurenceMail	x	x	x				x		x				**5**
Access Watch	x	x		x		x					x	x	**6**
ACL Manager				x	x		x						**3**
Active Wall		x		x	x							x	**4**
AIONCLOUD										x	x	x	**3**
Aobo Internet Filter for Mac	x				x								**2**
Armor2net Personal Firewall						x		x					**2**
Artica Proxy	x	x	x		x	x	x				x	x	**8**
AtomOS Kwick Key	x	x	x	x	x	x	x		x	x	x	x	**11**
AuthenWare				x		x			x				**3**
B@mbu cloud	x	x	x	x	x	x	x	x	x	x	x		**11**
Barracuda Web Application Firewall	x	x	x	x			x		x	x	x	x	**9**
BlueTalon											x		**1**
BluSapphire			x			x	x	x		x	x		**6**
BroadBot				x	x	x	x			x	x	x	**7**
bt-Enterprise					x						x		**2**
Business Email Security	x	x		x	x	x		x		x		x	**8**
CacheGuard-OS		x									x	x	**3**
Catbird				x		x				x			**3**
CertHat				x					x				**2**
Cigloo Browser Isolation Management Platform			x	x							x	x	**4**
CimTrak Integrity Suite				x		x							**2**
Cloudbric											x	x	**2**
CloudEye				x	x	x	x			x	x	x	**7**
CloudFish				x								x	**2**
ClrStream	x	x	x										**3**
Comodo cWatch													**0**
Constellation Analytics Platform			x	x			x				x		**4**
Constellix									x			x	**2**
Cornerstone MFT Server			x	x									**2**
CryptoMite									x		x		**2**
Cyberator													**0**
Cyberint				x			x			x	x		**4**
CyberReveal										x	x		**2**
Cybersecurity											x	x	**2**

ISSN 1869-0459 (print)/ISSN 1869-2885 (online)

© 2020 International Research Association for Talent Development and Excellence

yBlock					x						x	**2**
Cybowall				x		x				x			**3**
Data Rover EP				x									**1**
DataDome bot management solution				x	x		x			x	x	x	**6**
DATCOM								x					**1**
Declude Security Suite	x	x	x							x			**4**
DESlock			x						x				**2**
DESwrap							x						**1**
Devasted Antivirus	x	x	x			x		x	x				**6**
eviceLock			x	x							x	x	**4**
Devknox										x	x		**2**
Difenso					x	x	x	x	x	x	x		**7**
ditno. Network Firewall				x							x		**2**
DNS Firewall							x		x				**2**
DragonSoft DVM										x			**1**
DynaZip Max Secure							x		x				**2**
E8 Security				x			x						**2**
east-tec InvisibleSecrets						x	x						**2**
Encrypted Data Gateway Engine									x				**1**
Enterprise Security				x								x	**2**
EntryProtect		x						x					**2**
Evident.io							x			x			**2**
eVigilPro		x		x	x						x	x	**5**
Ezeelogin SSH Gateway				x					x				**2**
FireEye Enterprise											x		**1**
FireLayers											x		**1**
FlowTraq				x	x		x						**3**
Fortscale						x						x	**2**
Genian NAC				x	x		x			x	x	x	**6**
GridinSoft Anti-Malware		x				x	x	x		x	x		**6**
HaltDos	x	x		x			x			x	x	x	**7**
IMMUNIO							x			x	x		**3**
Infiltrator	x	x	x				x						**4**
InfiSecure	x					x	x			x	x	x	**6**
Intelligent Management Center				x									**1**
Intruder									x	x			**2**
iPrism Web Security	x	x	x		x	x	x	x		x	x	x	**10**
IronSFTP							x						**1**
Kenna							x			x	x		**3**
Key Manager Plus											x		**1**
Kiuwan Code Security										x			**1**

L7 Defense									x		x	**2**
Lancera									x			**1**
Lockspam Pro 3.0	x		x						x			**3**
LogPoint				x	x	x			x	x		**5**
LogRhythm Network Monitor					x	x					x	**3**
MailSite Fusion	x	x										**2**
Marble Security						x						**1**
MB				x						x	x	**3**
MePin						x	x	x	x	x		**5**
Metapacket											x	**1**
MyIP.io VPN				x	x		x					**3**
NCP							x	x				**2**
Nfusion		x	x		x		x		x	x		**7**
Onion ID								x				**1**
Outpost Firewall Personal Pro		x	x			x	x		x			**6**
Ozon		x	x				x		x	x	x	**6**
Perfecto Encryptor						x						**1**
PerimeterX							x			x		**2**
Primo VPN							x					**1**
Pulse				x		x			x	x		**4**
Qrator				x			x		x		x	**4**
RBLTracker							x	x	x	x		**4**
RDS-Shield				x		x	x		x	x		**5**
Safe@Office					x						x	**2**
SafeInternetEmail	x	x	x					x		x		**5**
Safend Protector		x										**1**
SafenSec		x	x									**2**
SecureNok		x		x	x	x						**4**
SecureTrack				x	x		x			x	x	**5**
Security Framework								x				**1**
Security Manager by NetIQ					x							**1**
Security Manager by FireMon				x	x					x	x	**4**
Security Shield		x							x			**2**
Security Solutions										x		**1**
Sentinel IPS	x		x			x	x			x		**5**
Sepior			x			x	x	x	x	x		**6**
SmartFlow				x	x	x	x		x	x	x	**7**
SmartWall TDS				x		x					x	**3**
Snyk									x			**1**
Spam and Virus Blocker	x	x	x									**3**
Sqreen				x	x	x	x		x	x	x	**7**

ISSN 1869-0459 (print)/ISSN 1869-2885 (online)
© 2020 International Research Association for Talent Development and Excellence

SSProtect									x				**1**
StealthDisk Mobile			x				x		x				**3**
Tanium Endpoint Platform										x			**1**
The ZoneRanger							x					x	**2**
Themis									x		x		**2**
ThreatSentry				x		x	x					x	**4**
Unistal Anti Virus	x	x											**2**
Vaccine46	x	x				x		x		x			**5**
Vallum GMI Agent				x	x								**2**
vArmour						x	x						**2**
VFind Security ToolKit		x											**1**
Violet	x	x	x	x	x	x	x	x	x	x	x	x	**12**
VIPole							x		x				**2**
Vormetric				x			x				x		**3**
XD Air		x		x						x	x		**4**
Zada Suite			x	x	x	x	x			x	x		**7**
Count	**51**	**68**	**49**	**73**	**44**	**57**	**79**	**32**	**41**	**79**	**83**	**58**	**211**

ISSN 1869-0459 (print)/ISSN 1869-2885 (online)

© 2020 International Research Association for Talent Development and Excellence