A Comprehensive Review of Endpoint Security: Threats and Defenses

Abu Kamruzzaman
Dept. of Eng., Physics and Tech
Bronx Comm. College/CUNY
Bronx, NY, USA
Abu.Kamruzzaman@bcc.cuny.edu

Sadia Ismat
Professional Security Studies
Dept, New Jersey City University
Jersey City, NJ, USA
sismat@njcu.edu

Joseph C. Brickley
Professional Security Studies
Dept, New Jersey City University
Jersey City, NJ, USA
jbrickley@njcu.edu

Alvin Liu
Department of IS and Statistics
Baruch College/CUNY
NY, NY, USA
student@baruchmail.cuny.edu

Kutub Thakur
Professional Security Studies Dept
New Jersey City University
Jersey City, NJ, USA
kthakur@njcu.edu

2022 International Conference on Cyber Warfare and Security (ICCWS) | 978-1-6654-8939-3/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICCWS56285.2022.9998470

***Abstract* — Endpoint Security/Protection is vital to an enterprise's cybersecurity platform. There are many endpoints a malicious actor can attack to infiltrate and gain access to a system and steal data. These different endpoints are continuously growing as more people switch to remote work or even use their work devices. Due to this, endpoints are more susceptible now than before because of the increased pathways cybercriminals can take to infiltrate a system. This paper will discuss the importance of endpoint security management, the type of attacks a cybercriminal uses, the different types of endpoints, and how cybersecurity specialists can combat and prepare protection for these endpoints. In addition, there will be examples of other vendors that provide endpoint security and explain how their software/antivirus can mitigate endpoint attacks.**

Keywords—Endpoint, Anti-virus, Ransomware

I. INTRODUCTION

Endpoint Security is a category of cybersecurity that secures endpoints or entry points from being exploited by malicious hackers or attacks. An endpoint is any remote device on a network that communicates back and forth with the network it is connected to, such as laptops, desktops, tablets, servers, and phones [1]. In an organization, many types of endpoints within a network give cybercriminals different avenues to attack a system [2]. An attacker's techniques are ransomware, vulnerability exploits, email phishing, and drive-by downloads [3]. A ransomware attack would be made to gain money from an organization or business by encrypting their data and having them pay for it. As a result, organizations use different types of endpoint protection to protect their systems [4]. Some of this endpoint protection is IoT Security, Anti-Virus Software, URL Filtering, Application Controls, Network Access Controls, Browser Isolation, and Cloud Perimeter Security. Anti-Virus software identify, block, and remove malware on devices [5]. The paper highlights on the Endpoint Attacks and Defenses in section II on Ransomware, Email Phishing, Vulnerability Exploits, Drive-by-Downloads, Waterholes, IoT Threats and Endpoint Protection section III describes IoT, Anti-Virus, URL Filtering, Application Controls, Network Access Controls, Browser Isolation, Cloud Perimeter Security. This paper also focuses into Endpoint Security Vendors in section IV with highlight on the McAfee's, Cloudstrike, ESET Endpoint Protection Platform. In the concluding remarks the authors emphasize importance on the Endpoint Security.

II. ENDPOINT ATTACKS AND DEFENSES

A. Ransomware

Ransomware is a malware used on file encryption on a device making the files and system not usable anymore [6]. Ransomware is usually a technique used to force victims to pay a certain amount of money. Cybercriminals will threaten the victims by publish the data on payment refusal and explain how they will publicly slander them as a form of extortion [6]. This causes the victims to become scared and more swayed to pay the cybercriminals because their data can be leaked all over the internet, and their organization's reputation will worsen. Ransomware have severe impact as business is not able to access data or unable to perform business due to encryption [6].

To protect against ransomware, organizations must be prepared and have quick thinking. Organizations should have offline, encrypted data backups and regular tests [6]. This removes the need to pay for data while data is in local system. Organizations need to have a Ransomware Response Checklist to respond and mitigate the effects of ransomware quickly.

B. Email Phishing

To give an overview of Email Phishing, phishing is a term that must be understood. Phishing is considered a social engineering attack to steal victims data with login info and sensitive information such as credit card numbers [7]. In an email Phishing, a user is tricked into clicking an URL to be affected with the installation of a malware. Common email phishing attacks are hidden in mass- distributed emails, such as organization emails or even educational emails [7]. These emails catch the victim off guard because it

gives a sense of false sense of security due to the fact it is sent from their organization or school, and they unknowingly click the link, which leads to compromised information and network access to the hackers. Email Phishing is so popular and can easily catch victims because cybercriminals go to great lengths by using the same phasing, typefaces, logos, and signatures to make the email look legit [7]. Two-factor authentication (2FA) can be used to prevent email phishing.

C. *Vulnerability Exploits (Zero Day Attack)*

A zero-day vulnerability is an unknown security weakness or software defect that an attacker can target. It's called a "zero day" because software vendors were unaware of vulnerabilities in their software and there was no zero day to fix the issue with a security patch or update [8]. Zero-day exploits typically target government agencies, large corporations, and individuals with access to valuable business data, and those using a vulnerable system, hardware devices, firmware, and IoT [9]. Zero-day attacks are perilous for companies and businesses because it is challenging to detect where and when these attacks happen. As a result, these attacks are most likely to succeed because no countermeasures are taken [9].

It is impossible to stop zero-day attacks because a cyber security system can't be perfect, meaning there will always be vulnerabilities within a security system. However, there are ways to lower the chances of experiencing a zero-day attack. Vulnerability scanning is a type of scanning that can detect some zero-day exploits. They can see these exploits by running simulation incidents on software code and conducting code analysis to discover new weaknesses [9]. Organizations can deploy a full endpoint security solution that blends the use of next-gen antivirus (NGAV), endpoint detection and response (EDR), and threat intelligence [8]. With a complete endpoint security solution, organizations can optimize defense and implement the best prevention technology in preparedness if an attack occurs.

D. *Drive-by-Downloads*

A drive-by download is an unintentional malicious code or program downloaded into a computer or device. This attack is forced because the user does not realize they have downloaded the malicious code or program. Attackers exploit vulnerable apps, operating systems, or web browsers to perform drive-by downloads [10]. There are two ways malicious drive-by downloads can get onto your device. These are allowed without knowing the full meaning. This means performing an action that leads to infection (clicking a link, downloading a Trojan horse) [10]. Second is downloading the malicious software entirely unauthorized without any notifications. An example is when an attacker injects a malicious component into a vulnerability that infects users who visit the website without prompting or taking action [10].

Drive-by download attacks can be prevented. Use computer admin account for program installations. Without admin privileges, the hacker cannot download malicious programs or codes [10]. Keep web browser, operating system, and internet security software up to date; this tip is self-explanatory because new updates and patches help seal the gaps in the defense. Avoid websites that contain malicious code and carefully read and examine security pop-ups on the web before clicking [10]. Users should be visiting mainstream and well-established sites to decrease their chances of a malicious download. Carefully reading and being meticulous before clicking can significantly reduce the chances of a drive-by download. An example of a diagram of drive-by-download attacks can be seen below in figure 1.

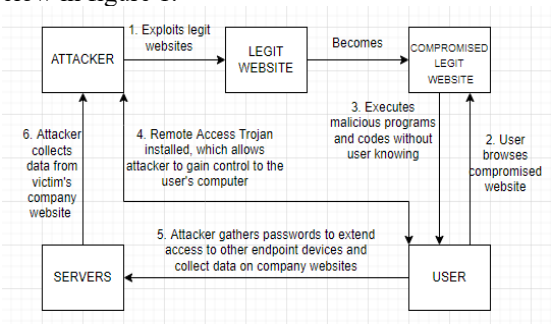

Figure 1: Diagram of a Drive-by-Download Attack (self-drawn)

E. *Waterholes*

A waterhole attack is a strategic attack compromising a website. Attackers use waterhole attacks for financial gain and build their botnet (a network of hijacked computers and devices infected with malware controlled by a hacker) [13]. Waterhole attacks occur when an attacker finds a vulnerability on a public website, compromising the site and infecting it with their malware [13]. After the attackers have placed their malware, they prompt users to visit these seemingly harmless websites by using contextual emails directing them to specific parts of the compromised site [13]. When a user reaches these compromised sites, drive-by downloads happen, and the user has malicious code/programs downloaded on their computer without knowing [12].

Combining both users are more likely to be infected. Web gateways detection are essential to defend from waterhole attacks [13]. For better security, users should use an advanced malware analysis solution to check for malicious behavior on visited websites [13]. Another way to protect against waterhole attacks is to look for an email solution and protection that scans for threats within emails. Waterhole attacks can be minimized through the click-through reduction on malicious emails.

F. *Threats to IoT Devices*

Users must understand what IoT devices are. IoT devices are hardware components such as sensors, gadgets, devices, and machines. These devices can be programmed for specific applications and can transmit

data over the Internet and other networks [14]. Smart watches, intelligent fire alarms, smart televisions, medical sensors, and fitness trackers are some IoT examples which have daily usage. As a result, these devices have potentially high risks of being hacked due to IoT built-in security being straightforward and not considering the more extensive infrastructure and connectivity picture [15]. IoT devices have many vulnerabilities because they lack the computational capacity for built-in security, and built-in protection due to limited budget for developing a secure firmware [20].

III. ENDPOINT PROTECTION

A. IoT Protection

Three levels of IoT security need to improve to be truly effective. The device, the connection, the cloud. IoT device security must protect device and user identities, ensure device integrity, and protect operational and personal data on each device [15]. IoT device traffic is unencrypted for connection security, putting personal and confidential data at severe risk [16]. To protect IoT connectivity, IoT security must ensure secure application, data traffic, and data security in transit for all types of connections over networks [15]. For cloud security, IoT devices need to provide the required trust for data centers and public clouds while protecting data and ensuring privacy. A single malware protection software or agent cannot protect IoT devices dues to the vast array of hardware and operating systems that IoT devices have [16].

B. Anti-Virus Protection

A critical factor in cyber security and endpoint security is the usage of antivirus software. Antivirus software is a type of software that is designed to detect, prevent, and eliminate malware on devices; some of this antivirus software can have the capability to detect worms, bots, and trojans [18]. The key features of antiviruses include the ability to run scans manually and automatically, protection for apps, and fighting against most types of malwares. In addition, antivirus software usually has internet safety features like malicious website detection, blocking automatic downloads, and scanning for malicious entities [18]. Furthermore, to have proactive security, antivirus solutions have automated updates to guarantee the endpoint is safe compared to the newer threats [18].

Although antivirus software is a pivotal part of an organization's security, it can be considered the follow-up to endpoint security. Endpoint Security is different because it provides a centralized portal that allows IT and other security professionals to remotely monitor activity, investigate suspicious traffic, and install and configure software [18]. This is unlike an antivirus, which is only personalized to one user and protects one user from malware and other threats. Another significant difference between the two is how endpoint security offers enhanced protection against nontraditional threats using technologies like data encryption and data access controls, preventing unauthorized employees from accessing specific categories of data [18]. Endpoint security protects against threats like data loss, phishing, and drive-by malware. It includes all the capabilities of antivirus software, yet antivirus is still a vital part of endpoint protection.

C. URL Filtering

URL Filtering is to prevent employee's accessing harmful web pages to prevent malware infiltration into the endpoints. URL Filtering is vital to endpoint security because users spend most of their time at work on the computer, visiting websites to do research or even surfing the web for personal use. As a result, this kind of unrestrained web activity exposes organizations to a variety of security and business risks, including threats from security breaches, potential data loss, and potential lack of compliance [20].

URL filtering compares all web traffic against a URL filter database and allows or denies access based on the information in the filter database [20]. The filtering method consists of creating a URL profile specifying each action and policy type for that specific URL Category. These categories are blocked sites, allowed sites, defined IT policies, and blocked or allowed URL filters [22]. Defined IT categories are policies that will enable users to visit certain websites at a particular time [22]. The blocked or allowed URL filters category is where an organization doesn't determine access to a specific site but defines the categories for these sites. For instance, an organization can create a category where the site is accessible, but it might be distracting to users, or even sites that are questionable to provide access [22].

There are two types of URL filtering databases, local databases, and cloud databases. Local database lookups have a list of frequently accessed websites that ensure maximum performance and minimal latency [21]. While cloud database lookups support coverage for the latest sites and can be updated in real-time, organizations always have an updated record of what areas they should be allowing or blocking [22]. URL filtering encourages employees to be more productive by blocking access to distracting sites and preventing them from being attack victims.

D. Application Controls

Application controls are a type of security that protects endpoint devices by recognizing the difference between safe listed files and blacklisted files passing through an endpoint in a network [22]. To implement application controls, users need to identify what have approved applications and implement control rules to ensure that only authorized applications can run. The ways to maintain application control rules are using a management program and frequently updating application control rules to protect systems from newer vulnerabilities [24]. Application controls are significant because they were primarily

designed to prevent the download and spread of malicious threats and prevent the installation and use of unapproved applications within an organization.

Windows 10 and above users can download and use application control software. WDAC (Windows Defender Application Control) was released with Windows 10, allowing businesses to control drivers and applications required to run on their windows clients [25]. In addition to WDAC, Windows released a feature called AppLocker, which helps prevent end users from running unauthorized software on their computers. However, this security feature did not meet the servicing criteria to be considered as a security feature. You can deploy AppLocker to complement WDAC and add per-user or per-group shared device rules. Some of these rules prevent some users from running certain apps and allow some users the freedom to run apps [25]. Windows recommend the best practice to enforce WDAC at the strictest level possible for your organization and use AppLocker to lock down restrictions [25] further.

E. Network Access Controls

A network security Network Access Control (NAC) to keep unapproved users and machines away from private networks. NAC is important for endpoint security defense because an increasing number of non-corporate devices connecting to the internet. For example, employees that bring their own devices and connect to corporate networks or employees bring corporate devices home. NAC ensures also the protection of vendors, visitors, and contractors connecting to the corporate network [26].

Essential NAC functionality restricts network access to specific users and areas of the network. NAC also prevents unauthorized access to data through limiting employee's access to the corporate intranet with data restriction [26]. NAC blocks access from endpoints that are not compliant with corporate security and prevents malicious code or programs from entering the network from external endpoints.

Pre-admission, and post-admission are two basic types of NAC. Pre-admission security happens before granting network access to a user. The device or user access permitted if they follow the security policies [26]. A post-admission NAC happens after the user is already connected but wants to enter a secure part of the network. Post-admission NAC would determine whether these specific endpoints would have significant roles in accessing resources or not.

F. Browser Isolation

Browser isolation is designed to keep your browsing activity safe by separating the process of loading a web page from its display [27]. Browser isolation loads web browser content and code away from the users, then executing the code on the user's device showing content. Loading the web browser content away from the user prevents potential malicious webpage code from running on a user's device. It contains risk to the networks to the endpoint is connected. There are three main types of browser isolation: Remote browser isolation, local browser isolation, and client-side browser isolation.

Remote Browser Isolation is shown below in figure 2. It employs the idea of browser isolation, but it runs the user's browsing activity on cloud servers controlled by the cloud provider and pushes the resulting web pages to the user's device so that the user can see web pages such as The difference is that you can display average [27]. In addition, to further protect an organization and its users, actions like clicking submissions, forms, and links are all transmitted to the cloud server. All loading and processing will be done to the cloud before displaying the output.

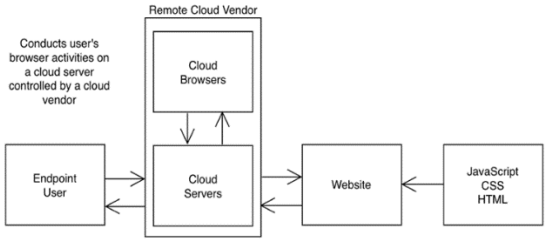

Figure 2: Remote Browser Isolation(Self drawn)

Local browser isolation works in the same way as remote browser isolation, but instead of running in the cloud, the function is performed on a server within your organization's private network. An example of an On-Premises Browser Isolation can be seen below in figure 3. Some organizations prefer this because it reduces latency compared to remote browser isolation. However, there are many downsides, like providing their servers dedicated to browser isolation, which is expensive. In addition, isolation occurs within an organization's firewall, making it more vulnerable to attacks because there is one less layer that attack must bypass, and on-premises browser isolation is difficult to expand on [27].

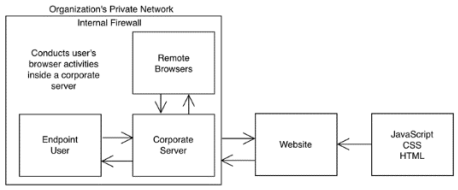

Figure 3: On-Premises Browser Isolation (self-drawn)

Client-side browser isolation works on user devices using virtualization and sandboxing. An example is shown in Figure 4 below. Virtualization is the process of dividing a computer into multiple virtual machines, one virtual machine does not affect the others [26].

Thus, browser isolation can happen by loading the code and processes on a virtual machine and displaying it on another virtual machine, securing the user's computer. Another way client-side browser isolation happens is through sandboxing. Sandboxing

is a malware detection tool to test malware and malicious files to check the activity [25]. So, Client-side browser isolation leverages this tool by using sandboxing to keep browser activity in a sandbox.

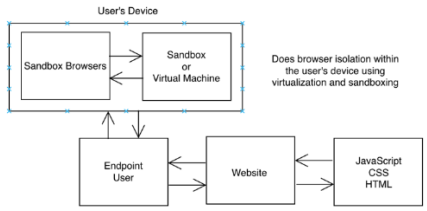

Figure 4: Client-Side Browser Isolation(self-drawn)

G. *Cloud Perimeter Security*

A network perimeter is the boundary between an organization's secure internal network and the Internet [28]. The network perimeter is the actual physical perimeter, and anyone trying to access this internal data must be inside the physical corporate building. Due to this, if an attacker tries to infiltrate the data, they will have to do so with the help of an internal employee.

However, with the introduction of the internet, more data was pushed online, this allows data to leave the corporate network and allow attackers to enter the network. With the advent of the cloud, employees can now access data and applications from anywhere, even over the insecure Internet rather than being in an organization's secure internal network.

Therefore, to protect data from these attackers, identity and access management (IAM) has become very important to control access to data and prevent data leakage [28]. With cloud perimeter security, identity has become the most critical factor in protecting data rather than location and device. IAM policies prevent any type of employee from accessing cloud data, create structure, and overall keep data more secure. As an example, Amazon Web Services (AWS) provides an employee's IAM policies within Amazon S3 (Amazon infinity scaling database). The employee's IAM policies allow the user to store objects in directories and enable them to get an object from the guide [29].

IV. VENDORS

Commercial vendors offer various endpoint security protections. McAfee's MVISION Endpoint Security, CloudStrike Falcon Platform, and ESET Endpoint Protection Platform are special endpoint security software.

McAfee's MVISION endpoint security platform explains how we use the five pillars of our endpoint security platform to deliver unique proactive threat intelligence and countermeasures across the entire attack lifecycle. These five pillars include: Prevent, Detect, Investigate, Response, and Manage Attack Surface. Each of the pillars has safety precautions if an attack is detected.

To manage attack surfaces, organizations must configure specific and unique risk profiles based on the organization's structure. McAfee allows users to manage attack surfaces using their MVISION Insight which gives options on what threat campaigns organizations are most susceptible to and what individual security can be used to combat the threat. The management of attack surface as the first line of defense provides threat intelligence, unique risk profiles, and prioritizing steps to protect against threats [30] proactively.

The protection pillar is used to leverage advanced remediation and dynamic application containment techniques to protect against ransomware, grayware, and credential theft attacks [30]. Post protects against attacks by instantly responding to threats to close security gaps, detecting and protecting against fileless and script-based attacks, and enabling machine learning behavior to detect zero-day threats in near-real time. can be [30]. This pillar prevents threats from infiltrating the organization and causing more profound problems.

The detection pillar is used to quickly detect and respond to APT (advanced persistent threat) with integrated EDR (endpoint detection and response) controls. Using the integrated EDR controls, there will be less alert fatigue (frequent and repetitive alerts that fatigues the IT staff). As a result, there will be a reduction in mean time response allowing the increase in detection of attacks and ultimately stopping them from achieving their objectives [30]. The protection pillar also explains how their MVISION EDR software can capture real-time data, objects, and system changes. The detection in the software gives the user many tools to detect and mitigate future threats.

The investigation pillar uses McAfee's open XDR capabilities, such as making better and accelerate decision-making with automated investigations leveraging data analytics correlations prioritizing threats, predicting assessments, and having proactive responses better to protect the system and organization [28]. Using XDR simplifies complex workflows and contains threats more efficiently. McAfee XDR in the investigative pillar can deliver total visibility and control across every attack vector. As a result, McAfee's XDR is useful for its proactive, data-aware, and open XDR software.

Response columns provide users with proactive and dynamic investigative guidance to adapt to each case [30]. In addition, the respond pillar can contain and stop threats across endpoints in real-time, lessening the overall damage. If a system has been hit with ransomware, files are all encrypted or damaged. McAfee's response to this would be to use enhanced remediation, which restores files that have been damaged and decrypts any encrypted files as well and destroys the ransomware.

CrowdStrike Falcon provides many of the protections MacAfee has, like XDR and EDR, but CrowdStrike highlights its technology with next-gen antivirus, firewall management, and device control. CrowdStrike says its next-generation cloud-native antivirus protects against all kinds of attacks, from malware to other advanced attacks, even offline [31].

In addition to next-gen antivirus, CrowdStrike Falcon uses firewall management to protect network security. Falcon's firewall management creates, enforces, and manages policies with a simple, centralized approach [30]. As a result, Falcon can defend against network threats and gain instant visibility to enhance protections and inform action. Unique protection that CrowdStrike Falcon provides is device control, which limits risks associated with USB devices. Device control provides insights and rules required to enable the safe usage of USB devices across the organization [11]. Device control also gains complete visibility on how USB devices are used in the environment and if they follow the organization's policies.

ESET stands out with its multilayered protections, cross-platform support, unparalleled performance, and worldwide presence. ESET's technology is powered by ESET LiveGrid, machine learning and human expertise. ESET LiveGrid is a cloud-based anti-malware system. Every time a zero-day threat like ransomware is detected, the threat is published and its behavior is monitored [17]. In addition, this exposure is spread across all endpoints within the system in a short amount of time without needing updates. The second technology ESET uses is machine learning. Machine learning uses a combination of neural networks and handpicked algorithms to correctly flag incoming programs and code as potentially unwanted or malicious [17]. The final technology ESET uses is human expertise. ESET states that they have world-class security researchers that share their expertise to make sure users advantages from optimum, round-the-clock threat intelligence [17].

Although these three technologies are fundamental to ESET's endpoint security, some features are vital to protecting a system. These features include ESET exploit blocker, which focuses on monitoring and blocking exploitable threats within applications like browsers, emails, and document readers [17], In-Product Sandbox, which identifies the real behavior hidden in threats in an isolated virtualized environment, and an UEFI scanner that checks and enforces pre-boot environment security and monitors firmware integrity [17]. These different types of endpoint security vendors all have special protection that makes them stand out from their competition. Users may prefer an endpoint security platform more than another because it fits their organization's architecture and benefits them more. Table 1 below highlights the comparative analysis of the products with respect to the security mechanisms discussed in the previous section II and section III.

TABLE 1. VENDORS COMPARATIVE ANALYSIS[19],[23],[32]

Products Comparative Analysis		
Vendors (VI)	***ENDPOINT ATTACKS AND DEFENCES (II)***	***ENDPOINT PROTECTION (III)***
McAfee	A, B, C, D	A, B, C, D, E
CloudStrike	A, B, C, D	A, B, C, D, E
ESET	A, B, C, D, E	A, B, C, D, E, F, G

V. CONCLUSION

Endpoint Security is securing entry points of user devices such as desktops, laptops, IoT devices, and any other devices that malicious actors might exploit. Endpoint Security is an essential factor in an organization's security protections because it ensures that sensitive data and leakage are protected from different types of attacks such as malware, phishing, ransomware, and other cyberattacks on the network and cloud. By knowing different kinds of endpoint attacks, users can prepare and be proactive in preparing for these attacks. In addition, knowing the different types of protections in endpoint security will allow the users to implement correct protections for their specified needs in the organizations. Endpoint security will continue to be a critical layer in cybersecurity because it deals with numerous avenues a threat actor can infiltrate a system. These avenues will continue to increase due to the increasing number of people working and the increasing number of endpoint devices they bring onto the corporate network. Endpoint security plays a vital role in protecting an organization's security.

References

[1] *What is an Endpoint?* (2022). Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/what-is-an-endpoint (last accessed 6/29/2022)

[2] Brickley, J. C., Thakur, K., & Kamruzzaman, A. S. (2021). A Comparative Analysis between Technical and Non-Technical Phishing Defenses. *International Journal of Cyber-Security and Digital Forensics*.10(1), 28-41

[3] Dudeck, R. (2022). *How to Defend Against Sophisticated Endpoint Attacks* [Review of *How to Defend Against Sophisticated Endpoint Attacks*]. World Wide Tech. https://www.wwt.com/article/endpoint-protection-crash-course (last accessed 6/29/2022)

[4] Brickley, J. C. & Thakur, K.(2021). Policy of Least Privilege and Segregation of Duties, their Deployment, Application, & Effectiveness. *International Journal of Cyber-Security and Digital Forensics*.10(1), 10(4): 112-119

[5] Trellix. (2022). *What Is Endpoint Antivirus?* [Review of *What Is Endpoint Antivirus?*]. Trellix. https://www.trellix.com/en-us/security-awareness/endpoint/what-is-endpoint-antivirus.html#:~:text=Endpoint%20Antivirus%20is%20a%20type,%2C%20bots%2C%20trojans%20and%20more (last accessed 6/29/2022)

[6] CISA. (2021). *RansomwarenGuide* [Review of *RansomwarenGuide*]. CISA.gov; CISA. https://www.cisa.gov/stopransomware/ransomware-guide (last accessed 6/29/2022)

[7] Imperva. (2020). What Is Phishing: Attack Techniques & Scam Examples: Imperva [Review of What Is Phishing: Attack Techniques & Scam Examples: Imperva].

Imperva.com. https://www.imperva.com/learn/application-security/phishing-attack-scam/ (last accessed 6/29/2022)

[8] CrowdStrike. (2020). *WHAT IS A ZERO-DAY EXPLOIT?* [Review of *WHAT IS A ZERO-DAY EXPLOIT?*]. CrowdStrike.com. https://www.crowdstrike.com/cybersecurity-101/zero-day-exploit/ (last accessed 6/29/2022)

[9] Imperva. (2020). *Zero-day (0day) exploit* [Review of *Zero-day (0day) exploit*]. Imperva.com. https://www.imperva.com/learn/application-security/zero-day-exploit/ (last accessed 6/29/2022)

[10] Kaspersky. (2022). *What Is a Drive by Download* [Review of *What Is a Drive by Download*]. Kaspersky.com. https://www.kaspersky.com/resource-center/definitions/drive-by-download (last accessed 6/29/2022)

[11] Crowd Strike. (2022). *Falcon Device Control for Endpoints & USB Security: CrowdStrike* [Review of *Falcon Device Control for Endpoints & USB Security: CrowdStrike*]. CrowdStrike.com. https://www.crowdstrike.com/products/endpoint-security/falcon-device-control/ (last accessed 6/29/2022)

[12] Mcafee. (2013). Watering Hole Attacks: Protecting Yourself from the Latest in Cyber Attacks [Review of Watering Hole Attacks: Protecting Yourself from the Latest in Cyber Attacks]. Mcafee.com. https://www.mcafee.com/blogs/enterprise/cloud-security/watering-hole-attacks-protecting-yourself-from-the-latest-craze-in-cyber-attacks/ (last accessed 6/29/2022)

[13] ProofPoint. (2022). *Watering Hole Attack* [Review of *Watering Hole Attack*]. Proofpoint.com. https://www.proofpoint.com/us/threat-reference/watering-hole (last accessed 6/29/2022)

[14] Arm. (2022). *What Are IoT Devices?* [Review of *What Are IoT Devices?*]. Arm.com. https://www.arm.com/glossary/iot-devices (last accessed 6/29/2022)

[15] McAfee. (2022). *Protecting the Internet of Things* [Review of *Protecting the Internet of Things*]. McAfee.com. https://www.mcafee.com/enterprise/en-us/assets/solution-briefs/sb-protecting-the-internet-of-things.pdf. (last accessed 6/29/2022)

[16] Paloalto Networks. (2022). IoT Security – What is It and How Does It Protect Your IoT Devices [Review of IoT Security – What is It and How Does It Protect Your IoT Devices]. Www.paloaltonetworks.com. https://www.paloaltonetworks.com/cyberpedia/what-is-iot-security (last accessed 6/29/2022)

[17] ESET. (2020). *Powerful Multilayered Protection for Desktops* [Review of *Powerful Multilayered Protection for Desktops*]. ESET.com. https://www.eset.com/fileadmin/ESET/INT/Products/Business/Endpoint/Endpoint/EES-Windows/v09/ESET_Endpoint_Solutions_Product_Overview.pdf. (last accessed 6/29/2022)

[18] Trellix. (2022). *What Is Endpoint Antivirus?* [Review of *What Is Endpoint Antivirus?*]. Trellix.com. https://www.trellix.com/en-us/security-awareness/endpoint/what-is-endpoint-antivirus.html (last accessed 6/29/2022)

[19] ESET, (2022) https://www.eset.com/us/ (last accessed 11/20/2022)

[20] TrendMicro. (2021). *IOT Security Issues, Threats, and Defenses.* [Review of *IOT Security Issues, Threats, and Defenses.*]. TrendMicro.com. https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/iot-security-101-threats-issues-and-defenses. (last accessed 6/29/2022)

[21] Paloalto Networks. (2022). *What is URL Filtering?* [Review of *What is URL Filtering?*]. Paloaltonetworks.com. https://www.paloaltonetworks.com/cyberpedia/what-is-url-filtering#:~:text=URL%20filtering%20limits%20access%20by,sites%20such%20as%20phishing%20pages. (last accessed 6/29/2022)

[22] Fortinet. (2022). *What is URL Filtering?* [Review of *What is URL Filtering?*]. Fortinet.com. https://www.fortinet.com/resources/cyberglossary/what-is-url-filtering#:~:text=Uniform%20Resource%20Locator%20(URL)%20filtering,content%20that%20employees%20can%20access. (last accessed 6/29/2022)

[23] McAfee Endpoint Security, (2020) https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-endpoint-security.pdf (last accessed 11/20/2022)

[24] Cyber.gov. (2020). *Implementing Application Control.* [Review of *Implementing Application Control.*]. Cyber.gov. https://www.cyber.gov.au/acsc/view-all-content/publications/implementing-application-control. (last accessed 6/29/2022)

[25] Microsoft. (2020). *WDAC and AppLocker Overview - Windows Security* [Review of *WDAC and AppLocker Overview - Windows Security*]. Microsoft.com. https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/wdac-and-applocker-overview. (last accessed 6/29/2022)

[26] VmWare. (2022). *What Is Network Access Control?: Vmware Glossary* [Review of *What Is Network Access Control?: Vmware Glossary*]. Vmware.com. https://www.vmware.com/topics/glossary/content/network-access-control.html (last accessed 6/29/2022)

[27] Cloudfare. (2022). *What is browser isolation?* [Review of *What is browser isolation?*]. Cloudfare.com. https://www.cloudflare.com/learning/access-management/what-is-browser-isolation/ (last accessed 6/29/2022)

[28] Cloudfare. (2022). *What is the network perimeter?* [Review of *What is the network perimeter?*]. Cloudfare.com. https://www.cloudflare.com/learning/access-management/what-is-the-network-perimeter/. (last accessed 6/29/2022)

[29] msp360. (2022). AWS Security In-Depth Part 2: Basics of IAM Policies [Review of AWS Security In-Depth Part 2: Basics of IAM Policies]. Msp360.com. https://www.msp360.com/resources/blog/aws-iam-policy/. (last accessed 6/29/2022)

[30] McAfee. (2020). *Endpoint Security: Trellix* [Review of *Endpoint Security: Trellix*]. Mcafee.com. https://www.mcafee.com/enterprise/en-us/solutions/mvision-endpoint-security.html. (last accessed 6/29/2022)

[31] Crowd Strike. (2022). *Falcon Prevent: Cloud-native Next-Generation Antivirus (NGAV)* [Review of *Falcon Prevent: Cloud-native Next-Generation Antivirus (NGAV)*]. CrowdStrike.com. https://www.crowdstrike.com/products/endpoint-security/falcon-prevent-antivirus/ (last accessed 6/29/2022)

[32] CrowdStrike Falcon® Prevent: Cloud-native Next-Generation Antivirus (NGAV), (2022) https://www.crowdstrike.com/products/endpoint-security/falcon-prevent-antivirus/ (last accessed 11/20/2022)