Managing and Supporting Endpoint Security Operations with Advanced Technical Solutions

Mohammed Mustafa Khan

Abstract

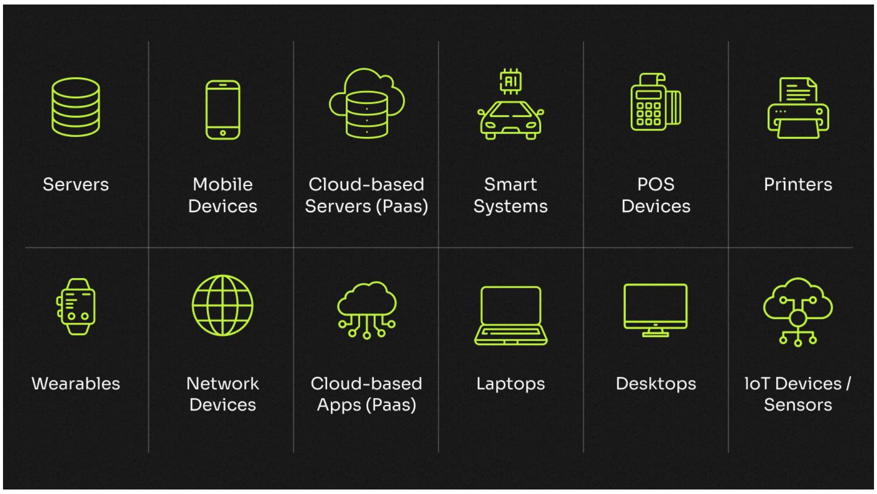
Keeping your business protected from cyber threats is a tremendous aspect, more so when it pertains to endpoint devices that connect to the corporate network in today's digital economy. Cybercriminals aim to hijack the endpoint devices by subjecting them to malicious activity that can infiltrate and gain unauthorized access to the system and modify, steal, or even delete data for their interest. Data has become a shared resource in many organizations via various endpoint devices. Endpoints are prone to attacks. The establishment of endpoint security operations has become a non-negotiable initiative since endpoints have become a fundamental component of an organizational system. The range of endpoint devices used by organizations today is likely all of them come from different manufacturers. Some contain bugs and flaws which can be easily exploited. As the number of endpoints continues to grow, organizations face increasing risks of cyber threats. This paper discusses the management and support of endpoint security operations with advanced technical solutions.

Keywords: Endpoint security, Attacks, endpoints

1.0 Introduction

In the contemporary business environment, corporate data is an indispensable asset and critical element that powers economic growth. The most profitable industry creates, collects, stores, and secures information like intellectual property creating a competitive advantage. Endpoint devices including servers, workstations, laptops, and tablets store this information. Data has become a primary target for attackers. This has led to the establishment of endpoint security operations which is a subset of cybersecurity that protects endpoints from exploitation by attack vectors. An endpoint is any device connected to a network and performs duplex communication thus carrying information from one point to another. Endpoint devices are the gateway for data breaches. Ponemon reports that in 2020, the average cost of data breaches was $8.64M. The agency also outlines that it takes almost 280 days for institutions to identify and contain data breaches [1]. The more time it takes to remediate the security breach event the more lateral damage and disruption it will cause to organizations. There are various pain points from the report that eloquently demonstrate the need to manage and support endpoint security operations with advanced technical solutions. This paper provides an overview of endpoint security operations, the need for managing and supporting endpoint security operations, and different types of endpoint security solutions. Additionally, the paper is centred on different approaches used to manage and support the Integrity of Endpoint Security Operations.

Diagram showing Various Endpoint Devices



2.0 Literature Review

Organizations continue to rely on diverse and distributed endpoint devices necessitating endpoint security operations to be part and parcel of cybersecurity. Arfeen et al. (2023) conducted a research study on the frequency of how endpoint devices are susceptible to malicious attacks and found that endpoint devices were the entry point of cyber threats. Additionally, Ponemom surveyed how users are addicted to their mobile devices, the report revealed that 73% of the mobile users were addicted to their devices. The importance of protecting these endpoints is demonstrated by the ever-evolving number of intelligent threats like advanced persistent threats and ransomware that have a normalcy of exploiting weaknesses in endpoint protection.

Data is sprawling at an accelerated pace. Techniques for processing and analyzing data are critical for ensuring endpoint security operations. The adoption of artificial intelligence and machine learning to support big datasets and detect anomalies has provided a window of opportunities for endpoint security solutions. Research performed by Reddy Maddireddy & B. (2021) shows how machine learning algorithms can discover patterns in network traffic that may signal an intrusion. Additionally, the authors demonstrated the adaptive nature of AI technology in the enablement of instant response to emerging threats without human intervention.

3.0 Overview of Endpoint Security Operations

3.1 Meaning of Endpoint Security Operations

Endpoint security operations comprise hardware, software, and processes that protect endpoint devices used by corporations and employees from cybersecurity threats. Common examples of endpoint devices include the following: desktop computers, laptops, tablets, smartphones, servers, printers, workstations, ATM machines, medical devices, and Internet of Things (IoT) devices [11]. Endpoint security operations involve employing security methodologies, measures and techniques like intrusion detection systems, zero trust approach, and monitoring solutions like SIEM tools to mention a few to discover and respond to vulnerabilities and attacks at the endpoint individual level.

3.2 Reason for Managing and Supporting Endpoint Security

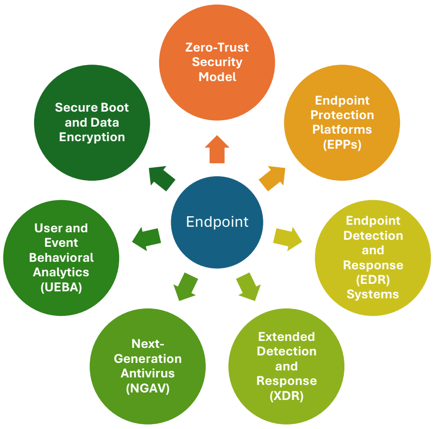
End-user devices and applications are the driving factors that enable corporate communication via corporate networks across organizations. Endpoints are the notorious access points for cyber-attacks. These end devices have become primary targets for hackers whereby they launch sophisticated attack vectors to intercept the data that resides, transmitted or data that is in use by these devices [11]. As organizations are modernizing their on-premise environment and shifting to the cloud, it has enabled employees to work remotely and even the executives to access company data anywhere, anytime. Bring Your Own Device technology has been embraced by various organizations exposing the company data to a wide attack surface. Endpoint devices act as the entry point for attackers and thus must be managed and supported adequately to prevent common attacks including ransomware, phishing, malware, and all other attacks outlined in OWASP top 10.

3.3 Cybersecurity Landscape

The cybersecurity landscape is ever-evolving, with new security threats emerging that target endpoints. These threats include ransomware, phishing attacks, and zero-day exploits, each generating unique challenges for security teams. Ransomware attacks, for instance, can encrypt critical data on endpoints, demanding a ransom for its release, while phishing attacks trick users into revealing sensitive information or downloading malicious software. Zero-day exploits take advantage of vulnerabilities in software that are unknown to the vendor, making them difficult to defend against [1]. The rise of remote work that rose during the COVID-19 pandemic and the widespread use of personal devices for business purposes bring your own device have further complicated endpoint security, as organizations must now secure a more diverse and distributed range of devices. The growth of IoT devices that tend to lack powerful security features and organizations using different endpoints from various vendors rendering management of endpoint ambiguous adds another layer of complexity to endpoint security operations.

4.0 Advanced Technical Solutions for Endpoint Security Operations

General Endpoint Security Tools


Zero-Trust Security Model
Endpoint Protection Platforms (EPPs)
Endpoint Detection and Response (EDR) Systems
Extended Detection and Response (XDR)
Next-Generation Antivirus (NGAV)
User and Event Behavioral Analytics (UEBA)
Secure Boot and Data Encryption
Endpoint

4.1 Zero-Trust Security Model

The entire value chain such as employees, business partners, stakeholders and suppliers access the company data using multiple devices from distributed and remote locations. This poses cybersecurity challenges to the internal endpoint devices. Remediation of these risks is very simple and easy. Security teams need to implement the Zero-trust technique. This framework works on the principle of trusting nothing and verifying everything [5]. Every access activity that is occurring must be verified, starting from the applications trickling down to the user by monitoring the data sources accessed by applications or a user. Zero-trust approach ensures there are no policy violations by ensuring the right user, has the right access to the company data for the right reasons. Additionally, it is a proactive technique that supports real-time threat detection thus minimising damage before lateral spread. The capabilities of the zero-trust security model are multi-factor authentication, micro-segmentation and continuous monitoring.

For instance, back in July 2020, a Twitter hack erupted. The attackers capitalized on weak security measures to gain unauthorized access to high-profile accounts and manipulated other users through social engineering [9]. The hacker tricked individuals into sending them Bitcoins and to be refunded doubled amidst COVID COVID-19 pandemic. The hacker walked away with $120, 000 worth of Bitcoin. Accounts that were scammed included Bill Gates, Joe Biden, and Elon Musk. This scenario indicates the crucial requirement of employing multi-factor authentication as a feature of the zero-trust security model.

4.2 Endpoint Protection Platforms (EPPs)

Comprises of antivirus, antimalware, personal firewalls, and host-based detection and prevention systems (IDPS) that provide effective security solutions to remediate threats [10]. Additionally, EPPs provide data encryption to secure vital information that resides at endpoints. The personal firewalls protect the ports from executing malicious programs that may lead to data breach events. The host-based IDPS monitors the features of a host and the events happening with the host and blocks any unusual activity. EPPs can be incorporated with other security systems in an organization to provide collective effort in managing and containing cyber threats. EPPS features include data loss prevention, threat prevention, and device control.

4.3 Endpoint Detection and Response (EDR) Systems

Traditional security mechanisms cannot identify and address the advanced cyberthreats, this is where the EDR systems come into play. EDR systems do not use the traditional method of signature-based mechanisms to detect and respond to threats. EDR systems are designed with superior technologies such as machine learning, and artificial intelligence that use behavioural analysis to discover anomalies that may indicate security breaches [10]. EDR systems are used to countermeasure sophisticated tactics like the Advanced Persistent Threats Attack Vectors. It is applied at the individual level of an endpoint device. EDR can aid detect even the most minute modifications in files, networks and registries that aid security teams disclose malicious activity masked that plain eyes cannot see.

4.4 Extended Detection and Response (XDR)

XDR extends EDR capabilities. XDR solution integrates data from heterogeneous sources including email, servers, network, and cloud security stores the data analyses and correlates the data to provide advanced threat detection. Just like the EDR systems, XDR uses machine learning and artificial intelligence to carry out predictive analytics that correlate security data and discover complex attack patterns. It provides real-time detection of cyber threats and utilizes playbooks to provide reports. Additionally, it has a centralized management dashboard that provides a high level of visibility to threat actions [10]. EDR solution makes a world of difference in remediating the modern cybersecurity threats.

4.5 Next-Generation Antivirus (NGAV)

The Next-Generation Antivirus solution has immense capabilities of preventing all types of attacks by maximizing the use of neural networks to detect and respond to unknown and known attacks. The solution comprises machine learning, artificial intelligence, and behavioural analytics [12]. It monitors and reacts to techniques, tactics and procedures used by attackers. NGAV is different from other solutions because does not utilize the traditional signature-based mechanisms of identifying attacks using signatures. The solutions can block both malware and non-malware attacks. NGAV solution depends on a cloud-based infrastructure. It can be deployed in different environments including on-premises or cloud platforms.

4.6 User and Event Behavioral Analytics (UEBA)

UEBA utilizes machine learning algorithms, behavioural analytics, and deep learning to inspect the behaviour of users and endpoints on a corporate network [12]. It discovers the unusual behaviour, inspects if it has security issues and alerts the security team. This solution provides a mechanism for detecting insider threats. anyone can be an insider including employees, and vendors may have access to admin passwords and gain access to sensitive company data. Insider threats are difficult to discover and even harder to contain because they have multiple touchpoints. It can only detect once a user starts executing their actions, for instance, if a user downloads 4GB of files who had a normalcy of downloading 50MB, UEBA treats this activity as an anomaly and blocks its operations or notifies the security team depending on the policy that was configured.

4.7 Secure Boot and Data Encryption

Rootkits and boot-time threats can be prevented by ensuring the boot process of endpoint devices utilizes trusted software from the vendor [8]. To accomplish a secure boot process, Unified Extensible Firmware Interface (UEFI) functionality must be enabled since it ensures the computer or servers boots only on trusted software applications and also eliminates any bugs that are embedded in an application. UEFI is superior to BIOS (Basic Input Output System) pertaining to security defense against threats and also UEFI performs faster than BIOS. Additionally, Full Disk Encryption which is a combination of the BitLocker with Trusted Platform Module (TPM 2.0) provides maximum protection of data in drives. These technologies must be implemented to ensure any authorized access cannot tap the data stored in hard disk drives.

5.0 Best Practices for Endpoint Security

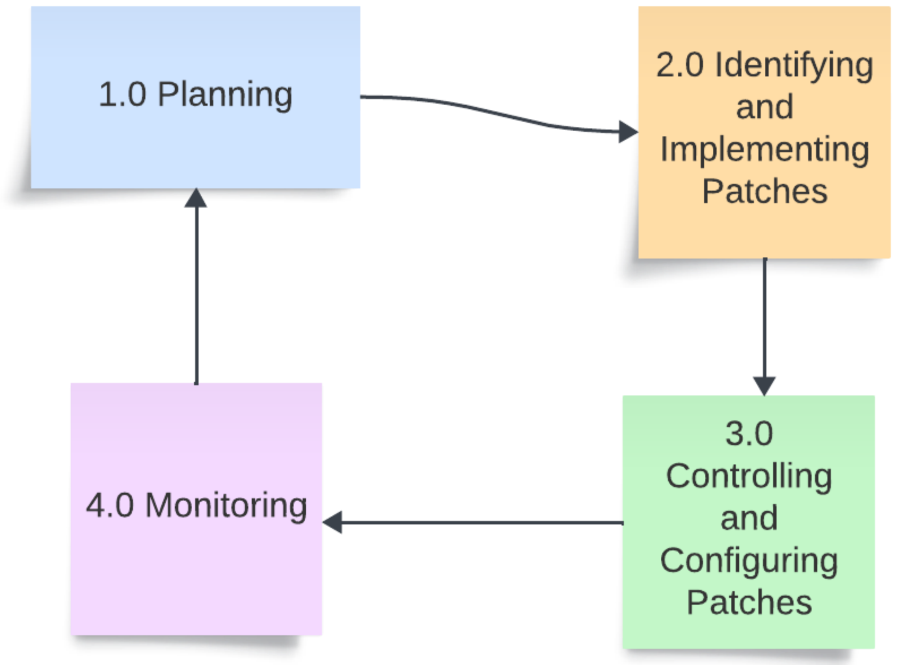
5.1 Employee Training and Awareness

Employees need to be trained on the organizational and regulatory standards that manage endpoint security operations. Advocacy programs such as training employees to create awareness may aid in avoiding clicking suspicious email attachments and avert themselves from social engineering schemes such as phishing [11]. Additionally, training imparts and disseminates knowledge to employees thus inducing employees with the capability of correctly applying their own judgement. IT security teams need to create a regular training program that ensures consistent knowledge sharing across the organization. a study conducted by Ponemon reports that 59% of respondents articulate threat sharing enhances the cyber resilience of organizations. Sharing security breaches during this training program will boost the security posture of endpoint devices.

5.2 Software Patching

The threat landscape is dynamic and keeps evolving with sophisticated techniques. Institutions need to embrace changes at an accelerated pace to get ahead of cyber threats. One way of staying ahead of the game is by ensuring software patches are implemented diligently. It is imperative to keep all the software updated since it aids in minimizing the risk of security breaches [6]. In May 2017, a ransomware attack named WannaCry exploited a vulnerability in Microsoft Windows that was running on an older version [7]. Companies like Telefonica and FedEx were disrupted with over 200, 000 computers worldwide. The detrimental effects of the ransomware disrupted services. The ransomware would have been remediated by patching the software diligently. Security teams should adopt an effective patching of software programs. Components such as drivers, operating systems, third-party applications, and firmware must be patched with the latest security updates.

Figure showing the process of Patching a Software


1.0 Planning
2.0 Identifying and Implementing Patches
3.0 Controlling and Configuring Patches
4.0 Monitoring

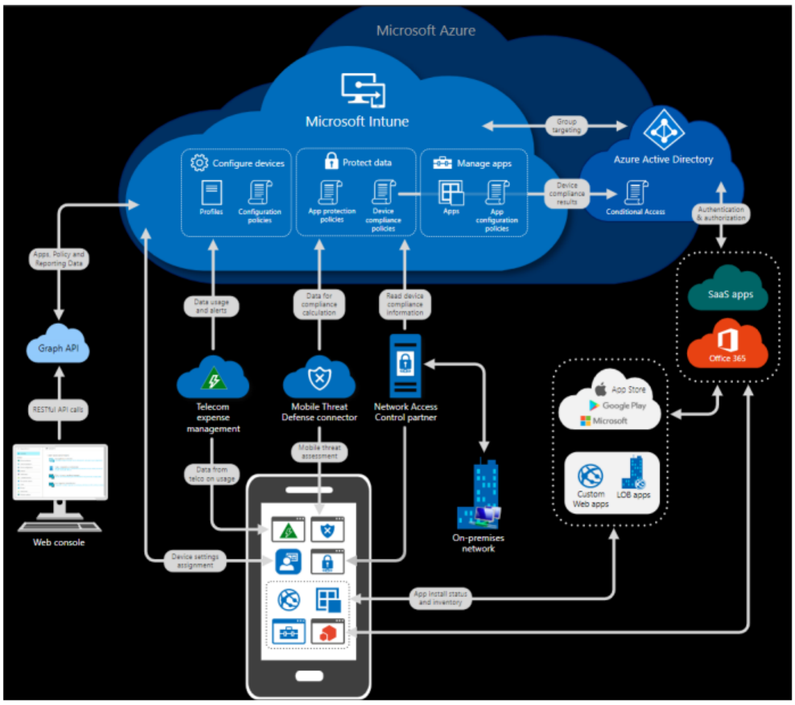
5.3 System Hardening

The purpose of system hardening is to lower security risks by eliminating potential points of attack and minimizing the attack surface of the system [8]. It helps in managing the endpoint security. System hardening involves a number of techniques to ensure the endpoint security best practices are met. It includes disabling unnecessary services and ports that are not in use, application of the least privilege framework and configuration of security settings as per the manufacturer's manual. System hardening makes it tough and strenuous for attackers to discover and exploit weaknesses inherent in systems.

5.4 Control the Endpoints using Dashboards

Institutions have many endpoint devices and managing individual devices always becomes a bottleneck to the IT security team. Centralizing the management of endpoints is the premier foundation because it aids in overseeing all the devices and simplifies management using a single interface. Normalizing the use of a cloud-native approach combined with technologies like Intune and Entra enables IT teams to gain effective control of all the endpoints in distributed departments and also branch offices [4]. The security operation teams can set conditional access for each device by creating different policy groups and associating each device with the specified policy group. One example of the policy rule that can be enforced is that compliant devices only access the company data. This policy will bar any devices that do not meet the compliance threshold not to accessing the company data. Additionally, granular management via role-based access control in Intune and Entra ID will validate the endpoints have the right access to the company data. The sign-in logs and audit trails are also centralized which allows a formidable track of all actions and access across the network.

Diagram Showing the Architecture of Microsoft Intune



6.0 Conclusion

Endpoint security is a dynamic field, demanding continuous adaptation. No one solution can address the attack vectors appropriately, thus organizations ought to combine some solutions to secure endpoints. Organizations must embrace advanced technical solutions, collaborate, and prioritize visibility. Institutions can effectively manage and support endpoint security operations by combining advanced technical solutions. It is crucial to be cognizant of the fact that the battle against cyber threats is continuous, but with the right tools and technologies, institutions can fortify the endpoint security operations.

7.0 Reference

1. “Home,” *Ponemon Institute*, 2023. https://www.ponemon.org/
2. A. Arfeen, S. Ahmed, M. A. Khan, and S. F. A. Jafri, “Endpoint Detection & Response: A Malware Identification Solution,” *2021 International Conference on Cyber Warfare and Security (ICCWS)*, pp. 1–8, Nov. 2021, doi: https://doi.org/10.1109/iccws53234.2021.9703010.
3. B. Reddy Maddireddy and B. Reddy Maddireddy, “Enhancing Endpoint Security through Machine Learning and Artificial Intelligence Applications.” 2021 December Available: https://redc.revistas-csic.com/index.php/Jorunal/article/download/226/190
4. D. Adame, “CSUSB ScholarWorks CSUSB ScholarWorks Electronic Theses, Projects, and Dissertations Office of Graduate Studies 8-2021 MANAGING AND SECURING ENDPOINTS: A SOLUTION FOR A MANAGING AND SECURING ENDPOINTS: A SOLUTION FOR A TELEWORK ENVIRONMENT TELEWORK ENVIRONMENT.” Available: https://scholarworks.lib.csusb.edu/cgi/viewcontent.cgi?article=2454&context=etd
5. P. Pönkänen, “Zero Trust Guidelines for Enterprises,” *www.theseus.fi*, Jun 2023. https://www.theseus.fi/handle/10024/802983

6. Wang, “AI-Enhanced Software Vulnerability and Security Patch Analysis - ProQuest,” *Proquest.com*, April 2023. https://www.proquest.com/openview/5e48ca64cbe4663debaae815aecde43c/1?pq-origsite=gscholar&cbl=18750&diss=y (accessed Aug. 10, 2024).
7. “Indicators Associated With WannaCry Ransomware | CISA,” *Cybersecurity and Infrastructure Security Agency CISA*, Jun. 07, 2018. https://www.cisa.gov/news-events/alerts/2017/05/12/indicators-associated-wannacry-ransomware
8. J. Wayburn, “System Hardening Guidelines: Critical Best Practices,” *Perception Point*, Sep. 21, 2021. https://perception-point.io/blog/system-hardening-guidelines-critical-best-practices/
9. P. Witman and S. Mackelprang, “The 2020 Twitter Hack -So Many Lessons to Be Learned,” *Research and Practice Journal of Cybersecurity Education, Research and Practice*, vol. 2021, no. 2, Feb. 2022, Available: https://files.eric.ed.gov/fulltext/EJ1332789.pdf
10. T. Lewis, “Endpoint Defense as Code (EDAC): Configurable Contextual Analysis of Process Behaviors From Kernel/User Event Tracing,” *Masters Theses & Doctoral Dissertations*, Feb. 2023, Available: https://scholar.dsu.edu/theses/427/
11. G. Maayan, “7 Tips to Boost Endpoint Security | IEEE Computer Society,” *IEEE Computer Society*, Dec. 16, 2019. https://www.computer.org/publications/tech-news/trends/7-tips-to-boost-endpoint-security
12. Sri Rupin Potula, Ramani Selvanambi, Marimuthu Karuppiah, and D. Pelusi, “Artificial Intelligence-Based Cyber Security Applications,” pp. 343–373, Jan. 2023, doi: https://doi.org/10.1007/978-981-99-2115-7_16.