REDEFINING ENDPOINT SECURITY THROUGH NEXT-GEN MONITORING TOOLS

***Raunak Choudhary, Parul Pachori, Nisha T N**

Symbiosis Centre for information Technology (SCIT), Pune , Symbiosis International (Deemed University), Pune, India , raunak.choudhary@associates.scit.edu

Symbiosis Centre for information Technology (SCIT), Pune , Symbiosis International (Deemed University), Pune, India , parul.pachori@associates.scit.edu

Symbiosis Centre for information Technology (SCIT), Pune , Symbiosis International (Deemed University), Pune, India , nisha@scit.edu

Abstract.

Over the years, both attacks and attack patterns got significantly changed. There is an inclusion of a massive number of unknown threats exposed for the first time, zero-day attacks being one of the best examples of that. Endpoints are most vulnerable to attacks, and are the primary target of attackers. To give Endpoint more security, various new tools and techniques evolved, like Next-gen antivirus solutions (EDR, XDR, etc.), which have artificial intelligence-enabled and will observe behavior rather than just signature. This, in a way, has redefined the way we approach Endpoint security. One of the significant aspects of endpoint security is the monitoring tools that analyze all the endpoints and other security assessment points available inside the organization. They provide various attack indicators, including the attack pattern, tactics and techniques used, source and target of the attack, impact and risk mitigation steps. Multiple sensors and other detectors provide alerts of different severity, and the monitoring team takes steps based on that. Artificial intelligence becomes crucial here as it studies the history of the attack source and the target system or network. This paper analyses and enumerates these new techniques which enables the next generation end point security. We also describe the way in which these technologies can be plugged together to provide better detection results.

Keywords. Endpoint security, Monitoring tools, Endpoint Detection and Response, Artificial intelligence.

1. INTRODUCTION

Cyber-attacks are constantly evolving in sophistication and scale, reaching such an extent that the World Economic Forum considers it the second most threatening risk for global commerce over the next decade.[1] Endpoint security is the process of guarding against dangerous threats and online attacks on gadgets like desktops, laptops, mobile phones, and tablets. Businesses may defend against cyber-attacks using endpoint security software to secure employee work devices on a network or in the cloud. A company network connects endpoints with each other, such as a computer to a printer, and with internal structures, such as servers, databases, intranets, and extranets [2]

The state-of-the-art protection provided by security staff is typically using multiple tools to monitor different parts of networked systems for security. While each of these tools may provide unique information, they suffer from drawbacks: (a) they provide information limited to a specific view of a network, (b) operators must develop expertise in multiple cryptic tools that change frequently, and (c) multiple tools do not currently provide cross-cues or fusion for events in complex environment. [3]

When we talk about AI-enabled monitoring tools, logs are at the center of research. They analyse the logs more quickly and provide an in-depth analysis of the attacks. Some widely used tools like Security information and event management (SIEM) and Endpoint detection and response (EDR) have already enabled AI in most engines. That has provided a positive response from their client, and soon it is going to be a practice in the industry.

2. LITERATURE REVIEW

Successful endpoint security demands a proactive information security system rather than a reactive one to create and run the management tools for endpoint security of different OS-based devices and mobile devices. Improvements are also be made to the information security lifecycle for "Policy" to configure an endpoint, "Real-time protection" technology to detect and filter malware, "Detection" to confirm the occurrence of abnormal symptoms or threats, and "Remediation" to deal with and recover from the actual damage.[4] Endpoint security attacks are becoming more frequent and deadly. Thus, businesses need to be ready for the shifting tides of vulnerabilities and exploits as well as potential crises and emerging threats. Endpoint security requires ongoing attention, resources, and planning; developing and executing endpoint security strategies are just the beginning.[5]

The research states that by detecting or even stopping many cyberattacks in their early stages, advanced pattern recognition and correlation algorithms are making their way into security systems, this in particular. This reduces the potential impact of these attacks. Adopting frameworks that are both explainable and comprehensible must go hand in hand with the tighter integration of artificial intelligence and machine learning into present EDRs.[6] The open-source EDR is a low-cost security solution with high predicted value in terms of flexibility, use, and scalability. It can be utilized in next-generation digital platforms that develop hyper-connectivity, hyper-intelligence, and global scale. For the first time, according to MITRE attack, attack detection, and coverage analysis were made possible in this investigation by open-source EDR. A few stages displayed a low detection rate due to insufficient query settings to identify each stage's specific threats.[7]

Many aspects were taken into account when analysing the actual effectiveness of EPP and EDR. The EDR success rate is a crucial factor to consider when deciding whether or not to use this product. EDR is preferable when there is a high likelihood of success and a low likelihood that the risk will result in paralysis. EPP is preferable, though, if anything is different and either of the two requirements is incorrect. The majority of EDR providers can promise high success rates in both detection and defence, and the business must fend off the attack. To ensure the safety and security of a corporation, we firmly advise taking into account both goods.[8]

The primary objective is to determine how the monitoring tools have redefined endpoint security. How the endpoint security is more secure now and how it can tackle some of the most critical threats. This will also focus on the reactive and proactive models of threats and their mitigation steps. Zero-day attacks, Top trending attack patterns will be a crucial area of

research. During cyber-attacks, the decision-making process and mitigation plan are the most critical steps, as quicker identification will result in lesser damage.

3. ENDPOINT SECURITY

3.1. What has changed in Endpoint Security?

Endpoint security is a technique to secure the organization's entry points of end-user devices against ever-evolving cyber threat attacks. Mobile phones, Desktops, laptops, tablets, and other network-capable devices are the primary endpoints being secured.

In the past, a server on the company's internal network was used to implement traditional endpoint protection. The endpoint server updates every network endpoint's installed endpoint software. The endpoint server not only sends endpoint updates but also serves as an authentication server, confirming connections outside and inside the network. How is endpoint security changing to tackle these threats, given the ongoing changes in the threat landscape and attack vectors?

The evolution of endpoint security over time and various trends that can be foreseen for the future will be examined in this paper. We will also examine certain endpoint security technologies and solutions and how they're affecting the way endpoint defensive mechanisms operate.

3.2. Moving from traditional antivirus to next-gen antivirus

Endpoint security has redefined itself throughout time, moving from conventional signature-based antivirus software to more sophisticated next-generation antivirus solutions that leverage sophisticated and automated technology, better endpoint detection and response, and the Operating System oriented Positive Security strategy.

Earlier, most endpoint security protection was provided by installing antivirus software, which was only as effective as its antivirus signatures. This had been the situation for as long as antivirus software had been used to defend endpoints. However, recently most things have changed, and malware is now capable of considerably more nuanced antivirus evasion. The endpoints need to be secured more effectively.

Traditional AVs had the significant drawback of requiring frequent virus signature updates, making them only as effective as their available updates. However, next-generation antivirus software introduced a method that made it possible to identify malware based on machine learning and artificial intelligence rather than signatures. This has become more prevalent in the last decade, and since then, it has grown significantly. Table 1 explains some of the major upgradation happened in NGAVs.

Even after the emergence of the Next-Gen Antivirus solution, there are still some concerns around endpoint security listed *below.*

1. Since NGAVs are only being educated on current malware, their inability to detect zero days and brand-new malware.
2. Inability to detect file-less malware since NGAVs can only perform static file analysis and are not signature-based.
3. The drawback of artificial intelligence is that attackers use it for bad purposes. Hackers using artificial intelligence, thereby rendering them ineffective, can create Malware that cleverly avoids NGAVs.

Table 1. DIFFERENCE BETWEEN TRADITIONAL AND NEXT-GEN ANTIVIRUS SOLUTION

Traditional Antivirus Solution	**Next-Gen Antivirus Solution**
Using Signature to identify the attacks.	Using behavior to identify the attacks.
Usually it relies on the hardware and that needs to be installed at the physical premises.	In this cloud-based solution is available where there is no need for hardware or software specifically.
Its focus is on detecting malicious activities at the endpoint alone.	It generally uses a larger variety of threats, which includes modern-day attack vectors.
Operational costs are high	Less operational costs
Unable to detect unknown threat as it uses only signature database to identify the attack.	Using the latest technology, it detects the anomaly of the file and thus able to cater unknown attacks too.

3.3. Emergence of Next-Gen Monitoring Tool

Monitoring tools play a vital role in detecting and responding to cyber incidents as they are the first line of defence for any organization. Endpoint detection and response(EDR) provides visibility into most of the problems left across by the antivirus solutions. Security departments can now use EDR solutions to perform console alerting and reporting, advanced response to security issues, expand geographic support over vast regions, manage detection and response, and one of the most crucial capabilities to date: third-party integration.

Security teams now have the insight they need to find problems that might otherwise go undetected due to EDR security solutions, which keep track of all endpoint, workload activity, and events. Continuous and thorough visibility into what is occurring on endpoints in real time must be offered by an EDR system. An EDR tool provides sophisticated threat detection, investigation, and response capabilities, such as alert triage, threat hunting, suspicious activity validation, incident data search, and suspicious activity validation.

Alongside EDR, there are multiple other technological advancements like XDR and MDR, which talks about the broader coverage of endpoint security. Not only do they provide

additional security features, but also they cover more attack surfaces too. An enterprise may proactively defend itself against cyber threats due to the next-generation cybersecurity technology XDR (Extended detection and response). It achieves this by giving unified visibility across the various attack channels that a cyber-threat actor might use to target an enterprise's network. A security-as-a-service option called MDR (Managed Detection and Response) was created as a replacement for an internal Security Operations Center (SOC). An MDR solution gives business access to the tools and security knowledge it needs to defend themselves against online attacks.

Security information and event management (SIEM) is yet another crucial monitoring tool that most organizations adopt. It provides visibility into entire systems and networks from a centralized dashboard which helps to detect and respond in a faster WAY. MACHINE learning and other AI-based approaches are used by next-generation SIEMs to speed up the identification of dangerous activities. This methodology of using advanced technology is known as User and Entity BEHAVIOUR Analytics (UEBA). This monitors every system activity to determine what constitutes "acceptable BEHAVIOUR." Alarms are raised when these criteria are violated. The tactic is a triage method to concentrate on potential hazards for further investigation. ON-BOARD advancements accelerate the initial detection of a zero-day attack in detection techniques. The threat information is promptly submitted to the intelligence pool and downloaded for immediate action by other Next Generation SIEMs worldwide.

4. ARCHITECTURE OF A NEXT-GEN MONITORING TOOL

With the rise in cyber threats, monitoring tools are coming with more advanced and customized features for their clients. These include the integration of all the devices and technologies across the network into a single consolidated tool, such as next-gen SIEM or EDR. With the help of this, clients can see all the alerts and incidents in a centralized console which is easier to monitor.

Figure 1 demonstrates a typical architecture of how a Next-Gen security monitoring tool and the components that it possesses. These tools dive deep into the prevention and detection of malicious alerts.

4.1 Activities involved inside prevention

Prevention of threat actors is the initial yet critical element of any next-gen monitoring tool. This possesses various techniques like mobile device management, Host intrusion prevention system (HIPS), Patch management, firewall and proxy policies, Encryption of data, Vulnerability Management, Device Application, web application control, etc. Mobile device management includes policies that revolve around the removal of media, storage media, and all other devices which carry information outside the organization. Security of these devices and proper reporting of unauthorized activities should be alerted appropriately inside the tool. A host-based intrusion detection system is not only capable of monitoring the alert but also provides in-depth analysis of their response through the host and network segmentation. Another key component of these tools is the management of firewall and proxy policies. They help in the prevention of network-based attacks by fine-tuning alerts. This tool also offers Vulnerability management services in order to protect the infrastructure beforehand. Overall, the Prevention component within any next-gen monitoring tool aims at protecting the infrastructure before the attack by removing the vulnerability, securing it from the threat actors, and mitigating the risk.

4.2 Activities involved inside detection:

Detection is the backbone of any monitoring tool as they provide the information to the first line of defense. It helps the team to analyze the threat actors and their sources in order to find the root cause. The initial phase of detection starts with incident management, where the incidents are managed and segregated based on the priority of the alerts. Another aspect of detection is the handling of false positives, as they are one of the key concerns for any security monitoring team. These tools help in reducing false positives through the use of behavior-based technologies like AI and ML. Real-time monitoring is another key feature and constitutes threat hunting and modelling to a greater extent. These tools also do the detection of malicious scripts and source code reviews. In the end, it provides a centralized console where we can analyze and monitor all the alerts and key information related to those..

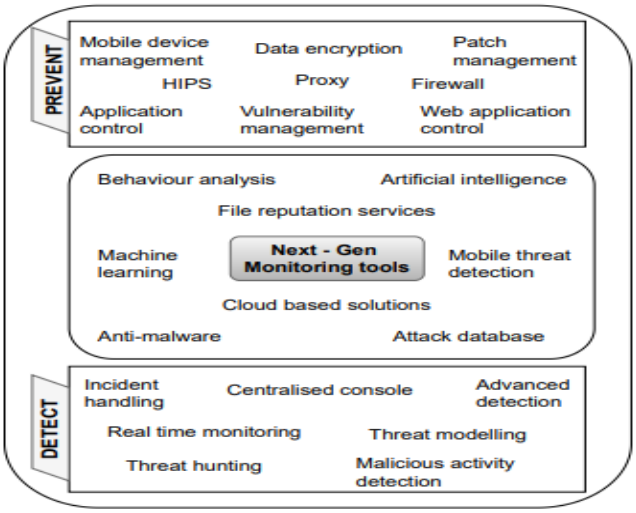

Figure 1 : Architecture of next-gen security monitoring tools

The above-mentioned architecture is just a visualization of the key components inside any next-gen monitoring tool. This may vary from vendor to vendor and technology to technology based on the need of the client environment. However, most of the elements will remain in the tool in some or the other way. The threat database will also change based on the vendor as indicators of attack (IOC) will not be the same for each tool.

5. HOW EFFECTIVE ARE THESE MONITORING TOOLS AGAINST THE CYBER-ATTACKS?

Every day, new attack tactics and vulnerabilities are found. The company probably has firewalls, IDS/IPS, and antivirus programs that scan the IT infrastructure from the perimeter to the endpoints for indicators of Suspicious activity. Many of these solutions, meanwhile, lack the ability to recognize advanced persistent threats and zero-day attacks. The organizations may already have monitoring technologies like SIEM, which combine data from all security measures into a single correlation engine, but which also have the potential to generate a significant number of false alerts, i.e., false positives. As a result, it's crucial to

fine-tune the monitoring tools and offer meaningful information for incident response and real-time threat detection.

These monitoring tools provide a higher level of protection by ensuring more endpoint visibility, fetching details from threat databases, and using behavioural protection. Using only signature-based techniques or indications of compromise (IOCs) results in "silent failure," which paves the way for data breaches. Behavioural techniques that look for indications of attack (IOAs) are essential for effective endpoint detection and response because they let us know about a suspicious activity before a breach takes place. All these features are inculcated in next-generation endpoint security monitoring tools. As we know, nothing is fully secured in cyber security, yet these tools provide a significant amount of security against threats.

6. CONCLUSION

Throughout the research, we have tried to analyze endpoint security according to the current trends and also studied the evolution of endpoint security in phase wise manner. In the initial phase, traditional antivirus was more vigilant for securing endpoints, but with the more advanced threats, these search engines got many loopholes. Furthermore, we described the next-generation antivirus tools like EDR, XDR, MDR, SIEM, etc. Also, we highlighted their effectiveness against advanced cyber-attacks.

Although there are some concerns regarding the effectiveness of these monitoring tools, they still provide mainly real-time analysis and detection, which has made the jab of the defence team relatively smooth. The evolution of tools and their associated search engines protect huge umbrellas of threats. The usage of advanced technologies like Artificial intelligence, Machine learning, Internet of things has made a significant contribution to accuracy as well. No matter their size or industry, firms in the twenty-first century operate in a dangerous environment. Threats to cyber security that existed 20 years ago are now a reality. Whether we like it or not, cyber-attacks will stay prevalent and are probably going to get more frequent and more intense in the future. Despite the fact that there are a number of defences against these threats, we might argue that monitoring and identifying cyber security threats is one of the best ones. It entails taking a proactive approach to problem-solving by seeing problems early on before they become much worse.

7. REFERENCES

[1] Karantzas, G., & Patsakis, C. (2021). An empirical assessment of endpoint detection and response systems against advanced persistent threats attack vectors. Journal of Cybersecurity and Privacy, 1(3), 387-421.

[2] Slate, S. (2018). Endpoint Security: An Overview and a Look into the Future. Lat. Am. Polit. Hist, 9780429499340-15.

[3] Barlow, W. Y. J., & Haberman, K. L. M. Two Visual Computer Network Security Monitoring Tools Incorporating Operator Interface Requirements.

[4] Yoo, S. J. (2018). Study on Improving Endpoint Security Technology. Convergence Security Journal, 18(3), 19-25.

[5] Slate, S. (2018). Endpoint Security: An Overview and a Look into the Future. Lat. Am. Polit. Hist, 9780429499340-15.

[6] Karantzas, G., & Patsakis, C. (2021). An empirical assessment of endpoint detection and response systems against advanced persistent threats attack vectors. Journal of Cybersecurity and Privacy, 1(3), 387-421.

[7] Park, S. H., Yun, S. W., Jeon, S. E., Park, N. E., Shim, H. Y., Lee, Y. R., ... & Lee, I. G. (2022). Performance Evaluation of Open-Source Endpoint Detection and Response Combining Google Rapid Response and Osquery for Threat Detection. IEEE Access, 10, 20259-20269.

[8] Chandel, S., Yu, S., Yitian, T., Zhili, Z., & Yusheng, H. (2019, October). Endpoint protection: Measuring the effectiveness of remediation technologies and methodologies for insider threat. In 2019 international conference on cyber-enabled distributed computing and knowledge discovery (cyberc) (pp. 81-89). IEEE.

Biographies

Raunak Choudhary received the bachelor's degree in Electronics and Electrical Engineering from Kalinga institute of industrial technology in 2018 and currently pursuing Master's degree in IT business management from Symbiosis International university. He is an information security enthusiast and his research areas include application security, Infrastructure and Network security, and Threat hunting**.**

Parul Pachori received bachelor's degree in computer engineering from Ahmedabad Institute of Technology, Gujarat Technological University in 2020 and is currently pursuing master's degree in Information Technology Business Management from Symbiosis Centre for Information Technology, Symbiosis International University. She is currently studying information security management and research areas include information security, privacy, network security and cyber threats.

Nisha T N is an Assistant Professor at Symbiosis Centre for Information Technology (SCIT), a constituent of the Symbiosis International University (SIU), Pune. She is a Graduate in computer science from Calicut University and Post Graduate in Computer Management from Pune University, India. She completed PhD in Computer Science from Symbiosis International University, her research in the area of Information security, specialized in network intrusion detection and has a teaching experience of ten years in the areas such as information security, programming, Algorithm analysis and data structures.