Endpoint: The Start Point of Cyber Security

Enhancing Cyber Security through advanced Endpoint Security

In the realm of cyber security, the term endpoint refers to connected devices on a network such as desktops, laptops, servers, mobile and IoT devices. Endpoints are the interface where human beings who are the weakest link in Cyber Security normally interact. Endpoint security, therefore, is one of the prominent components of cyber security. It involves securing data associated with endpoints from exploitation by threat actors through management of vulnerabilities and patching of software.

Organizations of all types and sizes such as healthcare, finance and defense are at risk from increased volume of organized cybercrime. Being the interface where human beings who are the weakest link in Cyber Security normally interact, these devices are the main targets of malicious actors. Endpoint security has emerged into advanced technology from traditional antivirus solutions for providing faster and comprehensive protection from sophisticated malware and modern zero-day attacks.

Need of Endpoint Security

Endpoint security is considered as crucial for cybersecurity due to a variety of reasons. The number and variety of endpoints are increasing day-by-day. With the introduction of remote work culture and advancement in the BYOD policies, perimeter security is becoming insufficient to prevent all kinds of malicious activities. The threat landscape is becoming complex due to increased capability of hackers to introduce new ways of accessing the digital assets and manipulate the information. Data being the most prominent asset for an organization in today's environment, the organization can be put at the risk of insolvency through illegal access and theft of that data.

Endpoint Security Architecture

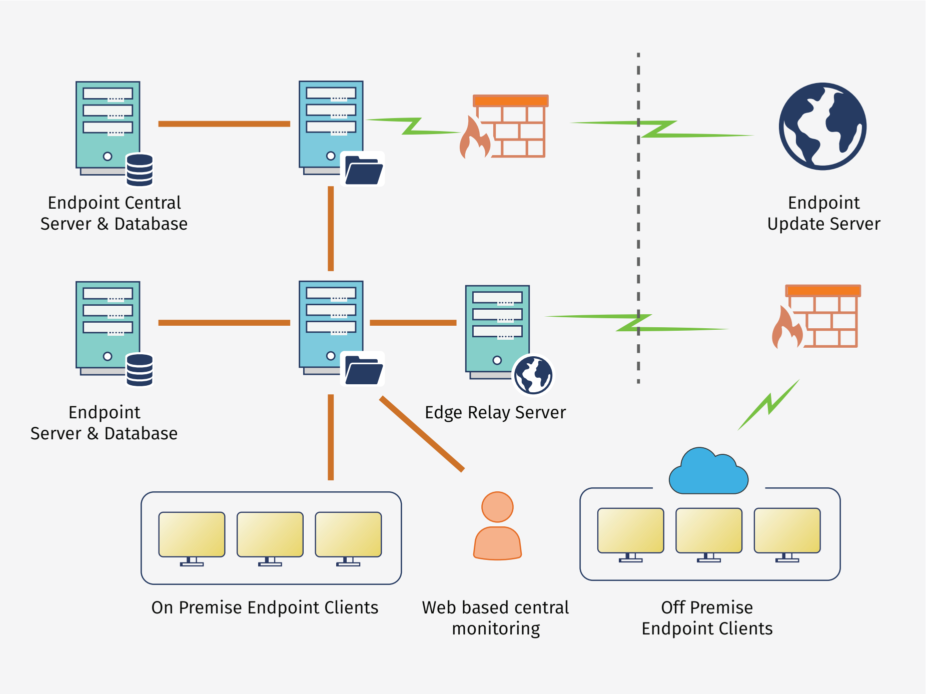
The figure illustrates the architecture of a typical endpoint security solution. The prime component in this deployment is the Central Endpoint Server which receives the security updates from the Endpoint Update Server and also functions as a centralized manager. The central server further distributes the updates among a set of Endpoint Servers to which the on premise client systems are connected. Endpoints such as laptops and mobile devices that are outside the organization's intranet are connected to the Endpoint Servers through an Edge Relay Server. The Endpoint Server provides advanced threat protection techniques combined with detection and response through the agent installed in clients. It responds to attacks in real-time and provides immediate and effective protection against zero-day attacks. A web-based central monitoring console is also provided for better visibility to the administrator in managing the endpoint clients.

Evolution of Endpoint Security

The business of endpoint security started in late 1980s with the introduction of antivirus solution which is a signature based malware recognition system. With the increased popularity of e-commerce and internet, detection of malicious activities has become more complex and can no longer rely on signatures. Traditional endpoint solutions have become incapable to handle sophisticated and emerging threats like file-less malware and zero day attacks. Therefore, advancement is required in end point security solutions with the proposition of more integrated, multistage defense system to handle the outsmart attackers. Advanced endpoint security requires detection and correction of hidden threats in seconds, in place of months. This is possible only with the automation of sharing threat intelligence among connected components for detection and correction of threats while teaming up of humans

Diwan Hauym Khan
Scientist-F
dhkhan@nic.in

Kirshna Kumar
Scientist-B
kirshna.kumar98@nic.in



with machines. Traditional endpoint security solutions such as firewall, antivirus, reputation, and heuristics are integrated with machine learning and artificial intelligence to detect and prevent advanced threats with nearly same speed as of threats.

Traditional Antivirus

Antivirus is an endpoint solution developed for the detection, prevention and elimination of malicious actors such as viruses, worms, and Trojans on end point devices based on large database of malware signatures. The antivirus solutions detect malware with the scan of files and directories based on patterns that matches the malware signatures on file. Antivirus software is provided by a number of vendors, with the versions developed for small businesses, personal use and large enterprises. The antivirus software has the capability to scan the system on-demand as well as at scheduled intervals. They also warn the user before visiting the malicious sites by virtue of its safety features. Further, they have the capability to identify different types of threats that are attacking the endpoint device. The major limitation of these solutions is that they are able to recognize only known threats and need to update signature database for new threats.

Advanced Endpoint Security

Cyber world requires advanced endpoint security solution as applicability of traditional solutions is limited only to known threats. Advanced endpoint security integrates features of traditional solutions such as firewall, antivirus, reputation, and heuristics with Behavioral Analysis, Machine Learning and containment. Besides, Endpoint Detection and Response (EDR) is also integrated to detect and prevent file-less, zero-day and script based threats like ransomware. The key capabilities of advanced endpoint security solutions are explained below.

Security Analytics: In security analytics, data related to endpoints is aggregated and analysed using security analytics tools for the detection of potential attacks. Malicious activities and associated harmful effects are identified and mitigated to avoid the damage caused by them.

Machine Learning: Machine learning is one of the prominent components of artificial intelligence (AI), through which enormous data is analyzed for behavioral learning of endpoints. Based on behavioral learning, malicious activities are identified and automatic security processes such as quarantining the endpoint and/or issuing of alerts are triggered. In present working environment, Machine Learning has become one of the important techniques for the detection of advanced threats at endpoints such as novel and zero day attacks.

Real-Time Threat Intelligence: Real-time threat intelligence provides updates from external security agencies about novel security threats such as zero-days, file-less malware and other trending malware in the cyber world. It expedites threat analysis, detection and prevention in the real-world scenario.

Internet of Things (IoT) security: With the advent of smart everything (like smart cities, smart industry, smart healthcare) IoT has incredible impact and proliferation in every domain of life. According to surveys, the count of IoT devices connected worldwide will cross a trillion towards the end of this decade. These devices are highly vulnerable to cyber threats due to their limitation in computation, network capacity and storage, and ubiquitous nature. Therefore, IoT security requires self-healing and automated mechanism for detection of threats, avoidance of data compromisation and reduction of response and downtime.

Endpoint Detection and Response (EDR): EDR integrates rule-based automated analysis and response capabilities with the endpoint data gathering and real-time persistent monitoring. The main focus of EDR is on identification and investigation of suspicious activities at endpoints along with automation for faster detection and response. Threat intelligence feed from various sources enhances the efficiency of EDR solution for the identification of advanced exploits such as zero day and multi-layered threats. Some EDR solutions utilize Artificial Intelligence and machine learning for the automotive investigation and analysis about potential threats.

Endpoint Encryption: Encryption is the technique to encode data on endpoint devices in unreadable format to make it unusable for unauthorized actors. For authorized users the data would be decrypted with the associated decryption key to make it accessible. Sensitive information of critical applications such as healthcare, banking, defense, etc. is protected from unauthorized access using endpoint encryption. Using this technique, the operating system can be protected from “Evil Maid” threats which install corrupt boot files and key logger.

Extended Detection and Response (XDR): XDR is an enhanced form of EDR with improved detection and response capabilities using real-time data. It is a SaaS-based technique that collects data across multiple components and correlates it by utilizing behavioral analysis, threat intelligence and data science techniques. XDR has the ability to optimize response with increased visibility and advanced context while reducing the scope and severity of attack.

Conclusion

Attackers usually target endpoints devices as the start points for malicious entity. Advanced security solutions are required for quick detection, analysis, blocking, and containing of threats. For this purpose, the endpoint security technologies need to collaborate with each other and share threat intelligence.

For further information, please contact:
Diwan Hauym Khan
Scientist-F
National Informatics Centre, A-Block, CGO Complex
Lodhi Road, New Delhi - 110003
Email: dhkhan@nic.in, Phone: 011-2430 5608