Requested by Client: I am looking to build out a small section of technical overview on the topic of: Endpoint Security. Subsections should include: What is Endpoint Security? Types of Endpoint Security Endpoint Security vs Protection Challenges of Endpoint Security Solutions The content should be written without voice, be agnostic and informative providing useful links and references to any factual claims. 1,200 words.

What Is An Endpoint?

An endpoint is a device that connects and communicates with a network, serving as important aspect of a network perimeter. Endpoints can include desktops, smartphones, tablets, IoT devices, workstations, laptops and servers.

For cybersecurity purposes, an endpoint is a gateway that attackers can use to infiltrate a network to conduct malicious activities. It is a point of vulnerability within a network that requires sufficient protection in order to ensure that the network will be secure from cyber threats. Multiple endpoint vulnerabilities in an enterprise's network can result from:

- Threats aimed at mobile device access and networks
- The use of personal devices in the workplace for work purposes
- Telecommuting and the use of Wi-Fi networks

Endpoints are a frequent target of attackers because of their susceptibility to malware and other cyber threats. As the various types of endpoints that enterprises use continue to evolve and multiply, it is necessary to properly adapt the security solutions in order to have sufficient protection.

What is Endpoint Security?

Endpoint security is the process of safeguarding the various components in a network from internal and external threats. In addition to incorporating threat intelligence services, endpoint security measures include prevention, detection and responsive solutions that provide security for the devices within a enterprise via a central management portal.

The rising prevalence of threats infiltrating networks through endpoints indicates that centralized network protection does not provide sufficient protection for a network. In order to have adequate security, the access points of networks must be better guarded to curtail the vulnerability that comes with remote device usage. The prevention of security breaches requires vigilance against not only unknown and known cyber threats, but also the deficiencies of traditional antivirus technologies. Endpoint security has evolved from the use of only traditional antivirus software solutions to providing comprehensive fortification from the evolving and sophisticated advanced cyber threats like zero-day threats and malware.

The ultimate objective of endpoint security is to protect an enterprise's data and network by protecting endpoint devices. With the proper endpoint security solutions in place, enterprises can streamline their cybersecurity efforts, using multi-tier protection at the areas of access.

An enterprise's endpoint security should feature key characteristics and capabilities, including:

- Protection for all applications
- The use of automation to leverage threat intelligence for preventative uses
- The ability to intercept known and unknown threats
- An infrastructure that facilitates communication and collaboration between endpoint defenses
- The ability to manage diverse collections of endpoints

- A high level of execution that does not compromise user productivity or application performance and efficiency
- A centralized management platform that lowers costs, increase visibility and streamline operations
- Being uniquely suited for the security needs of the enterprise
- The ability to preserve the security of both legacy and modern network systems
- Proactive internet security that includes filtering and internet protection for endpoints and that provides safe browsing
- A degree of protection against targeted attacks that reduces the time lapse between detection and containment from days to fractions of a second
- Threat intelligence that provide actionable data that security analysts can use to immediately locate threats and infiltrations, determine the reasons for their occurrence, determine the length of exposure and respond timely and accurately

Types of Endpoint Security

Endpoint security can be broadly divided into two categories: enterprise-based and consumer-based. While the purpose of both solutions is to provide protection, enterprise endpoint security provides a number of features that consumer-based endpoint protection does not and that are necessary in order to provide an enterprise with the appropriate level it endpoint security requires. One of the main differences between the two is the presence of a centralized administration and management for enterprise-based endpoint security. Tracking of employees' devices, remote management, establishing endpoint permissions for administrative privileges, more endpoints are other distinguishing capabilities of endpoint security.

Another distinction between types of endpoint security solutions is installation. On-premises solutions are installed directly on the network for deployment. Cloud-based endpoint security is executed from the cloud and typically requires a subscription.

Endpoint security can also be distinguished by the type and level of it security capabilities:

- **Endpoint Protection Platform.** An EPP is a preventative tool that provides device-level detection and obstruction of threat by conducting real-time protections by scanning and inspecting files when they enter a network. A typical type of endpoint protection is the conventional antivirus, which features antimalware. EPPs also include personal firewalls, data loss prevention, data encryption, intrusion prevention.

- **Endpoint Detection and Response.** EDR provides continuous monitoring of all applications and files that traverse an endpoint. It uses features of next-generation antivirus and other tools to detect anomalies, provide alerts, conduct forensic investigation and implement endpoint remediation all in real-time. The threat visibility it provides is more than that can be provided by endpoint protection platforms.

Endpoint Security vs Protection

Endpoint security and antivirus protection have the same objective, which is to provide protection for an enterprise's devices, systems and data. However, the manner in which they achieve this objective and the scope of the protection they provide is very different.

As a concept, endpoint security refers to the entire arsenal of security tools enterprises use to protect endpoints from internal and external threats, while antivirus is considered one of the components of endpoint security. In addition to anti-virus protection, endpoint security typically includes firewalls, monitoring tools, mobile device management solutions, intrusion detection tools, encryption, logging tools and other components that helps to stop advanced persistent threats and targeted attacks. Endpoint security provides protection for an entire network, including the endpoints. Antivirus protection is only applies to an individual device within a network.

Another important different between endpoint security and antivirus protection is that type and scope of that each provide protection from. Antivirus solutions usually provides protection against a particular type of attack, mainly malware. As with the scope of protection it provides, endpoint security provides protection from a wide range of attacks. Because of this, endpoint security solutions have advanced features that are not offered by antivirus protection solutions. Endpoint security solutions are also located at each endpoint of a network as well as the on the network's central management server.

Challenges of Endpoint Security Solutions

- **Securing remote personnel**. Research shows that 46 percent of enterprises conduct operations in multiple countries. This can result in remote workers using endpoint security solutions with that have unreliable and obsolete setups.
- **Personnel and skill shortages.** Not having properly trained staff is one of the main to using endpoint security solutions to launch effective response to endpoint threats.
- **Managing the infrastructure.** Between legacy security solutions, such as traditional antivirus technology, and all of the other security tool infrastructure on the premises that an enterprises uses to manage their endpoint security, it can be difficult to ensure that upgrades are properly maintained and that there is sufficient computing power and storage.
- **False positives.** The results of an online survey of cybersecurity professionals showed that the majority of 53 percent of the respondents estimate that the rate of false positive endpoint security alerts they receive is between 10 percent and 49 percent.
- **Inefficiency in isolation.** The sophisticated and emerging threats that are assailing enterprises are able to outpace isolated endpoint security solutions. The integration of endpoint security solutions is a key factor in the ability to detect, locate and correct covert threats within seconds, rather than in days.