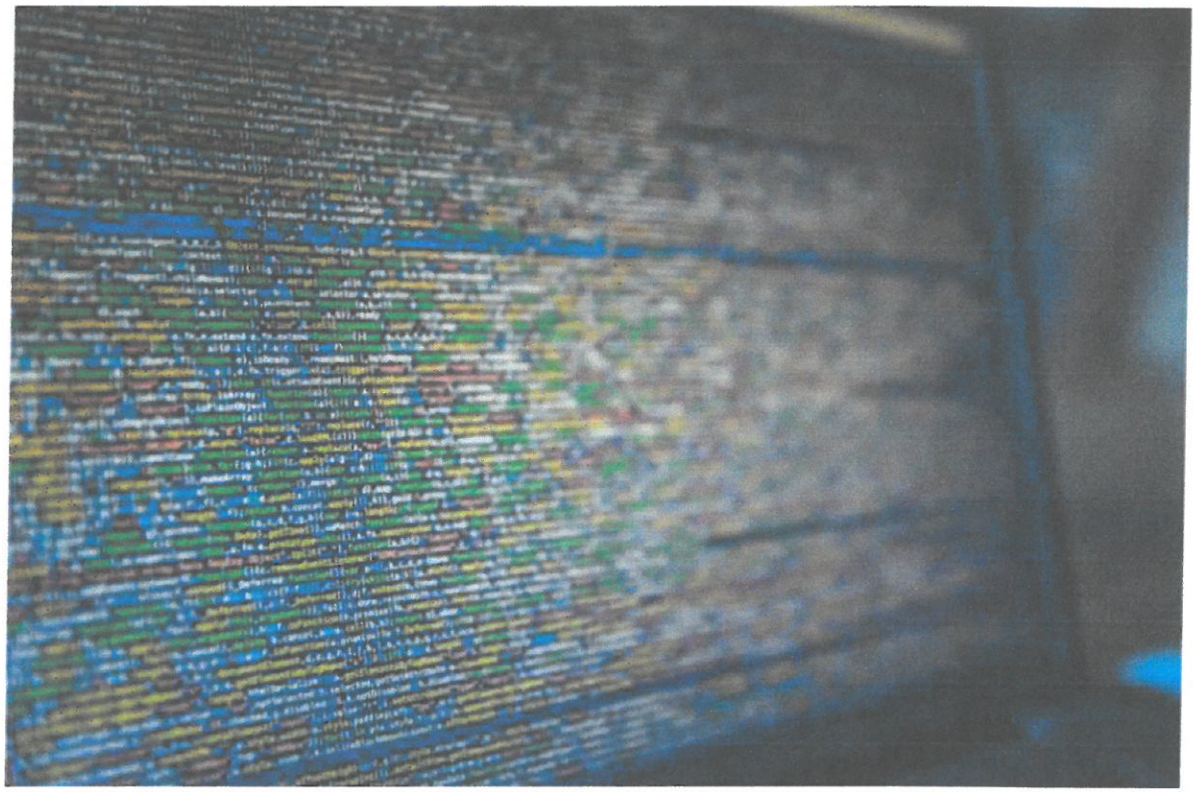
HEADQUARTERS
ARMED FORCES OF THE PHILIPPINES CYBER GROUP
Camp General Emilio Aguinaldo, Quezon City

CYBERSECURITY BULLETIN: 2022-09

WHAT IS ENDPOINT SECURITY AND HOW DOES IT WORK?



1. Background:

Endpoint security, or endpoint protection, refers to securing endpoints – such as desktops, laptops, and mobile devices – from cybersecurity threats. Endpoints can create entry points to organizational networks which cybercriminals can exploit. Endpoint security protects these entry points from malicious attacks.

It is a part of a broader cybersecurity program that is essential for all businesses, regardless of size. It has evolved from traditional antivirus software to comprehensive protection from sophisticated malware and evolving zero-day threats.

2. Importance of Endpoint Security

In recent years, the number of endpoints within businesses has increased. This has been especially the case since the Covid-19 pandemic, which has led to increased remote working around the world. With more employees working from home or connecting to public Wi-Fi on the go, enterprise networks now have more endpoints than ever. And every endpoint can be a potential entry point for attacks.

Businesses of all sizes can be targets for cyberattacks. It is increasingly difficult to protect from attacks that enter through endpoints, such as laptops or mobile devices. These devices can be hacked, which in turn can lead to data breaches. It's

estimated that 70% of successful data breaches originate on endpoint devices. As well as causing reputational damage, data breaches can be costly. Data is often the most valuable asset a company has – and losing that data, or access to that data, can put the entire business at risk.

Not only is the number of endpoints increasing – driven by the rise in remote working – but businesses also have to contend with an increase in the number of types of endpoints, thanks to the growth of the Internet of Things.

Businesses need to protect their data and ensure visibility into advanced cyber threats. But many small and mid-sized businesses lack the resources for continuous monitoring of network security and customer information and often only consider protecting their network once a breach has already taken place. Even then, businesses can focus on their network and infrastructure, leaving some of the most vulnerable elements – that is, endpoint devices – unprotected.

The risks posed by endpoints and their sensitive data are an ongoing cybersecurity challenge. Moreover, the endpoint landscape is evolving, and businesses – small, medium, and large – are targets for cyberattacks. That's why it's important to understand what endpoint security is and how it works.

3. How does Endpoint Security work?

The terms endpoint protection, endpoint security, and endpoint protection platforms are often used interchangeably to refer to centrally managed security solutions organizations use to protect endpoints. Endpoint security works by examining files, processes, and systems for suspicious or malicious activity.

Organizations can install an endpoint protection platform – EPP – on devices to prevent malicious actors from using malware or other tools to infiltrate their systems. An EPP can be used in conjunction with other detection and monitoring tools to flag suspicious behavior and prevent breaches before they take place.

Endpoint protection offers a centralized management console to which organizations can connect their network. The console allows administrators to monitor, investigate and respond to potential cyber threats. This can either be achieved through an on-location, cloud, or hybrid approach:

a. On-location

An on-location or on-premises approach involves a locally-hosted data center that acts as a hub for the management console. This will reach out to the endpoints via an agent to provide security. This approach is seen as a legacy model and has drawbacks – including creating security silos, since administrators can typically only manage endpoints within their perimeter.

b. Cloud

This approach enables administrators to monitor and manage endpoints through a centralized management console in the cloud, which devices connect to remotely. Cloud solutions use the advantages of the cloud to ensure security behind the traditional perimeter – removing silos and enhancing administrator reach.

c. Hybrid

A hybrid approach mixes both on-location and cloud solutions. This approach has increased in prevalence since the pandemic has led to increased remote working. Organizations have adapted their legacy architecture and adapted elements of it for the cloud to gain some cloud capabilities.

EPPs that use the cloud to hold a database of threat information free endpoints from the bloat associated with storing this information locally and the maintenance required to keep these databases updated. A cloud-based approach is also quicker and more scalable. Some larger organizations may need on-premises security for regulatory reasons. For smaller and mid-sized businesses, a cloud-based approach is probably more suitable.

Endpoint security software usually includes these elements:

- Machine-learning to detect zero-day threats
- An integrated firewall to prevent hostile network attacks
- An email gateway to safeguard against phishing and other social engineering attempts
- Insider threat protection to guard against threats from within the organization, either malicious or accidental
- Advanced antivirus and anti-malware protection to detect and remove malware across endpoint devices and operating systems
- Proactive security to facilitate safe web browsing
- Endpoint, email, and disk encryption to protect against data exfiltration
- Ultimately, endpoint security offers a centralized platform for administrators, improving visibility, simplifying operations, and allowing threats to be quickly isolated.

Ultimately, endpoint security offers a centralized platform for administrators, improving visibility, simplifying operations, and allowing threats to be quickly isolated.

As well as the acronym EPP, you will also come across the acronym EDR in relation to endpoint security. EDR stands for 'endpoint detection and response'. In general, an endpoint protection platform or EPP is considered passive threat protection, whereas EDR is more active since it helps investigate and contain breaches that have already occurred. An EPP will protect each endpoint by isolation, whereas an EDR will provide context and data for attacks that span multiple endpoints. Modern endpoint security platforms typically combine both EPP and EDR.

4. Endpoint Devices

A network endpoint is any device that connects to an organization's network from outside its firewall. Examples of endpoint devices include:

- Laptops
- Tablets
- Desktop computers
- Mobile devices
- Internet of Things devices
- Wearables
- Digital printers

- Scanners
- Point of sale (POS) systems
- Medical devices

Essentially, any device which communicates with the central network can be considered an endpoint.

5. Recommendations

The basic requirements for an organization may consist of a decent firewall and an antivirus solution. However, for midsize and large organizations, implementing the tips below can enhance endpoint security, decrease the threat of ransomware or viruses and prevent block threat actors. In the long term, an organization that has successfully established endpoint security, will not be so vulnerable to endpoint attacks.

a. Identify your endpoint

The first step you should take to secure endpoints is cataloging and assessing vulnerabilities. Once you have this data, you can enable network access only to the approved devices and prioritize the most risky and sensitive endpoints. Keep in mind that any endpoint in the network demands protection.

b. Data Access Policy

Many businesses do not have the basic protocols for data storage, access, and usage. Any organization striving to secure its information must outline the data classification levels. For example, data can have a public, restricted or critical access in case of personal or financial information. An organization should define which employees and departments can access each type of data. This can be done with user authentication procedures, such as two-factor authentication. The protocol should notify admins directly of any security breach.

c. IoT Security

IoT devices and printers often have default settings and passwords, which makes them an easy target for attackers. To limit this vulnerability, change passwords regularly release software updates, and maintain the hardware and firmware of all your systems and computers. Windows users, for example, can use automatic deployment rules (ADR) to update or patch their computers.

d. Data Encryption

Encrypt critical and restricted data stored on premises or in the cloud. You can encrypt entire hard drives or specific files, depending on your needs. In addition, to secure data in transit, update all web communication to secure HTTPS protocols. Encrypt emails using Pretty Good Privacy (PGP) or S/Mime encryption. Access remote desktops via Virtual Private Networks (VPN).

e. Enforce Bring Your Own Device (BYOD) Policy

A Bring-Your-Own-Device (BYOD) policy determines the level of support an IT department can provide for computers, smartphones and tablets owned by

employees in a corporation. For example, a BYOD policy can include a list of allowed apps and devices in the network, the data they can access, and the websites they can visit. Organization with sensitive information should provide their own laptops or smartphones with restricted and authorized apps and message encryption features.

f. Advanced and Automated Endpoint Protection

Basic solutions for endpoint protection such as antiviruses and firewalls have been in the marketplace for many years. While antiviruses are good in catching known threats using a blacklist, they are struggling to detect sophisticated types of malwares. Firewalls also have their own vulnerabilities. This is why advanced endpoint detection tools use automation to adjust to ever-evolving threats like fileless malware and phishing attacks.

g. Awareness

Make sure everyone in the organization knows how to avoid cyber security threats and risks. Organizations should invest in educating their employees about basic security practices, such as secure password tips and how to identify phishing emails. This type of education should be conducted frequently because of the ever-evolving threats.

4. Dissemination

The information provided is intended to increase the security awareness of AFP personnel and to help them behave more securely within their work environment. The increased awareness is intended to help improve the organization's overall cybersecurity posture. All units and offices are given permission and are encouraged to redistribute this bulletin that will benefit the AFP organization as a whole for educational, and non-commercial purposes.

References:

- *https://www.kaspersky.com/resource-center/definitions/what-is-endpoint-security*
- *https://www.computer.org/publications/tech-news/trends/7-tips-to-boost-endpoint-security*