Introduction to Cyber Security

Security Layers

Module 2 – Part B

End-Point Security

- Endpoint security solutions protect endpoints such as mobile devices, desktops, laptops, and even medical and IoT devices.
- Endpoints are a popular attack vector, and the goal of an attacker is to not only compromise the endpoint but also to gain access to the network and the valuable assets within.
- It includes continuous monitoring, rapid time to detection, and architectural integrations. With threats continually increasing in sophistication and frequency, it is more important than ever to deploy an effective endpoint solution.
- Endpoint security solutions take a cloud-based approach for endpoint security to instantly access the latest threat intelligence without requiring manual updates from security admins.
- This allows for faster and more automated responses. They continuously monitor all files and applications that enter your network and have the ability to scale and integrate into your existing environment.
- Cloud solutions offer scalability and flexibility and are much easier to integrate and manage. There is also less overhead since there is no infrastructure to maintain and the installation process is faster and simpler.

Types of End-point Security

1. Endpoint protection platform (EPP)

- ✓ An EPP solution is a preventative tool that performs point-in-time protection by inspecting and scanning files once they enter a network.
- ✓ The most common endpoint protection is a traditional antivirus (AV) solution.
- ✓ An AV solution encompasses anti-malware capabilities, which are mainly designed to protect against signature-based attacks.
- ✓ When a file enters your network, the AV solution will scan the file to see if the signature matches any malicious threats in a threat intelligence database.

Contd…

2. Endpoint Detection and Remediation (EDR)

- ✓ An EDR solution goes beyond simple point-in-time detection mechanisms.
- ✓ Instead, it continuously monitors all files and applications that enter a device.
- ✓ This means EDR solutions can provide more granular visibility and analysis for threat investigation.
- ✓ EDR solutions can also detect threats beyond just signature-based attacks.
- ✓ Fileless malware, ransomware, polymorphic attacks, and more can be detected using EDR solutions.

Contd…

3. Extended detection and response (XDR)

- ✓ Where EDR improved on malware detection over antivirus capabilities, XDR extends the range of EDR to encompass more deployed security solutions.
- ✓ XDR has a broader capability than EDR.
- ✓ It utilizes the latest and current technologies to provide higher visibility and collect and correlate threat information.
- ✓ Employing analytics and automation to help detect today's and future attacks.

Why End-point Security is Important?

- An endpoint security strategy is essential because every remote endpoint can be the entry point for an attack, and the number of endpoints is only increasing with the rapid pandemic-related shift to remote work.
- According to a Gallup Poll, a majority of US workers were remote in 2020, with 51% still remote in April of 2021.
- The risks posed by endpoints and their sensitive data are a challenge that's not going away.
- The endpoint landscape is constantly changing, and businesses of all sizes are attractive targets for cyberattacks.

https://www.crowdstrike.com/cybersecurity-101/endpoint-security/

Contd…

- According to the FBI's Internet Crime Report, they received an increase of 300,000 complaints over 2019, with reported losses over $4.2 billion.
- The Verizon 2021 Data Breach Investigations Report found "Servers are still dominating the asset landscape due to the prevalence of web apps and mail services involved in incidents".
- Each data breach, costs on average $3.86 million globally with the United States averaging at $8.65 million per data breach according to Ponemon's "Cost of a Data Breach Report 2020".
- The study identified the biggest financial impact of a breach was "lost business," making up almost 40% of the data breach average cost.

How End-point Protection Works?

- Endpoint protection solutions work by examining files, processes, and system activity for suspicious or malicious indicators.
- It offers a centralized management console from which administrators can connect to their enterprise network to monitor, protect, investigate and respond to incidents. This is accomplished by leveraging either an on-premise, hybrid, or cloud approach.
- The "Traditional or legacy" approach is often used to describe on-premise security posture that is reliant on a locally hosted data center from which security is delivered.
- A "Cloud-native" solution built in and for the cloud. Administrators can remotely monitor and manage endpoints through a centralized management console that lives in the cloud and connects to devices remotely through an agent on the endpoint.

Endpoint Protection vs Antivirus Software

- **Endpoint security software** protects endpoints from being breached – no matter if they are physical or virtual, on- or off-premise.
- It is installed on laptops, desktops, servers, virtual machines, as well as remote endpoints themselves.
- **Antivirus** is often part of an endpoint security solution and is generally regarded as one of the more basic forms of endpoint protection.
- Instead of using advanced techniques and practices, such as threat hunting and endpoint detection and response (EDR), antivirus simply finds and removes known viruses and other types of malware.
- Traditional antivirus runs in the background, periodically scanning a device's content for patterns that match a database of virus signatures. Antivirus is installed on individual devices inside and outside the firewall.

Core Functionality of an Endpoint Protection Solution

1. Prevention: NGAV

- Traditional antivirus solutions detect less than half of all attacks. They function by comparing malicious *signatures*, or bits of code, to a database that is updated by contributors whenever a new malware signature is identified.
- The problem is that malware that has not yet been identified, or *unknown malware*, is not in the database. There is a gap between the time a piece of malware is released into the world and the time it becomes identifiable by traditional antivirus solutions.
- Next-generation antivirus (NGAV) closes that gap by using more advanced technologies, such as AI and machine learning, to identify new malware by examining more elements, such as file hashes, URLs, and IP addresses.

Contd…

2. Detection: EDR

- Prevention is not enough. No defenses are perfect, and some attacks will always make it through defenses and successfully penetrate the network.
- To prevent silent failures, an Endpoint Detection and Response (EDR) solution needs to provide continuous and comprehensive visibility into what is happening on endpoints in real time.
- Businesses should look for solutions that offer advanced threat detection and investigation and response capabilities.

Contd…

3. Managed Threat Hunting

- Not all attacks can be detected by automation alone.
- The expertise of security professionals is essential to detect today's sophisticated attacks.
- Managed threat hunting is conducted by elite teams that learn from incidents that have already occurred, aggregate crowdsourced data, and provide guidance on how best to respond when malicious activity is detected.

Contd…

4. Threat Intelligence Integration

- To stay ahead of attackers, businesses need to understand threats as they evolve. Sophisticated adversaries and advanced persistent threats (APTs) can move quickly and stealthily, and security teams need up-to-date and accurate intelligence to ensure defenses are automatically and precisely tuned.
- A threat intelligence integration solution should incorporate automation to investigate all incidents and gain knowledge in minutes, not hours.
- It should generate custom indicators of compromise (IoCs) directly from the endpoints to enable a proactive defense against future attacks.

CrowdStrike's Advanced Endpoint Protection

- **CrowdStrike's NGAV solution, Falcon Prevent,** has a 100 percent rating for detecting both known and unknown samples of malware with a false positive rate of zero percent.
- **Falcon Insight EDR,** collects and inspects event information in real time to prevent and detect attacks on endpoints. Built on CrowdStrike's cloud-native architecture, Falcon Insight records all activities of interest for deeper inspection.
- **The CrowdStrike Falcon Overwatch,** Falcon Overwatch identifies and stops over 30,000 breach attempts per year. When a threat is discovered, the Overwatch team can take action within seconds.
- **CrowdStrike's Falcon X platform,** provides the ability to instantly analyze any threats that reach an organization's endpoints. With Falcon X, organizations finally have the ability to get ahead of adversary activity, and stay ahead.