4.1. Security Toolkit: Endpoint Detection and Response (EDR)

What Everyone Needs to Know

Endpoint Detection and Response (EDR) refers to a type of software solution that is the next evolution of traditional antivirus solutions. Attackers just don't stick to a single game plan anymore. They've adapted and modified their methods to be much more fluid. Today's cat and mouse game has evolved beyond the static lists that traditional antivirus solutions can deal with. EDR solutions continuously monitor what is happening with your office's network so that staff can rapidly investigate and stop potential security incidents.

What IT Needs to Know

EDR provides deep visibility into the status of your network and allows for threat hunting capabilities to detect and block suspicious activities. It also gives you increased forensic capabilities, which allow for administrators to build a timeline of events to determine the impact of a breach. Additionally, many insurance companies are now requiring EDR solutions to be in place for organizations.

EDR is better than traditional antivirus because it can more organically respond to threats. Traditional antivirus software relies on a database of known attacks that needs to be constantly updated by vendors. These databases are good at detecting whatever the most recent attack was, but not so good at preventing new and emerging threats. EDR relies on event and behavior analysis, which helps it detect both known and unknown threats. EDR solutions can also provide you with a timeline of an attack, giving you information such as how it occurred and what it's trying to do, along with the capability to isolate, quarantine and remediate the infected endpoint(s). EDR can help you detect and respond to ransomware attacks, fileless attacks, and zero-day attacks.

Ransomware attacks are designed to encrypt your data and demand a ransom payment to unlock your files. This is now being combined with exfiltration techniques where attackers steal your data before they encrypt it and then threaten to release this information in the dark web if payment is not received.

Fileless attacks rely on what you already have in your environment, making it hard to detect and remove from your environment. PowerShell, for example, is a built-in Windows tool used by administrators but in the wrong hands, can be used to launch these types of attacks.

Zero-day exploits are new vulnerabilities that attackers have begun to exploit before developers have had a chance to patch. This often leads to developers having to scramble to update their systems which can take days. These attacks are sudden and require immediate attention and/or action by IT administrators.

Again, EDR helps administrators detect and respond to all of these types of attacks.

Solutions to Consider

Crowdstrike: Website, Pricing
SentinelOne: Website, Pricing
Checkpoint: Website, Pricing
VMWare: Website, Pricing

Resources

“What is Endpoint Detection and Response” (Crowdstrike)
“What Is Endpoint Detection and Response (EDR)?” (McAfee)
Last updated on December 15, 2023.
Print

Table of Contents

NEWS

News & publications

The news about recent activities for needed peoples.

More News

24 Mar 2023

Project Spotlight: UpToCode

Because everyone has a right to a safe home, Northeast Legal Aid (NLA) is…

Continue Reading

28 Feb 2023

Member Spotlight: Josh Lazar

We are heading south to Florida today to meet community member Josh Lazar, the…

Continue Reading

Our Partners


MAP
MICHIGAN
ADVOCACY
PROGRAM
LSC
America's Partner
for Equal Justice
LEGAL SERVICES CORPORATION