What Is EDR and Why Do You Need It?

Devolutions

ATTACKERS TAKE ADVANTAGE OF THE FACT THAT MOST ENDPOINTS ARE OPERATED AND MAINTAINED BY EVERYDAY PEOPLE

In today's volatile technology landscape, threat actors use poorly-secured endpoints as a backdoor into the network. These attackers take advantage of the fact that most endpoints are operated and maintained by everyday people, who often don't have the ability to recognize an endpoint attack, let alone protect against it.

Endpoint Detection and Response (EDR) security provides organizations with the means to monitor, detect, and respond to endpoint threats. Through the application of EDR solutions and practices, organizations gain visibility into the endpoint of the network. EDR also provides organizations with the tools to protect the network against incoming threats as they occur.

What Is Endpoint Detection and Response (EDR)?

Endpoint Detection and Response (EDR) is the sub-field of endpoint security responsible for proactively defending the network against endpoint threats. EDR security is composed of practices and technologies that actively monitor endpoint activity, identify threats, and trigger automatic responses to attacks.

In 2013, Anton Chuvakin of Gartner, recognized an emerging type of technology and set of practices that provided visibility into the endpoint of a network. He coined the term Endpoint Threat Detection and Response (ETDR). Over the years, the term has been shortened to EDR.

What Is an Endpoint Threat?

Endpoints are located at the furthest end of a network and are usually found on devices such as smartphones, tablets, Internet of Things (IoT) devices, servers, and workstations. Endpoints can either be privately owned or mainly operated by users. For the most part, however, such users aren't IT experts.

When people connect their devices to a network, they create a point at the end of the network. The connection can be done via a Wireless Access Point (WAP), mobile broadbands, or Direct Internet Access (DIA). Once the endpoint gains access to the network, it also gains a certain level of privilege, as granted by the admins.

Each endpoint has the potential to introduce vulnerabilities and/or malware into the network. If the endpoint is privately owned, it's most likely poorly secured. If the endpoint is owned by the company, but there's no endpoint security in place, then network admins won't have the visibility needed to protect the network against endpoint threats.

Types of Endpoint Threats

According to the 2019 Endpoint Security Trends Report, 70% of breaches originate at the endpoint. The study analyzed more than six million enterprise devices and discovered that the main cause of an endpoint breach was an existing vulnerability, and only 42% of endpoints were actually protected from threats.

Endpoints are easy targets for threat actors that use them to initiate a variety of attacks. Usually, threat actors use the endpoint as a means to an end — the network and the data it contains. Once they have the data, they then sell it to the highest bidder, ransom it for a hefty sum, or use it to commit financial and identity fraud.

Here are a few types of attacks that turn endpoints into a dangerous threat:

- **Phishing** — Attacks that target email users. Victims get an email that mimics a legitimate entity, tricking the user into revealing sensitive information or downloading malware.
- **Malvertising** — Malicious ads that contain malware. Victims click on legitimate websites and get infected with malware.
- **Ransomware** — A form of malware that blocks the victim's access to their data. Victims have to pay a ransom to get their data back.
- **Drive-by downloads** — Victims click on legitimate-looking websites, links or software updates. The click downloads malware or ransomware without the victim's knowledge.
- **Unpatched vulnerabilities** — Users who don't update their systems on a regular basis often fall prey to attacks. Threat actors use unpatched vulnerabilities to gain access to the network.

How EDR Works

EDR security solutions provide real-time visibility into network endpoints, as well as proactive capabilities for identifying and responding to endpoint threats. To enable these capabilities, EDR solutions make use of the following mechanisms:

1. Data collection — Collect data generated by activities at the endpoint, such as communication, user logins, and process execution.
2. Data recording — Log real-time data about endpoint security events. Security teams use this information to respond to security incidents as they occur.
3. Detection engine — Perform behavioral analysis, which establishes a baseline of normal endpoint activity and identifies which anomalies represent malicious activity.

To provide real-time endpoint visibility and analysis, EDR solutions perform these three tasks on a continual basis. Once a threat is detected, the EDR solution will alert admins and/or apply a pre-configured threat response.

Why You Need EDR

1. Endpoint visibility

EDR solutions provide visibility into the network endpoint, where there is often chaos and insufficient security. It's hard to protect against something you don't see, and many threats attack your blind spot.

But unlike Endpoint Protection Platform (EPP) solutions, which only offer visibility at the device level, EDR solutions enable endpoint monitoring at the network level.

2. Real-time incident detection and analysis

EDR solutions enable continuous monitoring. You'll gain the advantage of setting up automated processes that hunt down threats at the endpoint. Threat detection capabilities vary from vendor to vendor, but most scan for patterns and look for anomalies that represent malicious activity. Solutions powered by Artificial Intelligence (AI) continue to study the network, users and events, providing security teams with the most current information.

3. Automated incident response

Once you set up your EDR solution, the processes are deployed automatically. Everything from threat detection to incident investigation to event alerts is automated. Some EDR solutions even enable automatic incident response. You can set up triggers and watch your EDR solution apply real-time fixes. You'll get alerts for the event, and you'll be able to monitor how the EDR solution is keeping your network secure.

Conclusion

EDR solutions expand the security perimeter, enabling visibility into endpoint activity within the network. There are a variety of EDR solutions available, so you can compare and choose the solution that best suits your needs and budget.

If possible, go with an AI-powered EDR solution, as this will provide you with continuous automation and education capabilities. The EDR solution will continue to study your network and security events, improving the insights it gathers over time. This will help you gain a high level of analysis, and you'll be better prepared to respond to events.