META EAGLE
{MORE THAN JUST TECHNOLOGY}

Endpoint Detection and Response Demystified

eBook

Table of Contents

Ransomware. Zero day malware. Fileless attacks. Phishing and privilege escalation.

These all represent clear and present dangers to your networks, businesses, and personally identifiable information (PII).

For years, antivirus (AV) solutions were the major players on protecting customer endpoints. But as the threat landscape has shifted, we've seen the emergence of newer solutions built to deal with some of the problems inherent in AV.

You may have heard the term endpoint detection and response (EDR) crop up over the past few years. These solutions were put on the market specifically to adapt to the evolution of the threat landscape (and to recognize it will continue to evolve faster than humans can often keep up with). You may be curious about what these solutions are and why they stand apart.

We'll demystify these solutions today and, hopefully, show you why they're so integral to the future of cybersecurity.

What exactly is EDR?

Anton Chauvin of Gartner® originated the term endpoint detection and response, using it to describe a "family of new tools focused on visibility, and from prevention to detection for the endpoint."[1] EDR is a multifaceted solution that can best be described as expanding AV into a whole new realm.

Everything modern AV can do, EDR takes a step further—providing security and (more importantly) peace of mind. These include, but are not limited to:

- Monitoring
- Threat detection
- Allow listing and deny/exclude listing
- Threat response
- Integration with other cybersecurity solutions

Whether it's from using artificial intelligence (AI) to monitor for new threats and suspicious endpoint behavior, or automated rollback after a ransomware event, EDR solutions have developed multiple responses to increase the depth of protection IT can be used in organisations

[1]"A Short History of EDR," Reed Exhibitions Ltd. infosecurity-magazine.com/opinions/history-edr/ (Accessed September 2020).

Let's take a closer look at this new weapon made for your cybersecurity arsenal.

Where EDR fits in the cybersecurity universe

EDR centers on protecting endpoints. Given the number of threats that spawn daily, AV and other traditional endpoint security products can fall short for managing attacks across large numbers of endpoints. When we talk about traditional AV, it's typically from a passive standpoint. AV can only detect and quarantine known threats—those that have been previously identified.

Many AV solutions operate on traditional virus signatures. When a file gets discovered as malware, it generates a hash that then gets added to a virus signature database. AV programs then scan for files that match a known virus signature in their database, then quarantine the file.

Therein lies the rub—AV requires regular signature updates. This means there is often a gap in coverage between when a virus is discovered and when your customers become protected. Plus threats that haven't yet been discovered can operate in the wild before you can even get an update. It's a reactive approach.

In contrast, EDR is proactive. Comprised of monitoring software and endpoint agents, EDR solutions use integrated machine learning and advanced AI to identify suspicious behaviors and address them regardless of whether there's a signature. For example, if several files change at the same time, chances are it's more likely a result of an endpoint attack rather than user error.

Cybercriminals themselves have been proactive. Many have developed methods of evading traditional AV solutions. Some might develop malware that changes signatures regularly to avoid matching a known signature in an AV database, while others may use fileless attacks and set up a new admin account on an endpoint with strong privileges. An EDR solution looks for unusual behaviors on an endpoint (compared to a baseline), then takes action accordingly. This allows you to meet proactive cybercriminals with proactive defenses.

AV can only detect and quarantine known threats—those that have been previously identified.

The only constant is change

The world is in a constant state of flux, and technology is no different. The cloud has changed our lives in immeasurable ways, from the rise of e-commerce to enterprise-based solutions that billions of individuals rely on daily. Yet as technology advances, cybercriminals find new ways to exploit these changes and compromise company data. Data is arguably your customers' greatest asset—so how do you help safeguard it?

AV can only detect and quarantine known threats—those that have been previously identified. Like the cloud, AI and machine learning promise to change much of the way we do business and live our lives. AI and machine learning power EDR solutions, acting as the engine that fuels greater threat protection and allows it to recognise and deal with advanced threats.

An EDR solution uses machine learning to establish a baseline of behavior for an endpoint. From there, EDR discovers behaviors that veer from the baseline. This is where EDR excels—asking questions like:

- Has this endpoint performed this activity before?
- Does this file or behavior exhibit unusual patterns?
- Why are secured files being looked at or hit?

In essence, EDR solutions use AI to discover indications of a compromise without having to rely on known indications of compromise (which can be subverted). Advanced polymorphic viruses (those that can generate modified versions of themselves to counter detection) and zero day threats (which target and exploit a previously unknown vulnerability) will slip by solutions that can't ask and answer these questions. EDR not only asks these questions; it also provides the answers we need to address the threats—with options to kill, quarantine, remediate, and roll back.

How EDR solutions can respond to threats

EDR solutions don't just detect threats—they can also act on them. When an endpoint agent discovers a threat, a good EDR solution springs into action via the central monitoring system. The central monitoring system analyzes and correlates threats. Depending on which EDR solution you use, you can even visually trace the genesis of the threat and its path to the endpoint.

Meta Eagle Endpoint Detection and Response (EDR), for example, lets you see this attack timeline so you can understand the lifecycle of the attack. You can use this information to help prevent future threats, but it's also extremely helpful in showing tangible proof of the value of your security services to customers.

While AV and disk encryption are valid ways to secure your endpoints, EDR offers capabilities that help futureproof your users' machines. These include near real-time file analysis and alerts,

detailed forensics, offline protection, the ability to disconnect from the network to help prevent further spread, and the killer feature—infected file rollback.

In fact, let's look at how a solution like Meta Eagle EDR can help with ransomware. The common drill with ransomware goes as follows: someone opens an attachment or email, or visits a webpage with malicious script, and they're greeted with a notification that all their files are encrypted. The cybercriminal will only return their files after they pay a princely sum in Bitcoin or another cryptocurrency—except there is no guarantee they will get their data back. Many corporations are unwilling to risk paying a ransom because of this lack of a guarantee.

It can happen to anyone, and the facts are staggering:

- Businesses experienced an average of 16.2 days of downtime at the end of 2019 due to ransomware[2]
- One business will be hit every 11 seconds by a ransomware attack by 2021, according to some predictions[3]
- The predicted cost of damages due to ransomware in 2021 is $20 billion[4]

Meta Eagle EDR offers ransomware rollback to help you offer the greatest value to your clients. This feature uses advanced technology to take snapshots of the endpoint at regular intervals (set at the administrator's discretion). If ransomware hits, it only takes a few clicks to roll back the endpoint disk image to a previous point in time, helping save your customers significant time and money.

Meta Eagle **EDR and RMM**

Meta Eagle EDR uses AI and machine learning to detect endpoint threats. Not only can it detect suspicious behaviors at the endpoint level, it can also respond to those threats on your behalf based on set policies. You can even set it to automatically roll back endpoints to a known safe state after a potential attack—and reveal full timelines to show your a tangible, clear way that we've protected you from threats.

Plus Meta Eagle EDR is integrated within Meta RMM, our remote monitoring and management platform designed to help you get up and running fast and start monitoring devices in minutes. This means you can monitor endpoints and networks from the same dashboard as endpoint security. Meta RMM offers multiple other security layers available from the same dashboard, including patch management, web protection, backup, and disk encryption

2 "Ransomware Costs Double in Q4 as Ryuk, Sodinokibi Proliferate," Coveware. coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate (Accessed September 2020).

3 "Global Cybercrime Damages Predicted to Reach $6 Trillion Annually by 2021," Cybercrime Magazine. cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/ (Accessed September 2020).

4 "Global Cybercrime Damages Predicted to Reach $6 Trillion Annually by 2021," Cybercrime Magazine. cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/ (Accessed September 2020).

About Meta Eagle

Meta Eagle empowers enterprises to navigate the digital evolution. With a flexible technology platform and powerful integrations, we make it easy to monitor, manage, and protect customer systems, data, and networks. Our growing portfolio of security, automation, and backup and recovery solutions allow you to focus on running your business. Meta Eagle simplifies complex ecosystems and enables customers to solve their most pressing challenges. We provide extensive, proactive support—monitoring, maintenance and planning that allows you to

WORK HARD FROM ANYWHERE

metaeagle.co.uk