
EDR & THREATLOCKER®

What is an EDR?

Endpoint Detection and Response or EDR, monitors and records activities and workloads taking place on a device. Using various techniques, EDRs will work to detect any suspicious activity and respond accordingly. EDR enables IT administrators to view suspicious activity in near real-time across an organization's endpoints. Focusing on behavioral patterns and unusual activity, EDRs will work to block threats and protect devices. Many organizations rely on EDRs to make them aware of and protect themselves from any emerging cyber threats on their endpoints.

Is EDR enough?

While an EDR may seem like a great tool, as with all solutions, often it's not enough to rely on it alone. Many EDRs provide excellent logging and diagnostics for IT administrators; however, when it comes to responding to threats, the fact remains that there is still a decision being made as to what is good and bad behavior.

When an EDR detects a problem, it often looks for a known threat, using signatures, heuristics, or behavioral patterns to decide if something can be trusted. While this approach may work the majority of the time, for new and emerging cyberattacks and zero-day exploits, it must get these decisions right 100% of the time. By definition, a zero-day attack is an attack that uses a previously unknown vulnerability to gain access or cause damage to your systems. This can make it difficult for the EDR to detect malicious activity.

This is why organizations should implement a Zero Trust endpoint security solution in addition to their EDR solution.

How Does EDR Work?

The logging capabilities of EDR solutions can provide up-to-date, real-time insights into endpoints, as well as always being on the lookout for emerging threats.

Primary EDR Functions:

- Monitor and collect activity data from endpoints that might pose a threat.
- Analyze data and work to identify any threat patterns.
- Automatically respond to any identified threat, work to remove or contain them as well as notify security personnel.
- Forensics and analysis tools to research identified threats and search for suspicious activities.

How Does a Zero Trust Security Solution Help?

A zero trust security solution like ThreatLocker® focuses on blocking everything and only allowing the applications required as well as limiting application interactions. While a zero trust solution can work seamlessly and independently, it also compliments an EDR or XDR solution. When ThreatLocker® is paired with an EDR or XDR, both unknown and known threats will be blocked immediately and anything that is detected would result in a notification to alert your security operations center to check for any further action needed.

ThreatLocker is a Zero Trust endpoint security solution built to help prevent cyberattacks. The ThreatLocker solution comprises five key components, Allowlisting, Ringfencing™, Elevation Control, Storage Control, and Network Access Control (NAC). Each of these elements complement an EDR solution and work together to provide unified protection.

ThreatLocker® works by denying all applications from running except those that are explicitly allowed. This means untrusted software, including ransomware and other malware, will be denied by default. This is known as Allowlisting.

In many cases, it is difficult if not impossible for an automated tool such as an EDR to decide what is good or bad behavior of an application.

Unfortunately, EDRs may not be able to detect when an application is being weaponized against an organization. This is more commonly seen during zero-day attacks where unknown vulnerabilities are used to exploit organizations. The ThreatLocker solution, Ringfencing™, can help to solve this problem.

Ringfencing™ controls what applications can do once they are running. By limiting what software can do, ThreatLocker® can reduce the likelihood of an exploit being successful or an attacker weaponizing legitimate tools such as PowerShell. Ringfencing™ allows you to control how applications can interact with other applications. For example, while both Microsoft Word and PowerShell may be permitted, Ringfencing™ will stop Microsoft Word from being able to call PowerShell, thus preventing an attempted exploit of a vulnerability such as the Follina vulnerability from being successful.

Under normal operations, all applications permitted on an endpoint or server are able to access all data that the operating user can access. This means if the application is compromised, the attacker can use the application to steal or encrypt files. Ringfencing™ allows you to remove file access permissions for applications that do not need access and even remove network or registry permissions.

ThreatLocker® NAC is an endpoint firewall that gives you total control over network traffic, which ultimately helps you to protect your devices. Using custom-built policies, you can allow granular access based on IP address, specific keywords, or even agent authentication, or dynamic ACLs updated in real time by the ThreatLocker agent. Rather than relying on an EDR to determine if network traffic is good or bad, Network Access Control can give you total control over your traffic, helping you to mitigate attacks before they have the chance to exploit your network.

Having an EDR is a great step towards having a strong cybersecurity stack, however, it is not a one-stop solution. Zero Trust solutions like ThreatLocker® are able to build upon the security EDRs provide to give