MORPHISEC

Why is Endpoint Detection and Response Not Enough to Stop Ransomware?

Alert Overload

To stop ransomware, supply chain attacks, data theft, and other advanced attacks, endpoint detection and response (EDR) and extended detection and response (XDR) solutions must be configured to their highest alert settings, creating a sea of false alerts. This slows down your systems, applications, and teams handling IT support tickets and threat analysis.

What if you could eliminate false alerts?

Low EDR

Alert Mode

The result?

Threats are getting by your cybersecurity defenses

High EDR

Alert Mode

The result?

System degradation

40%+
False Positives

31%
Uninvestigated Alerts

83%
of companies have Alert Fatigue

Reactive, Not Proactive

If you use a standard EDR/XDR alert setting and nothing is beeping, that can be worse than too many alerts. (It likely means your EDR is failing.) EDR is designed for reactive detection and response, not proactive prevention. But what if you could use the standard EDR setting without missing advanced attacks? Leading analysts say Automated Moving Target Defense (AMTD) augments EDR effectiveness with best-in-class prevention for a true defense-in-depth strategy.

Resource Hogs

EDR /XDR and managed detection and response (MDR) need expensive staff trained in detection, response, and analysis. Ponemon research shows teams spend 25 percent of their time on false alerts. Teams without false alerts usually have settings too low, risking ransomware, brand damage, and lawsuits. Consider a managed services provider for MDR and EDR services, combined with AMTD to stop advanced threats that bypass EDR.

Can't Stop the Baddest Guys

EDR stops attacks that have known signatures and behaviors, but tests show most EDR is not effective against in-memory and fileless or runtime attacks. A research team in Greece tested a dozen top EDR solutions using Cobalt Strike MITRE ATT&CK tactics–and EDR clearly requires augmenting to stop advanced attacks. Many didn't even trigger alerts unless in ultra aggressive mode, which causes alert overload. Top analysts say AMTD is a game changer that eliminates this problem.

EDR	Alert Setting	CPL	HTA	EXE	DLL
Vendor #1	Standard	Block / A	Block / A	Fail / NA	Block / A
Vendor #2	Standard	Fail / A	Fail / A	Fail / NA	Fail / NA
Vendor #3	Standard	Fail / Na	Fail / NA	Block / A	Fail / NA
Vendor #4	Standard	Block / Na	Block / NA	Block / A	Fail / NA
Vendor #5	Standard	Fail / A	Fail / A	Fail / NA	Block / A
Vendor #6	Standard	Block / A	Block / A	Block / A	Block / A
Vendor #7	Standard	Block / A	Fail / A	Fail / NA	Fail / NA
Vendor #8	Standard	Fail / A	Block / A	Block / A	Fail / NA
Vendor #9	Ultra Aggressive	Block / A	Block / A	Block / A	Block / A
Vendor #10	Standard	Block / A	Block / A	Fail / NA	Fail / A
Vendor #11	Standard	Fail / A	Block / A	Fail / A	Fail / A
Vendor #12	Standard	Fail / NA	Fail / NA	Fail / NA	Fail / NA

A = Alert LA = Low Alert NA = No Alert

*STAR High Alert setting, high false positive alerts, PowerShell activity issues

Department of Informatics, University of Piraeus, Greece

Shifty Malware

Ransomware adversaries are big businesses. They employ polymorphic (shifting) techniques to lay low and bypass EDR, especially on standard alert settings. Most EDR & XDR use static defenses that do stop common attacks in low alert mode. However, to detect shifty malware, their agents need to be in high alert mode, which taxes CPU and memory resources. Servers crawl or crash. Performance declines and users complain.

AMTD

What if your defense was also shifty? AMTD uses lightweight agents and polymorphic prevention to outsmart the bad guys without impacting performance.

Creepy Ransomware

Malware often creeps across networks, sometimes for weeks, before triggering ransomware. Most EDRs either miss advanced attacks, or catch them too late. A threat that evades your EDR can move laterally across your network and attack critical systems, anywhere and any time. Analysts say response needs to be within minutes, not days or weeks. AMTD responds in seconds.

Light on Linux

Most EDR and XDR solutions aren't purpose-built for Linux attacks. These solutions use generic Windows tactics and don't employ Cloud Workload Protection Platform (CWPP) or server workload capabilities. Or worse, they're simply desktop solutions running on servers. Don't settle for this. AMTD for Linux is designed specifically for attacks on Linux servers.

About Morphisec

Founded in 2014, Morphisec, a pioneer in blast radius resiliency, keeps your business safe by intelligently anticipating and neutralizing threats - minimizing the impact and blast radius of cyber incidents and ensuring uninterrupted business operations without the need for constant tech team intervention or impact to performance.

Powered by Automated Moving Target Defense (AMTD) technology, the next evolution of cybersecurity, Morphisec protects over 7,000 organizations across nine million Windows and Linux endpoints, servers and workloads. Morphisec stops thousands of advanced attacks daily at Lenovo/Motorola, TruGreen, Cipla, Citizens Medical Center, and many more. Learn more at www.morphisec.com

To learn more, visit morphisec.com/demo