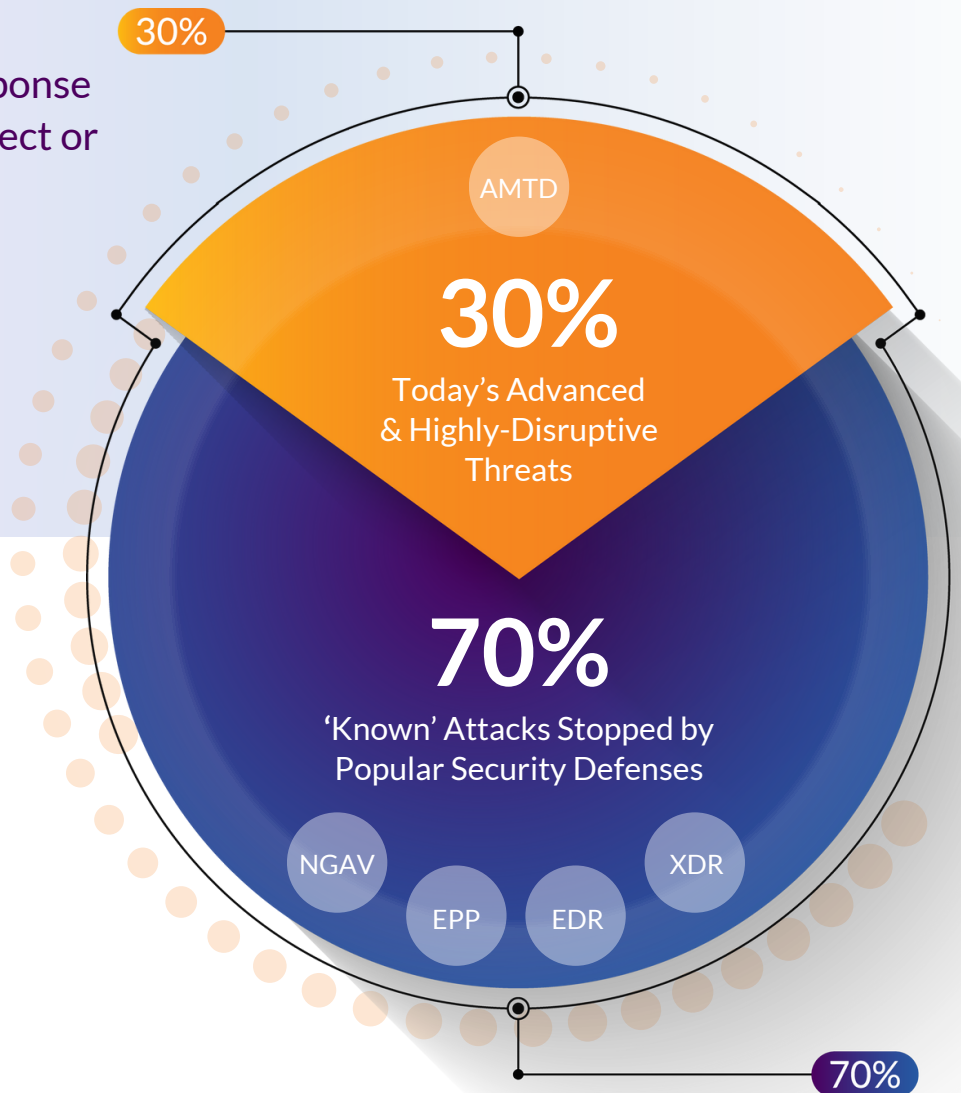


Endpoint Detection & Response

Featuring Automated Moving Target Defense

On its own, traditional endpoint detection & response (EDR) security fails to detect or prevent as much as 30% of modern sophisticated cyber threats, leaving businesses susceptible to malicious intrusion and compromise.

Omega's EDR solution is fortified with automated moving target defense (AMTD) technology, helping businesses close this growing security gap with enhanced detection and remediation capabilities that keep critical data safe from harm.



Why do businesses need enhanced EDR protections?

Recent studies show that evasive threats increasingly bypass Next-Gen Antivirus (NGAV), Endpoint Protection Platforms (EPP), and Endpoint Detection & Response (EDR & XDR) solutions.

Traditional EDR Captures: most "known" attacks, especially those with recognized signatures or behavioral patterns.

Next-Gen AMTD Captures: the remaining 'unknown' threats, including advanced malware variants and supply chain attacks that often lead to ransomware.



Features & Benefits of EDR + AMTD

Omega's EDR security service delivers 360-degree transparency and oversight of your company's endpoints with a fully flexible architecture that protects cloud, on-premise and hybrid environments. Combining critical endpoint monitoring, investigation and response with the enhanced capabilities of automated moving target defense (AMTD) – which detects and mitigates 'unknown' threat signatures – our EDR solution delivers a prevention-first security enhancement and helps businesses reduce vulnerabilities and stay vigilant against today's most sophisticated attacks.



Proactive Threat Hunting

monitors stealthy behavior across all your organization's endpoints



Data Retention

exceeds typical retention periods for maximum historical analysis



One-Click Remediation & Rollback

simplifies response and restores deleted or compromised files



Automated Moving Target Defense (AMTD)

uses memory polymorphism to deceive attackers and protect against advanced threats on Windows and Linux systems

How Omega's EDR Solution Works

- 01 Detect »** Gain extensive visibility into your overall endpoint security, leveraging Omega's in-house team for round-the-clock monitoring that doesn't interfere with your daily operations.
- 02 Deceive (via AMTD) »** If complex threats bypass the first line of endpoint security detection, moving target defense technology steps in. Utilizing next-generation deception tactics like polymorphism, AMTD uses machine-learning to deploy decoy targets and trap threats, continuously adapting and reconfiguring to outmaneuver persistent attacks.
- 03 Investigate »** Advanced threat intelligence prioritizes endpoint events and delivers deep analysis for rapid diagnosis. With access to forensic data, our SOC analysts can provide your team with critical information to guide future security incident analysis and aid in overall IT budgeting and decision-making.
- 04 Respond »** In the event cyber threats are detected, EDR facilitates rapid recovery capabilities. Isolation and quarantine features stop threats in real time, limiting damage to the rest of your endpoints. Plus, roll back to earlier states with one easy click to ensure you don't lose access to critical data.



Let's Talk About EDR