PRODUCT BROCHURE

Datto EDR

Endpoint Detection & Response — Advanced Threat Hunting

Antivirus stops known threats. EDR stops everything else. Datto EDR provides behavioral threat detection, automated containment, forensic investigation, and guided remediation — closing the gap that AV alone cannot cover.

97%	197 days	<60 sec
of advanced malware evades traditional AV	Average dwell time without EDR	Automated endpoint containment time

Degarmo Technologies | degarmo.tech | July 2026

AV VS EDR

Why Antivirus Alone Is Not Enough

AV prevents. EDR detects, investigates, and responds — even when prevention fails.

UNDERSTANDING THE GAP

Antivirus is a prevention tool — it blocks known threats before they execute. But modern attackers use techniques specifically engineered to bypass prevention: living-off-the-land attacks using legitimate Windows tools, encrypted payloads, fileless execution, and slow-burn intrusions that stay under the radar for months. EDR is designed to catch what slips through.

Capability	Antivirus (AV)	EDR
Detection Method	Signature & heuristic matching	Behavioral analysis + MITRE ATT&CK mapping
Response	Block/quarantine on detection	Contain, investigate, remediate, report
Visibility	File-level detection events	Full process tree, network, registry, memory
Dwell Time Coverage	Misses slow-burn intrusions	Detects lateral movement & persistence
Forensics	None	Full attack timeline and root cause analysis
Threat Hunting	Not available	Proactive hunt across all endpoints

HOW EDR MAPS TO THE MITRE ATT&CK; FRAMEWORK

Datto EDR maps all detected behaviors to the MITRE ATT&CK; framework — the industry-standard taxonomy of attacker techniques. This means every alert tells you not just what happened, but where it fits in the attack lifecycle and what the attacker likely intended.

EDR detects and blocks at Execution and beyond — limiting attacker progress through the kill chain.

PLATFORM CAPABILITIES

Detect. Contain. Investigate. Remediate.

Datto EDR closes the loop on every detected threat — from initial alert to full resolution.

CORE EDR CAPABILITIES

Behavioral Threat Hunting

Continuously searches all endpoint telemetry for indicators of compromise — including techniques that generate no alerts until they are correlated into a pattern.

Automated Endpoint Containment

On confirmed threat detection, the affected endpoint is automatically isolated from the network in under 60 seconds — stopping lateral movement while investigation continues.

Full Forensic Timeline

Every process, network connection, file write, and registry change is recorded in a searchable timeline — enabling complete root cause analysis of any incident.

Guided Remediation

After containment, Datto EDR provides step-by-step remediation guidance — removing the attacker's foothold, cleaning persistence mechanisms, and restoring normal operation.

Incident Reporting

Every confirmed incident generates a structured report documenting the attack vector, TTPs used, scope of compromise, and actions taken — ready for leadership and compliance.

Compliance Evidence

EDR activity logs and incident reports satisfy NIST CSF, HIPAA, PCI DSS, and CMMC requirements for continuous endpoint monitoring and incident response documentation.

Managed EDR — Investigation Without the Burden

EDR generates a high volume of telemetry that requires security expertise to interpret. Degarmo Technologies reviews all EDR alerts, performs triage, investigates confirmed detections, and coordinates remediation — so you get the protection without the analyst overhead.

Stop Assuming. Start Knowing.

Most businesses have no idea whether an attacker is already inside their network. Degarmo Technologies can deploy Datto EDR across your endpoints and run a threat hunt to find out — definitively.

- **Free Threat Assessment Available**
- **EDR Live in Days**
- **Managed Investigation & Response Included**

Visit degarmo.tech | Oklahoma City, OK | Veteran-Owned MSSP