datto
A Kaseya COMPANY

Datto EDR

Advanced Endpoint Threat Detection and Response for MSPs

Many of today's cybercriminals can bypass traditional defenses at will. This leaves businesses exposed to ransomware, credential harvesting and other types of attacks that can cost $8,000 per hour from the time of the known attack to remediation. Now more than ever, businesses need advanced endpoint threat detection and response (EDR) in addition to having an antivirus (AV) installed on each endpoint.

Unfortunately, most small and medium-sized businesses can't afford to use traditional EDR solutions which are costly and cumbersome to deploy and manage. The same goes for Managed Service Providers (MSPs) that may lack the resources and professional expertise required to effectively utilize traditional EDR.

This leaves many MSPs and their customers open to ransomware, fileless malware, credential harvesting, data loss and other cyberattacks.

Highly-effective endpoint detection and response designed for the MSP

Tailored for today's MSP, Datto EDR provides effective endpoint detection and response in an affordable, easy to use, manage and deploy package. Unlike other EDR products that are built for large-scale enterprise SOC teams, Datto EDR eliminates common EDR issues, such as high-cost, management complexity and alert fatigue. Each alert comes with a quick, easy-to-execute set of response guidelines to support your team in isolating infected hosts, terminating processes, and collecting additional evidence.

- Sophisticated threat detection and response: Datto EDR detects suspicious behaviors and threats that evade traditional defenses so you can respond quickly, before significant damage is done.
- Click-to-respond: Datto EDR allows you to take action against advanced threats right from your alert dashboard. Isolate hosts, terminate processes, delete files, and more without wasting precious seconds.
- Detect fileless attacks with behavioral analysis: Our patented deep memory analysis ensures you are informed of even the most elusive threat actors.
- MITRE ATT&CK mapping: Alerts are mapped to the MITRE ATT&CK framework to provide context and helpful clarity to your team, reducing the security expertise required to effectively respond.
- Smart Recommendations: Our seasoned security analysts have distilled their experience into automated mitigation recommendations, so our alerting engine will help your team through the remediation process in a quick and efficient manner.
- Scalable, remote response actions: The unique click-to-respond feature supports your team in taking action against threats as quickly as they are detected to reduce potential damage.
- Deep integration: Ideal for MSPs, Datto EDR integrates with Datto RMM for efficient endpoint management, and for SMBs who use the Kaseya IT Complete platform, Datto EDR integration eliminates the need to switch consoles for a seamless endpoint security experience.

Feature highlights

Complete Endpoint Protection

Datto EDR allows for the management of Microsoft Defender Antivirus, enabling proactive, real-time endpoint protection without additional agent installation. It identifies malware automatically based on suspicious and malicious behaviors at the endpoint, such as unusual processes, unexpected startup locations and modifications in registry keys, file system or file structure. Datto EDR enforces a secure configuration and adds monitoring capabilities, further enhancing endpoint protection.

Key prevention features:

- Block potentially unwanted applications
- Block risky DNS requests
- Quarantine threats
- Alert management inside EDR console
- Scheduled and ad hoc scans
- Manage exclusions

Datto EDR's ability to prevent threats consistently scores very high in independent testing. Used in conjunction with Microsoft Defender Antivirus, it provides top value while reducing MSP costs.

Detection

Datto EDR detects suspicious behaviors, as well as fileless malware and ransomware, automatically terminating the malicious activities and isolating infected endpoints to prevent further spread of a cyber attack.

Key detection features:

- Real time endpoint security monitoring
- Deep memory monitoring & analysis
- Advanced threat detection combining static detection with behavior and anomaly-based detection
- MITRE ATT&CK mapping
- Behavioral-based ransomware detection and containment
- Modular threat hunting capabilities
- Real-time escalation through alerts, integrations, Webhooks and email

Datto EDR's advanced real-time detection and isolation capabilities reduces time to response to the minimum. Enhanced by remote response capabilities, Datto EDR helps prevent the spread of malware within the infected organization.

Threat Intelligence & Analysis

Backed by a threat intelligence and analyst team that constantly investigates previously unknown and suspicious malware samples, Datto EDR is always up allowing protection from the latest threats.

Key features:

- Integrated threat intelligence from numerous intelligence and community sources
- Malware sandbox analysis
- Analysis of cryptographic hashes of executables
- Digital forensic analysis of previously unknown and suspicious threats
- Threat enrichment & categorization service
- Advanced correlation engine

With Datto EDR, you can be sure that your endpoint security reflects the most up-to-date threat intel and forensics, reducing the risk of missing unknown threats.

Response

With Datto EDR, MSPs can easily respond to cyber incidents as they occur. And do that from a remote location. Using a unique console, MSPs are empowered to take the following response actions:

- Device Isolation
- Process termination
- Execution of threat response scripts across multiple devices
- Templated threat remediation recommendations

These capabilities, together with advanced security dashboards offering a single-pane-of-glass into all security alerts and device compliance issues, enable MSPs to respond immediately to cyber threats when needed, minimizing downtime and reducing loss.

Integrations

- Kaseya IT Complete
- Datto RMM
- Datto Managed SOC, powered by RocketCyber
- Integration via API
- Webhooks (SIEM, ticketing systems)

Supported Platforms

- Windows
- Linux
- MacOS

datto
A Kaseya COMPANY

Corporate Headquarters
Kaseya Miami
701 Brickell Avenue
Suite 400
Miami, FL 33131

partners@datto.com
www.datto.com
888.294.6312

Global Offices
USA: 888.294.6312
Canada: 877.811.0577
EMEA: +44 (0) 118 402 9606
Australia: +61 (02) 9696 8190
Singapore: +65-31586291