Managed Detection & Response

MDR Complete Solution

MDR is only as good as its ability to manage, detect, and respond to security issues across your endpoints and network. Make sure yours is complete!

A complete Managed Detection and Response (MDR) offering should include a mix of network and endpoint security. While focusing on the endpoint is important, it is not enough; many of today's sophisticated cybersecurity threats are network born and not endpoint-based—driving the necessity of network telemetry, not just endpoint analysis.

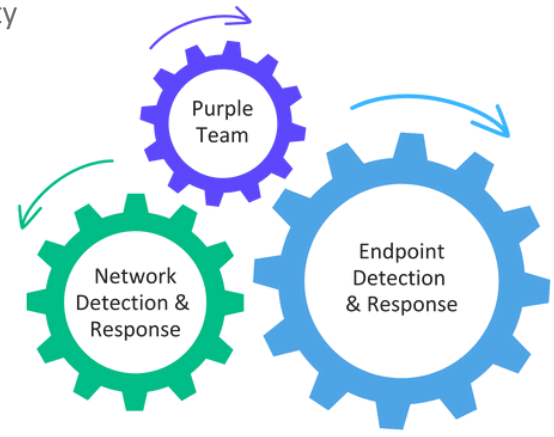
You can't close the holes adversaries will exploit without visibility into vulnerabilities and network telemetry. To effectively combat today's threat actors, it is critical for a complete solution to go beyond just the endpoint.

Up-level Your Security Stance

Our MDR delivers differentiated endpoint and network detection and response, security controls validation, and vulnerability assessment, external and cloud posture management — consolidating multiple technologies into one easy-to-consume solution.

MDR Complete offering is a fully managed detection and response service with a fully manned Security Operations Center (SOC), available to back your security organization 24x7.

Managed via our globally available multi-tenant SaaS platform, it's an ideal entry-level security offering for small to mid enterprises. On-ramping is quick and easy, and costs are predictable and affordable.



KEY BENEFITS

- No need to build, staff and manage—we do it for you!
- One comprehensive platform eliminates redundant endpoint agents and lowers OPEX
- 97% customer support satisfaction and 96% of customers recommend
- Ransomware solved through superior behavioral AI
- Network visibility through sensors
- Rogue device detection
- Autonomous protective responses trigger instantly
- Time saving, fatigue-reducing forensic timeline for incident responders and threat hunters
- Purple teaming provides peace of mind

CONTACT US

MDR Complete

MDR Complete combines endpoint and network detection and response, vulnerability assessment, and automated purple teaming —all managed and monitored by our 24x7 security operations team. MDR is our entry-level SOC offering for small or highly distributed companies with limited infrastructure requirements.

Built-in Static & Behavioral AIs detect and prevent a wide range of attacks in real time before they can cause damage. Our MDR offering protects against known and unknown malware, trojans, hacking tools, ransomware, memory exploits, script misuse, bad macros, and more.

- **True merging of EPP, EDR & NTA** with EDR, NDR, VA, & SCV functions.
- **Threat intelligence** is integrated through our platform and AI functions.
- **Agents are autonomous** and apply detection and prevention technology even without cloud connectivity and will trigger protective responses in real-time.
- **Fast recovery** gets users back and working in minutes without re-imaging and writing scripts. Any unauthorized changes that occur during an attack can be reversed with a single-click remediation for Windows.
- **Secure Global SaaS management interfaces**. Choose from US, EU, and APAC localities. Data-driven dashboards, policy management by site and group, incident analysis with MITRE ATT&CK integration, and more.
- **Firewall Control** for control of network connectivity to and from devices, including location awareness.
- **Device Control** for control of USB and Bluetooth/BLE devices and peripherals.
- **Network Sensors** provide rogue visibility to uncover devices on the network that are unmanaged and need protection.
- **Vulnerability Management** for insight into 3rd party apps on endpoints that have known vulnerabilities—mapped to the MITRE CVE database and classified by the CVSS scoring system.
- **Forensic timelines** for fast RCA and easy recovery.
- **Integrated threat intelligence** for visibility into both benign and malicious data.
- Active threat hunting by **MITRE ATT&CK® Technique**.
- Purple Teaming with **Synthetic ATT&CKs** built on MITRE TTPs.
- **IoC Defenition** and tracking for zero-day threats for enforcement by the EPP functions.
- **24 x 7 x 365 Security Operations Center** (SOC):
  - Identify, Protect, Detect & Respond
  - Active Threat Hunting
  - Continuous Incident Response (CIR)
  - Document and perform Post Action Reports

Stop ransomeware and other fileless attacks with behavioral AI and strong autonomous remediation.

KEY FEATURES

- Distributed Endpoint Security
- Distributed Network Security
- Vulnerability Assessment
- Security Controls Validation (Purple Teaming)
- 24 x 7 x 365 Security Operations Center (SOC)
- 365 days threat incident history
- Integrated intelligence and MITRE ATT&CK® threat indicators
- External & Cloud Posture Management
- Data-driven Dashboard Security Analytics
- Global SaaS implementation. Highly available. Choice of locality (US, EU, APAC)
- Flexible administrative authentication and authorization: SSO, MFA, RBAC
- Role-based Administration

MDR Features	Complete
Global SaaS Platform	
Secure, High Availability, Role-based Access	✓
Extended Historical Data Storage (available 14-365+ days)	✓
Blue Teaming	
24 x 7 x 365 Security Operations Center (SOC)	✓
Active threat hunting	✓
Real-time identification and response to threats	✓
Continuous Incident Response (CIR)	✓
Post Action Reports	✓
Threat Hunting by MITRE ATT&CK® technique	✓
Automated IoC watchlist and alerting	✓
Deep Visibility Mark Benign threat flagging for enforcement/response	✓
Incident Analysis (MITRE ATT&CK®, timeline, explorer, team annotations)	✓
Red Team	
Operating Systems Vulnerabilities	✓
Third-party Application Vulnerability (Win, Mac)	✓
Internal & External Vulnerability Assessment based on MITRE CVE/CVSS	✓
Continuous External Pentesting (CPT)	✓
Monthly Internal Simulated ATT&CK® modeling MITRE TTPs	✓
External & Cloud Posture Management based on CIS Benchmarks	✓
Network Detection	
Analytics, Rogue Device Detection, IoT Control	✓
OS Firewall control with location awareness (Win, Mac, Linux)	✓
Unmanaged Device Visibility	✓
Quarantine/Isolate Devise(s) from the network	✓
Endpoint Protection & Detection	
Manual / Auto file fetch (Windows, Mac, Linux)	✓
Secure Remote Shell (Windows Powershell, Mac & Linux bash)	✓
USB device control (Win, Mac)	✓
Bluetooth® / Bluetooth Low Energy® control (Win, Mac)	✓
Static AI & Cloud file-based attack prevention	✓
Behavioral AI fileless attack detection	✓
Autonomous Threat Response / Kill, Quarantine, Isolate (Win, Mac, Linux)	✓
Autonomous Remediation Response / 1-Click, no scripting (Win, Mac)	✓
Autonomous Rollback Response / 1-Click, no scripting (Win)	✓
Agent anti-tamper	✓

Windows agents
All Windows workstation starting with 7 SP1 through Windows 11

All Windows Server starting with 2008 R2 SP1 through Server 2022

Mac agents
Big Sur, Monterey, Ventura, Sonoma

Windows Legacy agents
XP, Server 2003 & 2008, POS2009

Linux agents
Ubuntu, Redhat (RHEL), CentOS, Oracle, Amazon AMI, SUSE Linux Enterprise Server, Fedora, Debian, Virtuozzo, Scientific Linux

Container Support
Kubernetes self-managed v1.13+ [self-managed, AWS Kubernetes (EKS), Azure AKS]

Virtualization & VDI
Citrix XenApp, Citrix XenDesktop, Oracle VirtualBox, VMware vSphere, VMware Workstation, VMware Fusion, VMware Horizon, Microsoft Hyper-V