MANAGED DETECTION AND RESPONSE
ACCELERATE AND SIMPLIFY THREAT DETECTION, INCIDENT RESPONSE

SOLUTION OVERVIEW
Managed Detection and Response (MDR) accelerates and simplifies threat detection, incident response and compliance management for IT teams with limited resources. MDR is an affordable, efficient and comprehensive managed security solution that integrates threat intelligence and expert engineers to speed detection and response times to cybersecurity events.

Deploy security monitoring and incident response for your whole network without taking existing resources away from revenue-generating projects or adding expensive security talent to budget.

KEY CAPABILITIES
- Fully managed
- Unified solution
- Complete visibility
- Monitors and reports
- Cloud and on-premises
- Peace of mind
- Total detection
- Compliance
- Expert engineers

24/7/365 OPERATIONS CENTER
- Detects emerging threats across your network
- Validates threats during alert investigation and initiates incident response
- Monitors entire network for threats, including cloud and on-premises
- Supplies complete visibility for immediate answers and immediate response
- Manages and reports on compliance (SOC2, NIST, GDPR, PCI, HIPPA, NERC, CIP and more)

"Recently, a user unwittingly clicked on a link which downloaded aggressive malware. Magna5 was able to quickly detect the malware and block it from contacting its source. They saved us from losing data or having locked files. Magna5 has been a great business partner by helping us achieve an excellent cybersecurity posture."

- ANONYMOUS FINANCIAL COMPANY, Pittsburgh, PA
Customer since 2010
MANAGED DETECTION AND RESPONSE
Multiple capabilities, one trusted solution

CORE FUNCTIONS
• **SIEM**: correlate and analyze security data across networks with log management and event correlation.
• **Vulnerability Scans**: identify vulnerabilities within active networks and assets to avoid compromise.
• **Intrusion Detection**: detect malicious traffic with network IDS, host IDS and file integrity monitoring.
• **Behavioral Monitoring**: identify suspicious behavior and compromised systems with netflow analysis and availability monitoring.
• **Asset Discovery**: know who and what is connected to your environment at all times.
• **Compliance Management**: simplify compliance regulations with real-time reporting and continuous management.

CONNECTED SECURITY
• Integrated third-party security and productivity tools collect critical data from cloud-based and on-premises infrastructures, as well as cloud services, to centralize data and make it easier to investigate and respond to threats.
• Triggered-action responses communicate important data to third-party tools to close the loop of threat detection.
• Gain insights into trends and anomalies within third-party applications to fully connect security posture throughout entire environment.
• Applications include: Office 365, G Suite, Amazon, Microsoft Azure, Carbon Black, Palo Alto, Cisco Umbrella and more.

INCIDENT RESPONSE
• Backed by the Magna5 Operations Center that is fully-staffed 24/7/365 to ensure complete security of your entire network.
• Magna5's security experts act as an extension of an in-house team by monitoring, validating and responding to real-time threats.
• When a security event occurs, Magna5 is notified and takes immediate action to escalate and assist with the issue.
• Full remediation support available.
• Save time and money by filling expertise gaps and eliminating the need to hire additional in-house and expensive personnel.

Making Smart Connections to Keep Business Data Secure