Fidelis Cybersecurity

DATASHEET

Fidelis Managed Detection and Response (MDR) Service

Providing 24x7 Visibility Across Your Infrastructure to Reduce Dwell Time

The Challenge

In the cybersecurity battle, no organization is immune to attack. Despite organizations having many tools in their security stack, data breaches continue to occur at alarming rates. Once attackers breach the perimeter they have, on average, over 100 days to move throughout the network and steal sensitive data before they are detected.[1] This is why the industry is recognizing the need to shift from a vulnerability-centric approach to one that is threat-centric. "Managed detection and response improves threat detection monitoring and incident response capabilities via a turnkey approach to detecting threats that have bypassed other controls."[2]

MDR, Not MSSP to Deliver Unmatched Expertise

Many MSSPs are now calling themselves MDR, but while MSSPs are reactive and vulnerability-centric in their approach, MDR providers are proactive and threat-centric. The Fidelis MDR service is run by a team of expert security operations professionals, forensic analysts, incident responders, and threat hunters - many of whom have come out of the US Intelligence community. These experts have been called in to successfully run critical IR projects in response to many of the largest data breaches on record. Our analysts are accustomed to finding and rooting out attackers that were undetected by other security tools and services.

Combining the expertise of our MDR analysts with the power of Fidelis' technology, organizations are assured of faster response to terminate attacks as they occur, the eradication of threats, and improved protection of sensitive data.

[1] 2018 Ponemon Cost of Data Breach Study

[2] Gartner Market Guide for Managed Detection and Response Services, Toby Bussa, Craig Lawson, Kelly M. Kavanagh, Sid Deshpande, 31 May 2017

Key Benefits:

- See across all ports and protocols, endpoint activities, lateral movement, and data theft
- Extend visibility to legacy systems, shadow IT, and IoT devices using Fidelis Deception®
- Drill deeper into content via patented Deep Session Inspection™
- Decode executables and scripts to detect malicious activity in transit
- Automatically validate network alerts at the endpoint to ensure faster response
- Lure attackers and malicious insiders away from critical assets and data to decoys and breadcrumbs that look and feel real
- Enable full visibility and threat hunting by storing rich network and endpoint historical metadata

Capability	Fidelis MDR	Other MDR Providers	MSSPs
24x7 Threat Detection and Response	●	●	●
Integrated technology stack including Endpoint, Network and Deception	●	●	●
Proactively hunt for threats on your network and endpoints	●	●	●
Threat research and analysis included as part of base MDR offering	●	●	●
Conduct proactive investigations for unknown threats	●	●	●
Triage and remediation included in the same price and offering	●	●	●
Deep Session Inspection to thoroughly analyze network traffic and metadata	●	●	●
Tight integration with Deception to create breadcrumb trails and leverage Windows AD to misdirect and gather information on attackers	●	●	●
Access to technology included in the service (not just report portal)	●	●	●
Intelligence-based Threat Detection (IOC's, IOA's, behavior anomalies, 3rd party intel)	●	●	●
Team of seasoned Threat Detection experts available via phone, email, text	●	●	●
Manage Firewalls, IPS and security infrastructure	●	●	●

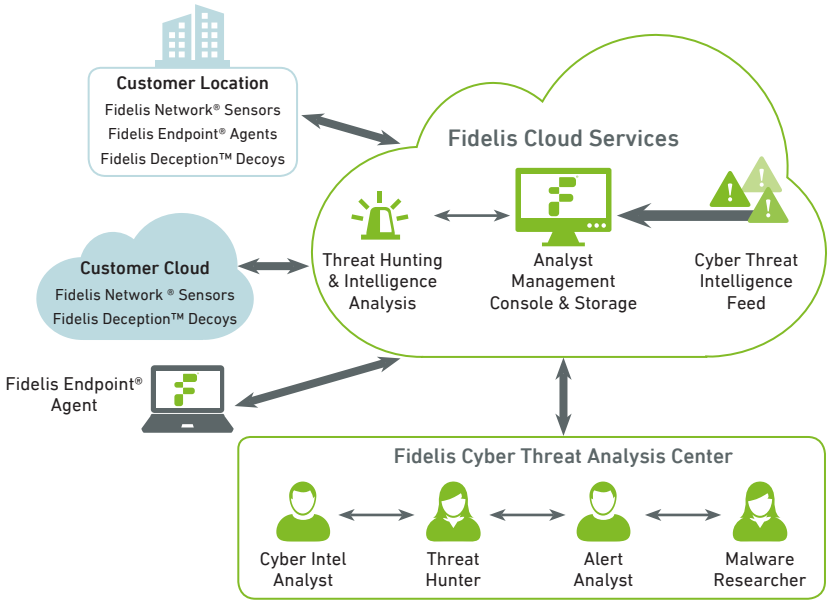
Enforcing Your Security Policies and Compliance Requirements

The Fidelis Managed Detection and Response service keeps organizations and their sensitive data safe from advanced attacks that traditional perimeter-centric, signature and log-based security tools alone have not prevented. The MDR service is powered by the Fidelis Elevate™ platform, which integrates network visibility, data loss prevention, endpoint detection and response, and deception into one unified security solution. Our 24x7 Threat Analysis Center is staffed by a team of highly trained security analysts and incident responders who proactively hunt for threats, fully investigate and respond to detected threats, and stop attacks and data theft.

The Fidelis MDR team verifies and enforces your security policies and compliance requirements to ensure the highest standards. Instead of worrying about alert workflows and turning your enterprise data protection policies into action, you can feel confident with a full-service solution that focuses on detection, response, and guidance on remediation.

Fidelis Has You Covered

Our MDR service delivers enterprise-grade security to organizations of all sizes. Augment your existing SOC with proactive threat hunting or have us act as your trusted security team running the Fidelis Elevate platform. With Fidelis MDR, you gain a competitive edge with the benefits of unmatched security expertise and a unified security operations platform that has been designed to protect the most complex environments.



Fidelis MDR Services

The Fidelis Difference: Advanced Threat Detection and Response to Terminate Attacks and Prevent Data Theft

Fidelis MDR monitors your environment and manages the Elevate platform to:

- Proactively discover new activity on your infrastructure
- Detect threats in real-time and retroactively by analyzing network and endpoint metadata based on Deep Session Inspection®, threat intelligence, endpoint events and logs, machine learning, and sandboxing
- Delay attackers and insider threats by disguising your network with decoys, detecting intruders, and luring adversaries away from your critical assets
- Automate response by jumpstarting playbooks, preventing malware, terminating attacks from multiple angles, and stopping data theft — within seconds or minutes, not days or hours

Fidelis MDR is the only security service that includes deception to lure adversaries away from critical assets and sensitive data to decoy environments that look and feel real. By ensuring faster threat detection and response to advanced threats and preventing data theft, our MDR service enables you to focus on your core business.

Trusted and Proven By the World's Largest Organizations, Delivering MDR for All

Fidelis solutions are enterprise-grade and trusted by some of the world's largest organizations — including 12 of the Fortune 50, 24 of the Fortune 100, and many government agencies — to protect their data. Our technology is innovative, from a rich heritage in network DLP to breach detection to EDR to deception defenses enabling automated detection and response across networks, endpoints and cloud environments. Our expertise is deep and proven as Fidelis security experts have been called in post-breach to manage incident response for some of the largest data breaches on record. With Fidelis MDR, organizations, whether large or small, gain the benefits of enterprise-grade technology and proven expertise scaled to meet the different needs of security teams.

Contact Us Today to Learn More

Fidelis Cybersecurity | 800.652.4020 | info@fidelissecurity.com

Fidelis Cybersecurity is a leading provider of threat detection, hunting and response solutions. Fidelis combats the full spectrum of cyber-crime, data theft and espionage by providing full visibility across hybrid cloud / on-prem environments, automating threat and data theft detection, empowering threat hunting and optimizing incident response with context, speed and accuracy. Fidelis is trusted by Global 1000s and Governments as their last line of defense. Get in the hunt. For more information go to www.fidelissecurity.com.

