ASPIRE MANAGED DETECTION & RESPONSE (MDR)

THE MDR ADVANTAGE

A stronger security posture that protects against threats with an expert team of analysts and incident responders

Advanced automation and response platform with built-in threat intelligence

Management and prioritization of alerts across cloud, network, and endpoints with defined response playbooks

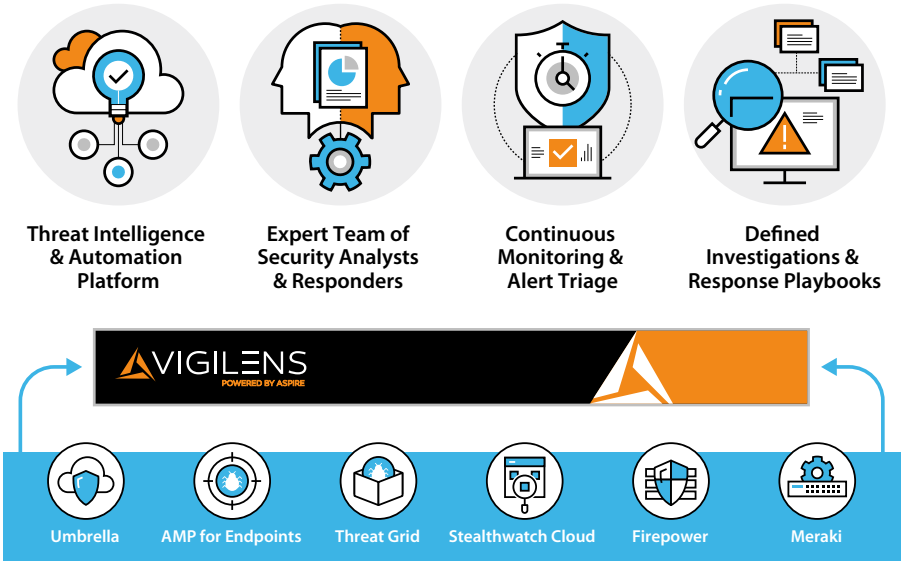
Powerful integrated security architecture providing greater visibility and context

24x7 analysis, investigation, and response to detect and respond to security threats faster

NEXT-GENERATION MANAGED SECURITY SERVICES TO MONITOR, DETECT, AND RAPIDLY RESPOND TO THREATS

The evolving threat landscape and increased risk of breach is causing cybersecurity to be a boardroom-level concern for most organizations. Security teams today are struggling with expanded attack surfaces and an overwhelming number of alerts. Often combined with disparate tools and insufficient in-house security expertise, the result is gaps in security, higher operational costs, and increased risk to the business. Your company's security depends on being able to recognize advanced threats and respond to malicious activity quickly. Aspire Managed Detection & Response (MDR) services provide 24x7 visibility, detection, and response capabilities across cloud, network, and endpoints.

Aspire MDR combines an expert team of security analysts and incident responders with industry-leading threat intelligence, an automation and security incident & event management (SIEM) platform, and defined response playbooks. The service leverages Cisco's integrated security architecture to advance defense capabilities by delivering 24/7 threat monitoring, detection, and response. Delivered from Aspire's Network & Security Operations Center (NSOC), our team exposes potential adversaries by prioritizing threat activity to identify which events require action. Built-in automation, threat intelligence, and customized playbooks reduce the mean time to detect and contain threats with relevant, meaningful and prioritized response actions. The core MDR security technologies are managed by Aspire, with access provided to your team for more efficient collaboration on investigations and response activities.



WWW.ASPIRETRANSFORMS.COM
ASPIRE TECHNOLOGY PARTNERS | 25 JAMES WAY, EATONTOWN, NJ 07724 | (732) 847-9600

ASPIRE
Powering Business Transformation

ASPIRE MANAGED DETECTION & RESPONSE (MDR)

ACCELERATE THE MATURITY OF YOUR SECURITY OPERATIONS

Powered by automation and advanced analytics, Aspire's VIGILENS platform ingests data and sifts through events, gaining visibility and valuable context from multiple layers of detection. Aspire security analysts and incident responders are alerted to threats occurring within your cloud, on-premise network, and endpoints. Working as an extension of your IT operations, our team provides clarity to attacks and expert guidance to eliminate threats quickly and prevent malicious activity.

Aspire MDR features:

- **Detection** is driven by ingesting, correlating, and analyzing data from multiple layers of security technologies. Leveraging integrated threat intelligence, statistical analysis, and machine learning, the MDR platform reduces mean time to detect and contain threats. Advanced technologies and proven methodologies provide higher confidence in triggered alerts.
- **Analysis** is performed to verify threats utilizing automated enrichment from the core security technologies. Integrated threat intelligence helps determine validity, identifies attacker attributes, and the potential impact and scope of an alert.
- **Investigation** by our NSOC team identifies accompanying indicators of compromise or attack and determines impact and urgency. When malicious incidents, malware, ransomware, and other destructive events are detected, we make intelligence-driven decisions to respond with relevant recommendations and meaningful guidance.
- **Response** utilizes advanced technologies and automation, with established case management tools and methodologies to contain, mitigate, and eradicate threats using response playbooks and customized action plans.
- **Cyber Threat Intelligence** gathered from a broad set of sources to corroborate and contextualize threats.
- **Client Portal** provides access to the core MDR technologies as well as dashboard, ticketing, reporting, and the case management interface – offering IT operations visibility to all activities.
- **A Dedicated Customer Success Manager** is your internal advocate to ensure all aspects of service delivery meet your expectations.
- **Incident Response** retainer services provide emergency on-site resources for breach containment, identifying root cause, and designing strategies to remedy any underlying issues.

AN INTEGRATED SECURITY ARCHITECTURE WITH MULTIPLE LAYERS OF PROTECTION

- Cisco Umbrella enforces DNS-layer security to proactively block threats before they reach your network or endpoints.
- Stealthwatch Cloud provides broad visibility into your cloud resources, internal network, and can even identify threats within encrypted traffic.
- Advanced Malware Protection (AMP) for Endpoints continually evolves your endpoint defenses with deep malware analysis, preventing malicious files from spreading.
- Threat Grid with advanced sandboxing analyzes the threat new malware poses to your specific environment and helps prioritize proactive defenses.
- Firepower Next-Generation Firewall (NGFW) delivers the deepest network and security visibility to quickly detect and stop threats as they occur.

cisco Partner

Gold Certified
Master Specialized in Security
Cloud and Managed Service Provider

Aspire MDR is powered by VIGILENS™.
To learn more, please visit www.AspireTransforms.com