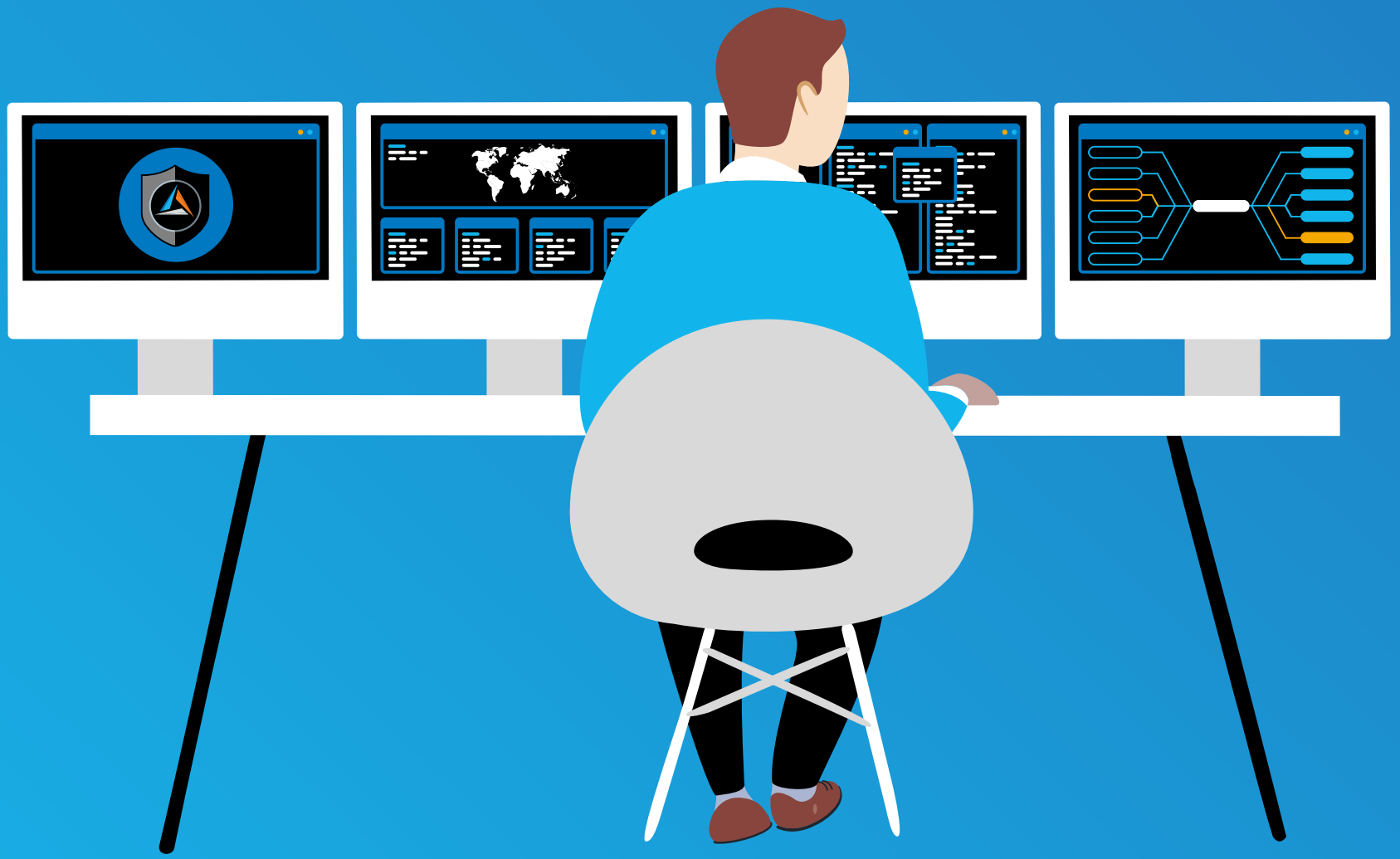
ASPIRE
Powering Business Transformation™

Cisco Partner
Master Security Specialized
Master Networking Specialized
Master Collaboration Specialized
Gold Integrator

Aspire Managed Detection and Response FAQ



Aspire MDR FAQ

Q **What is Managed Detection and Response (MDR)?**

A Managed Detection and Response services provide customers with remotely delivered security operations center functions.

MDR services enable organizations to:

- Quickly detect potential attacks
- Investigate threats
- Actively respond to incidents
- Mitigate risks

MDR providers collect real-time relevant logs and contextual information from endpoints, networks, cloud services, and applications. Then experienced security experts analyze the data to determine appropriate actions.

Aspire MDR FAQ

Q **Why do I need MDR?**

A An increasing number of threats are mounted each day using social engineering, link bait, smishing, deep fakes, and other attack vectors. Once identified, each potential attack creates an alert, causing a veritable overload of warning messages. That's a lot of information for your IT staff to handle alongside their daily duties. And it requires a niche set of talents. MDR has trained expert cybersecurity analysts and incident responders with 'eyes on glass' 24x7x365. Their sole task is to analyze and prioritize every alert.

Organizations that have an established and solid security posture need visibility to the ongoing threats in their environment. With MDR, threats are quickly managed, detected, and immediately responded to even before they happen.

Q **What foundational security technologies are required for the MDR service to be most effective?**

A MDR providers can leverage your current investments in security tools already deployed in your environment. The core security tools include cloud-based DNS security, network traffic analytics, endpoint protection, and next-gen firewall.

Aspire MDR FAQ

Q

What does MDR include?

A

A reliable Managed Detection and Response (MDR) is a next-generation cybersecurity protection that delivers 24x7x365 threat detection and response by combining:

- An expert team of security analysts and incident responders
- Integrated threat intelligence and automation
- Defined investigations and response playbooks
- Relevant, meaningful, and prioritized actions to respond to threats faster

Aspire MDR services provide 24x7 visibility, detection, and response capabilities across your on-prem and cloud environments, network, and endpoints.

It leverages an integrated security architecture to deliver 24x7x365 threat detection and response from our global but regionally-based Network & Security Operations Center (NSOC). It helps reduce mean time to detect and contain threats faster, with relevant, meaningful, and prioritized response actions.

Aspire MDR FAQ

Q **Can Aspire MDR monitor cloud applications, remote and on-prem infrastructure?**

A Aspire MDR can collect telemetry and other insights from applications such as Office 365 and IaaS environments like AWS to extend monitoring capabilities to the cloud. To provide more visibility and context, we can monitor other available log sources from your existing IT and security infrastructure. These sources include cloud mail servers, authentication, endpoints, firewalls, IDS/IPS, domain controllers, and more.

Q **What are the benefits of Aspire MDR as a 24x7 service operating locally?**

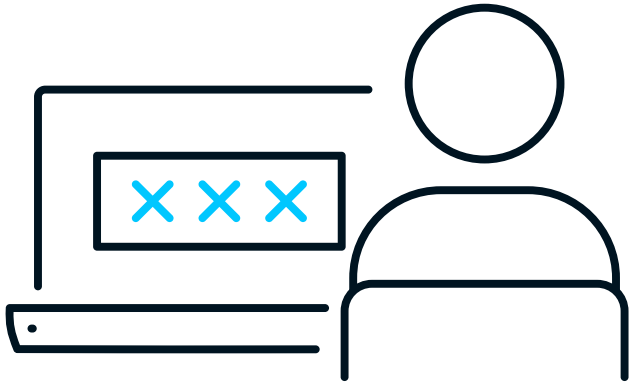
A Aspire MDR is a 24x7x365 full-service coverage. The Aspire Network & Security Operations Center (NSOC) is staffed around the clock by experienced security analysts and incident responders to identify and respond to potential threats quickly. Our NSOC team is 100% US-based, and all are full-time Aspire employees.

Q **How does Aspire MDR proactively safeguard my environment?**

A Aspire utilizes a proprietary platform called “VIGILENS”™ to ingest, correlate, and analyze log data from a broad set of sources across your network, endpoints, and cloud environment. The latest SIEM technologies, automation, machine learning, and integrated threat intelligence combine with a powerful rules engine to identify potential threats and trigger alerts for triage by our SOC Analysts.

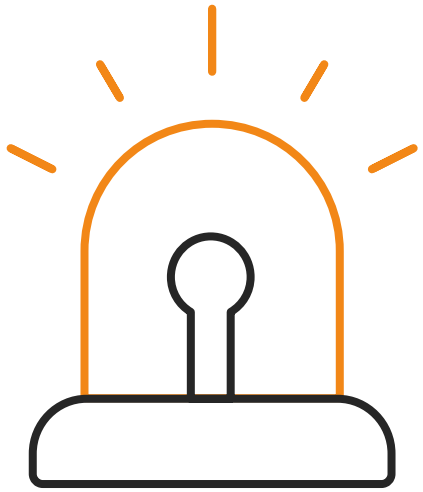
Aspire MDR FAQ

Q **How does Aspire verify a threat or suspicious activity is real?**



A Our SOC analyst team performs an analysis 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 a triggered alert.

Q **When/How are we alerted to potential security issues?**

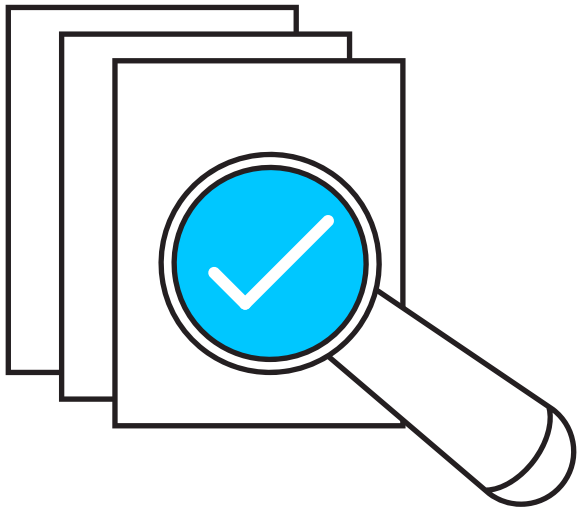


A The Aspire SOC will notify you via email or telephone according to a predefined communications plan when malicious incidents, malware, ransomware, and other destructive events are detected. In parallel, an Aspire incident responder will make intelligence-driven recommendations and work closely with your team to contain and remediate the threat.

Aspire MDR FAQ

Q **What reports are available?**

A Your dedicated Customer Success Manager (CSM) will coordinate a regular cadence (quarterly) to deliver root cause analysis on identified threats, review reporting and trends, and make recommendations for continuous improvement. Curated reports provide analysis, statistics, and trending data related to your security and health posture and associated threats.



To learn more about how Aspire MDR can enable your organization towards a stronger security posture, visit our website. Contact one of our experts at CyberSecurity@aspiretransforms.com.

ASPIRE
Powering Business Transformation™

AspireTransforms.com | 732-847-9600