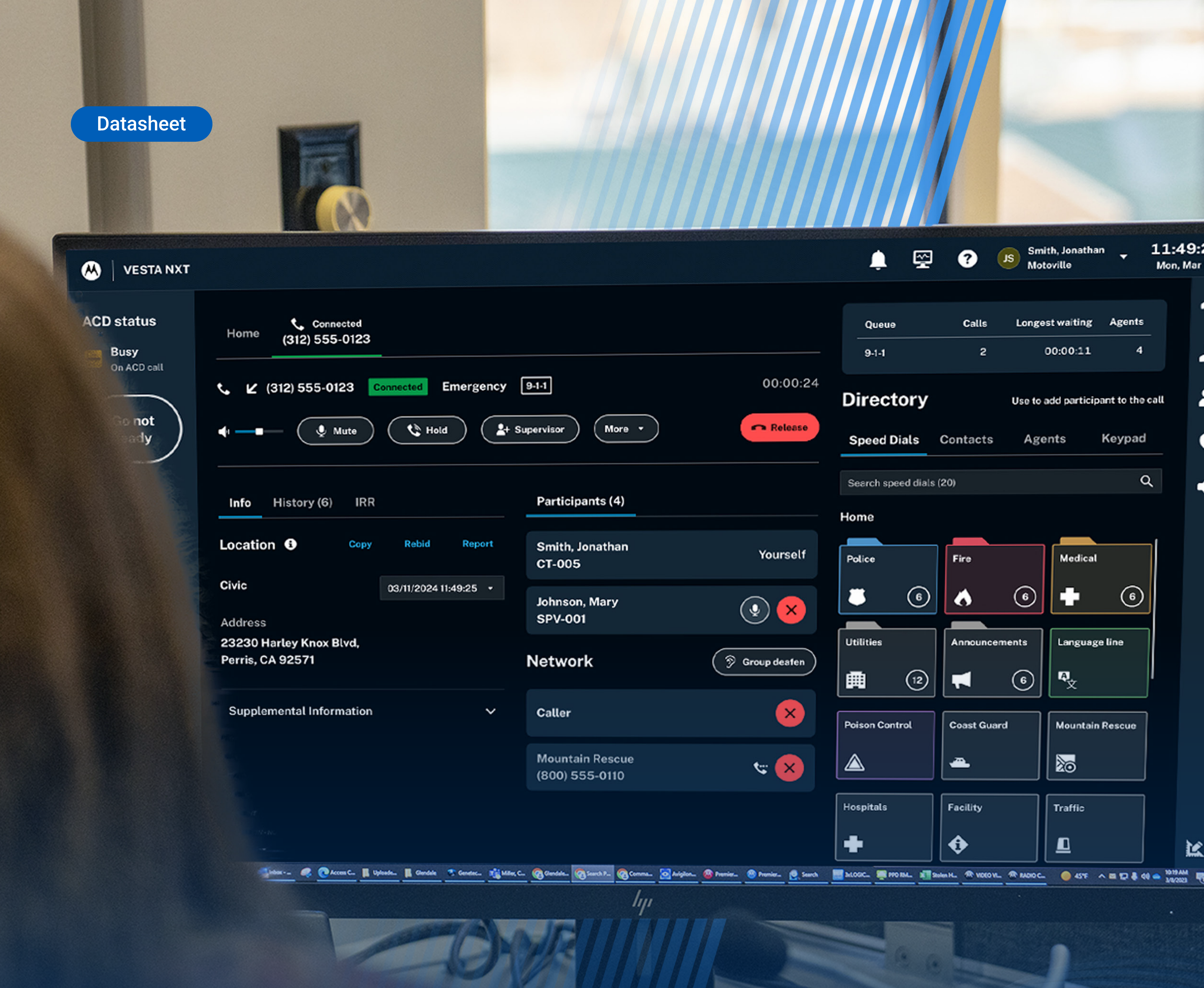
Datasheet



Managed Detection and Response for VESTA

Enhanced security and resilience for your emergency call handling system

MOTOROLA SOLUTIONS

Protect your call handling operations

In today's complex cybersecurity landscape, mission critical systems used by public safety agencies face increasing cyber threats. Such attacks to your VESTA emergency call handling system can severely impact system availability, compromise sensitive data and disrupt operations, putting lives at risk.

Motorola Solutions' Managed Detection and Response (MDR) service for VESTA uses best in class technology to protect your emergency call handling operations. It's designed and purpose built to protect your VESTA system from cyber attacks and maintain system confidentiality, integrity and availability, so that you can spend less time worrying about cyber threats and more time focusing on your mission to keep the public safe.

Your first line of defense is not enough

Endpoint Security, with its next-generation antivirus (NGAV) capabilities, is a vital first line of defense in your cybersecurity strategy, effectively blocking attacks as they happen and alerting our NSOC team so that they can notify you. But once cyber attackers gain access to your network, they can become a big problem, creating havoc in your systems. While NGAV will stop some cyber attacks, it may not detect the attackers in your network and cannot stop them from doing more harm.

A comprehensive approach

Our MDR service is built to detect these hidden threats and defeat the active attacker. Instead of just relying on NGAV to protect your endpoints, we actively monitor all phases of an attack. MDR for VESTA leverages a full set of security controls, including Endpoint Detection and Response (EDR), External Vulnerability Scanning (EVS), a Network Intrusion Detection System (NIDS) and Log Collection and Analytics to provide a comprehensive view of threats.

The NIDS protects your network from forced entry. Log Collection and Analytics detect attempts to move inside the network and enter connected systems. EDR software protects each computer and server endpoint from malicious activity or software.This creates a multi-layered approach to defending your VESTA system from cyber attacks and allows the NSOC to actively detect early signs of attacks and stop threats before they arise.

Thanks to these security controls, our experienced security analysts in the NSOC provide 24/7 monitoring, threat detection and rapid response capabilities to support your team. The impact is clear - we will quickly intervene in the case of an attack to help protect and maintain your call handling operations, while investigating the threat to eliminate the attacker and help you apply required security measures to protect your VESTA system. This results in you maintaining your operations and trusting the confidentiality and integrity of your data.

Key features

Designed and built for VESTA

Our MDR service is designed and purpose-built to work with your VESTA system and protect its availability and integrity from cyber threats. Its performance and interoperability with VESTA is continually tested and certified and it is fully supported by our service and engineering teams. Using this expertise our engineers have designed and optimized the reporting for VESTA emergency call handling, knowing exactly what normal looks like.

24/7 Network Security Operations Center

Our Network Security Operations Center (NSOC) provides 24/7 monitoring and brings cybersecurity expertise to your team. The NSOC is staffed by experienced, highly trained and certified cybersecurity professionals who continuously monitor your VESTA system for suspicious activity to stop threats and provide your technical support team alerts and reports to quickly and easily implement security countermeasures.

Our cybersecurity analysts are experienced in both public safety cybersecurity threats and VESTA Emergency Call Handling systems. They are ready to investigate threats and initiate a managed response whenever needed, night or day. They are there to help your team with their expert knowledge of both cybersecurity threats and VESTA systems.

Incident response support

When a cyber threat is detected, our NSOC analysts will engage with your team to respond to the threat. They will hold status calls with your team, perform compromise assessments and provide guidance to your team on system recovery. They will utilize the data collected by the ActiveEye platform to determine the extent of malicious activity and recommend the actions to mitigate the threat.

ActiveEye security platform

The ActiveEye Security Orchestration, Automation and Response (SOAR) platform serves as the central hub for your security operations. It collects and analyzes security data from your VESTA Emergency Call Handling system, differentiating between malicious and routine traffic to focus on actual threats.

ActiveEye co-managed portal

The ActiveEye web-based portal provides visibility to threat insights, event investigations, security reports, threat advisories and the status of any security cases. The platform provides a “single pane of glass view” offering full visibility into cybersecurity activity across the VESTA system, and even your land mobile radio system, computer aided dispatch and other public safety networks.

Our SOC will notify you on ServiceNow, but your security team can go further thanks to the co-managed platform ActiveEye, that gives you 24/7 visibility of everything that our NSOC analysts see. It also gives you the ability to access and review security data, configure alerts and notifications, perform security investigations and generate custom reports. The ActiveEye portal allows you to save queries, customize reports and set automatic alerts or notifications via email or other communication channels.

Advanced Threat Insights

With the optional Advanced Threat Insights (ATI) service our highly trained NSOC analysts provide threat intelligence and alerts specific to your industry and organisation. You will also have a named cybersecurity analyst to provide knowledge and expertise on how to best take action against any identified threats.

Security controls

Endpoint Detection and Response

Endpoint Detection and Response (EDR) is a powerful technology designed to safeguard your network's endpoints. EDR agents are deployed on your VESTA client workstations and servers to look for and identify anomalies, detect attacks and pinpoint threats.

With our MDR service, the NSOC analysts have access to the full EDR technology. This enables them to do much more than review blocked attacks and notify you. They can investigate and conduct threat hunting to respond to all malicious activity. Our team of NSOC security analysts will triage, contain and eliminate the threat, while blocking the attacker using the full capabilities of EDR to ensure your network remains secure.

ActiveEye Remote Security Sensor

Key to proactively fighting cyber threats, the physically deployed ActiveEye Remote Security Sensor (AERSS) can detect malicious activity in real-time, as well as provides remote collection of logs and network intrusion detection for your VESTA system. The AERSS enhances the situational awareness of both the NSOC and your team, providing enhanced perimeter threat intelligence compared to that provided by EDR on its own.

Log collection and analytics

The ActiveEye platform collects log data from systems, applications, networking components, and security systems within your VESTA environment via the AERSS. Analytics components and security policies process this data to identify policy violations and suspicious activity, providing critical context for tracking the origin of threats and identifying new attack patterns. Collected events are stored for a defined period, allowing for threat hunting and historical analysis.

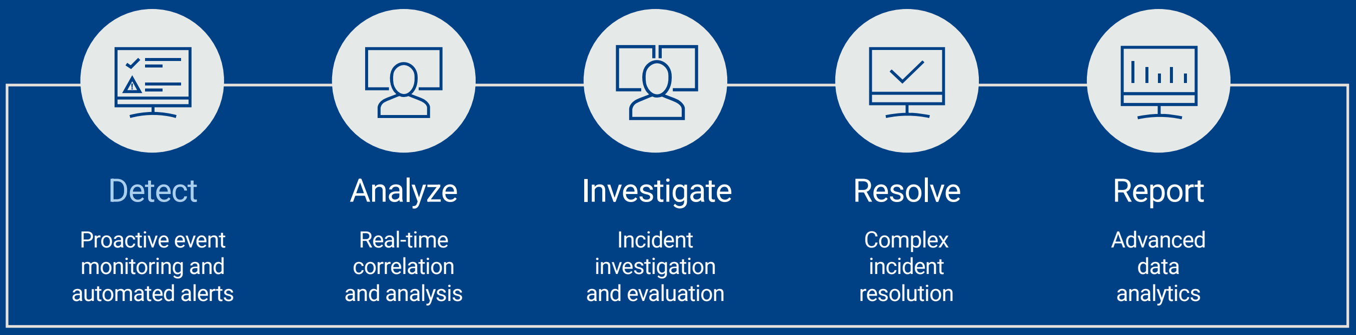
Network Intrusion Detection System

The AERSS also acts as a Network Intrusion Detection System (NIDS) within your VESTA Emergency Call Handling system to perform real-time signature and anomaly detection. The NIDS analyzes network traffic at both packet and flow levels to identify malicious activity and anomalous behavior, flagging these in ActiveEye and instigating a response to the threat.

External Vulnerability Scanning

Our cloud service includes External Vulnerability Scanning (EVS) to regularly scan internet-facing external network interfaces of your VESTA system for new software component vulnerabilities, insecure system or network settings. The regular scans allow the NSOC analysts and ActiveEye to identify vulnerabilities, provide risk scores using the Common Vulnerability Scoring System (CVSS) and recommend actions to remedy the vulnerabilities.

Systematic approach to mitigate risks



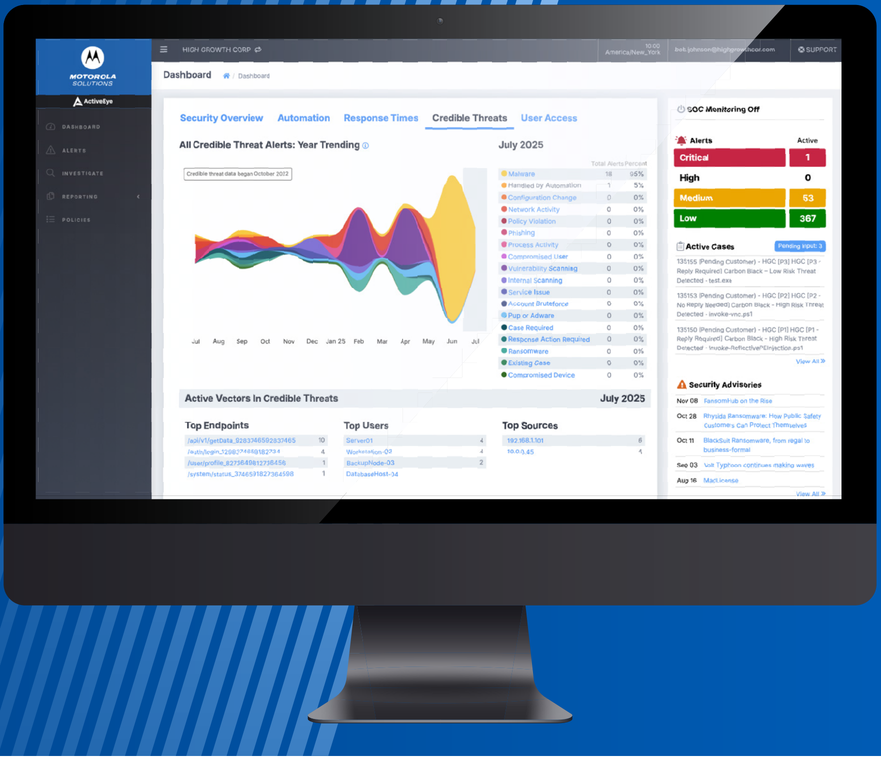
Detect
Proactive event monitoring and automated alerts

Analyze
Real-time correlation and analysis

Investigate
Incident investigation and evaluation

Resolve
Complex incident resolution

Report
Advanced data analytics



All Credible Threat Alerts: Year Trending

July 2025

	Total Alerts	Percent
Malware	18	95%
Handled by Automation	1	5%
Configuration Change	0	0%
Network Activity	0	0%
Policy Violation	0	0%
Phishing	0	0%
Process Activity	0	0%
Compromised User	0	0%
Vulnerability Scanning	0	0%
Internal Scanning	0	0%
Service Issue	0	0%
Account Bruteforce	0	0%
Pup or Adware	0	0%
Case Required	0	0%
Response Action Required	0	0%
Ransomware	0	0%
Existing Case	0	0%
Compromised Device	0	0%

Active Vectors In Credible Threats July 2025

Top Endpoints

/api/v1/getData_9283746592837465	10
/auth/login_1298374659182734	4
/user/profile_8273649812736456	1
/system/status_3746591827364598	1

Top Users

Server01	4
Workstation-02	4
BackupNode-03	2
DatabaseHost-04	

Top Sources

192.168.1.101	6
10.0.0.45	4

Alerts	Active
Critical	1
High	0
Medium	53
Low	367

Active Cases

135155 (Pending Customer) - HGC [P3] HGC [P3 - Reply Required] Carbon Black – Low Risk Threat Detected - test.exe

135153 (Pending Customer) - HGC [P2] HGC [P2 - No Reply Needed] Carbon Black - High Risk Threat Detected - invoke-vnc.ps1

135150 (Pending Customer) - HGC [P1] HGC [P1 - Reply Required] Carbon Black - High Risk Threat Detected - invoke-ReflectivePEInjection.ps1

Security Advisories

Nov 08	RansomHub on the Rise
Oct 28	Rhysida Ransomware: How Public Safety Customers Can Protect Themselves
Oct 11	BlackSuit Ransomware, from regal to business-formal
Sep 03	Volt Typhoon continues making waves
Aug 16	MacLicense

Benefits

Enhanced threat detection and response

The combination of EDR, ActiveEye platform's advanced analytics, real-time threat intelligence and 24/7 expert monitoring enables better identification of threats and a more rapid and effective responses to mitigate cyber attacks before they cause significant damage.

Reduced cybersecurity risk

By providing continuous monitoring and addressing vulnerabilities across your VESTA Emergency Call Handling system MDR significantly strengthens your overall security posture and reduces the risk of successful cyber attacks and impacts on your system availability, integrity and confidentiality.

Cost-effective security

Partnering with our MDR service can be significantly more cost-effective than building and staffing an in-house Security Operations Center trained on VESTA and public safety cybersecurity threats.

Reduced burden on your teams

Managing a comprehensive cybersecurity program can be challenging and resource-intensive. Our MDR service supplements your in-house skills with 24/7 expertise, freeing up your teams to focus on other critical tasks.

Complete visibility and control

The co-managed ActiveEye portal provides complete transparency into your security environment, allowing you to see detected threats, understand the actions being taken and generate customized reports.

Helps meet compliance requirements

The expanded MDR capabilities, including log analytics, network intrusion detection and the ActiveEye portal's reporting features, can significantly assist in achieving compliance with regulations such as the CJIS Security Policy.

Access to cybersecurity insights and expertise

Our NSOC is staffed with trained and accredited cybersecurity professionals experienced in threats to mission critical systems and how to respond to best protect your operations and the community you serve.

Your trusted partner

As a leading provider of cybersecurity services for public safety agencies and mission-critical systems, we understand your mission can only be as secure as your partners enable you to be. Our goal is to provide you with transparency, accountability and security that's built-in from the start.

Our expert team, industry certifications, robust policies and advanced technology uniquely position us to provide superior cybersecurity solutions that meet your current and future needs.

By choosing Motorola Solutions' Managed Detection and Response service for VESTA Emergency Call Handling, you gain a trusted partner dedicated to protecting your mission-critical operations with cutting-edge technology and expert analysis.

Global scale and experience

70+

Security experts focused on24/7 monitoring and response

1.7B

Security events proactively monitored each day

20+

Years of experience developing cybersecurity solutions

People

Experts with top industry certifications work hand-in-hand to ensure system availability and security

Process

Aligned to the National Institute of Standards and Technology (NIST) Framework

Technology

Real-time visibility into threat via our ActiveEye Security Orchestration, Automation and Response (SOAR) platform

To learn more, visit:

www.motorolasolutions.com/cybersecurity

MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A.