Fact Sheet

EDR for ASTRO

Next generation protection for ASTRO LMR systems

Endpoint Detection and Response (EDR) is the next generation of endpoint security for your ASTRO® system. It offers far greater protection than legacy antivirus software, significantly enhancing the existing cybersecurity protection already offered by Managed Detection and Response (MDR).

EDR goes beyond antivirus software to provide advanced threat protection. It creates a continuous stream of data from multiple endpoints on a network - devices such as laptops, servers and workstations - which is then analyzed in real-time to provide insights into potential security threats.

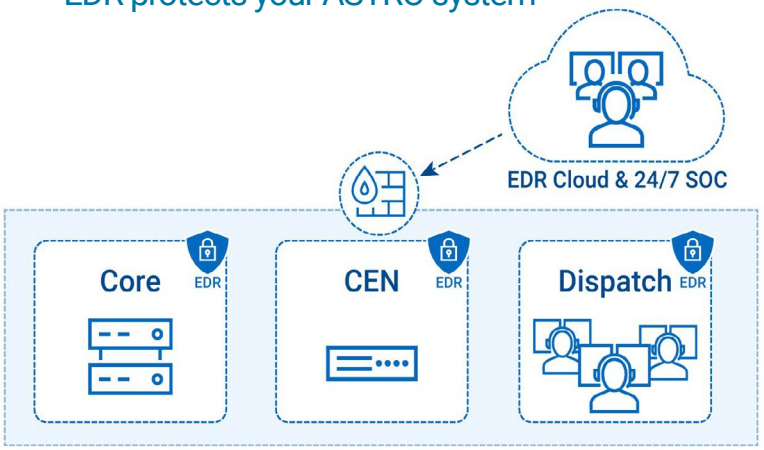
Unlike antivirus software, EDR is managed by our 24/7 Security Operations Center (SOC) cybersecurity analysts who will vet alerts for false positives, and then take or recommend action against identified threats. EDR provides the strongest possible detection and prevention capabilities to catch cyber threats that can bypass traditional antivirus software. EDR uses machine learning and behavior analytics to identify abnormal activities, thus offering enhanced threat protection. EDR also enables the SOC analysts to act in real-time to contain cyberthreats.

The EDR software that we use in our MDR service undergoes thorough testing by Motorola Solutions engineers in the ASTRO labs to optimize its policies and maintain Public Safety availability requirements.

Key Features:

- Improved threat protection - while both EDR and antivirus provide endpoint security, EDR is more advanced and can detect a wider range of threats than legacy antivirus.
- Real-time response - EDR enables the SOC to remotely contain security threats on endpoints in real time with a direct response.
- Purpose built and rigorously tested - Motorola Solutions performs thorough EDR testing and monitoring to meet public safety availability needs. Developed in conjunction with the ASTRO architects and thoroughly tested by the ASTRO product team, to reduce threats to system stability and availability.

EDR protects your ASTRO system



- Core Endpoints
  - Voice routing and processing
  - Network management applications
- CEN Endpoints
  - Data, authentication, logging
- Dispatch Site Endpoints
  - Dispatch, logging, and management

MOTOROLA SOLUTIONS

Integrated with ActiveEye

EDR is an endpoint security agent that is integrated into the ActiveEye security platform to provide additional threat detection, investigation and response actions to optimize protection of critical systems.

EDR integration with ActiveEye accelerates investigations by making necessary information available for analysts in a single platform where they can quickly access details of what caused an alert, its context and its history.

The platform enables analysts to initiate response actions (i.e. isolate host, ban or block a file hash, terminate a process) on endpoints to respond to detection of verified malicious activity within the system. Available responses are determined by pre-authorized customer security policies.

Why is EDR important?

EDR is an important enhancement to MDR as it provides the strongest possible detection and prevention capabilities. This dramatically strengthens your existing security position in the face of increasing cyberthreats and the growing sophistication of threat actors.

The industry has recognized EDR as the future for endpoint protection with the President declaring in Executive Order 14028 on Improving the Nation's Cybersecurity that "FCEB Agencies shall deploy EDR to support proactive detection of cybersecurity incidents".

EDR Benefits

- Provides the SOC with the ability to remotely detect and analyze a threat quickly and effectively, responding in real time.
- Continually monitors and collects data from endpoints within the ASTRO system, including the Radio Network Infrastructure (RNI), the Customer Enterprise Network (CEN) and dispatch consoles to detect, investigate and prevent potential threats.
- Identifies risky anomalous activity and advanced threats better than traditional antivirus.
- Uses machine learning and behavior analytics to identify abnormal activities in real time.
- Safeguards against common threats including ransomware and malware, even if the new variants have never been seen before.
- Limits blast attack radius and impact by enabling SOC analysts to take response actions directly, such as deleting malware files from a machine, which shortens time to resolution.

Learn more at
www.motorolasolutions.com/cybersecurity

MOTOROLA SOLUTIONS