



# ASTRO System Monitoring

Federal agencies must maintain system availability from external threats and technological failures. How do you protect your ASTRO system?

Safeguard your LMR systems from downtime with ASTRO System Monitoring, which allows you to maintain the confidentiality, integrity and availability of your systems while still benefiting from the ability to connect to outside systems and networks.

ASTRO System Monitoring combines the power of Network Event Monitoring, Security Monitoring and ASTRO Connectivity Service to the Core site. This comprehensive suite of services is tailored for federal agencies to help ensure your mission-critical system remains reliable and available 24/7, allowing you to focus on your mission.

**50% less**

Organizations with 24/7 event monitoring on their networks have 50% fewer outages.<sup>1</sup>

**15 days**

Downtime due to cyber attacks is, on average, 15 days.<sup>2</sup>

**\$1.4 million**

Efficient prevention measures can save up to \$1.4 million per cyber attack.<sup>3</sup>

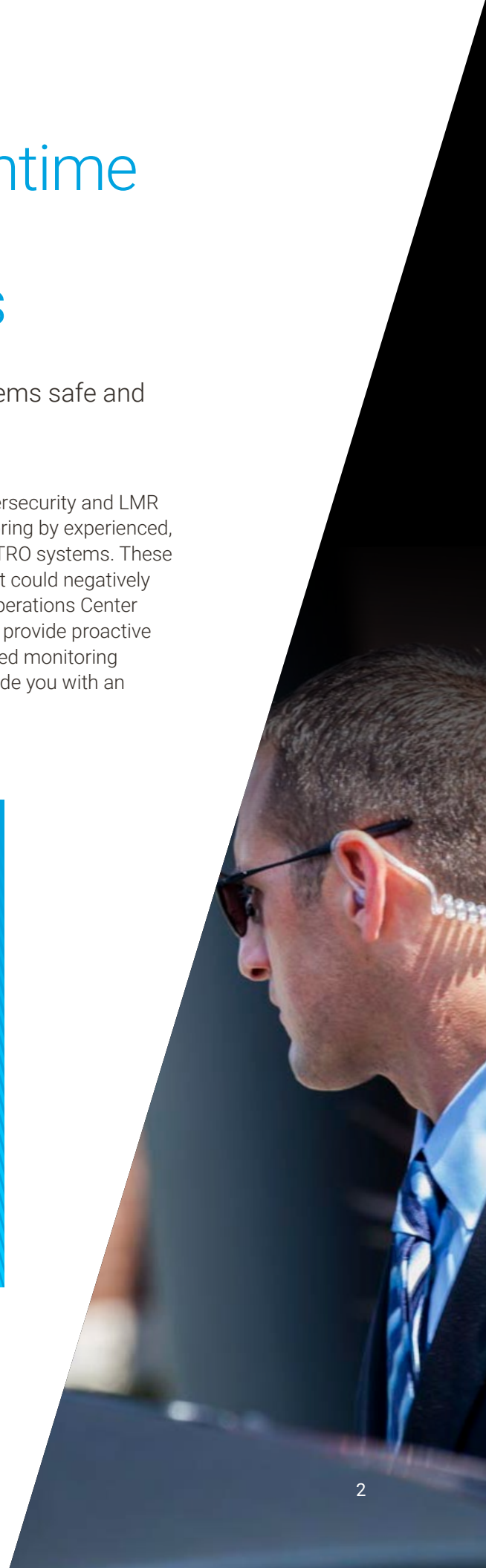
# Prevent and reduce downtime and outages with 24/7 monitoring by live agents

Partner with us so that we can focus on keeping your systems safe and technology efficient while you focus on your mission.

ASTRO System Monitoring provides you with 24/7 monitoring from our cybersecurity and LMR experts across multiple areas. With security monitoring you get 24/7 monitoring by experienced, specialized security technologists with years of experience working with ASTRO systems. These analysts monitor your systems to proactively help mitigate cyber threats that could negatively impact system availability. With Network Monitoring, our Federal Network Operations Center (NOC) experts will analyze unexpected technology-related events or failures, provide proactive alerts and help define the best path to resolution when needed. Our human-led monitoring teams work closely with, but independently from, our product teams to provide you with an independent evaluation that is tailored to your products.

## Features and benefits

- **Network Event Monitoring:** Quickly identify and address technical issues
- **Security Monitoring:** Maintain system confidentiality, integrity and availability by detecting and mitigating threats before impact
- **Reliable and secure connectivity:** Enable network event monitoring and security monitoring with a secure link to the Core
- **Real-time reporting:** Get insights into ASTRO system health, performance and cyber activity







## Stay focused on your mission with customized solutions

We understand that system availability is a must for federal agencies. This is why our services are specifically designed for your ASTRO systems and consistently tested for interoperability. Our analysts understand how cyber threats and technological failures specifically impact your industry and the best measures to prevent and mitigate these threats to keep your systems secure and available.

We also consistently incorporate the most recent threat intelligence into our security monitoring, which allows for rapid detection. In addition, with our ASTRO Connectivity Service, you can get a secure and integrated connection that is built for ASTRO systems. With ASTRO System Monitoring, you get experts who understand your technology and systems, which improves the ability to keep them safe and available at all times.



# ASTRO System Monitoring service packages



## Essential & Essential Plus

### Repair & support

- Infrastructure repair
- Self-installed patches
- Technical support
- Dispatch (Ess+)
- Onsite response (Ess+)
- Preventive maintenance (Ess+)



## Advanced & Advanced Plus

### Connect & respond

- Infrastructure repair
- Self-installed patches
- Technical support
- Dispatch
- Onsite response
- Preventive maintenance
- Remote update services
- Advanced exchange
- ASTRO System Monitoring
  - Security monitoring
  - ASTRO Connectivity Service
- MPLS/microwave monitoring (optional)
- Network updates/SUA (Adv+)



## Premier

### Operate & optimize

- Infrastructure repair
- Self-installed patches
- Technical support
- Dispatch
- Onsite response
- Preventive maintenance
- Remote update services
- Network updates/SUA
- Advanced exchange
- ASTRO System Monitoring
  - Security monitoring
  - ASTRO Connectivity Service
- MPLS/microwave monitoring
- Change management
- Problem management
- Cybersecurity risk assessment
- Availability commitment
- Performance management

To learn more, visit:

[www.motorolasolutions.com/cybersecurity](http://www.motorolasolutions.com/cybersecurity)

### Sources

1. <https://www.engineering.com/downloads/motorola/motorola-solutions-lmr-services-survey-report.pdf>
2. PSTA Public Safety Threat Report - Q1 2024.
3. <https://info.deepinstinct.com/value-of-prevention>



Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A. [motorolasolutions.com](http://motorolasolutions.com)

MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. ©2024 Motorola Solutions, Inc. All rights reserved. 06-2024 [MW06]