ASTRO®
A SECURE VOICE AND DATA PLATFORM

PROTECTING MISSION-CRITICAL COMMUNICATIONS

BROCHURE | ASTRO CYBERSECURITY CAPABILITIES

MOTOROLA SOLUTIONS

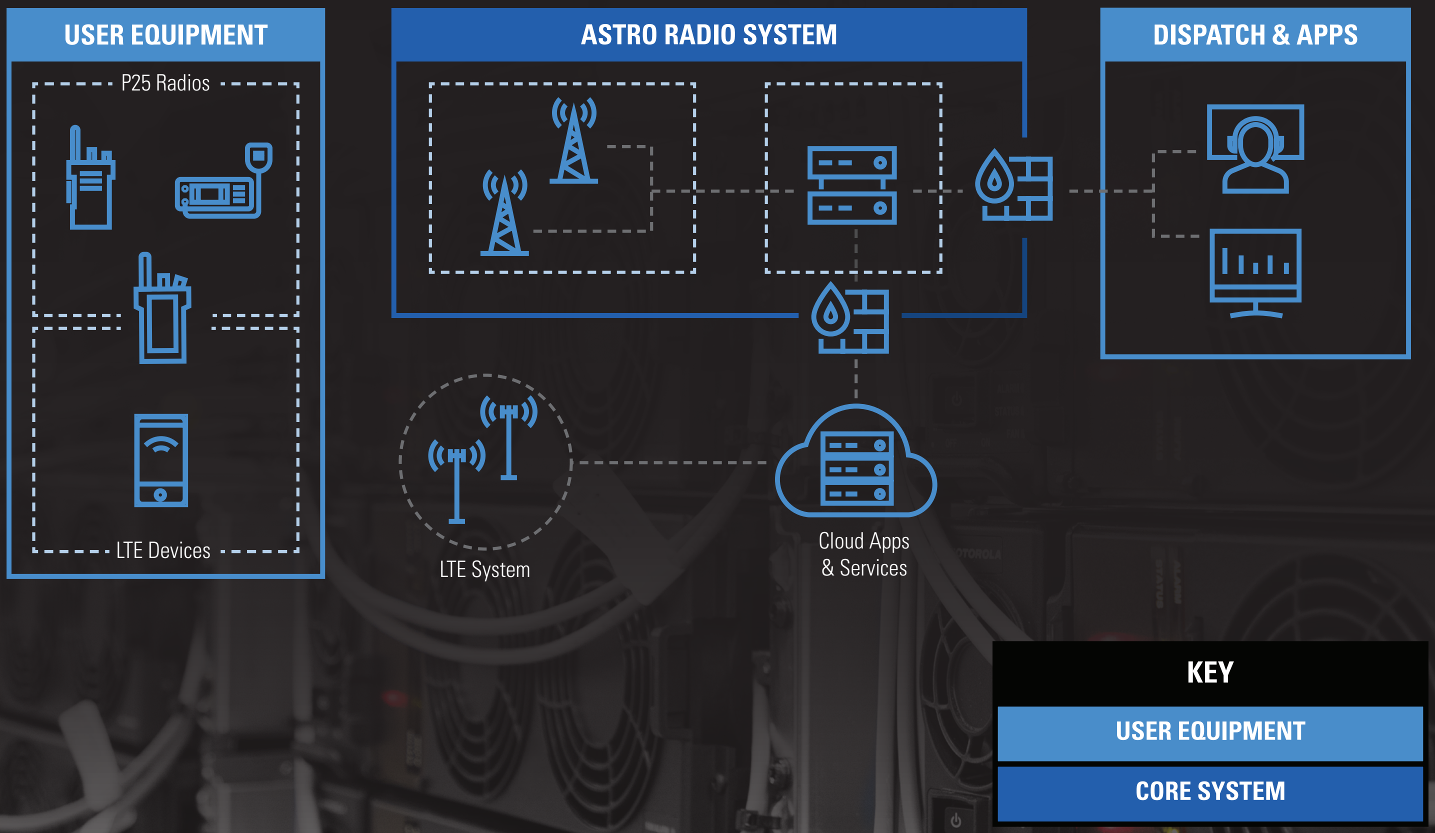
ASTRO CYBERSECURITY CAPABILITIES

ASTRO voice and data systems are more connected and interconnected than ever before. They span wide geographic areas to connect many agencies and organizations across large municipalities. They connect to other P25 systems, private and public broadband networks, as well as private enterprise networks and the public internet. These systems — and each device on them — represent a potential point of access that must be protected from unauthorized users, as well as compromised or corrupted communications.

The ASTRO® public safety platform exceeds the P25 industry standard and includes robust security measures to prevent unsanctioned use as well as protect against cyber threats. This brochure provides an overview of the cybersecurity capabilities within your ASTRO radio system that protect data integrity and ensure communications reliability.

A COMPLETE P25 SOLUTION

TESTED AND PROVEN, END-TO-END

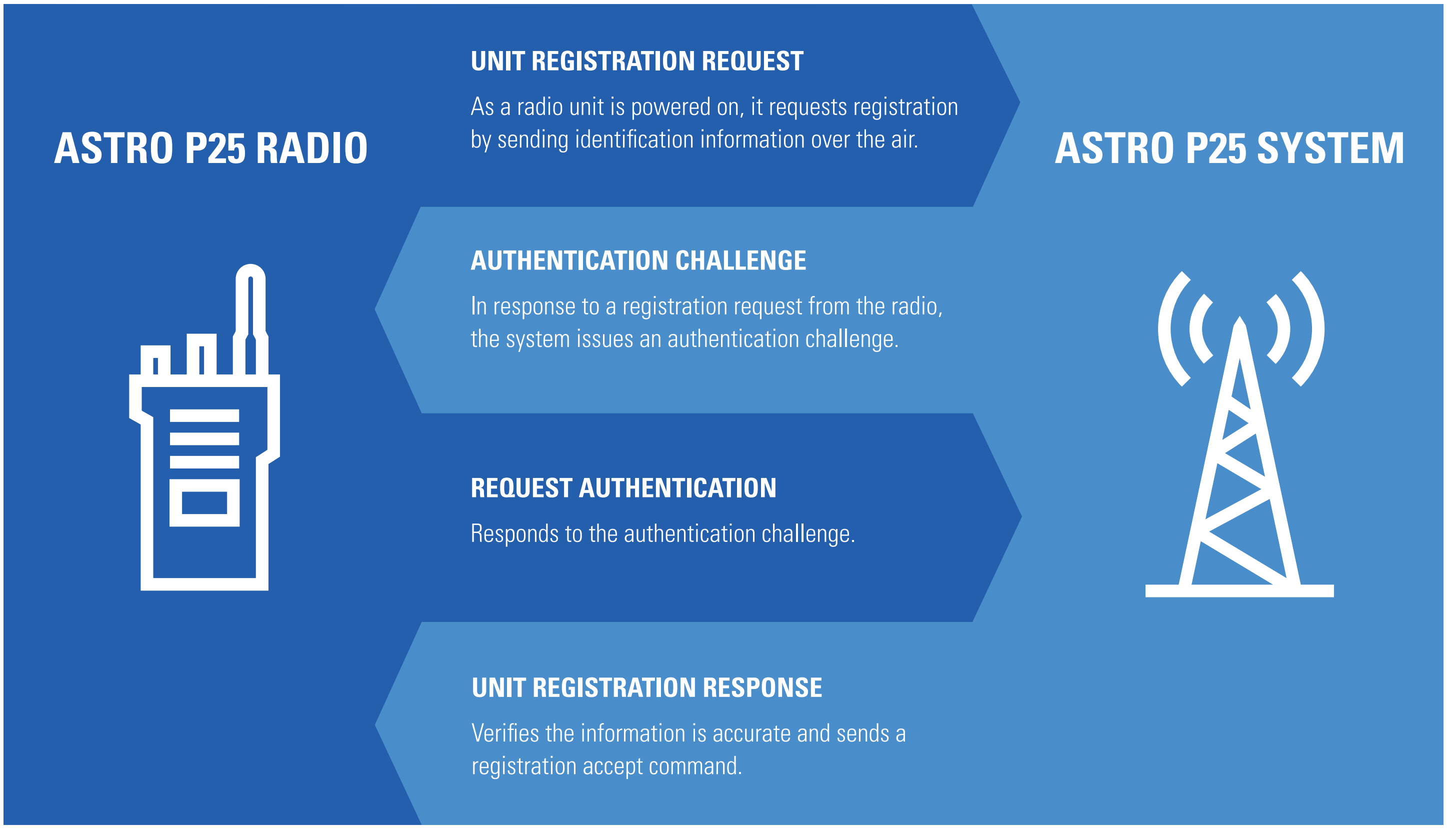


HOW WE SECURE THE ASTRO PLATFORM: USER EQUIPMENT

Unauthorized radios are those which cannot be verified and are one of the most important challenges ASTRO system managers face - and unfortunately one of the most common. Whether a radio has been cloned, stolen, or simply lost, restricting network traffic to authorized devices only is critical. ASTRO systems include several authentication and encryption tools to help you in this effort.

Radio Authentication uses a unique authentication key assigned to each radio that is also stored in the authentication center (AuC). The authentication key cannot be read from the radio and then cloned into another device. The correct key must be present in order for the radio to gain access to the ASTRO system. This provides an additional level of control for system owners and prevents unauthorized radios from joining the system.

Encryption Key Management is critical to the cyber resiliency of the ASTRO system. Our secure management ecosystem ensures your radio communications are secured with encryption keys that can be updated over-the-air. This rekeying option provides the convenience of not having users bring their devices into the shop for manual rekeying.



ASTRO P25 RADIO

ASTRO P25 SYSTEM

UNIT REGISTRATION REQUEST

As a radio unit is powered on, it requests registration by sending identification information over the air.

AUTHENTICATION CHALLENGE

In response to a registration request from the radio, the system issues an authentication challenge.

REQUEST AUTHENTICATION

Responds to the authentication challenge.

UNIT REGISTRATION RESPONSE

Verifies the information is accurate and sends a registration accept command.

AUTHENTICATION

The subscriber will be authenticated on power-up registration. If the subscriber fails the authentication challenge, the radio will be unable to register on the system and therefore unable to transmit or receive on the system.

DATA ASSURANCE: PROTECTING INFORMATION INSIDE THE CORE

Ensuring the integrity of data within the network is of equal importance to the overall security of the ASTRO platform. To enable security at every step of the way we employ a variety of methods, including secure access controls, data traffic monitoring and encryption, based on the National Institute of Standards and Technology (NIST) framework and industry best practices.

Service Access Architecture provides secure remote access via WAN, VPN, dial-up or a remotely located LAN. For security purposes, authenticated access can be provided via two-factor authentication, hard tokens or soft tokens.

Intrusion Detection System (IDS) monitors ASTRO network traffic for potential security threats using signature-based detection and anomaly-based detection. Both identification methods allow customers to react quickly to cyber threats.

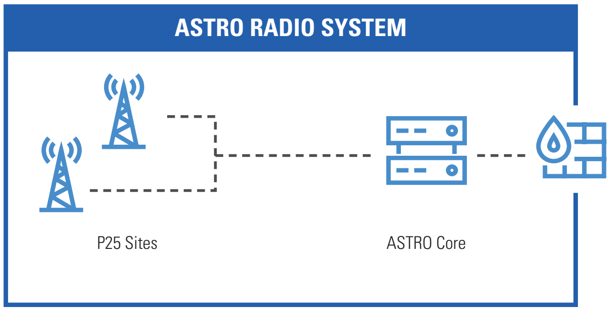
Secure Shell Protocols (SSH) provides an encrypted point-to-point connection between two machines where both ends have been authenticated. SSH minimizes the the potential for “man-in-the-middle” cyber attacks.

Router Encryption protects in-transit information as it passes through untrusted zones. This includes Wide Area Network (WAN) links and DeMilitarized Zone (DMZ), between the radio network interface, and the Customer Enterprise Network (CEN).

OSPF/BGP Router Authentication protocols use shared keys between peer routers to verify the integrity of data packet transmissions.

Ethernet Switch Port Security prevents unauthorized devices from network access by configuring ports in one of three states: MAC Port Locked – only the device with the correct MAC address, 802.1x – connections made to this port must be authenticated, or disabled, and no devices can connect to a port.

Centralized Authentication/Event Logging manages the unique identification of site administrative users and authenticates logins. Detection of suspicious events is recorded on a central server helping network technicians to promptly detect, diagnose and respond to possible security breaches.



CYBERSECURITY SERVICES FOR ASTRO

MANAGED DETECTION AND RESPONSE SERVICES

Detect cyber threats in both the ASTRO core and the customer enterprise network (CEN) with our Managed Detection and Response (MDR) services, powered by ActiveEye.

Our ActiveEye platform provides a single pane of glass for your operations team to monitor the security of your infrastructure, ensuring you’re always in the loop. As a co-managed security solution, ActiveEye ensures you have 24/7 visibility and can see what our security operations center (SOC) analysts see.

ADVISORY SERVICES

Get a comprehensive and systematic process for identifying, assessing and managing cybersecurity risk throughout enterprise and public safety IT and mission-critical systems. With our Cybersecurity Advisory Services, you will be able to fully understand your cybersecurity risk posture related to your organization’s operational environment. Motorola Solutions can provide a comprehensive assessment of your attack surface profile and detailed remediation recommendations, along with cyber exercises to gauge your team’s readiness to respond to a cyber incident and penetration testing to discover vulnerabilities, among other services.

To learn more, visit: **https://www.motorolasolutions.com/en_us/products/project-25-systems/astro-25-security.html**

MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, Il 60661 U.S.A. **motorolasolutions.com**