MOTOROLA SOLUTIONS MOTOTRBO NITRO AND THE NIST CYBERSECURITY FRAMEWORK

CYBER CLIMATE

Motorola Solutions uses a risk-based approach throughout our entire product development, implementation and operational support lifecycle. We strongly believe in three foundational pillars of cybersecurity: confidentiality, integrity and availability. We address these pillars with the application of protection, detection and response controls built with industry-leading people, processes and technology.

MOTOTRBO Nitro™, a hybrid cloud solution, is targeted towards a wide range of industries. Hence, there is a wide range of cybersecurity needs.

Organizations of all types are increasingly subject to data theft and loss, whether the asset is customer information, intellectual property, or sensitive company files. The National Institute for Standards and Technology (NIST), housed within the US Department of Commerce, has developed standards and guidance for information protection. One of the most important of these is the Cybersecurity Framework (CSF), which helps provide structure and context to cybersecurity. Private-sector organizations implement the NIST CSF not only to enhance their cybersecurity, but also to lower their potential risk of legal liability. We follow the NIST Cybersecurity Framework to protect the MOTOTRBO Nitro LTE Evolved Packet Core, Radio Access Network.

NIST FRAMEWORK

The following is a high level description of the of the NIST Cybersecurity Framework we apply.

CYBERSECURITY FRAMEWORK	SYSTEMATIC ANALYSIS AND PLAN
IDENTIFY **Assess Risks**	• Inventory critical assets and systems • Provide a thorough risk analysis
PROTECT **Develop Safeguards**	• Develop policies and procedures • Implement appropriate access and auditing controls
DETECT **Make Timely Discoveries**	• Continuous monitoring 24x7x365 • Enable auditing capabilities
RESPOND **Take Action**	• Establish a robust response plan • Create, analyze, triage and respond to detected events
RECOVER **Restore Functionality**	• Institute a recovery plan • Create improvements to prevent future attacks

CLOUD-BASED BROADBAND LMR SYSTEM

SERVICES PROVIDED TO SUPPORT NIST FRAMEWORK FOR NITRO

MOTOTRBO Nitro Data Center provides Citizen Broadband Radio LTE service (CBRS) based on 3GPP LTE standards to customers subscribing to the service. Our holistic approach to cybersecurity includes a range of controls:

CORE AND SUPPORTING SERVICES

The MOTOTRBO Nitro core and its supporting services are securely hosted in a highly available environment.

- Staffed by Motorola Solutions cybersecurity professionals, the MSI Security Operations Center monitors the network core 24/7/365. Specialized security technologists with years of experience working with communications networks provide uninterrupted monitoring of the radio network security elements to detect, analyze and respond to security events.
- Nitro security is based on NIST-800-187 Guide to LTE Security, which contains 3GPP Security best practices.
- Contains security hardened components guided by industry security best practices that are firewalled from untrusted networks.
- Software is vetted, scanned, and deployed regularly to mitigate any security vulnerabilities.
- Malicious-code and vulnerability scans are performed and definitions updated on a regular basis.
- Host Based Firewalls, Access Protection, and Exploit Prevention are deployed.
- Sensitive system data at rest within the data center is secured. **No customer data is stored in our data centers.**
- Sensitive data in-transit between the data center and the customer premises is secured via IPSec.
- Customer RANs are securely segmented to prevent traffic from flowing between customers.

NITRO CLOUD PORTAL

Provisioning and performance management is performed by application services that are securely hosted in the cloud.

- Data security, access control, key management and role based privileges are best-in-class, industry-standard security controls provided by cloud hosted services.
- Network access controls using firewalls and VPNs.
- Cloud services are monitored and scanned on a regular basis. .
- Portal access is secured with channel partner login credentials.

NITRO ON PREMISES RADIO ACCESS NETWORK

Nitro equipment is connected to the Nitro on premises RAN which connects to the shared Nitro LTE Evolved Packet Core. On premises Nitro equipment includes: CBSDs, Nitro On Prem Edge Gateway, PTP (Precision Time Protocol) Server, On Prem Network Switch and Firewall.

- On premises Nitro equipment is security hardened and configured. Motorola Solutions employees and our channel partners are trained to follow best practices when deploying equipment on premises.
- From on-prem equipment to the Nitro core, the signalling; bearer; and operations, administration, and management traffic are protected using IPsec.
- The CBSD traffic is protected on premises (between CBSD and on-premises firewall) using an additional IPsec tunnel.
- Software is vetted, scanned and deployed regularly to mitigate any security vulnerabilities.
- Contains security-hardened components guided by industry best practices that are firewalled from untrusted networks.
- Nitro RAN security is based on NIST-800-187 Guide to LTE Security, which contains 3GPP Security best practices. In particular, Nitro implements:
    - 3GPP encrypted air interface
    - SIM based access control and authentication
- CBSDs and the Nitro On Prem Edge Gateway are only configured remotely using secured protocols, with no local access.

HOW WE COVER THE FRAMEWORK ACTIVITIES FOR NITRO

IDENTIFY

Asset Management

- Asset & role management
- Open source review board
- System configuration artifacts

Business Environment

- Market verticals: Nitro is targeted towards a wide range of customers, which include manufacturing, hospitality, higher education, government, logistics/delivery and entertainment
- Customer engagements: Strong customer engagement to identify requirements
- Release & product lifecycle strategies: support roadmaps for releases with supporting product announcements, Motorola Solutions Cybersecurity Risk Management Framework for vendors

Governance

- Product & services governance
- Business risk owner

Cybersecurity Risk Assessment

- System & product risk assessments: against Motorola Solutions' Minimum Viable Secure Product (MVSP) requirements which are based on NIST Cybersecurity Framework
- Secure design review and audit
- Vulnerability scanning assessment & remediation
- Threat intelligence & communication
- Security self-assessment: internal penetration testing & remediations
- Cybersecurity risk assessments of third party vendor products

Risk Management Strategy

- Cybersecurity risk management
- Business risk owner
- Risk registry

Supply Chain Risk Management

- Supplier qualification
- Supply chain controls

PROTECT

Identity Management, Authentication & Access Control

- Authentication: 3GPP standard-based
- SNMPv3-based authentication from all devices
- IPSec based protection from on-prem Ffrewall to Nitro core for signalling, voice and OAM traffic
- IPSec backhaul in customer on-prem network from CBSD to on-prem firewall for protection of bearer and signalling traffic
- VPN based protection between Nitro cloud and core networks
- TLS protection between SAS proxy and SAS server
- Data at rest and in-transit protection using sensitive data classification and protection
- Access to information and system privileges are strictly segmented and limited by staff role and scope of responsibility

Awareness & Training

- Motorola Solutions personnel are required to receive regular and rigorous security training
- Security training is required for channel partners installing MOTOTRBO Nitro networks.
- Security training is available for customers.

Data Security

- Air Interface Encryption: 3GPP standard-based AES encryption
- End-to-end encryption of signalling, bearer and operation & management traffic: all traffic is encrypted based on 3GPP standards
- Encryption of sensitive data: encryption of key material per 3GPP recommendations

Info Protections & Procedures

- Secure development lifecycle
- Vulnerability management: vulnerability investigation & impact analysis and risk-based decision process
- Change control management
- Backup- and restore-capable products

Maintenance

- Pre-tested patch & anti-malware updates
- Regular maintenance release
- Product specific releases
- Emergency releases when needed with minimal disruption to services

Hardening and Patching

- Common hardening benchmarks: DISA STIG-based
- Anti-malware protection: for Linux and Windows-based components
- Network enforcements: secure boundaries between Nitro LTE core, on prem network, customer network, and the Internet

Centralized Logging (Syslog) & Auditing Capabilities

- From Linux and Windows-based devices
- From applications
- From network transport devices
- From security-dedicated products (malicious code detection and anti-malware)

DETECT

Detect Anomalies & Events

- Centralized malicious code detection and anti-malware reporting
- Centralized syslog log collection from operating system, applications, and network transport

Detection Process

- Abuse/misuse case testing
- Security assessments

Security Continuous Monitoring

- Event forwarding: all syslog events from Nitro core are forwarded to SOC for monitoring
- Northbound alarm forwarding: SNMPv3-based, supports authentication and encryption
- Alarms from Nitro core are monitored by Network Operations Center (NOC)

RESPOND

Communications

- Roles & responsibilities
- Coordinated communications

Improvements

- Secure development lifecycle
- Feeding findings and remediations back into the development cycle

Analysis

- Vulnerability investigation
- Threat intelligence analysis

Mitigation

- Customer issue resolution policy
- Incident management process
- Technical notification & updates

RECOVER

Planning

- Highly available Nitro LTE Core and Nitro cloud
- Automatic backup process for data in the Nitro LTE core and Nitro cloud
- Defined recovery procedures for Nitro LTE core, Nitro cloud, and Nitro on-prem equipment

Improvements

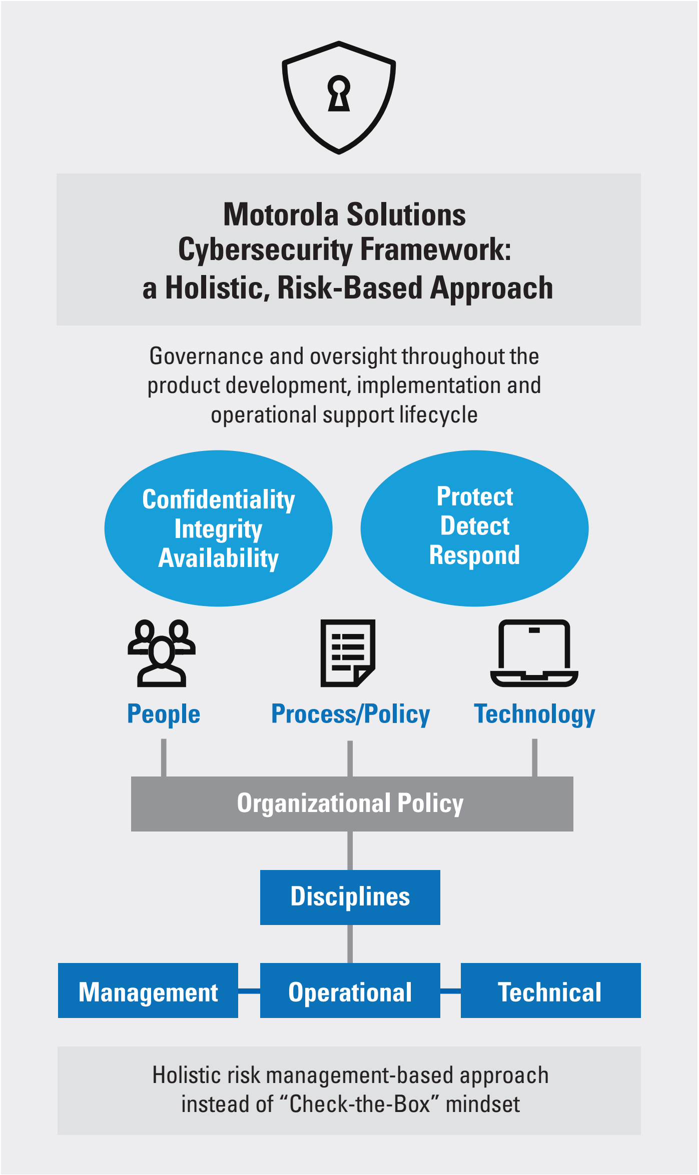
- Lessons learned: feeding findings and remediations back into the development cycle
- Process improvements: feeding findings and remediations back into the development cycle

Communications

- Motorola Solutions Services: directly interact with channel partners and customers as needed
- Customer engagement

CONCLUSION

MOTOTRBO Nitro follows the NIST Cybersecurity Framework to protect its LTE Evolved Packet Core, cloud portal and on premises Radio Access Network. Utilizing an industry standard framework leverages proven guidelines for securing systems. The framework helps with risk-based approaches throughout our entire product development, implementation and operational support lifecycle. It also better prepares the organization in identifying, detecting, preventing, responding and recovering in the event of a cybersecurity attack.



Motorola Solutions Cybersecurity Framework: a Holistic, Risk-Based Approach

Governance and oversight throughout the product development, implementation and operational support lifecycle

Holistic risk management-based approach instead of "Check-the-Box" mindset

MOTOROLA SOLUTIONS

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