



# Unified communications cloud security

Critical Connect and WAVE PTX offer advanced security features that keep your critical communications safe



# Unified communications cyber security framework

Government and commercial organizations use cloud-based solutions, such as Critical Connect and WAVE PTX, to keep field personnel connected, informed, and safe. Protecting the confidentiality, integrity and availability of these services is of paramount importance.

That is why we have adopted a holistic, risk-based approach to security for our Unified Communications portfolio, including **Critical Connect** and **WAVE PTX**. Our approach is built with the National Institute of Standards and Technology (NIST) Cybersecurity Framework at its core.

This approach focuses on mitigation options, continuous monitoring, diagnosis and remediation to evolve security practices.

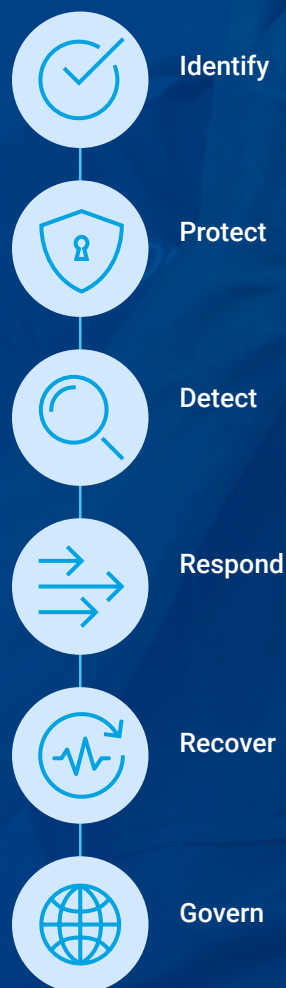
We use the NIST 800-53 standard as our baseline for application security, and applications must follow it for configuration, event logging, change management and other functions.

## Our approach to cybersecurity

A holistic, risk-based security strategy begins with identifying and reviewing the complete range of risks an organization faces. Based on risk prioritization, steps are identified to reduce risk or remediate a situation to protect the organization, people and assets concerned. Proactively confronting potentially hazardous situations before they become acute threats saves both time and money.

The NIST Framework maps cybersecurity into six functions: Identify, Protect, Detect, Respond, Recover and Govern. This white paper will review each function and highlight how the Motorola Solutions Unified Communications team accounts for each within our development process.

## NIST Framework



# Identify

**Asset management:** Motorola Solutions maintains an accurate and up-to-date inventory of assets (ISO 27001 Asset Register).

**SDLC:** Motorola Solutions has a well-defined and constantly refined secure software development life cycle that includes:

- Security requirements, secure design, threat modeling (STRIDE) and secure coding
- Product Secure Design Review and Security Assessment Reports with Motorola Solutions cybersecurity
- Data Privacy Assessment
- Training, coding guidelines with best practices from various industry standards (NIST, OWASP)
- CIS hardening and compliance with Department of Defense Security Technical Implementation Guides/ Security Requirement Guides
- Static and dynamic code analysis
- Vulnerability management
- Third-party software management (risk assessment, SCA)
- Penetration testing (web penetration, Red and Purple tests, protocol stack torture test certification, etc)
- Patch management

**Risk assessment:** Motorola Solutions conducts continuous and comprehensive risk assessments. These assessments follow organization risk management strategies, guidelines and best practices set by NIST, OWASP, CIS and other leading security organizations.

- Risk management is formal and managed by Motorola Solutions Corporate Cybersecurity.
- Each product risk has an associated risk level and treatment plan with risk owner approvals.
- Risk owner approval levels are commensurate with the risk level.
- Periodic Risk Register reviews are in place.

**Supply chain:** Policies and procedures are in place to identify and mitigate supply chain risks. Motorola Solutions' Corporate Enterprise Information Security conducts supply chain risk assessments, focusing on reviewing access to and security controls around source code.

## Design

Threat modeling  
Architectural review

## Code

Secure coding standards  
Manual and peer review

## Commit

Static code analysis  
Dependency management  
Container/function scans  
Cis benchmark analysis  
Security unit testing

## Accept

Dynamic scanning  
Security smoke tests  
Secrets management

## Deploy

Penetration testing  
Runtime monitoring  
Continuous patching

Build

Ship

Run

Software Development Lifecycle (SDLC)





# Protect

**Account management:** Unified Communications cloud applications have a role-based hierarchy with well-managed security privileges, secure authentication and authorization for both Motorola Solutions Operations, Administration & Maintenance (OAM) access and customer administrators managing devices' contacts/groups/user profiles.

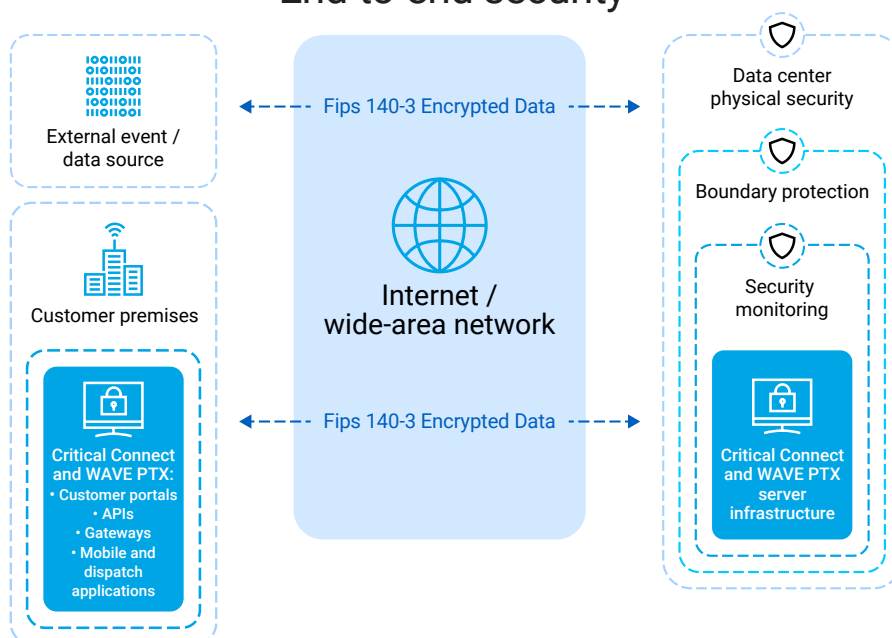
**Identity management and Access Control (end-users):** Applications include an integrated Identity Management (IDM) service.

- Mobile Client Access authentication credentials are established securely during device/user onboarding.
- All customer web portals support Two-Factor Authentication (2FA).

**Identity management and Access Control (OAM Access):** The system uses strict physical and logical access controls to protect information and resources from unauthorized access. For OAM role-based access, Motorola Solutions uses IT credentials with two-factor authentication (2FA). OAM Access is over a VPN connection from Motorola Solutions-provided devices.

- Access is based on our Access Control policy, which uses an internal ticketing system. It is granted after the manager and platform owner's approval. Role-based access is provided for privileged users.
- The process includes periodic review (currently 90 days) and automated deletions when users leave the company.

## End-to-end security







#### **Information protection and data security:**

- Data in transit is protected using secure protocols and encryption of application payload (AES 256). All control plane and web traffic is protected with FIPS-aligned encryption.
  - All external FQDNs are provided with public Certificate Authority (CA) certificates. The limited CA bundle to be used by the client applications (Android, iOS and Windows) for verifying the server's TLS certificate is further pinned into our application clients.
- Data at rest in the infrastructure is protected by access control including 2FA.
  - DB Encryption: sensitive information is stored encrypted.
  - Storage Encryption: In public cloud, Motorola Solutions uses secure storage with AES 256 encryption.
- Data at rest encryption in mobile client applications uses Android and iOS mobile security best practices.
- The integrated Key Management System (KMS) is 3GPP 33.180 compliant and supports MIKEY-SAKKE Identity Based Encryption (IBE) for key distribution and end-to-end encrypted PTT voice (SRTP, SRTCP).
- Personally Identifiable Information (PII) data in application logs does not leave national boundaries. Prior to transferring logs out of the system for troubleshooting, PII data is obfuscated using our field utilities software.
- Motorola Solutions offers Azure Express Routes integration for integrating on-premise systems with Azure-hosted Cloud services. This environment provides a private network extension into the cloud with QoS, high availability and low latency.
- Motorola Solutions Corporate Data Protection Office oversees data protection and privacy. All security/data privacy incidents must be reported to our Security Operations Center (SOC).



**Protective technology:**

- We deploy an industry-standard border gateway for perimeter defense, web application firewalls (WAF), application layer gateways (ALG), Network IDS/IPS and DOS/DDOS mitigations.
- We also deploy an Endpoint Protection Platform (EPP) to protect WAVE PTX and Critical Connect.
- Our solutions support micro-segmentation principles with 'zone' based firewall segregation and separation of containers based on applicable security controls.

**Cryptographic key management:**

- Cryptographic keys for TLS encryption are managed by privileged administrators. Private keys are regenerated annually when certificates are renewed.
- The integrated 3GPP 33.180 MIKEY SAKKE IBE-compliant KMS auto-generates, auto-rotates and auto-distributes keys.

**Configuration change management:** Our change management process has been audited for ISO 27001 compliance. Operations teams apply these policies for release upgrades and patch deployments.

- Cryptographic signing of software is in place for all customer downloadable software including Android and iOS mobile applications as well as the Dispatch plugin. Android and iOS mobile applications are updated using the platform app store.
- Server-side upgrades and patches are pushed using Motorola Solutions container registry.

**Vulnerability management:**

- We deploy industry-standard tools for vulnerability management (including automatic updates to CVE/CIS profiles).
- Our continuous delivery pipeline is integrated with vulnerability management of third-party software (3PS) and open-source software (OSS).





**Patching policy:**

- Motorola Solutions Patching Policy defines remediation and patching timelines for vulnerabilities based on their CVSS score and risk assessment. It may be noted that some 3PS/OSS packaged by RHEL are not explicitly managed by Motorola Solutions.
- Security vulnerabilities are generally patched within the remediation timelines or appropriate mitigating controls are deployed and risk assessed.

**Awareness and training:** Motorola Solutions has a training and awareness program that is mandatory for all employees, including role-based training. This includes several programs with varying re-certification cycles.

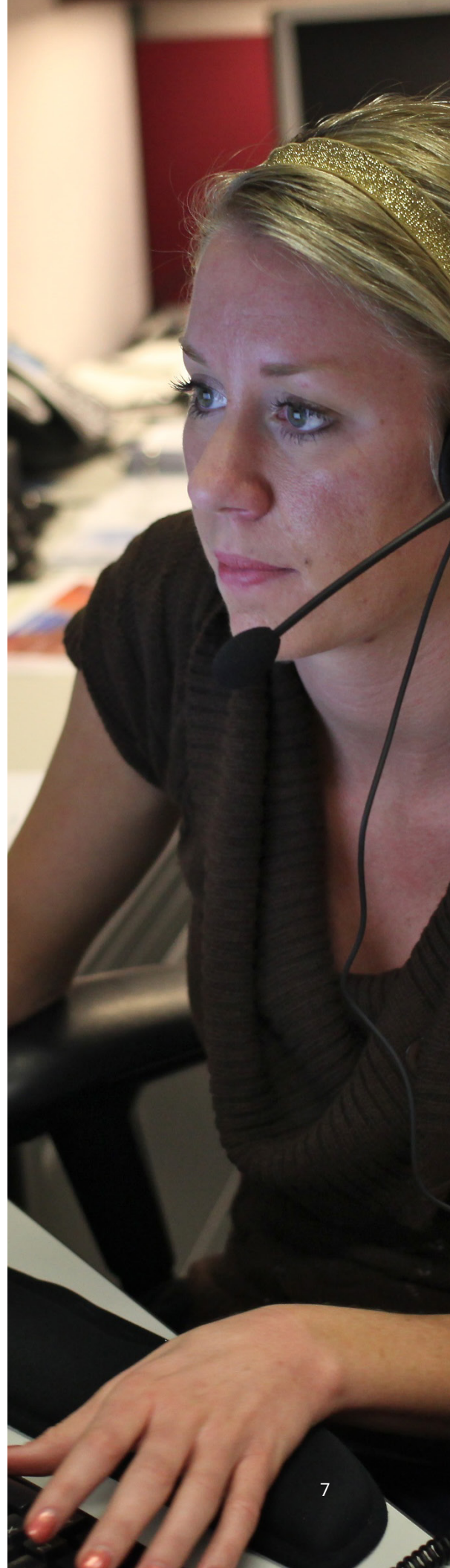
- Motorola Solutions umbrella information protection policy ensures appropriate information protection and all relevant privacy protections are foundational within Motorola Solutions and in the products and services Motorola Solutions offers to its customers. This policy establishes top-level Information Protection requirements for ensuring that risks to information assets, information resources, and customer solution offerings are managed in accordance with business goals, legal and regulatory requirements and professional standards.

We invest in the people with the expertise needed to constantly ensure security and compliance at all levels, from development and deployment, to real-time protection of systems.

**Physical and environmental protections:** Our solutions are deployed in geo-redundant data centers. Physical and environmental protections of the hosting environment are provided by data center providers. SOC 1 Type 2 report, SOC 2 Type 2 report, HIPAA and PCI-DSS certifications are available upon request.

**Governance, risk and compliance:** Our governance, risk and compliance program defines, disseminates and follows up with information protection policies, processes and procedures. All identified flaws are remediated, and the system is continuously assessed and monitored.

**Threat intelligence:** Motorola Solutions' Cybersecurity organization gathers threat intelligence, monitors industry vulnerabilities and interfaces with product teams on mitigation and correction. This process heightens awareness and allows for the correlation of events throughout the landscape, thereby making incident response more efficient.



# Detect

**Audit events and security events:**

Various system components generate a wide variety of application events, audit events and security events.

**Recorder:** Reports are made available to eligible customers to monitor all data and activity within their instance.

**Continuous monitoring:** The Motorola Solutions NOC monitors the system 24x7x365. Various health, KPIs, network and application events and alarms are monitored through a fully automated ingest pipeline. Monitoring alerts automatically trigger incidents. Various recovery actions are automated (e.g. process recovery is performed automatically in order of seconds).

**Cloud security platform monitoring:**

For Motorola Solutions hosted deployments, Motorola Solutions SOC (ActiveEye Platform) monitors our services running in Azure and AWS.





# Our holistic, risk-based approach to security

The latest cyber headlines offer fresh warnings that government agencies and enterprises must be ready for breaches of critical networks.

As these organizations are finding, the best protection is a proactive, holistic, and risk-based approach using the guidelines and best practices provided by NIST, ISO, OWASP and CIS.

## Compliance with industry standards and best practices



NIST Cybersecurity Framework (CSF)  
NIST 800-53 - Controls



ISO 27001 - Specification for an Information  
Security Management System (ISMS)



Open web application security project  
- Top 10 most critical web application security risks



Center for Internet Security globally recognized  
standards and best practices





# Respond

**Incident response planning:** Incident response planning and procedures are in place to properly handle and respond to incidents on time.

- Dedicated incident managers are assigned to handle incidents.
- Periodic incident response training is provided including tabletop exercises to simulate incidents, and feedback is provided for improvements.

**Reporting:** Incident reporting procedures are in place to ensure notifications (e.g. initial, updates and final) to stakeholders. After resolution, a detailed root cause analysis is prepared, including lessons learned and next action items. The root cause analysis and action items are tracked by the incident manager to completion.

**Improvements:** Motorola Solutions' continuous learning and ever-evolving best practices are incorporated into the Unified Communications processes.



# Recover

**Contingency plans:** Contingency plans for disaster recovery are in place. Our Unified Communications' systems generate backups, which are stored for the configurable retention period and can be used to recover the system.

**Recovery:** Built-in redundancy of 'hot active' geo-site with fully replicated, real-time information allows WAVE PTX services to recover automatically during a geo-failover event.



# Govern

Motorola Solutions has a well-established cybersecurity organization that provides governance, strategy, guidance and services to development teams throughout Motorola Solutions pertaining to cybersecurity process, risk management, software development lifecycle (SDLC) and compliance assessment.





# Our commitment to cybersecurity

Our Unified Communications cloud solutions comply with key industry best practices for security, including: the NIST Security and Privacy Controls for Information Systems and Organizations (800-53); the ISO 27001 - Specification for an Information Security Management System; the Open Web Application Security Project (OWASP); and the Center for Internet Security (CIS).

Motorola Solutions holds an ISO 27001 certificate with allied 27017, 27018 and Data Privacy 27701 as well as a SOC 2 Type 2 audit from a third-party audit organization. We have achieved TX-RAMP Level 2 Certification for our US WAVE and Critical Connect solutions. Critical Connect is also P25 CAP Certified for P25 ISSI Interoperability.

In addition to meeting global standards for information security and privacy practices, international Motorola Solutions WAVE and Critical Connect instances have undergone country-specific assessments that provide additional assurance to our customers (e.g. in Canada and Australia) during and after the procurement of our services.

These are some of the guidelines and best practices we follow when taking our applications through security reviews at each phase of their software development lifecycle. Even after deployment, we continue with ongoing assessments to find and repair vulnerabilities.

The Motorola Solutions CISA-recognized Public Safety Threat Alliance also makes it possible for Unified Communications customers to share threat information, raising cybersecurity awareness across all public safety member organizations.

For Unified Communications, the result is security that is proactively incorporated into the design of our applications, not bolted on reactively when incidents occur.

For our customers, the result is peace of mind knowing that their data and workflows are prepared to withstand attack.



# Why choose Motorola Solutions?

- Over 90 years of trusted innovation and business continuity
- Cybersecurity experts in mission-critical networks
- Comprehensive technology ecosystem offers value-added integrations
- Robust platform for API integrations
- Intuitive portals, tools and features support user experience
- One point of contact for technical support

For more information about protecting your data,  
visit [motorolasolutions.com/trustcenter](https://motorolasolutions.com/trustcenter)



Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A. [motorolasolutions.com](https://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. 09-2024 [BG09]