SECURING MISSION-CRITICAL COMMUNICATIONS

APX NEXT SERIES RADIOS AND APPLICATIONS

MOTOROLA SOLUTIONS

FOR PUBLIC SAFETY AGENCIES TASKED WITH KEEPING COMMUNITIES SAFE, THREE TECHNOLOGY TRENDS HAVE CONVERGED TO FORM A SEEMINGLY PERFECT STORM OF CHALLENGES.

First, public safety agencies are facing an explosion of data, making it difficult to store, access, and digest information efficiently. Second, agencies are hampered by outdated technology and legacy IT silos. In fact, according to a recent report, 40% of an agency's computers may be over seven years old and running decades-old software.[1]Third, growing cyber threats and advanced global criminal syndicates are increasingly targeting government at all levels. More than 70 percent of reported ransomware attacks in the U.S. target state and local governments. At least 180 public safety call centers were also targeted in the last two years.[2]

Operationalizing public safety data and applications in the cloud offers the best path forward to meet each of these challenges, but security remains a top priority. Today, cloud-based public safety solutions are simply more secure, more flexible, more resilient, and easier to maintain and update than on-premises solutions. But all cloud solutions aren't equal. As you evaluate cloud solution providers, it's critically important to understand the security culture, processes, and technology that differentiates them.

1. Bloomberg Businessweek, 2-28-19
2. World Economic Forum

THE BUILDING BLOCKS OF CLOUD SECURITY
PEOPLE. PROCESSES. TECHNOLOGY.

In the world of high-stakes public safety, trust is not given lightly. Motorola Solutions has earned that trust for more than 90 years, partnering with agencies like yours to build, deploy, and refine the most advanced mission-critical systems. Today we're expanding that trust through leadership and innovation by strengthening our mission-critical networks with cloud technology. And we understand as we normalize cloud utilization, the importance of cloud security is an unconditional priority.

To secure our cloud-based APX NEXT solutions, Motorola Solutions takes on most of the burden of building, hosting, maintaining, and securing systems so public safety agencies can focus on their own mission-critical tasks. We empower public safety with advanced technology and highly specialized talent, industry-leading processes, and cutting-edge technology. Together, this seamless orchestration of people, processes and technology form the backbone of our holistic risk management-based approach to security - one that's been highly successful for public safety agencies across the US.

PEOPLE

AT MOTOROLA SOLUTIONS, IT’S NOT A COINCIDENCE THAT OUR EMPLOYEES ARE LEADERS IN THE FIELD OF PUBLIC SAFETY CYBERSECURITY. THEY HOLD TOP INDUSTRY CYBERSECURITY CERTIFICATIONS AND COMPLETE REQUIRED CYBER TRAINING. THEN, WE CONTINUOUSLY AND AGGRESSIVELY INVEST IN THEIR CAREERS AND EXPERTISE WITH ONGOING TRAINING AND EDUCATION, BY LEVERAGING THE NIST NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION FRAMEWORK (NICE FRAMEWORK).

The NICE Framework provides the most up to date knowledge, skills, abilities, and tasks for each trainee. All courses are overseen by an expert third-party resource, with individualized curriculums and learning paths based on each employee’s specific needs. As courses are completed, a score is provided with links to learn more, so all cybersecurity employees can easily track and extend their progress as they sharpen their skills.

We also founded the Motorola Solutions Cyber Champions Program, which instills cybersecurity principles and knowledge at a grassroots level throughout our product and services organizations and ensures every development team has at least one security champion. In addition, the Motorola Solutions Threat Intelligence team creates a holistic view of the cyber threat landscape and how it impacts our customers’ business priorities and infrastructure. The team analyzes and communicates the capability, opportunity, and intent of a cyber threat targeting Motorola Solutions products and customers. This level of situational awareness provides stakeholders and decision makers with the information needed to prioritize resources and enable better security decisions.

From the day they’re hired and every day after, we ensure our teams’ skills remain sharp so they always stay ahead of changes in the fast-evolving cybersecurity industry. From extensive and ongoing training to our organizational structure, a pervasive focus on security runs through all aspects of our operations.

THE MOTOROLA SOLUTIONS CYBER CHAMPIONS PROGRAM

We believe security is a critical measure of quality that defines all of our products and services. The Motorola Solutions Cybersecurity Champions Program was created to ensure that cybersecurity thinking is woven tightly into the fabric of our company. To become a Cyber Champion, employees must pass a gauntlet of training modules as part of an 8-week onboarding and training process. Once certified, each Cyber Champion returns to their team, further infusing a fundamental security culture by relaying what they’ve learned to their peers. This grassroots approach has proven extremely effective, with more than 700 Motorola Solutions Cyber Champions and growing.

To learn more, visit our online
Trust Center.

PROCESSES

ALL MOTOROLA SOLUTIONS SOFTWARE AND SERVICES ARE GUIDED BY THREE CORE INFORMATION SECURITY PRINCIPLES THROUGHOUT THE DEVELOPMENT, IMPLEMENTATION, AND OPERATIONAL SUPPORT LIFECYCLE: CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY - OTHERWISE KNOWN AS THE CIA TRIAD. DATA AND INFORMATION MUST BE CONFINED TO PEOPLE AUTHORIZED TO ACCESS IT AND NOT BE DISCLOSED TO OTHERS; DATA MUST BE KEPT INTACT, COMPLETE AND ACCURATE; WITH HIGHLY RELIABLE AND REDUNDANT IT SYSTEMS THAT REMAIN AVAILABLE TO AUTHORIZED USERS WHENEVER NEEDED.

We believe that security must be a core pillar in every phase of development, from before a developer even touches a keyboard, to after a product is delivered. In both agile and waterfall development methods, security activities are deeply embedded into every step of our Secure Software Development Life Cycle (S-SDLC). Each of these activities must be completed before we move on to the next step.

PROCESSES ARE CRITICAL

Agile software development prizes speed and flexibility, allowing us to rapidly deliver new features while meeting your evolving needs. Our carefully considered and highly tested security processes ensure that no matter how fast we move, security remains a persistent and intrinsic priority.

Our S-SDLC is driven by continuous training for developers and other team members as outlined previously, along with five additional phases:

REQUIREMENTS

In a traditional SDLC, the requirements phase is where developers spend time understanding overall goals. But it's critical for development teams to understand cybersecurity risk and mitigation options from the very beginning of the development lifecycle. So, our Secure SDLC includes high-level security requirements that must be considered even in the earliest stages of the requirements phase. Our dedicated Product Governance, Risk and Compliance program blends risk-based and compliance-based security requirements to produce relevant and actionable security guidelines, checklists and best practices for our engineers and developers. We maintain and update these requirements regularly so they can be followed through every step of the development process.

DESIGN

As development begins, the design phase of the Secure SDLC is where we ensure cybersecurity requirements and controls are fully integrated into our products and applications. We perform security architecture reviews of all new products and features. These include in-depth technical questions and discussions around data flows, security boundaries, and "defense in depth" controls. We also perform in-depth threat modeling of both brand-new solutions and updates to an existing feature. For development teams following agile practices, these activities can be documented as security requirement stories and negative use cases.

IMPLEMENTATION

As our developers work to implement new features, we integrate automated security scanning to provide rapid feedback. Our goal is to discover security vulnerabilities as early as possible. By running scans in developers' normal Continuous Integration and Continuous Delivery (CI/CD) pipelines, we can provide near-immediate feedback on code defects, open source usage and dynamic scan results. .

VERIFICATION

As code is built and a release date approaches, we perform verification of our security requirements through both manual and automated processes. Using industry standard vulnerability scanning tools on completed systems in test labs, we can identify any vulnerabilities and misconfigurations that made it past the implementation phase. We also employ a dedicated red team that performs "ethical hacking" and regular penetration tests of our systems and applications to emulate real threats and identify flaws or vulnerabilities in our systems after they're built. Lastly, our scanners and automated processes check our products against regular industry standards, such as Center for Internet Security (CIS) Benchmarks and Defense Information Systems Agency's Security Technical Implementation Guide (DISA STIGS).

DEPLOYMENT AND MAINTENANCE

The final phase of the Secure SDLC represents an ongoing commitment to the security of our products post-release and throughout their entire lifetime. Automated and manual release gates and checklists ensure products and applications have passed all security checks before deployment. After release, we continue to test for weaknesses and vulnerabilities. Our public bug bounty program, external vulnerability scanning process and dedicated threat intelligence team are all used to identify and discover vulnerabilities that could arise after release. Continuous threat monitoring in our cloud and on-premise environments also send alerts in near real-time if any suspicious behavior is detected. This directly informs and improves the security of our products through regular patching and release cycles.

COMPLIANCE IS A TEAM EFFORT

We know compliance is important to our customers. It's critical to us too. The responsibility for compliance is shared among Microsoft Azure Government, Motorola Solutions, and you - the customer. We act as a true partner, helping your agency meet responsibilities to support compliance with even the most stringent legal and regulatory requirements.

We employ dedicated teams to sustain appropriate policies and procedures, protect customer data and support continued compliance of our products and services. These teams are staffed by our cyber, legal and compliance experts who have deep subject matter expertise in privacy, compliance and information security disciplines. With Motorola Solutions and Microsoft Azure Government, you have the support of thousands of cloud security and compliance experts to help maintain security at scale. Ultimately, with this support, your agency will be able to reallocate precious IT resources to more strategic tasks and your personnel can focus on public safety, not technology.

To learn more, visit our online resource on Compliance

TECHNOLOGY

IN ADDITION TO MOTOROLA SOLUTIONS' PEOPLE AND PROCESSES, THE UNDERLYING ARCHITECTURE OF OUR CLOUD OFFERINGS IS REINFORCED BY A MODERN AND COMPREHENSIVE APPLICATION OF SECURITY TECHNOLOGY. WE LEVERAGE STRICT LOGICAL CONTROLS WITHIN CLOUD ENVIRONMENTS THAT INCLUDE VIRTUAL MACHINES DEPLOYED IN SECURE VIRTUAL NETWORKS, ENCRYPTION, FIREWALLS, INGRESS CONTROLLERS, IDENTITY MANAGEMENT AND MORE, WORKING TOGETHER TO ENSURE PRIVACY AND SECURITY.

We further run Host Intrusion Detection Systems (HIDS) on each Virtual Machine to detect and block a broad range of threats. The HIDS leverages signature-based detection, as well as anomalous behavior detection methods to both identify and block zero day exploits. Secure "pipelines" are used to enforce many of the gates mentioned above that scan, test, and ensure only properly secured components can be deployed into the production environment.

Once deployed, our production systems are monitored using state-of-the-art Security Event and Information Management (SEIM) technology. Additionally, this security architecture is magnified by our cloud service provider, Microsoft Azure. The Microsoft Azure Government Cloud is built specifically for government-based, mission-critical applications and adds essential security layers. It offers full AES-256 encryption for data at rest and TLS encryption for data in transit, allows government-only environments, and requires CJIS compliance. It also requires SOC 2 reporting and a third-party audit of security practices.

PROTECTING ATTACKS FROM FOUR DIRECTIONS

APX NEXT RADIOS

Malicious software,
unauthorized use

P25 NETWORK

Unauthorized access,
redirection

CLOUD APPLICATIONS

Data access,
data tampering

COMMUNICATIONS

Interception,
denial of service

PROTECT THE RADIO

MOTOROLA SOLUTIONS KEEPS APX NEXT RADIOS SECURE IN THESE WAYS.

TRUSTED BOOT PROCESS:

APX NEXT series radios check the authenticity and integrity of its firmware during boot and during updates. If the firmware fails integrity or authenticity checks, it is prevented from being installed or executed. This ensures APX NEXT is executing trusted, unmodified firmware.

TRUSTED EXECUTION ENVIRONMENT:

Motorola Solutions runs critical crypto operations. APX NEXT series radios include a hardware-backed trusted execution environment for critical security functions and services, so they execute separately from the primary Operating System. This ensures that critical functions are protected from any vulnerabilities within the Operating System.

REAL-TIME THREAT PROTECTION:

APX NEXT radios include multi-layer real-time threat protection to actively self-detect and protect against Operating System and Application exploits / attacks, such as device rooting, privilege escalation, zero-days, code manipulation and flow attacks, run-time data manipulation and access, malware install, bypass of internal kernel security and access controls.

DEVICE USER AUTHENTICATION:

Multi-Factor Authentication (MFA) is supported. The authorization schema is implemented for access to data and services. The first authentication mechanism is a user password. The second is a PIN that is sent to the email associated with the account and must be retrieved on a different device. The user can sign-in once and all features configured for MFA will be signed in. The duration of the MFA session is configurable and survives power cycles.

SECURE DEVICE MANAGEMENT AND CONFIGURATION:

Programming and configuration of the device is secured to protect against tampering, unauthorized access, and information disclosure. New radio features, defect repairs, and security vulnerability remediations can be pushed seamlessly on a frequent cadence, or as needed.

DAR DATA SECURITY:

Sensitive data is encrypted while at rest (DAR). Credentials, certificates, private keys and P25 End-to-End symmetric keys are securely stored in FIPS 140-2 certified keystores.

FIPS 140-2 CERTIFIED SECURITY MODULES:

Hardware and Software security modules are certified to FIPS 140-2. Both LMR and broadband Data In Transit (DIT) encryption uses a FIPS 140-2 Level cryptographic module.

PROTECT THE P25 NETWORK

IT'S VITAL THAT THE APX NEXT FEATURES AND SERVICES DON'T ENDANGER THE EXISTING P25 COMMUNICATIONS SYSTEM. APPLICATIONS AND PROGRAMMING ARE PERFORMED OUTSIDE THE P25 NETWORK.

AES256 ENCRYPTION:

We begin with the current safeguards that exist in a current P25 system. All the familiar best practices such as AES256 Encryption remain in place - built into the standard. That is the benefit of using a public safety platform like P25: security is built-in from the beginning.

RADIO AUTHENTICATION:

It is also recommended that customers implement other optional features like radio authentication, to prevent unauthorized radios from getting onto the system.

INTERNETWORKING FIREWALL:

To prevent attacks to the P25 system originating from the internet, the solution includes an internetworking firewall to protect the CEN. This is in addition to the firewall already present in the ASTRO core. This additional firewall ensures that only the needed and approved SmartConnect communications go through the P25 network.

LOGGING AND MONITORING:

The Centralized SysLog maintains detailed records, for security monitoring and post-incident analysis. Data event logging, chain of custody and non-repudiation are supported through the use of security information and event management system.

CYBERSECURITY SERVICES:

Motorola Solutions offers as an additional service 24/7 monitoring of customer networks to protect and warn of ransomware threats and other cybersecurity risks.

PROTECT THE CLOUD APPLICATIONS

TO PROTECT THE DATA OF THE APPLICATIONS USED WITH APX NEXT PORTFOLIO OF RADIOS.

MICROSOFT AZURE GOVERNMENT CLOUD:

For State and Local US Customers, Motorola Solutions uses the Microsoft Azure GovCloud to host the APX NEXT application services. Our customers benefit in big ways:

1. To be on GovCloud, we need to fulfill minimum security requirements. Microsoft enforces standards that give you confidence that the service is built to a high standard.
2. GovCloud infrastructure is intrinsically hardened for public safety use. This includes Load Balancers (to mitigate Denial of Service attacks), strong physical security, and hardware redundancy.
3. The operators for Azure Gov Regions have undergone screening and all the operators are also US Citizens and on US Soil which is not the case for the US Commercial clouds.
4. The Gov Cloud infrastructure and operations have undergone review, evaluation and approval by the states. Azure Gov has the CJIS Trusted Provider Agreements in place for all these states.

SOC MONITORING AND INCIDENT RESPONSE:

In addition to Microsoft's own security monitoring of the Azure Infrastructure, Motorola Solutions has an experienced 24x7 security operations center that monitors our cloud deployed applications for unauthorized or anomalous activities and other indicators of potential compromise. To support the monitoring capability we rely on state of the art cloud security components including modern web application firewalls, host intrusion detection and prevention components, as well as Security Information and Event Monitoring elements. Additionally, Azure operates on a different layer to detect attacks that affect their ability to provide the services we rely on. They can also detect certain anomalous behaviour of our components. Between these two monitoring solutions we are able to detect and quickly react to potential attack activity.

APPLICATION SECURITY:

Secure development lifecycle and application controls are utilized to ensure data and application integrity, confidentiality and availability. Identity and Access Management solution is implemented for user and API authentication and authorization.

DAR AND DIT DATA SECURITY:

Sensitive data is encrypted while at rest (DAR) and in transit (DIT) with state of the art FIPS 140-2 approved cryptographic algorithm. Data event logging, chain of custody and non-repudiation are supported through the use of security information and event management system.

IDENTITY MANAGEMENT, ACCESS MANAGEMENT AND AUTHENTICATION:

In order to ensure no unauthorized users access the applications, HTTPS with OAuth 2.0 User Tokens secure the communications between user client/portal(s) and the cloud services of RadioCentral, CommandCentral Aware Mapping (SmartLocate), Kodiak Dispatch Client (SmartMessaging). Additionally, mutually authenticated TLS/HTTPS sessions utilizing device X.509 certificates from the Motorola Solutions PKI ensure only genuine Motorola Solutions subscriber devices access the applications.

PROTECT THE COMMUNICATIONS

TO PROTECT COMMUNICATIONS BETWEEN ALL THE SOLUTION COMPONENTS. BOTH APX NEXT VOICE AND DATA SESSIONS ARE ENCRYPTED ACROSS ALL TRANSPORTS (LMR P25, WI-FI AND LTE).

MUTUAL AUTHENTICATION:

Mutual authentication protects against "Man in the Middle" attacks with the X.509 certificate. This is between APX NEXT series radios and RadioCentral, SmartConnect, SmartLocate, SmartMapping, SmartMessaging cloud services.

LMR ENCRYPTION:

Motorola Solutions recommends that LMR P25 data and voice be encrypted.

BROADBAND ENCRYPTION:

Broadband voice communication is secured via Secure Real-Time Transport Protocol (SRTP). The associated SmartConnect Authentication key is established via Transport Layer Security(TLS) control. Broadband data communication is secured via TLS.

DIT DATA SECURITY:

Sensitive data is encrypted while in transit (DIT). Credentials, certificates, and keys are securely stored. Industry-standard secure protocols are used for DIT. Device interface security practices and controls are implemented for Wi-Fi, Bluetooth and USB.

OUR COMMITMENT TO PRIVACY

We recognize that your agency's data is essential to mission-critical operations. That's why the privacy of your data is our top priority. We adhere to essential privacy principles and promote ethical data management, together with transparency and accountability around our commitments to protecting and managing your data. You maintain continual ownership of your data, while we help you better store, manage, and analyze it. Our products and services are designed with secure engineering and privacy-by-design practices to protect your data and to assist and support your compliance obligations. Your data is always stored in datacenters located in your nation, with appropriate logging, employee screening and incident response practices.

To learn more, visit our online Privacy Overview.

ACCELERATING PUBLIC SAFETY IN THE CLOUD

As public safety agencies grapple with growing cyber threats, exploding volumes of data, and outdated, disjointed IT systems, cloud solutions offer the best method to combat all three connected challenges. The cloud is simply more secure, more flexible, more resilient, and easier to maintain and update than any other means to deliver public safety technology.

At Motorola Solutions, we're bringing the same trust and commitment to the cloud that we've built into our entire mission-critical ecosystem for more than 90 years. With industry-leading cybersecurity people, regimented processes, and modern technology ingrained throughout our organization and culture, we're defining what it means to secure public safety in the cloud today and beyond.

For more information, please visit:
www.motorolasolutions.com/apxnextradio

MOTOROLA SOLUTIONS

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