SECURING MISSION-CRITICAL COMMUNICATION IN THE CLOUD

CIRRUSCENTRAL

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 Second, agencies are hampered by outdated technology and legacy IT silos.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 strenghthening our mission-critical networks with cloud technology - CirrusCentral. And we understand as we normalize cloud utilization, the importance of cloud security is an unconditional priority.

To secure our cloud-based CirrusCentral solutions, we transfer 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 350 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-premises 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

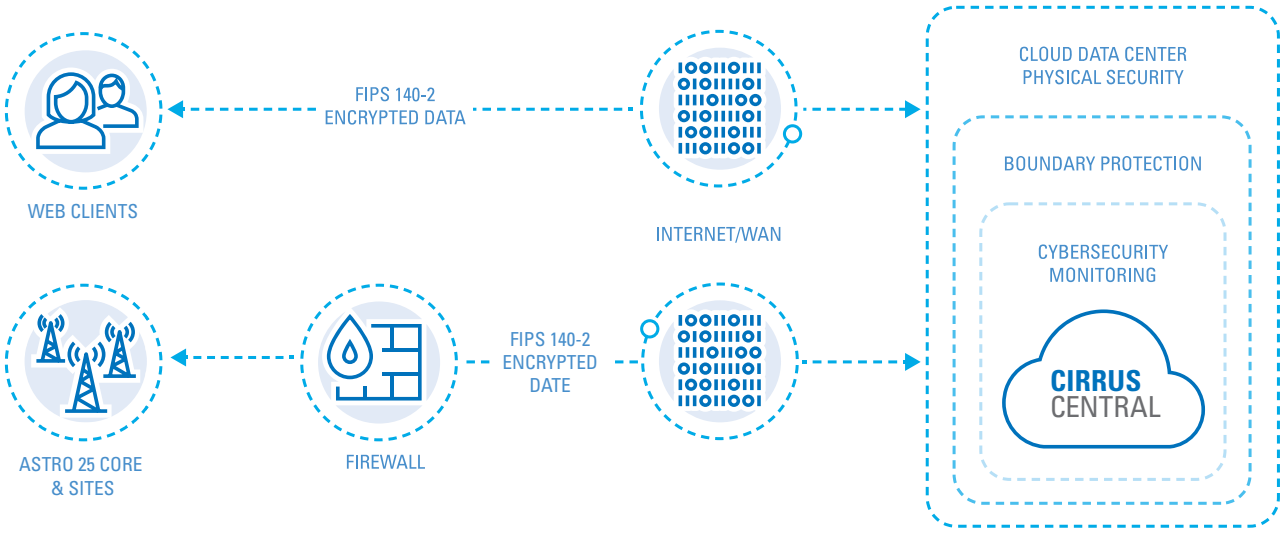
TECHNOLOGY

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.

END-TO-END CLOUD SECURITY



MICROSOFT AZURE GOVERNMENT

We run applications and store data in the extremely secure Azure Government cloud, with datacenters protected by layers of physical and logical security.

PHYSICAL SECURITY

Microsoft teams understand the importance of protecting your data and are committed to helping secure the datacenters that contain your applications and data. They design, build, and operate their state-of-the-art datacenters to strictly control physical access to the areas where your data is stored.[1]

BOUNDARY PROTECTION

Controls are in place to monitor and govern communication at the external boundary of the virtual network housing CirrusCentral information to prevent and detect malicious or unauthorized actions with protection devices including proxies, gateways, routers, firewalls, or encryption tunnels.

END-TO-END ENCRYPTION

All data is strongly encrypted end-to-end, meaning data is private and secured with FIPS 140-2 encryption provided by the TLS connection between client PC and the CirrusCentral Virtual Network. Trust between the client PC and the CirrusCentral servers is established by TLS using digital certificates and strong public key cryptography. Once server trust is established, symmetric keys used in the TLS communication are negotiated. The encryption endpoint acts as a strict policy enforcer and requires a minimum of TLSv1.2 encryption protocol. Under the TLS protocol each side negotiates a cipher suite (encryption suite). We require the use of FIPS approved cipher suites and we use a FIPS 140-2 certified encryption module to perform all encryption, compliant with the CJIS Security Policy.

COMPLIANCE

At Motorola Solutions, we are committed to employing privacy and security protocols that enable our customers to comply with the most stringent legal and regulatory requirements. In addition, we build on a strong foundation with an Azure architecture designed and managed to meet a broad set of international compliance standards, as well as region-specific and industry-specific standards. Rigorous third-party audits verify adherence to the strict security controls these standards mandate.

OWNERSHIP

For data privacy purposes, CirrusCentral customers maintain ownership of all data provided to CirrusCentral applications and always retain the rights and responsibilities of the data controller. Motorola Solutions assumes the role and responsibilities of the Data Processor and Data Custodian on your behalf. For data protection purposes, the final layers of security are ultimately reliant upon you, the customer, to protect your networks and devices that connect to CirrusCentral. This is achieved by implementing security controls such as building security, key cards, access controls, firewalls, passwords, antivirus software, network intrusion detection systems and more.

1. https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security

SECURING CIRRUSCENTRAL

SECURE ARCHITECTURE

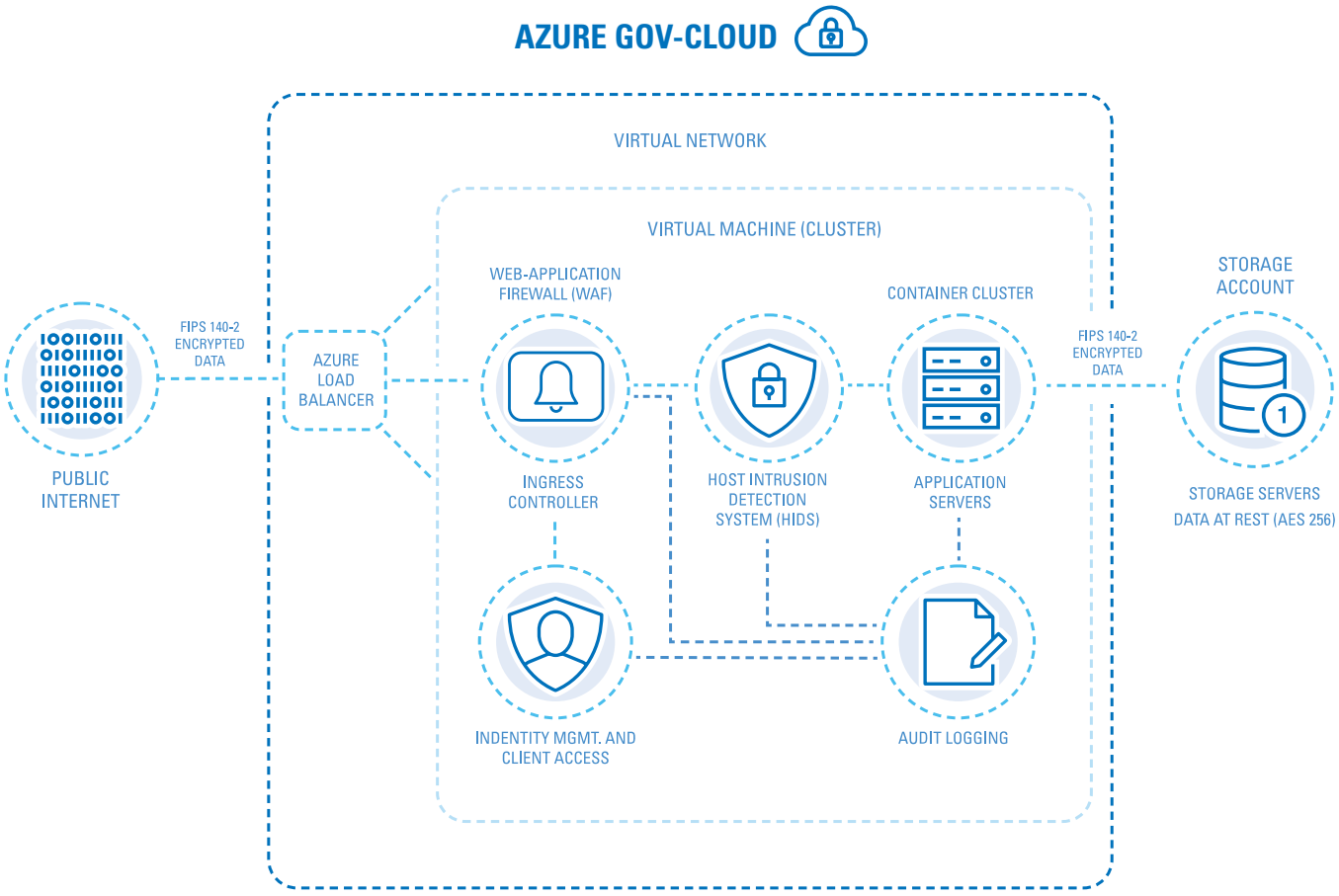
CirrusCentral leverages a logical multi-tiered architecture that includes load balancers, ingress controllers, firewalls, encryption tunnels and Host Intrusion Detection Systems for layers of protection along with necessary isolation and privacy of data and applications. We also deploy intrusion detection and prevention tools that are developed specifically for cloud-based containerized deployments. We further leverage Azure controls for traffic entering and leaving the system, including Access Control Lists and Security Groups that only allow traffic to flow between components that are authorized to communicate with each other. Administrative access to these networks is tightly controlled using public key cryptography.

VIRTUAL NETWORK

All CirrusCentral applications live in a secure VNET. Virtual Networks provide an isolated and highly secure environment to run virtual machines and applications. VNETs provide the first level of isolation between CirrusCentral, your data, and other Azure customers.

LOAD BALANCER

The first line of defense to your VNET, Azure load balancers are extremely effective at detecting, absorbing and rejecting most DDOS attacks to block attacks before they can ever touch the CirrusCentral VNET. They also forward traffic to the appropriate ingress controller for further validation.



INGRESS CONTROLLER

All users are required to authenticate with our identity management system and are issued standard OAuth or OpenID Connect tokens, which are used to govern the access control for each user. Ingress controllers police traffic and validate proper access and authorization to cloud services. They then validate digitally signed tokens for further system access and act as the end point for external TLS connections. NGINX is the reverse proxy for the system and requires a TLS1.2, TLS 1.3, and FIPS 140-2 level connection.

IDENTITY MANAGEMENT

Ingress controllers validate tokens, ensuring each request coming into the system must contain a valid token, which is cryptographically secure from the client PC. A token includes agency ID and scope, allowing access to particular applications or services, pending authorization.

WEB APPLICATION FIREWALL (WAF)

WAFs detect and block application layer attacks, block malicious IPs, and secure known vulnerabilities. The WAF blocks all known OWASP attack vectors, requests from known malicious actors, or any known signature based attacks. CirrusCentral uses only state-of-the-art latest generation WAF components.

HOST INTRUSION DETECTION SYSTEM (HIDS)

The HIDS used in CirrusCentral are cloud native systems deployed across VMs and containers to protect networks, monitor traffic and maintain operational integrity. The HIDS blocks unauthorized actions and requests from insecure sources, performs daily scans of the system, and provides real-time security audits and configuration, while logging and alerting anomalous behavior.

APPLICATION SERVERS

All applications run within a container with layers of inherent security built into the operating system. The security and network policies within the operating system control access to the server. The network controls also prevent containers from communicating with arbitrary endpoints unless explicitly configured to do so, which helps prevent lateral spread of a potential attack.

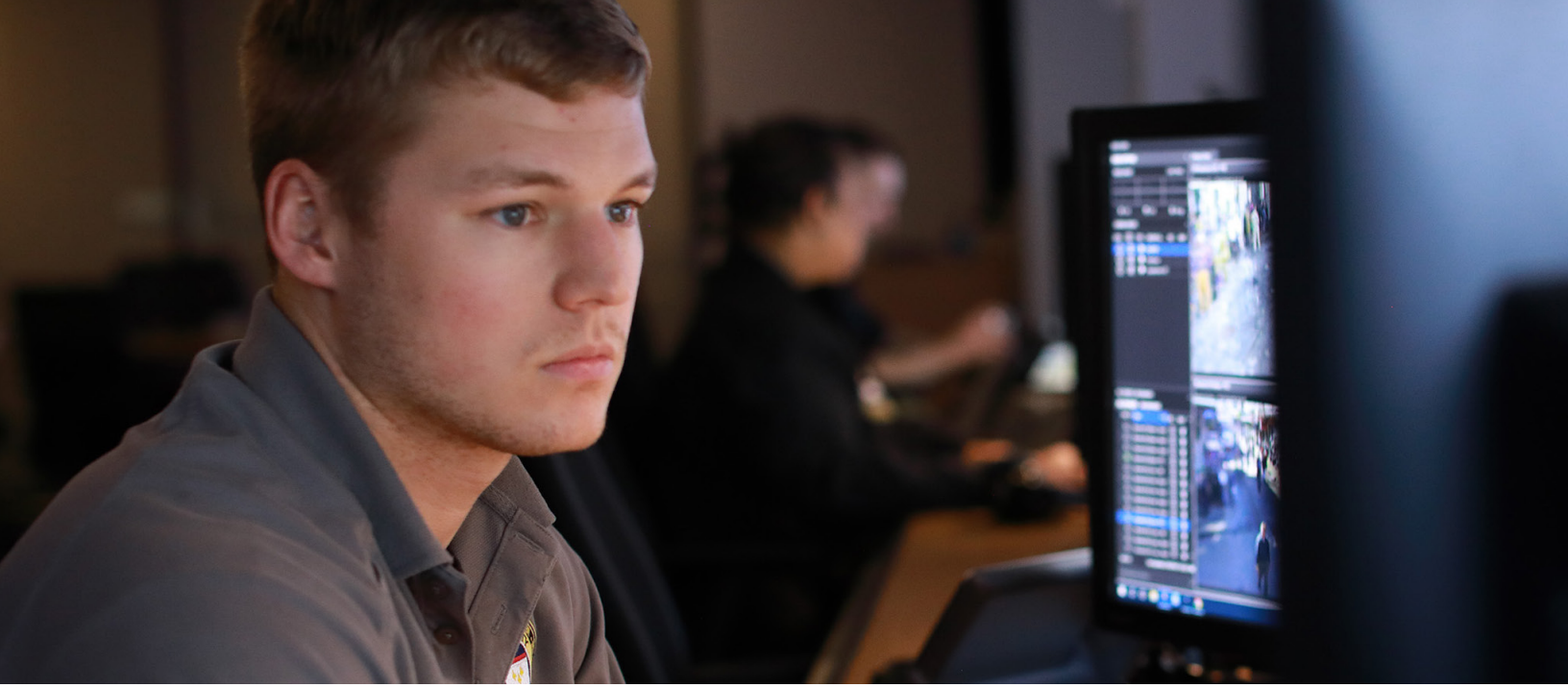
STORAGE ACCOUNT

All CirrusCentral data is stored in FIPS certified AES-256 encrypted form. We use an Azure encryption service that prevents us from accessing the encryption keys. Credentials used to access storage accounts are stored in the Azure key vault, which can only be accessed by the applications that need to read from and write to the account. Of course all communications between CirrusCentral applications and the storage accounts are over TLS tunnels and encrypted using FIPS certified AES-256.

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.

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 us on the web at:
www.motorolasolutions.com/cirruscentral

MOTOROLA SOLUTIONS

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