SOLUTION BRIEF
SMART PUBLIC SAFETY SOLUTIONS

DEPLOYING SMART PUBLIC SAFETY SOLUTIONS IN THE CLOUD

MOTOROLA SOLUTIONS

TRANSFORMING HOW YOU ADOPT TECHNOLOGY WITH GREATER SIMPLICITY AND SECURITY

Smart Public Safety Solutions empower your agency to transform data for increased responder and community safety. This means giving you solutions that transform how you avert, respond to and resolve incidents to keep you a step ahead of the rapidly-evolving public safety landscape.

Our CommandCentral platform, built with a security first approach, leverages the Criminal Justice Information Services (CJIS) compliant, GovCloud (US) region of the Amazon Web Services (AWS) Cloud, to deliver a broad suite of public safety applications. Using these cloud-based applications allows you to right-size for your needs from the start, while maintaining the flexibility to grow and expand in line with your operations in the future. Being in the cloud also ensures that the burden of dedicating valuable resources to maintain an optimal operation is no longer placed on you and your staff, and you can instead stay focused on your mission of maintaining community and responder safety.

ACTIVATE THE CLOUD – SIMPLIFY OPERATIONS

The expectation today is that information is instantly available, highly relevant and easily consumed. This can range from your officers receiving automatic weather alerts on their phones as they keep crowds safe at the big game, or receiving an alert about a warrant as they run a license plate at a traffic stop. These expectations, combined with the immense speed of innovation in new applications, devices and sensors (Internet of Things); the proliferation of video; and always connected citizens, along with shrinking IT budgets, puts IT organizations under more pressure than ever.

Cloud deployments lower capital and operating expenses while expediting the speed of new technology adoption. More importantly, by being CJIS compliant, they maintain the most thorough security policies, processes and procedures to ensure your operations stay protected. With the cloud-based CommandCentral platform, you can simplify the deployment of smart public safety data applications that responders need to perform their best with security you can trust.

CONSIDER THE TOTAL COST OF OWNERSHIP

RIGHT-SIZE YOUR INVESTMENT

Deploying new capabilities on-premise often means an upfront purchase of software and hardware. The investments require extensive planning and estimation of capacity needs for a five to eight-year lifespan. Conservative planning may result in capacity that is never used while aggressive planning may require larger, incremental investments down the road to expand capacity. Servers also have to be physically housed in facilities with considerations for redundancy and disaster recovery that factor into increased overhead expense.

With the cloud, subscribe to exactly what you need. As your operations change over time to meet the evolving needs of your community, cost scales linearly as on-demand computing capacity allows you to employ "just-in-time" increases in capacity, versus the more expensive "just-in-case" on-premise model. Cloud servers don’t require any facility investment, disaster recovery is built into the cost and you never have to think about the lifespan of the hardware.

OFFLOAD THE COMPLEXITY OF DEPLOYING TECHNOLOGY

Deploying software and hardware solutions requires IT time and expertise – both highly valuable and very scarce resources for any organization. The amount of time and the depth of expertise will vary by solution, but can lengthen the time-to-value of new investments. Training, which is necessary to prepare staff, can contribute to initial deployment costs. Other upfront efforts such as planning, architecture and IT approvals are followed by un-boxing, “racking and stacking” hardware and installing software. Configuration of applications, tuning parameters and potentially installing end user clients can then drag on for weeks or months after the initial purchase.

With the cloud, you remove the majority of time and expertise required so time-to-value can be realized within days after purchase. Browser-based access allows you to simply log in and start using new capabilities immediately, eliminating the majority of local on-premise planning, installation or configuration.

ELIMINATE THE BURDEN OF MAINTAINING YOUR NEW TECHNOLOGY

Often, one of the most overlooked areas when considering tradeoffs between cloud and on-premise options is the on-going maintenance of technology. Systems need to be maintained, logs rotated, file systems cleaned, backups performed, operating systems patched and extensive monitoring done of security posture, services and system health. With on-premise technologies, when something goes wrong or users cannot log in, your staff must troubleshoot, isolate the fault, triage with vendors and debug – time that not only consumes IT resources, but also significantly impacts operational continuity and performance.

Hardware failures will need to be repaired or replaced and software updates must occur at a regular cadence to preserve system integrity. It is easy to see how each piece of technology could consume IT time and energy, day after day, when new resources are needed for each new capability added. With a few upgrades, a handful of support calls and a hardware repair, you could be close to accumulating a month or more of internal support costs per year on the low end. For larger and more sophisticated systems, this could add up to a more significant fraction or even a full headcount annually.

In the cloud, the burden and cost of day-to-day system support is almost nonexistent. As part of your CommandCentral subscription, Motorola assumes all responsibility for operating and running your system on an ongoing basis. All standard maintenance and monitoring is performed 24x7 via dedicated experts who design, build and deploy the software. Updates and new features are installed every few weeks from Motorola, and users automatically get new capabilities the next time they log in.

Cloud deployments reduce the operational impact of faults and outages. This frees your staff to focus on strategic initiatives, instead of time-consuming tactical efforts, and drives greater value for responder and community safety.

PROTECTING YOUR COMMUNITY STARTS WITH PROTECTING YOUR DATA

SECURITY FIRST CLOUD DESIGN

Using a "security first" design, CommandCentral provides a unified security architecture that addresses various risks and attack vectors that could put your data in jeopardy. Through a layered security approach, we provide redundant protections of all applications, services and data running on the CommandCentral platform.

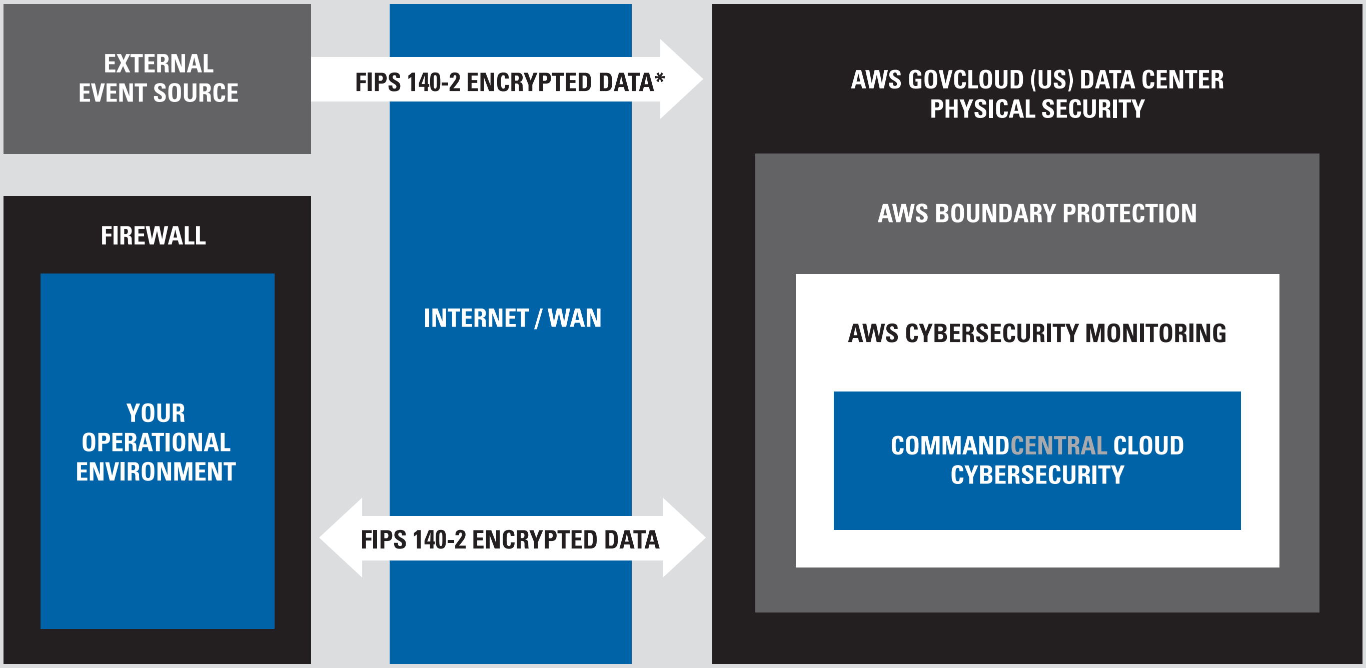
Built on the foundation of Amazon Web Services, your data is entrusted to an industry leader in secure, cloud computing and data storage. AWS GovCloud (US) provides the critical first layer of defense with physical and infrastructure security and controls in place that meet or exceed industry compliance standards (such as the CJIS Security Policy) and best practices, while being managed by US persons on US soil. Network segmentation then separates the open Internet from data in the cloud and establishes zones to contain threats to resources and data. From there, core CommandCentral cloud architecture and containerization controls the flow of information, strictly prohibiting direct data access, while proactive 24x7 security monitoring detects and blocks attacks and intrusion attempts. Finally, personnel hiring policies and authentication procedures ensure the most qualified people and processes are maintaining a strict security posture for you.

MAINTAIN COMPLETE CONTROL OF YOUR DATA

As data leaves your environment, we understand you need assurances that you have complete control of it. You maintain ownership of all data that is ingested or generated from using CommandCentral. This is a critical consideration as if you decide to leave our platform, you will receive all of your data, unlike with some vendors who may limit your ownership to only portions of your data.

Furthermore, our policy explicitly prohibits access, sharing or sub-licensing of your data for any reason other than to be used in conjunction with your application subscriptions. Bottom line, you are always in 100% control over who can access and use your data.

END-TO-END SECURITY FIRST DESIGN OF THE CLOUD


EXTERNAL EVENT SOURCE
FIPS 140-2 ENCRYPTED DATA*
FIREWALL
YOUR OPERATIONAL ENVIRONMENT
INTERNET / WAN
FIPS 140-2 ENCRYPTED DATA
AWS GOVCLOUD (US) DATA CENTER PHYSICAL SECURITY
AWS BOUNDARY PROTECTION
AWS CYBERSECURITY MONITORING
COMMANDCENTRAL CLOUD CYBERSECURITY

*Source Dependent

EMBRACE THE SECURE CLOUD ENVIRONMENT

AWS GovCloud (US) is an isolated AWS Cloud Region designed for US government agencies to move workloads into the cloud by helping them meet regulatory and compliance requirements for information assurance. The AWS GovCloud (US) framework allows US government agencies and their contractors to meet Criminal Justice Information Services (CJIS) security requirements, comply with U.S. International Traffic in Arms Regulations (ITAR), the Federal Risk and Authorization Management Program (FedRAMP) requirements and the Federal Information Security Management Act (FISMA).

Physical access to AWS data centers is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors.

In the AWS GovCloud (US) itself, network devices, including firewalls and other boundary devices, are in place to monitor and control communications at the external boundary and at key internal boundaries of the network. These boundary devices employ rule sets, access control lists (ACL), and configurations to enforce the flow of information to specific information system services.

AWS has strategically placed a limited number of access points to the cloud to allow for a more comprehensive monitoring of inbound and outbound communications and network traffic. These customer access points are called API endpoints, and they allow secure HTTP access (HTTPS), to establish a secure communication session with your storage or computing instances within the AWS GovCloud (US). The sessions are designed to protect against eavesdropping, tampering, and message forgery. To support customers with FIPS cryptographic requirements, the endpoint where TLS transactions terminate in the AWS GovCloud (US) are FIPS 140-2-compliant. In addition, AWS has implemented network devices that are dedicated to managing interfacing communications with Internet Service Providers (ISPs).

AWS uses a variety of automated security monitoring systems to provide a high level of protection within the AWS GovCloud (US) environment. They are designed to monitor server and network usage, port scanning activities and application usage. Unauthorized intrusion attempts, based on custom performance metrics thresholds, are also set to detect unusual activity.

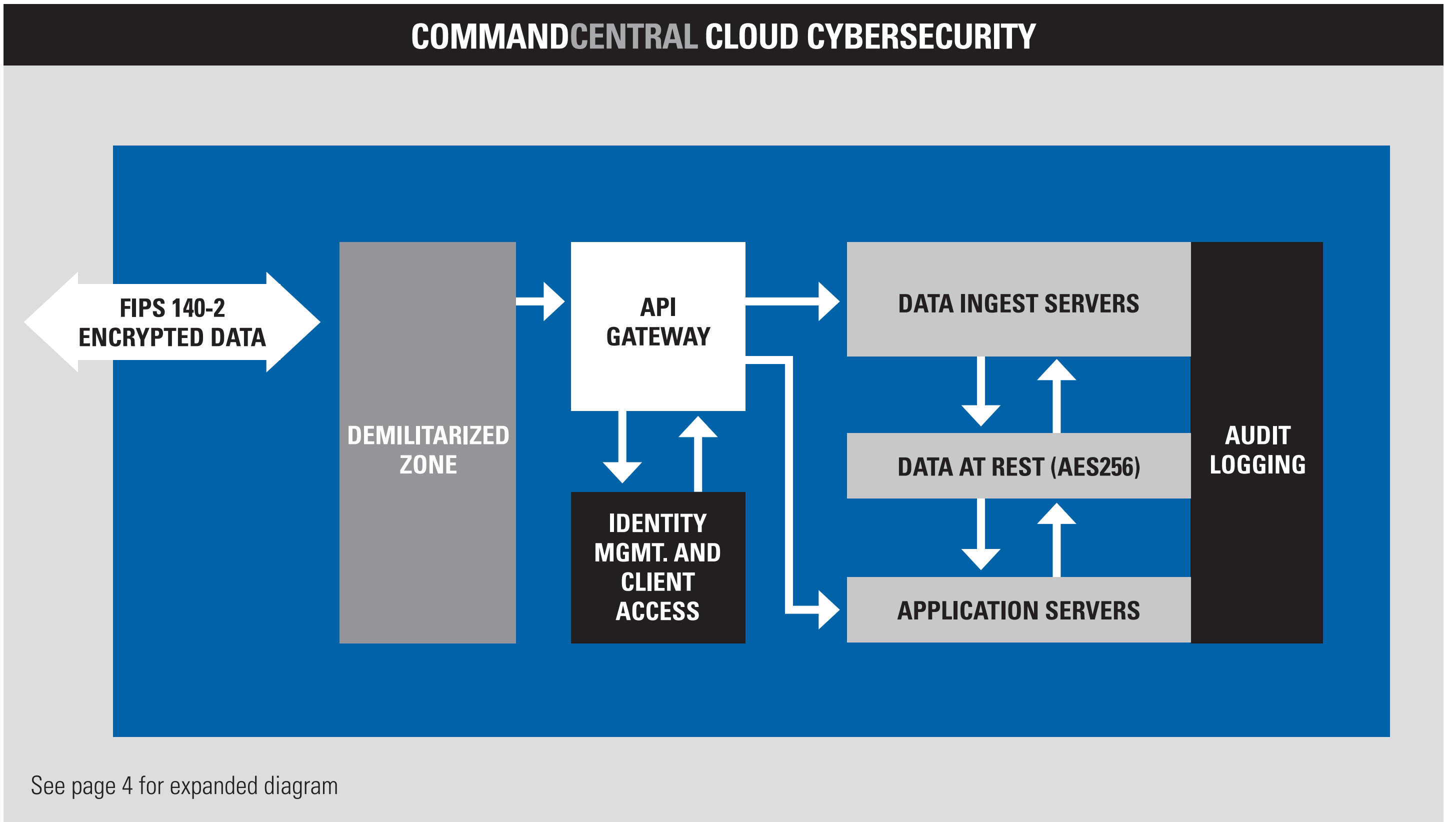
AWS security monitoring tools help identify several types of denial of service (DoS) attacks including distributed, flooding and software/logic attacks. When DoS attacks are identified, the AWS incident response process is initiated. In addition to the DoS prevention tools, redundant telecommunication providers at each region as well as additional capacity protect against the possibility of DoS attacks.

Routine, emergency and configuration changes to existing AWS GovCloud (US) infrastructure are authorized, logged, tested, approved and documented in accordance with industry best practices. Any updates to the infrastructure are done to minimize any impact on you and your services.

Inherent to leveraging a cloud environment for secure data management, is the ability to take advantage of automated security controls and compliance regulations that address scenarios you may not have yet considered.

AWS GovCloud (US) supports a variety of standards beyond CJIS, FedRAMP and FISMA in compliance with other solution providers and customers including:

- SOC 1/SSAE 16/ISAE 3402 (Formerly SAS 70)
- SOC 2
- SOC 3
- ISO 27001
- ISO 27002
- ISO 27017
- ISO 27018
- ISO 9001
- PCI DSS Level 1
- FedRAMP (SM)
- FISMA Moderate
- DIACAP
- FIPS 140-2
- ITAR
- DoD CSM Levels 1-3
- HIPAA
- MPAA
- IRAP (Australia)
- MTCS Tier 3 Certification
- EU Safe Harbor / EU Model clauses
- CSA
- FERPA
- UK G-Cloud
- Section 508 / VPAT
- IT-Grundschutz
- CJIS (Criminal Justice Information Service)
- 21 Vianet
- NZ GCIO
- FDA 21 CFR Part 11



See page 4 for expanded diagram

MINIMIZING RISK WITH DATA ENCRYPTION AND NETWORK SEGMENTATION

Encryption of data-in-transit and data-at-rest, as well as network segmentation “zoning", are applied as the initial defense layers from unauthorized network access in the CommandCentral cloud. This core security methodology stops the propagation of a threat such as malicious actors attempting to infiltrate the network.

Data-in-transit or information that flows over public untrusted networks such as the Internet, which connects your on-premise internal resources and end-user applications to the CommandCentral cloud, is secured via TLS based encryption. Communication starts with establishing identity authenticity on the cloud system with a RSA 4096-bit certificate key length. Once server trust is established, symmetric keys used in the TLS communication are negotiated. The CommandCentral encryption endpoint acts as a strict policy enforcer and requires a minimum of TLSv1 encryption protocol. The system also requires FIPS 140-2 certified cipher suites compliant with the CJIS Security Policy. Once data reaches the cloud, 256-bit AES encryption (AES256) is used to ensure privacy for data-at-rest.

To minimize exposure of assets on your network, CommandCentral is architected to never require direct communication from the cloud to your internal resources. As a result, your infrastructure is never exposed directly to the Internet. Eliminating direct access to your infrastructure also reduces your attack surface from reconnaissance, DDOS and malware attacks. Using standard ports and protocols (443/HTTPS) for all communication ensures security and simplifies processes by not having you open non-standard ports.

Network segmentation of CommandCentral and your internal resources along with end-to-end data encryption, serves to separate the outside world from your cloud services and contain traffic flows within specific, highly regulated environments. The segmentation significantly hinders threat actors from accessing the system and simultaneously diminishes their packet interception capabilities. Data encryption allows only legitimate users to access the servers and devices related to their duties.

LOCKING DOWN DATA ACCESS WITH APPLICATION SEGMENTATION

Like network segmentation, application and service segmentation-based cloud architectures isolate functional components to prevent malware, malicious input, intruders, system resources or other applications from interacting with the system as a whole, and any of its sensitive information. In the event of a compromise this also severely limits the ability for an attacker to successfully navigate within the cloud to access other critical resources.

The CommandCentral architecture separates data from the applications that utilize the data, restricting read/write access to the data through well-defined standard APIs. This architecture approach specifies the operations that can be performed – minimizing potential attack surfaces while at the same time enforcing strict data policies and audit logging. Resource segmentation also provides further protection from unauthorized user access.

The cloud architecture and application segmentation benefits extend even further, to the edge, through client connection points. CommandCentral supports browser-based access via HTML5 code which isolates the host machine and the other applications that run on it. Malware attacks are restricted from the client to limit any infiltration of the cloud. Data is also primarily processed in the cloud which minimizes client side transmission. Data that is sent, is also not cached or stored where it could be picked up and viewed later. This segmentation also protects data in bring-your-own-device (BYOD) environments, where users may introduce devices that are outside the control of IT but can still rest assured they are maintaining security and control of the data.

For even more control, federated single sign-on (SSO), built upon open industry standards, restricts who has access to what applications and data in the CommandCentral cloud. A standards-based identity provider utilizes authentication and federation protocols to validate the user via their primary credentials and issues authentication tokens that assert the user's identity. For those who want to apply bring-their-own-identity, we provide federation services to the agency identity provider, using either SAML 2.0 or OpenID Connect.

MAINTAINING COMPLETE VISIBILITY WITH SECURITY MONITORING AND ALERTING

Constant and total visibility is key to securing the CommandCentral cloud. We track all activity and interactions with applications to have a comprehensive view of the system's security posture. Technologies are employed throughout the development process and operating environment to monitor, alert to and shut down potential threats.

Our security first mindset ensures that security controls are part of the development process, not just initial deployment. Architecture and design decisions are made and scrutinized to ensure the latest security paradigms are being followed and attack surfaces minimized. Once code is written, toolsets and manual static code analysis ensures code is structured within industry best practices. Test environments are set up with compiled code and vulnerability scans are run to ensure no holes or vulnerabilities exist in applications, libraries or operating systems before being deployed for production.

Once transitioned to a running production environment, an additional set of security tools offer another layer of protection. Network scans and penetration testing are implemented against the external and internal environment, on containers, databases and network infrastructure. Operating systems and software libraries are closely monitored for updates and disclosed security vulnerabilities, and are patched to assure the most up-to-date protection. Firewalls restrict access to all but a well-defined set of ports and protocols to specific network addresses while Intrusion Prevention Systems (IPS) also detect, log and block all unauthorized access to the system.

PERCENT OF USERS IMPACTED BY ATTACK[1]

	CLOUD	ON-PREMISE
MALWARE	11%	56%
RECONNAISSANCE	6%	18%
APPLICATION	4%	16%

ENSURING THE MOST QUALIFIED PERSONNEL ARE KEEPING YOU OPERATIONAL

Both Motorola and AWS have strict policies and procedures for hiring personnel to work on and maintain access to the CommandCentral platform and AWS GovCloud (US) respectively.

In compliance with the CJIS Security Policy, both Motorola and AWS provide FBI fingerprint cards and personal information of personnel, to allow state of residence background checks. All personnel have signed CJIS Security Addendums as well as have certificates for appropriate security awareness training as outlined by the CJIS Security Policy. We also both conduct criminal background checks, as permitted by law, as part of pre-employment screening practices for employees commensurate with the employee's position and level of access. Accounts are reviewed every 90 days and explicit re-approval is required or access to resources is automatically revoked. Policies are also in place to identify functional responsibilities for the administration of logical access and security.

The AWS network as well as Motorola access points to the network are segregated from their respective corporate networks and require a separate set of credentials for logical access. Motorola maintains strict policy compliance to prevent the disclosure of personal and identity information, and has controls to protect against unauthorized access to confidential customer information.

Personnel employed to work on the CommandCentral platform or AWS GovCloud (US) are also prepared to act on a cybersecurity incident response plan in event of a breach. The plan prepares the team with knowledge and protocols to take direct and immediate action. First, the team is directed to identify and contain the threat to minimize exposure. Then remediation locks down the threat and eradicates it to prevent ongoing execution and exposure. Clear notification to customers on the incident follows to provide transparency.

MISPERCEPTIONS ABOUT THE CLOUD

MYTH	REALITY
I don't own my data in the cloud.	Each agency will retain full ownership of their data and have the ability to retrieve the data uploaded or created in Motorola's cloud applications.
I won't have control over who has access to my data in the cloud.	Your data will only be available based on strict adherence to the applications being used and the policy you determine. A permissions-based structure restricts access to data based on individual rights and roles, and on policies set forth by the agency that owns the data.
I'm going to lose privacy and security of my data.	Each agency will set the parameters for their data in the enterprise environment. Security will be set up based on those parameters to allow access to those that should see the data, and restrict access to those who should not. CommandCentral meets all the CJIS Security Policy requirements.
This will replace my current systems.	Motorola has created a technology framework that helps you extract more value from your existing data, preserving your current technology and workflows.
My data will be centrally located, increasing the risk of data loss.	Centralized data minimizes the attack surface area and decreases the touchpoints for threat actors. More so, AWS offers redundancy to ensure a single zone failure would not result in loss of data.
The cloud is going to cost me significantly more.	Cloud deployments reduce operational expense by minimizing your need for complex IT resources, connectivity and infrastructure. Reduction in these needs creates cost savings.

SOURCE:

1. Alert Logic Cloud Security Report, 2014

To learn more about Cloud-Based Smart Public Safety Solutions,
visit **motorolasolutions.com/ilps**.

Motorola Solutions, Inc. 1301 East Algonquin Road Schaumburg, Illinois 60196, U.S.A. 800-367-2346 **motorolasolutions.com**

MOTOROLA SOLUTIONS