Cloud Fundamentals - A Whitepaper

DECEMBER 2020

Authors

IJIS Institute's CJIS Advisory Committee

CJIS Compliance and Transition to Cloud Solutions Working Group

IJIS Institute

Acknowledgments

This document is a product of the IJIS Institute; a private nonprofit alliance working to promote and enable technology in the public sector and expand the use of information to maximize safety, efficiency, and productivity.

We would like to extend a special thanks to the CJIS Compliance and Transition to Cloud Solutions Working Group.

IJIS Mission

To drive public sector technology innovation and empower information sharing to promote safer and healthier communities.

CJIS Advisory Committee

CJIS Compliance and Transition to Cloud Solutions Working Group

Comments and Questions

Your comments and questions are welcome! Please contact the IJIS Institute at **info@ijis.org** or 1-703-726-3697.

Table of Contents

Appendix

1 | Cloud Fundamentals Overview

A law enforcement agency's computing infrastructure is designed to support various operating conditions. However, major disasters and events, such as hurricanes, tornadoes, floods, major winter storms, or even hosting the Super Bowl, can strain computing infrastructure past its breaking point. This was even more apparent during the COVID-19 pandemic when many public safety agencies quickly adopted cloud solutions to sustain their operations, often earlier than they may have previously planned. Adopting new cloud solutions will continue past the COVID-19 pandemic, so agencies must clearly understand their capabilities and limitations. This paper describes the basics of cloud computing and the role that the cloud can play in public safety. It will also provide a brief introduction on critical security and compliance considerations.

2 | Cloud Fundamentals

Cloud computing was commercialized in 2006 with the launch of Amazon Web Services (AWS), with Google Cloud Platform (GCP) and Microsoft Azure joining later as the industry's three powerhouses. Nlets then launched its Nova-hosted computing service, which offered the public safety community an additional hosting option. This first presence defined the way many people understand the cloud today — as "someone else's computer." Today, the cloud is so much more due to its rapid and seamless scalability when compared with traditional on-premises data centers, as well as the cloud-only solution capabilities that the public cloud provides.

The cloud is IT infrastructure and software, which is housed, operated, orchestrated, maintained, upgraded, and decommissioned by a cloud provider. However, the cloud's real power comes in what agencies without traditional "on-premises" operational burdens can do. At its core, the cloud is centered around the same basic operational principles of any modern data center: virtual compute, virtual storage, and network function virtualization, with additional software capabilities available only through a cloud platform. Two fundamental features of cloud computing include a "pay-as-you-go" model and on-demand services where agencies can use as much or as little as needed to accomplish organizational objectives.

With these strong foundations in place, service providers can use these and other services to handle more of the workload and deliver purpose-built products. For example, many people bank online. Behind the scenes, a bank may host its own solutions or outsource the infrastructure of its applications to a cloud provider so that the bank does not have to spend time, energy, and resources on maintaining the environment. It might also use capabilities such as Artificial Intelligence (AI) and Machine Learning for fraud detection from its cloud provider. All of this infrastructure is invisible to the bank's customers who use its online banking tools.

Like banks, public safety agencies choose cloud solutions to drive several critical benefits. One benefit is that the cloud provides dynamically scalable resources to support an agency. When there is a need for additional computing capacity, an agency can simply consume more resources rather than having to purchase and deploy additional hardware. This is especially important when the need for additional capacity is driven by a surge, such as a critical incident. The agency can immediately increase its resources, such as computing power, storage, and bandwidth, and then later reduce those resources to normal operating levels after the incident. Without the cloud, an agency in this position would re-direct people and budget to add hardware to its own data center to meet the surge demand and then be left with newly acquired hardware sitting idle but consuming resources into the future.

Another benefit from using the cloud is that an agency can increase the resilience of its computing infrastructure. Cloud service providers can create "geo-resilience" by storing multiple copies of critical data in different data centers that are hundreds of miles apart so that an event that affects one area won't interrupt the continuous delivery of computing services. Today, many agencies have recovery plans based on off-site storage of back-up files, but this only highlights one of the most powerful capabilities that the cloud delivers. When an on-premises solution goes down, it can be restored through back-up files, but a cloud solution is replicated across multiple data centers and wouldn't go down in the first place.

3 | Cloud and Public Safety

Every hour of every day, our nation's first responders and 911 personnel rely on a patchwork of telecommunications and public safety applications to protect their residents and save lives when time matters the most. Whether it's a 911 public safety answering point (PSAP), a computer aided dispatch (CAD) system, a records management system (RMS), or a mobile communications network, most of these systems must be available and operational when time matters most. Downtime is not an option. (See Appendix 1 for common cloud use scenarios.). These critical technology systems are usually implemented as stand-alone solutions, and integration with other solutions is not a primary consideration. This means that a new public safety solution often requires dedicated hardware, software, and network connectivity that enables the solution to be deployed and working independently from other systems. This siloed approach often leads to redundancy in certain types of data across independent systems and increases the technical staff workload to keep the growing inventory of applications and hardware highly available for first responders with minimal risk of downtime.

Embracing cloud computing makes public safety grade computing an affordable reality. With cloud computing, public safety agencies can build highly resilient systems in the cloud by using the cloud providers' data centers and regions to achieve extremely high recovery time and recovery point objectives. Today's reality is that service availability of 99.999% and more (Public Safety Grade[1]) is available in the cloud without the agency having to procure, install, and maintain a single piece of hardware. The cloud levels the playing field by allowing any agency of any size to either build their own solutions in the cloud or subscribe to existing solutions hosted in the cloud to meet their critical justice and public safety application needs.

Access to accurate and timely information is also crucial for justice and public safety agencies to accomplish their missions. Information, such as criminal histories, stolen vehicles, arrest warrants, judicial records, 911 calling locations, sex offenders, and countless other sources, is the lifeblood of justice and public safety professionals. Without access to this critical information, protecting citizens and saving lives can be a more challenging job. Ensuring that this information is available when needed is an enormous task that is the responsibility of every IT professional who serves our justice and public safety agencies. Constrained budgets and limited personnel resources make this job even harder. The budgets simply do not exist in most justice and public safety agencies to build and implement systems that are flexible to withstand extraordinary events. Cloud computing can support agencies through these extraordinary events and deliver the critical access to accurate and timely information that justice and public safety agencies need.

[1] Defining Public Safety Grade Systems and Facilities Final Report, 5/22/2014, National Public Safety Telecommunications Council (NPSTC). http://www.npstc.org/download.jsp?tableId=37&column=217&id=3066&file=Public_Safety_Grade_Report_140522.pdf

4 | Security and Compliance Considerations

When justice and public safety agencies move IT infrastructure to cloud provider services, a model of shared responsibility between the cloud provider and the agency is created. This shared model can help relieve the agency's operational burden as the cloud provider operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. The agency assumes responsibility and management of the guest operating system, including updates, security patches and other associated application software, as well as network and virtual firewall configuration.

Major public cloud companies invested heavily in compliance programs to provide independent attestations (if applicable) to the various compliance requirements that justice and public safety agencies would likely be required to implement. The government community cloud environments offered by the major public cloud providers provide compliance frameworks for the FBI's CJIS Security Policy (CJIS), the Federal Risk and Authorization Management Program (FedRAMP), the Service and Organization Controls (SOC) developed by the American Institute of Certified Public Accountants, the Federal Information Processing Standards (FIPS), the Health Insurance Portability and Accountability Act (HIPAA), and many more. The number of cloud provider personnel dedicated to these compliance efforts, as well as the technical controls implemented, far exceeds the normal capabilities of any given agency to provide the same level of compliance in their own data centers, networks, and applications. Instead of having to build these controls as the demand for new services emerges, inheriting the full array of cloud controls often accelerates the agency's adoption of new capabilities, allowing them to take advantage of new services that they previously had to delay or were not within budget.

This move to the cloud has become common with companies in the private sector that migrate all or some of their infrastructure to the cloud. Public safety agencies are beginning to follow the same route by using cloud services and infrastructure. While some considerations are common between the two sectors, there are many that apply exclusively to public safety and criminal justice agencies. Some agencies were reluctant to operate in an environment outside their physical control and beyond the boundaries of their own secure location. This was driven by the enormous statutory responsibility these agencies had as the stewards of sensitive criminal justice information. As public safety and criminal justice agencies consider the security implications of using cloud services, it can be helpful to consider three critical elements required to establish trust: security, compliance, and ownership.

Security

The availability of security controls and active monitoring of those controls vary by provider but ultimately need to satisfy the ability to manage granular, role-based access controls for the administration of the environment, as well as physical access to the environment. Protection from data breaches is paramount as is the misuse of any system that could compromise CJIS data. Agencies can incorporate cloud-provided encryption controls to protect their data (See Appendix 2: Data Protection Through Data Encryption.). Cloud services require agencies to share responsibility with a cloud service provider to ensure that security controls are being appropriately applied. Public safety agencies rely on the cloud provider to meet those security controls, including finger-print based background checks for cloud provider employees who have access to the unencrypted data, systems, and networks on which the public safety agency's infrastructure runs.

Compliance

Compliance can be satisfied using policy frameworks already required by public safety agencies. The most common policy for law enforcement is the CJIS Security Policy, maintained by the FBI and managed through a multi-agency committee. CJIS is not a certification process and requires that an agency understand the controls that exist to determine compliance. Major cloud providers support CJIS compliance programs that an agency can review to understand what CJIS controls

they can inherit from the cloud provider under their shared responsibility model. Efforts are underway to map CJIS controls to other certified frameworks like FedRAMP to allow CJIS-capable providers to show by certified policy proxy that security controls have been implemented as required under the CJIS Security Policy. This is an important step towards an agency's ability to host their CJIS data and solutions in the cloud while maintaining compliance.

Ownership

The major difference between on-premises and cloud infrastructure is control. When using cloud services, public safety and criminal justice agency data will be stored and processed on infrastructure that is not entirely under the control of that agency. Agencies should ensure that the terms and conditions with the cloud provider are specific so that they maintain ownership and control over their own data. Controls to remove agency data securely and permanently from all storage locations and the ability for an agency to retrieve its data are critical attributes of data ownership. Without those two capabilities in place data ownership cannot be absolute, so public safety agencies should ensure that their cloud provider's agreement specifically states that it:

- Has no access to a customer's data by default;
- Doesn't inspect, approve, or monitor applications that a customer deploys into its cloud;
- Must log and audit all requests for access to a customer's data;
- Rejects any ownership claim to a customer's data; and
- Completely deletes a customer's data at its request and at the end of an agreement.

For public safety agencies, compromised data and insecure infrastructure have significant negative consequences for public trust and the ability for agencies to effectively perform their duties.

5 | Conclusion

Public safety agencies face many challenges, and meeting them often rests on having a powerful, resilient, and secure information technology infrastructure. With the appropriate security, compliance controls, and policies in place, the cloud can provide these important capabilities to support public safety agencies during normal operations and during major challenging events.

Security and compliance are critical factors where the same rules apply whether a law enforcement agency runs its own information technology infrastructure, uses the cloud, or both. This paper covered the fundamentals of cloud computing for law enforcement. A second follow-up paper will be published with further analysis and insights on these critical issues.

Appendix 1 - Cloud Use Scenarios

Contact Center Application Services

Contact centers are used by justice and public safety agencies of all sizes to communicate with their constituents. These answer centers provide services, such as requests for information, problem reporting, 911 answering services, 311 and other non-emergency number answering services, and a host of other services that constituents expect when they call or send a web chat, email, or text.

The technology serving these on-premises contact centers is often costly, inflexible, and designed to be used on-premises only. In extraordinary times, these on-premises centers cannot meet the increased call volumes. In the case of Work-from-Home orders, on-premises systems do not extend easily beyond the doors of the agency.

Cloud-Based Voice and Chat

Cloud-based contact technology provides a flexible omnichannel experience for voice and chat. Contact center agents can support their constituents from anywhere, including at home, in a secure, reliable, and highly scalable way. Hundreds or thousands of agents can be deployed quickly using cloud-based contact centers. Decisions about hardware purchases, software installation, call routing trees, and physical specialized network routing are all removed from the workload of IT professionals. Cloud-based contact centers can be easily scaled on demand as workload surges, such as during the 2020 coronavirus (COVID-19) pandemic. Because agents can work from any location, adding additional agent capacity is a straightforward and fast process.

Virtual Desktop Services

Today's justice and public safety professionals use a variety of computing devices to access critical information, including desktop computers, in-car mobile computers, tablets, handheld devices, and mobile phones. IT professionals at these agencies must keep all these devices operational according to their specific standards and continually apply security patches to ensure that critical data is kept secure. Added to these responsibilities is the need for comprehensive backup and recovery and a continual refreshing of end-user computing devices so that they can support all vendors and operate modern justice and public safety application software. Agencies bear these significant costs to manage today's end-user compute infrastructure.

Today's workforce is constantly evolving as flexible work arrangements become more common. Requirements for end-user compute flexibility increase when unexpected events occur, such as the coronavirus (COVID-19) pandemic , a major flood, or a snowstorm that affects people's ability to work in their normal locations.

Cloud-based virtual desktop services simplify and solve the end-user compute flexibility problem. Cloud-based services eliminate many administrative tasks associated with managing the desktop lifecycle, including provisioning, deploying, maintaining, and recycling desktops. These virtual desktops are always available when needed, and workers can access them in the cloud from anywhere with an internet connection and be productive regardless of their location. Critical data never leaves the secure encrypted storage in the cloud, which greatly improves the security of user data and reduces the overall risk surface area.

Appendix 2 - Data Protection Through Data Encryption

During the last several years, many data breaches worldwide have exposed the personal information of tens of millions of people. The growing list of major corporations and institutions where data breaches exposed personal information is a sobering reminder of the constant threat to data security worldwide. The exposed data included healthcare records, credit card numbers, passport numbers, names and addresses, location data, and many other forms of personally identifying information. In many cases, stolen data was in a plain-text, fully-readable unprotected format where the data was unencrypted, which would have made it unreadable to any unauthorized users.

Cloud computing services generally allow data to be easily encrypted in-transit and at-rest to ensure that it is protected in case of any unauthorized access. Some security policies that govern data protection in the justice and public safety environment, such as such as the FBI's Criminal Justice Information Services (CJIS) Security Policy, require data to be encrypted with symmetric encryption, which can support encryption operations on very large volumes of data. These encryption tools allow agencies to limit access to sensitive data to only those with logical access to encrypted data and encryption keys. Managing these symmetric encryption keys using a federally compliant cloud service and allows agencies to easily manage key rotation, while keeping their encryption master key private to their agency.