1901 Group LLC

NetApp®

Cloud considerations for managing evidentiary information

A high-performance disaster recovery solution for hybrid cloud architecture

Technical white paper

aws marketplace

Introduction

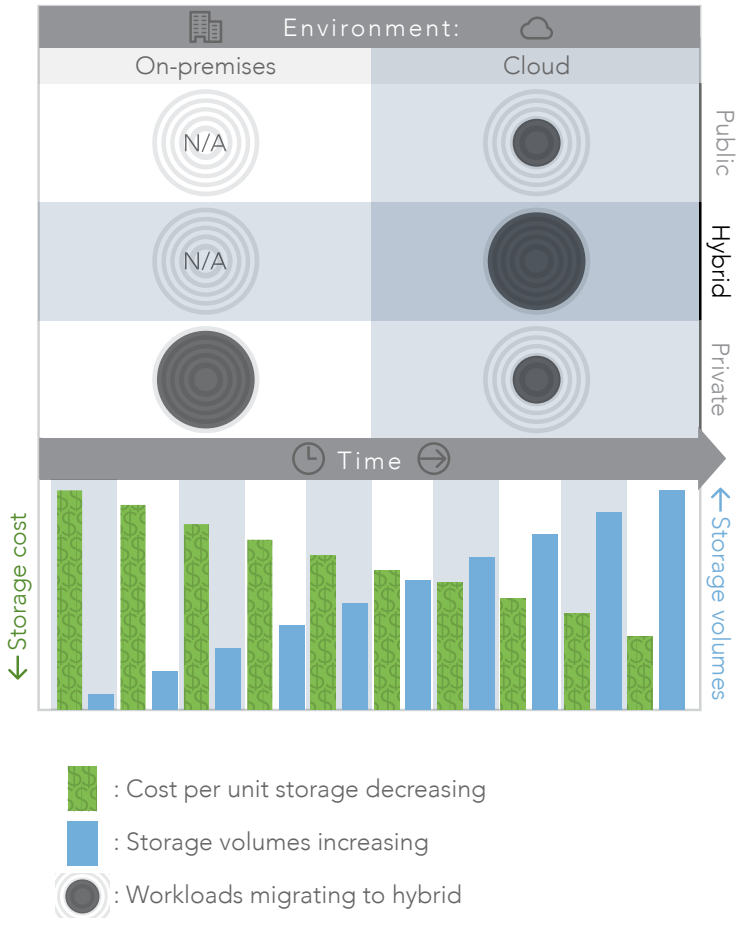
Predictions of exponential growth in the volume and complexity of electronic information abound, including forecasts for evidentiary video, voice, and data information. This growth is becoming a universal reality, and the cloud is a practical way to satisfy this demand.

However, for agencies who work with electronic evidentiary information, such as federal, state, local, and tribal law enforcement agencies and criminal justice agencies, it is important to carefully consider the nuances of what *cloud* means when considering solutions for information storage, information technology (IT) management, regulatory compliance, and disaster recovery.

This paper presents strategic and tactical considerations for agency executives, IT managers, and systems administrators and explores proven options and recommendations pertaining to the integrity, interoperability, portability, security, and cost-effective scalability of evidentiary evidence.

Macro considerations

1. The volume and complexity of electronic evidentiary information (voice, video, imagery, and data) is growing. In fact, electronic information growth is outpacing the decreasing per unit costs of information storage.
2. Evidentiary information involves a diverse number and type of information gathering devices, evidence management systems, and case management applications operating within and across on-premises and cloud environments.
3. The guiding security policy over on-premises and/or cloud evidentiary information systems is the Criminal Justice Information Services (CJIS) Security Policy[1], which incorporates Federal Information Security Management Act (FISMA) and National Institutes of Standards and Technology (NIST) standards.
4. The adoption of cloud services for production, test, development, backup, archive, and disaster recovery environments is accelerating.
5. *Hybrid cloud architecture* comprises a varying combination of on-premises (onsite), private cloud (offsite), public commercial cloud (offsite), and government community cloud (offsite) for storage, compute, network, and security capacities.



Federal law enforcement use case: an incremental path to hybrid cloud architecture

With 7,500 employees in 280 offices across the United States, a federal law enforcement agency annually stores and uses terabytes (TB) of data, including sensitive law enforcement and electronic evidentiary information. Many of the agency's activities are carried out in conjunction with task forces made up of state, local, and tribal law enforcement officers. In the event of an incident, law enforcement professionals from multiple organizations depend on rapid access to the agency's data and mission applications to protect the public.

The agency began a phased project to lower IT costs while modernizing its storage and compute infrastructure. The infrastructure consisted of more than 50 legacy mission applications, hundreds of physical and virtualized servers, and more than 1 PB of storage. The plan involved incrementally migrating legacy onsite systems to a carefully planned hybrid cloud architecture, with private cloud storage leveraging NetApp technologies and government-community cloud compute resources using Amazon Web Services (AWS) GovCloud capacities. Because the environment is a consumption-based, fixed-fee model with an as-a-service contract, the agency needs to pay only for what it uses.

The first step of the migration was to obtain an agency-issued authority to operate (ATO) declaration. This ATO leveraged the FedRAMP[2] authorized system security plans (SSP) of both 1901, the managed service provider responsible for monitoring and managing the private cloud storage, and AWS, which was responsible for providing the government-community cloud compute. By using FedRAMP authorized services, the agency compressed the time and cost associated with obtaining authorization from the typical 12-18 months to under four months.

Next, the plan involved quickly establishing modernized disaster recovery (DR) and backup capacities within a private cloud environment to ensure information control and chain-of-custody. This environment was designed to eventually become production storage, so that legacy storage systems could be incrementally decommissioned to reduce cutover risks.

Finally, high-speed interconnection was established to allow the private cloud storage to connect to government-community cloud compute resources. The interconnection and respective ATO was designed to allow the agency to consume commercial cloud compute, network, and applicable storage capacities as mission applications incrementally migrate to the desired cloud environments.

"As part of our strategy, we want to consume all infrastructure components, such as storage and servers and all supporting infrastructure activities like monitoring, management, maintenance, and technical refresh, as a service," says the chief of the agency's IT systems management division. "But we have to retain control of our data due to law enforcement requirements. With our hybrid cloud model, there's no question who owns the data, where it is physically stored, who has access to it, and when or if access has been made."

Working with 1901 Group, NetApp, and AWS, the agency implemented hybrid cloud architecture that aligns with Cloud First, FedRAMP, and recent modernization initiatives including Executive Order (EO) 13,800[3] and the Final Report on IT Modernization[4] while ensuring data control and governance complying with CJIS Security Policies, FISMA requirements, and NIST guidelines[5]. With NetApp Private Storage from 1901 Group, the agency now stores its data in a dedicated, FedRAMP authorized private cloud, and consumes infrastructure and DR and backup services on a per-TB basis.

Secure, direct, fault-tolerant connections to AWS GovCloud and Amazon Elastic Compute Cloud (EC2) provide rapid access to government or community compute resources. In the event of a domestic terror incident, which requires the agency to collect and share massive amounts of data, the agency can now quickly spin up the Amazon EC2 instances necessary to accommodate the incoming system requests and increase the amount of storage. This provides law enforcement officials timely access to the information they need to keep the public safe.

Lessons learned: hybrid cloud architecture strategy and tactics

Plan your hybrid cloud environment: Establish a strategic plan that anticipates hybrid cloud architecture in perpetuity. The IT services plan should include storage, network, compute, and security. By planning ahead, you can improve your ability to design, procure, implement, operate, and improve IT services in both the near-term and long-term.

Incorporate regulatory compliance and reporting into your strategic plan: Review all regulatory compliance text to ensure you understand what is required. For example, the CJIS Security policy[6] states:

> *"Administered through a shared management philosophy, the CJIS Security Policy contains information security requirements, guidelines, and agreements reflecting the will of law enforcement and criminal justice agencies for protecting the sources, transmission, storage, and generation of Criminal Justice Information (CJI)…The essential premise of the CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit, and from creation to destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information. The CJIS Security Policy integrates presidential directives, federal laws, FBI directives and the criminal justice community's decisions along with guidance from the National Institute of Standards and Technology."*

Leverage the continual investments made by AWS to comply with regulations: Regulatory compliance stipulations are always evolving. The General Services Administration and FedRAMP Program Office estimates that agencies have reduced or avoided system authorization costs by over $130 million[2], which is estimated to equate to approximately 30-40% of IT system authorization costs, by using FedRAMP Authorized service providers. As such, agencies should leverage the substantial investments made by FedRAMP Authorized Cloud Service Providers (CSPs)[7] to obtain and maintain Interim Authority To Test (IATT) and Authority To Operate (ATO).

Law enforcement customers and affiliates who manage CJI are using AWS offerings to dramatically improve the security and protection of CJI data; for example:

- Activity logging via AWS CloudTrail
- Encryption of data in motion and at rest via Amazon S3 server-side encryption, with the option to bring your own key
- Comprehensive key management and protection using AWS Key Management Service and AWS CloudHSM
- Integrated permission management (IAM federated identity management, multi-factor authentication)

1901 Group's In3Sight™ Platform received FedRAMP authorization for providing 24x7 monitoring and management of hybrid cloud architecture including legacy, government-owned assets, private cloud, government-community cloud, and commercial cloud capacities and services. 1901 Group's FedRAMP authorization documents comply with the Federal Risk Management Process,[8] which defines standards for cloud service providers to include security policies and controls for encryption of data at rest, encryption of data in transit, patch management, continuous monitoring, and incident response.

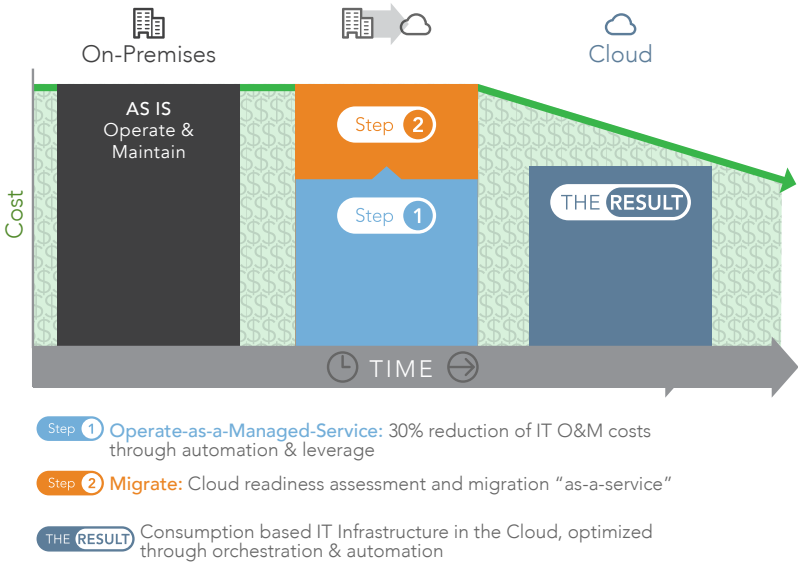
View disaster recovery, backup, and archive as preferred services for cloud: NetApp® ONTAP® Cloud for GovCloud, a software-only solution available in AWS Marketplace, provides a universal storage solution tuned for hybrid cloud architecture and offers business continuity, disaster recovery, and data management capabilities.

ONTAP Cloud is deployed and managed from OnCommand® Cloud Manager, as a virtual machine on Amazon EC2 instances, and enables virtual storage solutions directly on AWS including:

- Advanced storage efficiency to minimize cloud storage consumption through thin provisioning, data deduplication, and compression with zero-impact NetApp Snapshot® copies, providing nearly instant point-in-time data backups.
- Offsite encryption key management options, and the ability to provision both NAS and SAN storage with CIFS, NFS, and iSCSI support.

Consider a Cost Neutral Cloud Journey (CNCJ)

The federal law enforcement agency referenced earlier in this paper turned to 1901 Group to refresh its storage and compute infrastructure by migrating to hybrid cloud architecture, thereby gaining scalability and portability capabilities while also meeting a Department of Justice mandate to close or consolidate data centers. This transformation was enabled by a CNCJ strategy that reduced current operations and maintenance spending by 30%. In turn, the agency can apply those savings towards establishing hybrid cloud architecture to migrate mission critical data and applications to a modernized platform specifically designed for electronic law enforcement information.



Conclusion

Using the 1901 Group, NetApp, and AWS, the agency is blazing a trail for other law enforcement agencies interested in reducing IT costs while modernizing IT capabilities and services. The agency's use case is proof that it is possible for one of the largest federal law enforcement agencies to maintain control and governance of its electronic information (evidentiary and non-evidentiary) while dramatically lowering costs using the cloud.

About NetApp

NetApp provides a full range of cloud-based data services that accelerate digital transformation. NetApp works with its partners to realize the vision for the future of cloud data services.

About 1901

1901 Group, an AWS Partner Network (APN) Consulting Partner and NetApp Partner, provides managed services solutions designed for the rigors of public sector and high data sensitivity requirements leveraging AWS services and NetApp technologies.

About AWS Marketplace for GovCloud

AWS Marketplace enables customers to discover and subscribe to software that supports regulated workloads through AWS Marketplace for AWS GovCloud (US). AWS GovCloud (US) is an isolated AWS region designed to host sensitive data and regulated workloads in the cloud, assisting customers who have U.S. federal, state, and local government compliance requirements.

Contact Brendan Walsh for futher details: Brendan.Walsh@1901group.com.

Visit 1901 Group: https://1901group.com

[1]FBI, *CJIS Security Policy Resource Center*, Criminal Justice Information Services (CJIS) Security Policy Version 5.6 06/05/2017, CJISD-ITS-DOC-08140-5.6. https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center/view
[2]FedRAMP, *About Us*. https://www.fedramp.gov/about/
[3]Donald J. Trump, Presidential Documents, *Executive Order 13,800*. https://www.gpo.gov/fdsys/pkg/FR-2017-05-16/pdf/2017-10004.pdf
[4]CIO.gov, *Report to the President on Federal IT Modernization*. https://itmodernization.cio.gov/assets/report/Report%20to%20the%20President%20on%20IT%20Modernization%20-%20Final.pdf
[5]FedRAMP, *NIST Publications*. https://www.fedramp.gov/nist-publications/
[6]U.S. Department of Justice, Criminal Justice Information Services (CJIS) Security Policy, June 2017
[7]FedRAMP, *At a Glance*, Marketplace list of CSPs. https://marketplace.fedramp.gov/#/products?sort=productName
[8]Computer Security Resource Center, *Risk Management*. https://csrc.nist.gov/Projects/Risk-Management/Risk-Management-Framework-(RMF)-Overview

aws marketplace