Cloud:
Key Security Considerations for State Government

Trusted partner for your **Digital Journey**

Atos

Introduction

State government information technology leaders recognize that the success of their agencies' missions depends on taking full advantage of cloud innovation. At the same time, they must maintain consistent service levels, protect data and privacy, and support digital platforms for citizens.

As a result, government IT leaders and decision-makers realize that if security and compliance issues are not properly addressed, cloud migration projects could stall, and agencies might not reap the full benefits of the transition to public cloud infrastructures. Even worse, in today's dynamically-changing cyber threat environment, security breaches could result in the loss of sensitive agency and citizen data and cause the disruption of vital services.

Why move to the cloud?

For nearly a decade, state government IT departments have been working to achieve the agility, cost savings, innovation, and scalability benefits promised by cloud experts and providers. The cloud is basically a "model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources—networks, servers, storage, applications, and services—that can be rapidly provisioned and released with minimal management effort or service provider interaction," according to the National Institute of Science and Technology (NIST).

Cloud technology is the foundation for many government organizations' efforts to modernize their technology infrastructure and provide citizens with rapid and efficient delivery of services. For instance, agency leaders in the Commonwealth of Virginia are developing plans to identify locally hosted IT systems that can be migrated to public clouds over the next few years. Government officials are looking to speed up delivery of business solutions, reduce operational costs and maintenance requirements, while adding a layer of resiliency against disasters and service outages.

How to move to the cloud

Cloud migration requires a whole new set of processes, tools, workflows, and skill sets. As a result, government agencies are adopting a hybrid IT approach, combining the right mix of traditional IT, private cloud, and public cloud to meet mission goals. This approach allows agencies to integrate innovative technologies where needed and maintain legacy systems where it is suitable.

The digital transformation of traditional data centers is a crucial step toward moving to a hybrid or multi-cloud environment. By leveraging existing infrastructure and resource investments, technology managers can establish centralized governance, visibility, and control, as well as ensure workload portability and reduce the cost and complexity of a hybrid cloud environment.

Challenges to adoption

However, cloud computing has faced adoption challenges. IT managers understand the cloud can provide huge efficiency improvements and savings, but they also have concerns about security, compatibility, and funding. In recent years, cloud providers such as Amazon Web Services (AWS), Google, and Microsoft have moved to address those concerns, providing cloud infrastructures tailored to meet the security and compliance requirements of federal, state, and local government.

In the early stages of cloud adoption, many state government technology leaders tried to build cloud infrastructures using their own tooling and processes to incorporate their state's nuances and requirements. The result was an infrastructure that "was complex, hard to manage, with lots of tools, lots of people, and potentially a lot of areas for problems," said Michael Kollar, senior vice president and chief digital officer for Atos, a leader in digital services, providing consulting and systems integration services as well as big data and cybersecurity solutions. Now, IT and security teams don't have to worry about maintaining all the tools and expertise themselves and they can rely on it as a service they consume.

Why is compliance a special challenge for state government?

Maintaining security and compliance is challenging for state government for several reasons.

Cyber threats are increasing in complexity and intensity

As agencies extend their networks beyond their traditional data centers to connect with cloud infrastructures, mobile technology, and the Internet of Things devices, the attack surface that malicious attackers can exploit has expanded. State and local governments are under attack by adversaries who launch ransomware attacks, a type of malicious software that infects and restricts access to a computer until a ransom is paid. The attack on the city of Atlanta, Georgia, in March 2018 destabilized government services for an extended period. The virus used to attack the city—SamSam Ransomware—differed from other ransomware because it did not rely on phishing. Instead, the ransomware utilized a brute-force attack to guess weak passwords until a match was found. SamSam has been behind attacks on medical and government organizations since its discovery in 2016, with previous attacks on targets ranging from small towns such as Farmington, New Mexico, to the Colorado Department of Transportation and the Erie County Medical Center.

However, cloud security goes beyond malware protection. Many government leaders focus on malware, "but security is a lot broader coming from a cloud perspective," said Kollar. In the traditional data center, technology managers were concerned about data going out of the network. However, now they must also be concerned about data coming into the data center from endpoints, such as mobile devices and the public cloud. State technology managers now need tools that can perform pattern-based detection of suspicious activity to thwart security breaches inside data centers and cloud environments.

Funding for cybersecurity initiatives is insufficient

Due to a lack of internal IT resources, limited budgets and lack of formal processes to identify and thwart threats, agencies are often reactive when it comes to cybersecurity. Leading up to the Atlanta ransomware attack, the Atlanta government was criticized for not spending on upgrading its IT infrastructure, leaving multiple vulnerabilities open to attack.

Since 2010, state chief information officers have been challenged by insufficient funding and cyber talent availability, according to the 2018 National Association of State Chief Information Officers and Deloitte & Touche LLP Cybersecurity Study. Lack of cybersecurity funding, inadequate cybersecurity staffing, and increasing sophistication of threats are the top barriers state CISOs face in addressing cybersecurity challenges. The Study reflects insights from all 50 states on the CISO's role and budget, governance, and reporting.

Many states typically spend only 1 to 2 percent of their IT budget on cybersecurity, compared with federal agencies, which spend much more, according to the report. The U.S. Department of Transportation, for example, spent 5 percent of its IT budget on cybersecurity in 2018; the U.S. Treasury Department nearly 12 percent.

Staffing also continues to be a major problem for states, the report found. Among the obstacles: low salaries, competition from the private sector where the pay often is much higher, and a lack of qualified candidates. Moreover, most state IT security offices only have a small cyber team, according to the survey. More than half employed 15 or fewer full-time professionals.

The report recommends: advocating for dedicated cyber funding on the state level, seeking money from federal agencies and teaming with the private sector and local colleges and universities to provide a pipeline of new talent.

Source: 2018 National Association of State Chief Information Officers and Deloitte & Touche LLP Cybersecurity Study

Lack of cybersecurity visibility and control

The proliferation of security point products within the IT environment has resulted in an avalanche of security events and alerts overwhelming security operations teams. Moreover, the move toward hybrid and multi-cloud environments has added another level of complexity. Technology teams must have visibility into what is happening across on-premises IT, private and public cloud domains and how applications and systems are interconnected.

Security Information and Event Management (SIEM) systems, which aggregate relevant data from multiple sources, identify deviations from the norm and take appropriate action, can help security operations teams become more proactive in detecting and preventing security breaches across the various infrastructures, Kollar noted.

For example, a SIEM might detect a pattern of intelligent hacking occurring in a municipality. That event can be sent to a master SIEM system to determine if the pattern of attack is occurring in other agencies or municipalities across a state, allowing security operations teams to address potential incidents in an automated, proactive way.

For greater visibility and control across IT and cloud infrastructures, IT and security operations teams should deploy:

- SIEM systems to detect and manage security events and provide an automated response to security incidents.
- IT service management/cloud service management tools to address problem incidents and changes in an automated way to control data coming in and out of IT and cloud services.
- Cloud management platforms to deal with chargeback, utilization, and security from an overall governance perspective.

State and local government managers are using these technologies to gain visibility and control across on-premises and cloud infrastructures "to ensure that those services are running the way they should" and there is no data loss or system compromise, Kollar said.

Compliance with growing array of regulations

Federal, state, and local agencies have introduced a host of regulations and compliance guidelines to provide better protection for citizen data and greater transparency when security breaches occur. One example is the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the federal law that established data privacy and security requirements for certain entities and individuals aimed at safeguarding individuals' health information. State law enforcement agencies that want to share data with the federal government and other state agencies must comply with the FBI's Criminal Justice Information Services (CJIS) guidelines. For organizations with limited security staff, staying in compliance with regulations can be an arduous task.

Fortunately, the major cloud providers handle data that is subject to certain government regulation such as the Federal Risk and Authorization Management Program (FedRAMP), which assesses security for and authorizes cloud programs used by federal agencies. If a state or local agency's cloud vendor has received a FedRAMP authorization, they can be assured that it meets stringent security compliance regulations.

For example, Microsoft Azure Government, a FedRAMP authorized cloud provider, handles data that must comply with NIST 800.171, protecting Controlled Unclassified Information (CUI); International Traffic in Arms Regulations (ITAR), which controls the export and import of defense-related articles; Internal Revenue Service 1075, which provides polices for the protection of federal tax information; Department of Defense (DOD) Impact Level 4, for production workloads with export-controlled data, privacy information, and protected health information as well as other controlled unclassified information; and CJIS. AWS and Google Cloud are also compliant with numerous regulations.

Benefits of cloud deployment

Improve government and constituent services while containing costs. The integration of services for customer support extends to an agency's internal customers as well.

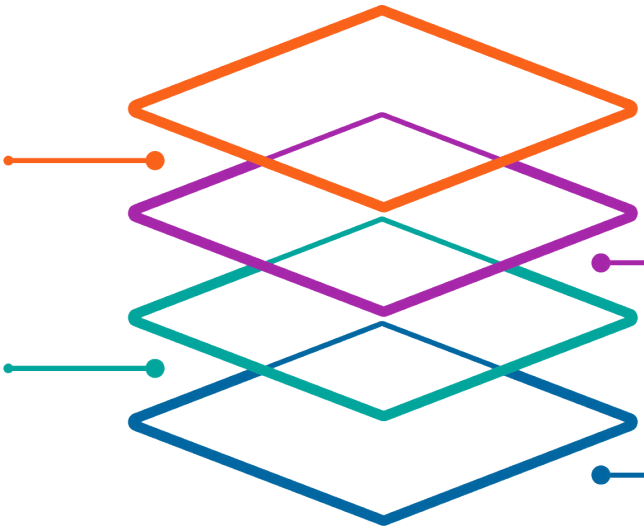
Accelerate innovation/time-to-value. Hybrid cloud gives developers access to traditional and cloud-native application resources, including self-service capabilities.

According to an IDC report, over 70 percent of federal government survey respondents indicate that cloud is significant or partially exceeding their expectations of driving innovations.

Increase agility and response to dynamic, distributed, and highly changeable workloads and mission needs.

Source: IDC InfoBrief, "Government IT Modernization and the Adoption of Hybrid Cloud," June 2018

4 layers of a hybrid cloud ecosystem



Layer One
Layer one is made of legacy infrastructure and applications in an organization's private cloud.

Layer Two
Layer two is made of modern applications and services in the public cloud.

Layer Three
The middle layer is an orchestration engine that ensures both sides stay in sync as it powers your hybrid environment of public and private clouds.

Layer Four
A fourth layer of cybersecurity is embedded in every layer. A constant focus on security is critical to ensuring that services integrated between the legacy world and the new digital ecosystem are protected, safe and reliable.

Key security considerations

As state technology managers embark or move further along on their hybrid cloud journey there are certain key security procedures and technologies they should consider, according to cloud security experts, including:

1. Ensure you have complete visibility. Complete visibility across private cloud, public cloud, and traditional infrastructure is a must. A lack of visibility creates greater security risks.

2. Does every asset have an owner? Every piece of a hybrid cloud architecture needs an owner. Within IT security, an owner must be identified for every asset, and the owner must be responsible for assigning privileges and segregation of duties over the asset.

3. Hybrid cloud needs hybrid security. As strategies around security continue to evolve, many agencies are adopting a hybrid approach to build more layers and depth into their security infrastructure. Some security technologies might reside on-premises, such as desktop antivirus, data loss prevention, and firewalls, as well as intrusion detection systems/intrusion prevention systems. Others might make more sense to run outside of the agency network, such as services that help mitigate distributed denial of service (DDOS) attacks.

4. Security and compliance. Not the same, but connected. There can be security without compliance, but never compliance without security, according to some security experts. It is important to understand the existing security controls used by the cloud provider and how they fit with an agency's security controls. Conducting a compliance controls evaluation before selecting a cloud provider or security vendor is an important security requirement.

5. Security tools must work well wth other tools. Assess how well a cloud provider's security tools integrate and work with your agency's tools. Many tools integrate well with one another. Cloud providers and security vendors should provide simple integrations with an agency's existing on-premises platform and tools.

6. Research and evaluate potential cloud providers. Know and understand the cloud platforms you're interested in migrating workloads to. Cloud providers might be better trained and better equipped to deal with potential threats.

7. Scale communication for the hybrid model. Hybrid cloud brings scalability concerns with regards to communication. Clear communication is a significant part of a strong security posture, especially when it comes to new vulnerabilities or incidents.

8. Do ongoing risk assessment. Building out a hybrid cloud environment with security from the outset is a great first step. But it remains a first step. Securing a dynamic hybrid cloud environment involves ongoing risk assessment to identify vulnerabilities.

9. Understand the role of all parties. When state government departments and agencies choose to adopt cloud computing, security is a major consideration in the planning, migrating, and operations and maintenance of critical IT systems. Agencies must consider the goals, planned cloud ecosystem, mission and business functions, processes, sensitivity of data, and processing capabilities. Agencies must fully understand the roles and responsibilities of themselves, FedRAMP, and cloud service providers (CSPs).

10. Security is ultimately the agency's responsibility. The overall responsibility for securing a system in a cloud computing environment belongs to the agency. However, the day-to-day activities and performance of security controls are distributed between the agency mission owner, users, agency IT security, and CSP. Depending upon the service model—Infrastructure-as-a-Services, Platform-as-a-Service or Software-as-a-Service—the specific division of responsibilities varies. It is necessary to understand roles and responsibilities, and information exchange between the government and CSPs to ensure total system security. CSP responsibilities must be clearly defined in the cloud acquisition and contract documents.

11. How do you handle multiple CSPs? Most government agencies have many IT systems supporting mission and business functions. Different CSPs offer different service models, and therefore operate under differing security expectations, requirements, processes, and information exchanges. When considering adopting cloud computing, agencies must factor in the simultaneous management of multiple CSPs, and the development of security processes that integrate the management and information flow between multiple CSPs and the government security center. Therefore, technology managers and planners must understand that the expected cloud ecosystem becomes necessary for the purposes of planning and executing secure cloud computing.

12. Look at the entire security framework. A comprehensive and clear cloud security strategy will provide a foundation for securing the agency's cloud adoption. The cloud security strategy should address both technical and non-technical aspects of security and provide an overall framework for securing the entire cloud ecosystem. It must also ensure security across the responsibility boundaries of the multiple agency organizations, and multiple CSPs.

13. Security policies and procedures. Has your state adopted them? Federal agencies have established security and privacy policies and procedures to protect their sensitive data within traditional, non-cloud, IT as well as cloud environments.

The Federal Information Security Management Act (FISMA) and the Federal Risk Authorization and Management Program (FedRAMP), for example, are both based on security controls and guidelines established by the National Institute of Standards and Technology (NIST). FISMA is a set of standardized guidelines government agencies could use to protect sensitive data. It addresses the storage and processing of government data. FedRAMP standardizes the approach to security assessments, authorization, and cloud service provider monitoring. It provides guidelines to agencies adopting cloud service providers on how to protect government data. In today's cloud environments, agencies must ensure that security extends across on—premises IT, hybrid, and multi-cloud infrastructures.

Sources: Hybrid cloud security: 8 Considerations, Kevin Casey, Enterprisers Project, July 27, 2017.

As CISOs implement the recommended security policies, procedures and controls, Kollar advises following this checklist:

Multifactor authentication, which ensures there is more than one method of authentication to verify the user's identity for a login or other transactions.

Encryption must be a tiered approach that addresses data-at-rest, data-in-transit, and data-in-use.

Adequate protection must be implemented for denial of service and distributed denial of service attacks.

Identity and access management to define identities and privileged users. IT and security teams must know who is using the systems. Consequently, they need to ensure that the user has the appropriate privileges for the type of data and access they need. This capability needs to be extended to the cloud.

Rights management / role-based access and control. This will help in assigning, monitoring and managing changing personnel roles within an organization.

Automation for patch management and other tasks to eliminate manual processes. Patching vulnerable software can't be done at scale manually, especially if an organization has over 100,000 desktops. It must be performed in an automated way.

Business continuity is needed to deal with denial of service or outages in the cloud. How do you deal with unforeseen activity?

Data management is critical in the development and execution of architecture, policies and procedures designed to manage the information lifecycle.

Move toward a DevSecOps mindset to evolve how IT and security operations work and support cloud environments. The goal of DevSecOps is to safely distribute security decisions at speed and scale to those who hold the highest level of context without sacrificing the safety required.

Continuous integration and continuous deployment (CICD) tools for the cloud will transform how developers traditionally build, test and deploy applications. Continuous integration is the practice of testing each change to your codebase automatically and as early as possible. Continuous deployment follows the testing that happens during continuous integration and pushes changes to a staging or production system.

Additionally, open source software is used to build cloud applications. Consequently, technology managers need to validate that the open source code doesn't have malicious code in it. As a result, they need to apply continuous inspection capabilities to monitor their DevOps code, making sure it does not contain any malware in it. CICD tools for the cloud need this critical capability.

Rights management and role-based management to integrate identity- and access-management platforms with the cloud.

Use cases for moving to the cloud

Improve government and citizen services while containing costs.

Modernize existing applications (replace, re-platform, refactor, and in the future containerize) and develop new cloud-native applications to rapidly meet changing mission needs and cyclical demands.

Maintain continuity of operations with cost-effective backup and disaster recovery.

Blending and analyzing substantial amounts of data from emerging technologies such as big data, analytics, and IoT.

The bottom line

Cloud services can be highly beneficial when properly implemented, but the cloud is not a panacea for every IT need. Cloud services can pose their own special risks, as can any powerful and innovative service delivery model.

Many large organizations think the job of security is to build motes around data centers and infrastructures to keep things out versus letting them in. However, that's a legacy perspective, Kollar noted. The threat landscape has changed. The only way state government decision-makers can take full advantage of the cloud is to adapt their security paradigms to outside-in versus inside-out.

Technology managers must consider three points to accelerate that transformation:

1. People: Legacy mindset needs to be done away with.
2. Process: Do it differently, not the way you did it before.
3. Technology: The cloud is not less secure. But it is more complex. Automation is critical!

For example, some of the most far-reaching security breaches have occurred because an IT worker failed to patch a vulnerable web server in an on—premises data center. Patching and configuration management need to be done both on—and off—premises. Regardless of where they happen, solid process management and solid technology enablement—meaning automation—will ensure that the appropriate policies are executed. An automated approach is key to managing change at scale and could very well prevent the next highly visible breach—if process and technology are leveraged appropriately.

Agencies should always examine all the issues relevant to their data and circumstances before determining whether and how to implement any cloud solution.

About Atos

Atos is a global leader in digital transformation with 120,000 employees in 73 countries and annual revenue of € 13 billion. European number one in Cloud, Cybersecurity and High-Performance Computing, the Group provides end-to-end Orchestrated Hybrid Cloud, Big Data, Business Applications and Digital Workplace solutions through its Digital Transformation Factory, as well as transactional services through Worldline, the European leader in the payment industry. With its cutting-edge technologies and industry knowledge, Atos supports the digital transformation of its clients across all business sectors. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and operates under the brands Atos, Atos Syntel, Unify and Worldline. Atos is listed on the CAC40 Paris stock index.

Find out more about us

atos.net

Let's start a discussion together

To learn more about Atos' security solutions:
https://atos.net/en/solutions/cyber-security