rubrik

EBOOK

How to Overcome the Risks of Government Data in the Cloud

TABLE OF CONTENTS

Each government agency has a defined mission to uphold—from upholding national security to establishing trade. But all agencies share a common goal to create policies and programs that support the well-being of their constituents.

Many agencies are using cloud computing or are planning to move to the cloud to support this goal. The cloud offers unique benefits for government agencies, such as flexibility and providing access to their data. But government agencies are also driving toward a cloud-smart initiative that helps them reap the benefits of the cloud while executing their adoption securely.

Because government entities serve a powerful function in their country, state, or locality—namely, in the services their constituents need in their daily lives—the data they hold must be protected by any means. That data can be exploited to devastating effect in the event of a cyberattack. Government agencies must fully understand their security requirements when moving to the cloud as part of the shared responsibility model. Not fully understanding and implementing security controls as part of a cloud migration can add tremendous risk to an agency, its citizens, and its partners.

BEHIND THE PUSH TO THE CLOUD

The Office of Management and Budget (OMB) is updating its legacy Cloud First strategy to increase government adoption of the cloud. This strategy is called Cloud Smart.

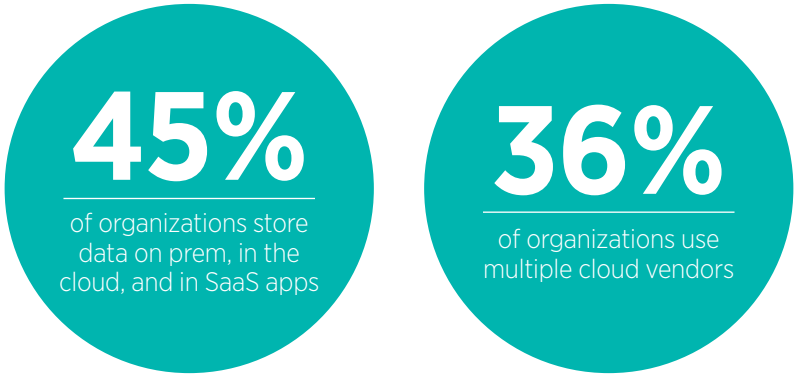
While the Cloud First strategy urged agencies to adopt cloud-based solutions as their first course of action, Cloud Smart focuses on thoughtful execution based on three main factors: security, procurement, and workforce[1]. For larger agencies, relying on a cloud-first approach is costly and difficult to secure using the shared security model.

And because no single cloud can support all government agencies, agencies need to decide which solution serves their—and their constituents'—needs best. Let's explore what's pulling government agencies to the cloud and some of the challenges that come with securing data in the cloud.

Environments are becoming increasingly dynamic, distributed, and complex, with data explosion driving the move to the cloud. Rubrik observed the amount of data stored in a typical environment is around 227 BETB, with the cloud housing 63 BETB. And in 2022, the average growth of secured data in the cloud was 61 percent.[2]

1 "From Cloud First to Cloud Smart," Federal Cloud Computing Strategy, Accessed June 15, 2023. https://cloud.cio.gov/strategy/.
2 "The State of Data Security: The Hard Truths of Data Security." Rubrik. Accessed June 15, 2023. https://www.rubrik.com/zero-labs.
3 "Data Breach Investigations Report," 2022, Verizon, Accessed June 15, 2023. https://www.verizon.com/business/resources/Tdd2/reports/dbir/2022-data-breach-investigations-report-dbir.pdf.

With more data than ever before, agencies also have to contend with that data being dispersed across multiple environments. For example, some teams could be relying on on-prem applications while others are lifting and shifting applications to the cloud or building cloud-native applications. Rubrik observed that 45 percent of global organizations secure data in a mix of on-premises, cloud, and SaaS, and 36 percent use multiple cloud vendors concurrently.[2]



Not surprisingly, as applications and data run across multiple public clouds with their own rigid operational boundaries, government agencies can quickly deal with complexity. Teams need to configure the same native backup, compliance, monitoring, and recovery operations across every workload, every account, every cloud, and every SaaS and enterprise application.

To add to the complexity, teams need to implement the same workflow multiple times across different environments. And this level of labor-intensive work is a recipe for human error. Bad actors can take advantage of security gaps, like minor cloud misconfigurations, or use simple phishing attacks to get access to critical data and infrastructure.

When cybercriminals and nation-state adversaries target government agencies, their motivations are not just financial (80 percent), but also espionage (18 percent), ideology (1 percent), and even a grudge against the government entity (1 percent)[3]. Espionage, in particular, is a growing problem among government entities, and without adequate data security measures in place, entities can expect to deal with more than just high costs.

A cyberattack could put operations at a standstill, affecting constituents as well as the targeted government entity. The cloud offers appealing security measures and gives entities better visibility into their data—but cloud computing isn't a perfect solution, and cybercriminals are well versed on the vulnerabilities.

WITH GREAT POWER COMES GREAT RESPONSIBILITY

While more government entities are moving to the cloud, over half of adopters are struggling to maintain security. 23 percent of federal agencies say that they can "maintain the greatest security control over their strategic data" in a FedRAMP-authorized cloud platform. But 57 percent of early cloud adopters and 60 percent of late adopters cite "security assurance" as the greatest challenge in the cloud. [4]

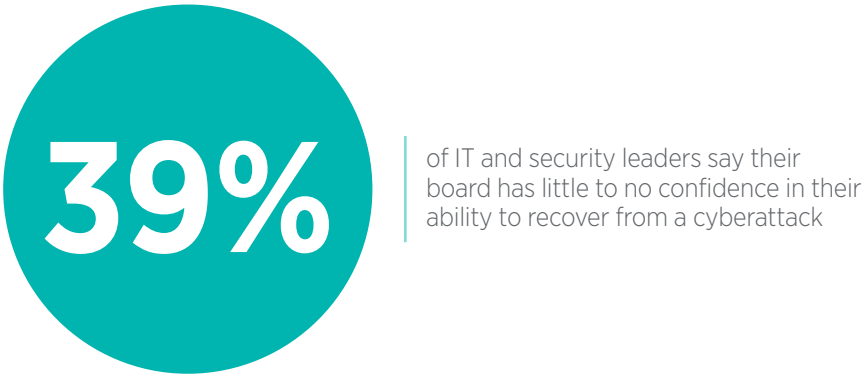
Government data stored in the cloud often can contain sensitive information about citizens, so government entities have an obligation to make sure that data is secure. But espionage and exfiltration of data in the cloud can render that important, sensitive data inaccessible, possibly exploiting millions of constituents by posting their personal data for sale on the dark web.

Cybercriminals are aware of how valuable government data is and are trying all possible means to access it—including through the cloud. Government entities are as susceptible to common attack vectors, like phishing, as the private sector. A simple misconfiguration—like human error—is often all that's necessary for an attacker to gain entry.

Once an attacker gains entry, they can escalate privileges to access cloud infrastructure. From there, they can move laterally and bypass all security controls. Finally, they can access critical data, potentially steal it, and then encrypt or wipe it before demanding a ransom payment.

But here's the problem: Encryption is almost never the final phase of a cloud-based attack. Cybercriminals can and often do have open access to an agency's systems for days before they make their presence known, and it often takes several days—or weeks—for the affected agency to get back on its feet depending on the severity of the attack.

While government agencies have invested heavily in security tools, many still can't recover their data with speed, confidence, and trust. 39 percent of IT and security leaders surveyed believe their board of directors or C-level leaders have little to no confidence in their organization's ability to recover critical data and business applications in the event of a cyberattack.[2]



There are several reasons why government agencies may struggle to recover:

- Their backups may not offer insights into the scope and impact of cyberattacks.
- Their backups may not be immutable, which means if they're compromised, an agency can't revert to a clean copy of their data.
- An agency may not test their backups, leaving them unprepared for a real cyber event.
- They struggle to identify which systems and or applications were compromised in an attack.
- Agencies may have to hunt for the correct backups to use. Some may live with their cloud team, some with application developers, and some simply may not exist at all.
- Their teams need to master different policy models and workflows unique to each cloud provider, toggling between multiple systems to restore data.

Government entities need to make sure the data stored in the cloud is resilient against cyber incidents, so they can continue serving their citizens.

HOW TO PROTECT YOUR DATA IN THE CLOUD

Securing data in the cloud comes down to three things: 1. Withstanding attacks by making sure the data is readily available, 2. Understanding data risks and exposures, and 3. Making sure data can be recovered without the risk of reinfection when a cyber incident occurs. A cloud data security approach based on zero trust architecture and cyber recovery can offer government entities the ideal foundation for cyber resilience.

First, government agencies need their data to be readily available. Air-gapped, immutable, access-controlled backups enable agencies to withstand cyberattacks, malicious insiders, and operational disruptions. CISA recommends that government agencies maintain offline, encrypted backups of critical data, and regularly test the availability and integrity of backups in a disaster recovery scenario.[5]

Second, government agencies need to understand the risks to their data. A data risk assessment and an anomaly detection engine can help agencies continuously monitor data risks like sensitive data exposure and detect cyber threats, such as ransomware. CISA recommends that agencies use automatic updates for antivirus and anti-malware software and signatures to ensure tools are properly configured to detect "precursor" indicators of malware and ransomware.[5]

Third, in the event of an attack, government agencies need to be able to return to business as quickly as possible. Automation and quarantining can help agencies contain threats and rapidly recover their applications, files, and objects while avoiding malware reinfection. That way, agencies can resume normal operations and continue serving their constituents with minimal interruption and data loss.

But protecting government data in the cloud doesn't have to be complicated, fragmented, or require multiple tools. As data continues to grow, government agencies need centrally managed, consistent, cloud-agnostic protection of all their data.

And government agencies can be in an even better position to secure all their data—cloud, on-prem, and SaaS—if they have a single solution that can do it all.

HOW RUBRIK CAN HELP

Rubrik Security Cloud for Government helps government agencies develop a strong cyber posture and ensure fast cyber recovery—all on a single platform. The platform fits the requirements for data protection in the cloud that this paper has outlined.

Rubrik is immutable by design, which prevents unauthorized change, encryption, or deletion of data by storing data in a proprietary format and verifying it with data integrity checks.

Rubrik also helps government agencies accelerate their response time by enabling agencies to continuously monitor for emergent cyber threats, including ransomware and sensitive data exposure.

And if something happens to the production environment, Rubrik can help government agencies surgically and rapidly restore impacted apps, files, or objects by containing threats and orchestrating recoveries while avoiding malware reinfection.

Rubrik can also protect on-prem, cloud, and SaaS workloads with a single SLA policy. It centralizes role-based access with single sign-on across the environment, reduces data risks with continuous monitoring for ransomware and data exposure, and creates operational consistency for rapid recovery across environments.

4 "Federal Perceptions of Cloud Security," 2022, FedScoop, Accessed June 16, 2023. https://cdn.fedscoop.com/federal-perceptions-of-cloud-security-report.pdf.
5 #StopRansomware Guide." 2023, MS-ISAC, Accessed July 20, 2023. https://www.cisa.gov/sites/default/files/2023-06/StopRansomware_Guide_508c.pdf.
6 Gayle Berkeley, "Rubrik Security Cloud – Government Is on the FedRAMP® Marketplace." June 13, 2023. Rubrik. Accessed July 20, 2023. https://www.rubrik.com/blog/company/23/6/rubrik-on-fedramp-marketplace.

Rubrik Security Cloud for Government is also in the process of achieving Moderate authorization by the Federal Risk and Authorization Management Program (FedRAMP®), a government-wide program that provides security assessment, authorization, and continuous monitoring of cloud products and services. Rubrik's FedRAMP® authorization validates its "... commitment to delivering cyber resilience for the largest, most regulated organizations in the world."[6]

Specifically, the FedRAMP® Moderate authorization helps government agencies protect much of their data, including Controlled Unclassified Information (CUI), which includes personally identifiable information (PII) and routine covered defense information (CDI).[6]

To learn more about Rubrik Security Cloud for Government, visit https://www.rubrik.com/industries/federal-government and https://www.rubrik.com/industries/state-local-government

BIBLIOGRAPHY

- "From Cloud First to Cloud Smart," Federal Cloud Computing Strategy, Accessed June 15, 2023. https://cloud.cio.gov/strategy/.
- "The State of Data Security: The Hard Truths of Data Security." Rubrik. Accessed June 15, 2023. https://www.rubrik.com/zero-labs.
- "Data Breach Investigations Report," 2022, Verizon, Accessed June 15, 2023. https://www.verizon.com/business/resources/Tdd2/reports/dbir/2022-data-breach-investigations-report-dbir.pdf.
- "Federal Perceptions of Cloud Security," 2022, FedScoop, Accessed June 16, 2023. https://cdn.fedscoop.com/federal-perceptions-of-cloud-security-report.pdf.
- #StopRansomware Guide." 2023, MS-ISAC, Accessed July 20, 2023. https://www.cisa.gov/sites/default/files/2023-06/StopRansomware_Guide_508c.pdf.
- Gayle Berkeley, "Rubrik Security Cloud – Government Is on the FedRAMP® Marketplace." June 13, 2023. Rubrik. Accessed July 20, 2023. https://www.rubrik.com/blog/company/23/6/rubrik-on-fedramp-marketplace.

rubrik

Global HQ
3495 Deer Creek Road
Palo Alto, CA 94304
United States

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com

EBOOK-Data-in-the-Cloud / 20231004