PROTECTING YOUR DATA IN THE CLOUD

Vormetric
Data Security™

EXECUTIVE SUMMARY

Cybersecurity is the hottest buzzword in government these days. But just because people are talking about it, doesn't mean they actually know how to achieve it. In reality, many government organizations are struggling to secure their data from internal and external threats.

Taken alone, cybersecurity is challenging. The speed of evolution and the consistency of attacks make it difficult for agencies to keep their network defenses up-to-date. When you add the difficulty of cloud transitions and the complexity of regulatory guidelines to the list of barriers, the task of security might seem overwhelming.

Nevertheless, enhanced cybersecurity can be achieved. To learn how, we spoke with Sol Cates, Chief Security Officer at Vormetric, and Robert Bigman, an Information Security Consultant and former Chief Information Security Officer in federal government.

They explained that safeguarding information through integrated encryption and key management allows agencies to overcome many common barriers to effective protection. However, applying these tactics requires an understanding of the scope and sensitivity of your agency information.

In this industry perspective, we explore:

- ↗ The challenges associated with cloud transitions and regulatory requirements.
- ↗ Three steps to achieving data transparency and security.
- ↗ The benefits of encryption and key management for cybersecurity.

Safeguarding government information is a difficult but necessary task for every agency and department. Successful organizations know which data requires protection and which security tactics to deploy. This brief explains how to achieve these dual objectives.

THE CHALLENGES OF REGULATORY REQUIREMENTS

Government leaders recognize the security challenges facing public sector organizations. Specifically, the National Institute of Standards and Technology (NIST), part of the Department of Commerce, has issued regulations and guidance to help agencies create effective cybersecurity strategies. Bigman explained how these standards can both benefit and burden agencies.

The Cybersecurity Framework, which offers standards, guidelines, and practices to protect critical infrastructure, is particularly useful. "It explains how organizations can get from where they're at now to where they want to be," Bigman said. "That's bigger than just technology; it's programmatic, budget, policies, processes, and integration of cybersecurity with other parts of the agency. It's frankly whatever you want it to be; that's why they made it so broad."

"Because it's so broad, there's no conflict to your architecture, whether you're running the data center and using the services in-house or outsourcing it to a cloud provider. In that sense, it has a lot of value," Bigman added.

However, he also warned that the Framework's flexibility might obfuscate security attempts. "In their attempt to be open-ended, I think [NIST] over-accomplished the task," Bigman said. "Most of the government agencies are used to very narrowly defined specifics, so what's actually happening in many cases is the organizations are fighting amongst themselves, trying to figure exactly what the Framework means."

Furthermore, Bigman noted that confusion over regulatory requirements and guidance also hinders security. In addition to the Cybersecurity Framework, NIST issued Special Publication (SP) 800-53 to detail items from the Risk Management Framework that specifically address security controls requirements in the Federal Information Processing Standards.

"Agency leaders tend to confuse the Framework and 800-53," Bigman said. "Although NIST has put out a lot of guidance on this, [the regulations] still confuse them. And then they put [the Federal Information Security Management Act] in, and they throw [Department of Homeland Security] regulations in, and frankly agencies get a little confused."

Even without this confusion, the details of SP 800-53 can be daunting. The most recent version, Revision 4, includes new security controls and enhancements to address advanced persistent threats, insider threats, and system assurance. It also addresses technology trends such as mobile and cloud computing. That's a significant amount of guidance that government organizations must digest and then apply.

ADDING COMPLEXITY TO SECURITY WITH MULTI-TENANT CLOUD

Yet NIST's guidance and controls are necessary considering the new technologies, and therefore new vulnerabilities, to which agencies are exposing themselves. Specifically, cloud computing and hosting present new security concerns that must be addressed.

"Even if cloud architectures have been built just for the government, you're still putting your information, infrastructure, applications, and workloads in somebody else's house," Cates said. That means agencies must not only have controls in place locally, but they also must find a way to ensure sensitive data is protected in the cloud.

Some cloud providers have security provisions in place. However, relying on that security isn't a risk that agencies should take because government organizations are ultimately responsible if their data is compromised. "You're getting cheap infrastructure or utilitarian computing and storage, but that's it. It's still on the organization to actually protect its information," emphasized Cates.

Ensuring sophisticated security transcends cloud architectures is an even greater concern for agencies that share their environment with other organizations. Called multi-tenancy, this cloud model places multiple organizations' data in a single hosting environment.

Although he recognized the model's advantages, Cates warned that multi-tenancy creates another barrier to cloud security: "Even though it's my cloud, I have multiple agencies there. So how do you actually build architectures and security practices that minimize or mitigate the risks that other tenants might bring to your environment?"

Some agencies deploy specific security solutions and protocols for data housed in the cloud. But that's not a best practice, Cates said, because "that's a lot of money to buy two of everything and edit everything to put separate controls in place in a multi-tenant cloud environment."

Still, agencies must ensure their data is secure outside their own data centers. Otherwise, multi-tenancy clouds may cause agencies to default on their regulatory compliance, decrease the cost-savings of cloud, and expose government information to other organizations. In the next section, we outline the steps to achieving data transparency and security.

THREE STEPS TO SECURING YOUR DATA

Agencies must take three steps to accomplish a security strategy that includes cloud and complies with regulations, Cates said.

↗ STEP 1: IDENTIFY YOUR DATA

Before agencies can secure their information, they must determine the scope and type of data that might require protection. This is no easy task. "I'll steal the three V's from big data," said Cates. "You have a lot of velocity. Your data is moving very fast to new locations in new ways. You have variety — where your data lives and what it looks like is drastically different than it was 10 years ago. And then volume is just increasing drastically. It's been said that every two years, data is doubling."

Unsurprisingly, this velocity, variety, and volume often hinder agencies from truly understanding their information. However, Cates stressed that it can be done.

"There are ways to identify your data and what it does for you, but you have to put in a lot a time and effort," he said. "And that's not just to buy one technology and get it done. You have to bring in the expertise to identify the information — where it is and what it looks like. At Vormetric, we coach our customers about how to identify their information, categorize it, and then classify it."

↗ STEP 2: ASSIGN USER RIGHTS

Categorization and classification are especially necessary in order to complete the second step to data security. Agency data isn't made safer simply by mapping where and what it is. Organizations must take the next step to delegate access to those who require it and restrict access to those who don't.

What's more, this designation of user rights must be applied to every employee and account. "Don't ever show the data to anybody who shouldn't see it," Cates said. "It sounds simple, but the problem is we have these things called administrators or privileged users inside of every system. How do you stop them from seeing the data? That's where many data breaches have happened. They're almost always from an administrator's privilege being abused."

Therefore, effectively assigning user rights is a two-fold objective. First, it means categorizing data rights by user group. Then, agencies must protect that same data from the very people who administer privileges.

↗ STEP 3: PROTECT YOUR DATA

Once your data is mapped and your user privileges are categorized, it's time to install protections that safeguard all of that data from anyone who shouldn't be able to access it. This is easier said than done.

As previously noted, government agencies' security solutions must comply with NIST SP 800-53. Additionally, protections must extend into a cloud environment where other organizations' information also resides. Finally, security systems and protocols should allow or restrict access for different users.

Unsurprisingly, these various requirements often lead agencies to adopt myriad security systems. But that tactic adds yet another level of security concern because agencies must then create a strategy to manage and maintain their multiple key and certificate management solutions.

In the next section, we explain how applying integrated encryption and key management can remedy these difficulties and secure your data.

INTEGRATED ENCRYPTION AND KEY MANAGEMENT AS A SOLUTION

One integrated solution can solve several problems associated with data protection in the cloud. Vormetric combines encryption at the file system level with integrated key and policy management. As a result, data in your cloud, database, or local file servers is protected from external threats and controlled for internal use.

Cates explained the basic premise: "Encrypt the information that's valuable. If it's sensitive or intellectual property or top-secret information, encrypt it. Then, through policy say who should have access to this data under what conditions: Who are you, what do you do, and how'd you get here? And based upon that, we'll give them access or not. It's as simple as that."

DATA SECURED IN THE CLOUD

Encryption is an especially beneficial tactic in multi-tenant cloud environments. "How do I ensure that the cloud provider or the agency who is a tenant in this environment can't see my data, even accidentally?" asked Cates. "The best way to do that is to encrypt it. Encrypt it and make sure that you as the agency own that encryption. That's where we've had a lot of success."

Encryption occurs before data enters the cloud, thereby protecting information without having to buy a separate security system for the new hosting environment. "I can say I want the control in my domain for my data, even as part of an interagency exchange in the cloud, but I don't want to buy two of everything," he said. "So we actually have a multi-tenant facility inside of our key managers that allows you to logically partition which key policies the data is governed by which administrators or domains."

By encrypting data before it leaves the network and maintaining keys locally, agencies can be confident that security won't depreciate as they transition to cloud environments. Other agencies may have access to the same cloud, but they will be restricted from accessing the same information because they won't have the keys to decrypt your data.

PRIVILEGED USER ACCESS REDUCED

Encryption not only allows agencies to partition information from external users, but also allows agencies to segment their data by internal cohorts. Only those users with the relevant key, assigned via security protocols, can access and decrypt data.

As an added benefit, Vormetric's method of encryption allows agencies to restrict privileged user access to information, even as administrators manage that data.

"Encryption's the only way to secure data in the cloud, but you have to do it in such a way that the administrator doesn't govern that encryption," said Cates. "Traditionally with encryption solutions that a lot of organizations are already using, there's this concept that somebody has to have the master key. If that person gets compromised, that account gets compromised, that server that it was sitting on is compromised, and then the game's over."

When Bigman was a federal CISO, his agency faced that exact risk. "The reason we bought Vormetric, and were most excited about it, was the ability to provide selective administrative privileges for the people with privileged access. It was really the first time we could have what we called 'black box capability' that enabled us to write our own rules about who would see what parts of the database and system files, regardless of what roles the computer itself said were being enforced."

In other words, "don't let the administrator be the governor of the data anymore. Let's let security be the governor of the data," Cates said.

SECURITY MANAGEMENT SIMPLIFIED

This method of encryption also reduces the burden on security personnel. Vormetric's "transparent" encryption means there are no changes required to agency applications, infrastructure, or business practices during deployment. Moreover, this encryption can be combined with Vormetric Key Management to further simplify security oversight and regulatory compliance.

Delineating access to data requires creating multiple keys for different user groups. In traditional security systems, as this data spreads to the cloud, managing these keys becomes even more difficult as new keys must be applied to off-premise data. However, integrated key management maintains centralized control of encryption keys, even as agencies leverage multiple technology solutions for their storage and analytics needs.

REGULATORY COMPLIANCE ASSURED

This central management also allows agency administrators to easily ensure ongoing regulatory compliance, because it offers administrators a consolidated view of all applied access controls. Additionally, an intuitive, web-based interface makes this information easily digestible and alterable when needed.

"Not only do we want to encrypt that data, but we also want to watch who's touching it," said Cates. "That's where we get a lot of benefit from a chain of custody. We can see every user, every application, every time that data was touched, and actually report upon that. People find that they can get some very good security intelligence from that."

For any attempt to access data under Vormetric's protection, a log of who accessed the data, when they did so, where the incident took place, which policies applied, and the resulting action can be generated. Administrators can then synthesize that information to determine which users might be a potential threat, which accounts may be at risk, and ultimately, what current security protocols may require alteration.

CONCLUSION

An increase in regulatory oversight, coupled with transitions to multi-tenant cloud environments, has offered significant benefits to many government organizations. Yet at the same time, these efforts have led many agencies to question their cybersecurity tactics. Even as agencies gain efficiencies, cut costs, and receive greater support from regulatory bodies, their systems become more complex and therefore harder to secure.

However, strong, centrally managed file and volume encryption combined with simple, centralized key management can remedy these concerns. An integrated, holistic solution provides security that administrators can trust to keep them compliant with regulatory standards and to protect their data.

ABOUT VORMETRIC

Vormetric (@Vormetric) is the industry leader in data security solutions that protect data-at-rest across physical, big data and cloud environments. Vormetric helps over 1,500 customers, including 17 of the Fortune 30, to meet compliance requirements and protect what matters — their sensitive data — from both internal and external threats. The company's scalable Vormetric Data Security Platform protects any file, any database and any application's data —anywhere it resides — with a high performance, market-leading solution set.

Vormetric
Data Security™

ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public sector professionals by serving as the knowledge network for government. GovLoop connects more than 150,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C. with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to Hannah Moss, GovLoop Researcher and Writer at hannah@govloop.com.

1101 15th St NW, Suite 900
Washington, DC 20005

Phone: (202) 407-7421 | Fax: (202) 407-7501

www.govloop.com
@GovLoop

GovLoop
1101 15th St NW, Suite 900
Washington, DC 20005

Phone: (202) 407-7421 | Fax: (202) 407-7501

www.govloop.com
@GovLoop