The Challenge of Data Security

Amid tripling of agency breaches, federal CISOs double down on protection.

Federal agencies have striven in recent years to modernize federal computing, adopting technologies such as cloud computing, collaborative tools, mobility and Internet-enabled sensors. The consensus is that these technologies will enable a transformed IT environment that will require flexibility, efficiency, accessibility, collaboration and security.

That last part – keeping sensitive data and systems secure – can keep some chief information security officers (CISOs) up at night.

Despite the extensive use of cybersecurity solutions designed to protect networks and infrastructure, cyber threats and attacks on federal agencies continue to climb. According to a recent report compiled by 451 Research, an IT consultancy, 57 percent of U.S. federal agencies have experienced data breaches in the past year, triple the number in 2016. Breaches at federal agencies occur at a higher rate than in other sectors.

Malicious threats are also becoming more sophisticated, enabled by ransomware that can cripple organizations: crypto malware, such as WannaCry; ransomware that locks users out of their systems; scareware that mimics antivirus software; leakware that threatens to publish personal information online if a ransom isn't paid; and even Ransomware as a Service. Other threat vectors include the Internet of Things (IoT), social engineering and phishing attacks, password cracking and man-in-the-middle attacks, which can occur when users work on unsecured wireless networks.

Cybersecurity Worries Slow Modernization

Cybersecurity concerns are getting in the way of IT modernization. Some agencies, for example, are reluctant to embrace cloud computing despite the government's cloud-first mandate, the more recent Cloud Smart strategy, and agencies' awareness of cloud's benefits to IT operations. The reluctance largely stems from uneasiness about storing critical data in the cloud and the perceived risks of using third-party cloud service providers. Entrusting a third party – even one vetted and approved by the U.S. government – to store data and control encryption keys isn't a risk some agency leaders are willing to take. 451 Research reported that 69 percent of agencies harbor concerns about the custodianship of encryption keys in the cloud.

Agency leaders also worry about protecting data in a modern enterprise environment in which data can seamlessly move between multiple clouds, data centers and mobile devices – and best-of-breed applications may exist in different clouds. The modern enterprise, charged with delivering continuous productivity and seamless service to customers, relies on a fluid workflow in which ever-shifting virtual teams collaborate across internal and external networks accessed on a growing array of client devices. In such an environment, the ability to control valuable and sensitive data is paramount.

"Like commercial organizations, government agencies have been using a variety of security solutions for decades, like VPNs and firewalls," says Dave King, chief technical director for cyber at General Dynamics Mission Systems. "That approach worked well for some time, but it doesn't work well for a modern enterprise where data is mobile and often shared externally to partners."

The visibility gap – the inability to see where data is at all times, along with when and how it is being used – slows some agencies' progress in attaining IT modernization. As the borders of enterprises widen and become more permeable – data travels inside and outside agencies, touching multiple users, devices and apps – the visibility gap tends to widen. In such a fluid environment, the issue of data security becomes more complex as does maintaining regulatory compliance.

Then there is the challenge of making security as frictionless as possible. Increasingly complex security tools require users to undergo significant training. In some cases, that complexity can lead even well-meaning users to bypass security measures and inadvertently expose data. In other cases, users may take actions they don't recognize as being potentially dangerous. Occasionally, insiders with malicious intent ignore security measures for their own gain. Regardless of intent, users who skirt security protocols put agencies at risk of exposing critical data to vulnerable devices, such as personal USB drives or smartphones, and accessing privileged administrator accounts from unsecure locations.

Borderless Enterprise

Finally, issues of governance and compliance present myriad challenges in a borderless environment. A task force within an agency might work closely with an external partner, sharing data back and forth. When that project comes to an end, how can that agency prove that it has been and continues to be in compliance with security standards regarding sensitive data? The same is true if an employee leaves the agency. How can the agency be sure that the employee doesn't continue to retain sensitive files?

"Especially today, agencies need better governance – the ability to control and enforce cloud-based services and data, wherever it is – without becoming non-compliant," King says. "An effective governance system will enable data tracking, ensuring that you know exactly where the data has been and who has touched it. It will also be able to demonstrate compliance with any regulatory requirements by pulling very clear reports about the who, what, when, where and how of file access."

All of these challenges can be solved, but they require a new approach to cybersecurity – one that first protects and encrypts the data itself – instead of relying on just network protection when data leaves the perimeter of an enterprise or relying on data storage protection. By protecting the data itself, agencies can move confidently ahead into the borderless future, ready for whatever comes next.

Hitting the Security Bullseye

In a complex threat environment, data-centric security solutions are finding the mark.

The Office of Management and Budget classifies federal data as a "high-value asset" for which unauthorized access, use, disclosure, disruption, modification or destruction could significantly undermine the country's security. Yet federal agencies often don't give data the protection it deserves, leaving the asset vulnerable to nation state attacks, exfiltration, and even insider threats.

A recent Cisco report revealed that hackers seeking to compromise government data are using increasingly sophisticated types of malware, leveraging advanced encryption techniques to avoid detection, and exploiting undefended gaps in security. A September 2018 GAO report warns that without major changes, these vulnerabilities may lead to additional security incidents and cyberattacks. The report calls for agencies to improve cybersecurity, including renewed efforts to protect sensitive data.

The security challenge has layers of complexity. Valuable government information is no longer housed exclusively in data centers. It can be almost anywhere – in data centers, in the cloud, on mobile devices. A single piece of data can touch many users, devices and applications spanning physical and digital locations, within and outside agency boundaries. As such, perimeter-based security and other traditional network security methods have become far less effective.

The Data Lifecycle

What's needed is a data-centric approach to security in which data is fully visible and protected for the entirety of its lifecycle, from the moment of creation until the time it is destroyed.

A data-centric security solution isn't bound by the network, the on-premise environment, the data center or the cloud. Rather, each piece of data is individually encrypted. Only the owner can determine who has access to the data at any given time.

"A strong data-centric solution doesn't care about how data gets from point a to point b, and it doesn't care who has it," explains Gerry Jankauskas, an architect at General Dynamics Mission Systems and product manager of the company's Route 66 Cyber™ product family. "Because security is attached to the data itself, instead of the network or the infrastructure, all data – even data that may fall into the hands of attackers – remains fully protected. If a hacker tries to open it or copy it, they simply can't do so."

To achieve data-centric security, agencies can use an Enterprise Digital Rights Management (EDRM) solution, which fully secures data wherever it travels, whether on premises, outside the organization and in the cloud. General Dynamics' EDRM solution, for example, uses high-grade encryption to encrypt each object independently from every other, issuing a unique key for each file. The solution protects data at rest, in transit and while in use. It allows agencies to track, audit and manage policies for all files in real-time, even after they are downloaded or sent to another device.

An important part of effective EDRM solutions is policy management, which allows only authorized administrators and users to control who views, accesses, and downloads specific files based on an individual's roles and privileges. Administrators can remove permissions when a project comes to an end, a user's role changes or an employee is terminated.

The EDRM approach is adaptable and efficacious in many situations. Consider the finance department of an agency that has responsibility for managing financial risk and performing quantitative analysis. To ensure that data remains secure and under the agency's control at all times, the finance department would need a way to secure, track and control access to financial models and sensitive data. An EDRM solution would ensure that any file leaving the agency's on-premise or cloud-based locations, whether through email, file shares or physical storage, would remain fully encrypted and accessible only by approved parties.

"It's a holistic approach, which is very appropriate in an environment where sharing, collaboration and the cloud are becoming ubiquitous," Jankauskas says. "EDRM is file type and device type agnostic, without impacting the everyday workflow of your business."

Tips for Secure Data Encryption

Authentication and encryption is the heart of virtually all cyber security solutions because, no pun intended, it provides the key to protect and unlock access to restricted information.

Encrypting data in the most stringent and comprehensive way possible ensures that sensitive data is inaccessible to attackers, even if they get physical access to files.

Here are 11 actions to keep your data safe

Seamless Business Integration

1 Choose a solution with an effective key management system that centralizes management of encryption keys throughout their lifecycle, from generation through deletion.

2 Retain control of your encryption key.

Pedigree/Coding Standards

3 Data encryption is not a DIY project. Don't build your own.

4 Choose a properly certified provider that adheres to rigorous NIST and FIPS standards.

5 Use software developed in the United States by cleared professionals for your high valued assets.

6 Avoid encryption solutions based on open-source technology. Only approved personnel should have access to the inner workings of your security mechanisms.

Standards Compliance

7 Insist on strong, high-grade AES 256-bit encryption that complies with strict coding standards and has undergone penetration and independent validation and verification testing.

8 Abide by "anytime, anywhere" encryption protocols that protect data at rest, in process, in transit, in the cloud and on premises.

9 Encryption should seamlessly integrate into your existing ecosystem without causing latency or changing workflow.

Hygiene

10 Regularly test encryption and recovery processes. Never keep data in the cloud with an encryption key.

11 Make sure your encryption solution generates long, random keys using approved algorithms.

The Defensible Audit

Data encryption and usage tracking improve agencies' compliance with reporting requirements.

More than half of U.S. federal agencies have failed a compliance audit due to data security issues in the past year, according to at least one recent report. The failure rate isn't surprising. As more agencies modernize IT infrastructure, embrace the cloud and encourage greater collaboration, sensitive data has become vulnerable. At times, insufficient data security has resulted in fines, lost jobs and the scrutiny of Congress and the news media.

Worse, the risk to data remains even when agencies take prescribed precautions, such as implementing anti-malware software, firewalls and intrusion detection and prevention systems. Those tools, while important, are designed to broadly protect the infrastructure, not specific data.

As a result, security gaps occur, most frequently during transition periods in the data lifecycle, such as when data is uploaded, copied or moved during typical business workflows. During these times, data leaks can occur, ranging from the theft of credentials and downloading of sensitive data to the planting of malicious bots. With security gaps present, auditors can't ensure that data is secure over time, nor can agencies prove that they are in compliance with applicable regulations.

To counter the growing threat of security breaches, some organizations are adding another layer of data-centric security. Solutions such as Enterprise Digital Rights Management (EDRM) and Cloud Access Security Brokers (CASB) encrypt and protect data, from creation to destruction, no matter where it travels or who accesses it.

Encrypting data from the moment of generation closes security gaps and provides full protection. whether data travels from workflow to workflow, from user to external collaborators between the cloud and on-premises locations. Fully protected data can't cause compliance or audit problems.

Data-centric EDRM and CASB solutions also enable visibility and tracking, which is critical to ensuring security. Without visibility into your agency's sensitive data and applications, protecting them is harder. Next-generation EDRM and CASB solutions help agencies track, audit and manage policies in real time, no matter how far from the agency the data travels or what cloud services are being accessed. Next-generation EDRM and CASBs must be extensible and future proof to protect unique mission data and applications, on premise and in multiple clouds. Agencies can apply and change policies, as needed, and adjust the level of controls, such as audit, alert, block, quarantine, delete, timeout, and view only.

"A proper EDRM with a CASB will cover many cloud activities, not just the sanctioned and supported applications," explains Jankauskas. "This holistic approach is continuous and complete for proactive protection and in the case where something may happen, reduces the time to detect and take action."

The Great CASB?

A cloud access security broker can reduce security risks in the cloud.

Recent revisions to the federal government's cloud strategy have raised expectations that agencies in the coming year will accelerate the shift of workloads to the cloud. As that occurs and the IT surface of attack grows, agencies will need tools to prevent the loss and leakage of sensitive data.

A Cloud Access Security Broker (CASB) can be an effective way to reduce the risk of security gaps in cloud services. Policies developed and maintained by an agency to control access to data serve to underpin CASB solutions, which enable agencies to see who is accessing its resources and whether those users are attempting to see data sets or use applications they don't have permission to access. A CASB provides a way to uniformly apply security policies across cloud applications with varying levels of security and across multiple clouds. A CASB tracks the location of data in every cloud-based application, encrypting each piece of data with a key controlled by the agency. Used correctly, a CASB can significantly reduce the threat of known and unknown risks for data leaks and cloud-based malware.

An advanced CASB solution would use machine learning techniques to deliver real-time data and threat protection across the dynamic enterprise cloud footprint. Such a solution would automatically adjust, learn, and adapt to new cloud applications, new malware threats, new types of sensitive data, and be able to analyze user behavior across time and applications. It uses that information to generate real-time alerts and fix problems before they get bigger. For example, such a CASB solution would prevent access by a user whose behavior deviates from typical patterns, for example. If a user tried to log into different applications from different locations within a matter of minutes, CASB would deny access. An ML based security solution is effective as it can evolve with the plethora of new collaboration tools as they emerge onto the enterprise.

The real-time capabilities of the most advanced CASBs are extremely important. It means that it is actually looking at every point and click as it happens, making sure users are allowed to take an action or preventing them from taking unsanctioned actions.

When choosing a CASB, flexibility is key. A policy-based solution can provide that flexibility, enabling agencies to control the type of cloud applications and data specific users can see or access.

An effective CASB also can help reduce the problem of shadow IT, in which users who may have good intentions attempt to access applications that aren't approved by the agency.

A next-generation CASB also fosters mobility by enabling approved mobile devices to connect to cloud-based applications. Users can set up their own apps, and their devices are automatically configured to communicate with the CASB proxy. The CASB automatically syncs with the organization's Active Directory. Because of fine-grained data usage control policies, an employee's access to files is easily revoked in scenarios such as them leaving the organization. Agencies no longer have to worry that users are downloading sensitive data to their mobile devices, and employees have fewer concerns about their own privacy.

As cloud usage continues to grow, protecting sensitive data will continue to be a challenge. For most organizations, CASBs will be a critical tool in protecting that data. According to Gartner, CASBs already have become a vital part of a cloud security strategy, and by 2020 more than half of large enterprises will use a CASB to protect cloud services.