Identity Access: The Key to Data Governance

MARKET TRENDS REPORT

govloop SailPoint immixGroup An Arrow Company

Introduction

There's no data more important than federal government data. The information federal agencies handle often contains large amounts of sensitive data, including intellectual property, strategic plans and personnel records. How this data is classified, protected and structured is vital to national security.

Unfortunately, the threats to federal data security are growing in both strength and number. Outside of agencies, nation-states, criminals, terrorists and hackers all endanger government data. Inside of agencies, anyone with access to sensitive information can unknowingly or deliberately compromise security and become an insider threat.

This reality means that data governance is crucial for federal organizations. Data governance is the process by which agencies classify, protect and structure their data. Strong data management begins and ends with equally robust identity governance, meaning agencies need to know the identities of those users accessing their networks and data. Without the right strategy, these organizations are in the dark about who's accessing what information and when.

GovLoop partnered with SailPoint, an identity governance solutions provider, on this report examining how identity and access control is at the heart of sound data management. The following pages offer insight on creating a data management model that meets federal standards while confronting modern cyberthreats head-on. They also feature expertise from Frank Briguglio, Public Sector Identity Governance Strategist, and Jim Russell, Director of Federal Sales at SailPoint.

BY THE NUMBERS

74%

of federal agencies have cybersecurity programs that are either at risk or at high-risk.

Source: The Office of Management and Budget (OMB)

400%

is how much the number of datasets available on Data.gov, the federal government's open data resource, increased between 2012 and 2016.

Source: Federal CIO Council

38%

of federal cyber incidents did not have an identified attack vector, suggesting limited situational awareness for agencies.

Source: OMB

186,467

datasets were available on Data.gov in 2016, up from 164,670 in 2015.

Source: Federal CIO Council

27%

of federal agencies reported that they can detect and investigate attempts to access large volumes of data.

Source: OMB

12,602

data centers were reported as open by federal agencies in 2017.

Source: Government Accountability Office (GAO)

THE CHALLENGE
Safeguarding Cybersecurity Amid Data Sprawl

The federal government handles massive amounts of data containing sensitive information about its operations, spending and workforce. This information ranks among America's most precious assets.

Unfortunately, data is a double-edged sword for the federal government. The large quantity of federal data makes it both valuable and difficult to manage. Rising data sprawl makes understanding this information daunting, and insights are missed as agencies store their data in isolated silos. Data sprawl occurs when data is moved from its original context, duplicating it and making it more difficult to find.

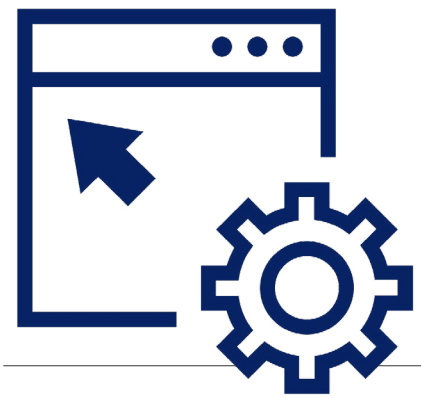
Unstructured data is especially problematic. The growing diversity and volume of unstructured digital content presents several challenges for agencies, such as determining the value of that data and who can utilize it.

Unstructured data, which includes formats like photos, satellite imagery and videos, also contains numerous security gaps that can be exploited. Sensitive data sitting in a structured endpoint, such as a database, becomes unstructured when it's moved or copied to a spreadsheet or document and stored in a file server where it's exposed.

"That's how we start to lose control of sensitive data," Briguglio said. "That's where the bleeding happens in the sprawl."

The federal government's workforce structure makes the situation worse. The various agency contractors, employees and private partners complicate the process of tracking data access and ownership across multiple mediums.

"It's taking data out of the IT realm and into the business realm," Russell said. "It's putting that information into much more casual hands as it relates to the forum where this data is possessed."



THE SOLUTION
Guarding Data With Identity Governance

Agencies need a strong data governance strategy for protecting their sensitive citizen and national security information from cybersecurity threats. This strategy must address how organizations govern the identities of their contractors, employees and partners. It must also decide how these users access agencies' data and networks while meeting federal cybersecurity standards.

Identity governance is the foundation of any successful data management strategy. It also helps agencies get a grip on who's accessing their data, how they're using it, when and why.

"All identities and their access privileges need a governance process around them," Briguglio said. "Looking at separation of duties within an application, it's probably one of the least complex security controls to implement. But it's probably also one of the controls that's omitted frequently."

Agencies that utilize identity governance see every step their users take and how they interact with data. This process provides organizations with more clarity about how their information is used.

"Identity governance is the process of managing an identity's lifecycle," Briguglio said. "It's that identity's access, entitlements, roles and permissions. It's then putting processes around that identity for auditing, certification and access review. It includes provisioning and de-provisioning these things throughout the lifecycle as needed."

Take the example of a federal contractor who is eventually hired as a full-time agency employee. The data access this person has may need specific limitations depending on their role when the information is accessed.

"It's moving across a user's whole lifecycle with the government," Russell said. "It's not only for their time with the government, but their time as an extension of the government, say, working as a contractor."

Identity governance is additionally valuable for preventing insider threats, or users who accidentally or purposefully expose data. Closely monitoring and limiting user access and identities reduces the risk of such individuals harming your agency. The alternative is a data leak that embarrasses your organization and leaves its sensitive information publicly exposed.

Our next section will help you avoid such crises by sharing best practices for improving your agency's data handling with identity governance.

BEST PRACTICES

Improving Data Governance

I. Classify your data

Getting identity governance off the ground requires understanding how your data should be classified. All federal data isn't equal – some information is publicly available, while other information has national security implications and must remain hidden. Finding where your data exists and properly classifying it ensures your information is stored with the right safeguards.

2. Set up your security controls

Once agencies have classified their data, they can determine who can access it, how, when and why. These decisions are essential for avoiding breaches that expose sensitive information and hurt organizational credibility. "We look at ownership, who has access to the data, the permissions model that makes the most sense and how to protect it," Briguglio said. "This is so you can keep enforcing those security and compliance controls wrapped around the data."

3. Add automation to the mix

Automation saves energy, money and time during data and identity governance. It allows the same control over user access and identities without sacrificing speed.

This lets agencies give their contractors tools as they're needed. It also helps organizations better govern their data while improving transparency.

Additionally, automation ensures that agencies don't stumble over shifts in their employees' entitlements and statuses. Automating access privileges after major changes like firings and promotions shields many of the data vulnerabilities that organizations have.

4. Take advantage of federal cybersecurity tools

The federal government's Continuous Diagnostics and Mitigation (CDM) program helps agencies strengthen their cybersecurity through identity governance and other tactics.

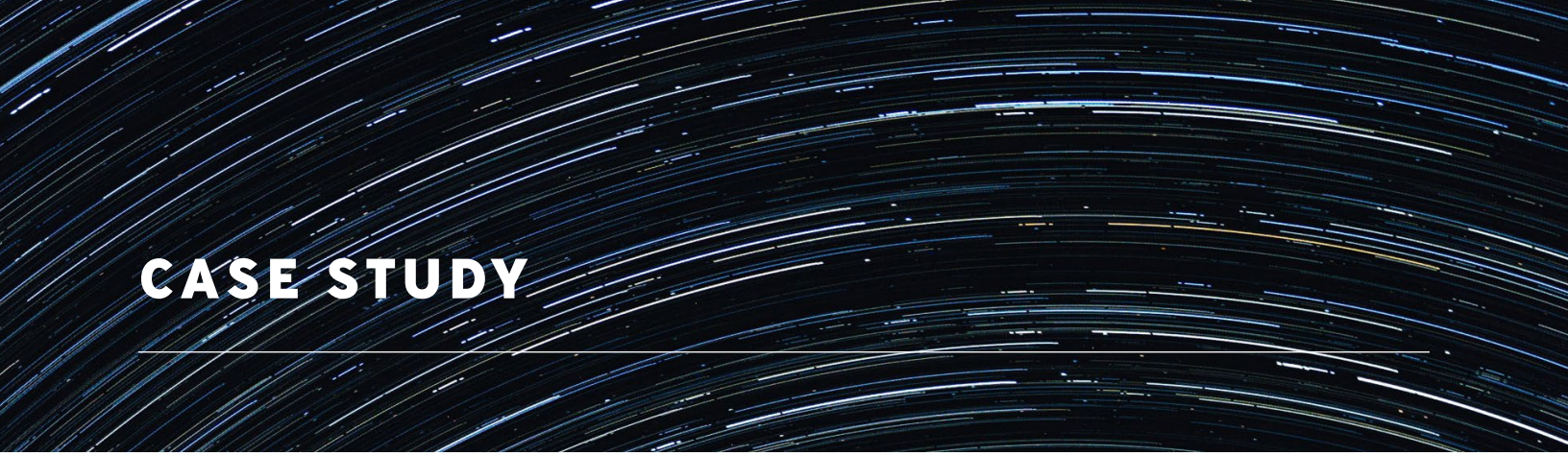
Launched in 2013, CDM uses agency-installed sensors to perform automated, ongoing searches for known cyber flaws and evidence of real-time or past attacks. This helps federal network managers prioritize their most pressing cyber risks and act accordingly.

The Homeland Security Department (DHS) announced in November 2018 that CDM is emphasizing capabilities over its four previously used phases. Still, CDM's Phase 2 remains relevant to identity governance, as it concerns who's on the network.

Phase 2 assists with identity governance through four interdependent functions that are useful for agencies. They are: management and control of account; access and managed privileges; trust determination for people who are granted access; credentials and authentication; and security-related behavioral training. This collection helps organizations improve their identity governance while meeting federal cybersecurity standards.

5. Work with the right vendor

Private sector partners can help agencies solve identity governance challenges. The best vendors offer solutions for carefully governing user access and identities involved with public sector data and networks. These tools must comply with federal cybersecurity standards while protecting all data regardless of its sensitivity.



CASE STUDY

One federal intelligence agency needed help retooling its identity governance strategy after several of its user accounts were compromised. The accounts were overexposed, meaning they had data access permissions that were higher than originally intended for those users.

"Those overexposed accounts were able to be compromised," Briguglio said. "That data was made publicly available."

SailPoint worked with the agency on curtailing data access to prevent further harm. The company also assisted the agency with implementing an identity governance strategy for avoiding and mitigating similar situations in the future.

"Our solution found many of the orphaned accounts, removed most of their permissions and took away the ability for recurring events," Briguglio said, referencing accounts that once belonged to users who had left the agency. "There was no more lateral movement from the orphaned accounts."

The agency ultimately resolved the problem by automating the process of stripping permissions from the accounts. Predictive and preventive measures then informed administrators when new attempts at accessing data occurred. This mitigated the organization's risk and prevented additional damage to its reputation.

HOW SAILPOINT HELPS

SailPoint's Identity Governance Suite is the first step in developing healthy data governance and fortifying cybersecurity. It's a collection of intelligence and security tools that also complies with federal benchmarks like CDM.

The Identity Governance Suite is fully automated and enables agencies to protect their data by limiting user access as needed. This gives organizations complete confidence in who is accessing their information and when. Agencies can allow or deny access as they see fit, granting permissions to employees, contractors and partners based on their mission objectives.

SailPoint's toolset also helps agencies comply with CDM Phase 2. Organizations can monitor and manage their users' data and systems access regardless of their location. The Identity Governance Suite also provides complete visibility for this data, as well as organizational applications and users. These abilities ultimately help agencies monitor and mitigate their risks.

"That's where the whole suite comes into play," Briguglio said. "It's a comprehensive user record with background information and information about learning and trust. You can build your security access controls around this record, your roles and separation of duties and enforce those on your unstructured data with the audit process wrapped around it."

Learn more here: SailPoint on Identity Governance

Conclusion

Federal agencies are responsible for navigating an increasingly treacherous cybersecurity landscape crowded with threats. Data governance helps them classify, protect and structure their sensitive information while driving toward mission success.

Data governance is most useful, however, with identity governance powering it. Identity governance reveals who's accessing federal data, how, when and why. This knowledge is crucial for detecting, preventing and stopping the multiple cyberthreats menacing organizations.

Agencies are also accountable for complying with federal cybersecurity guidelines. Meeting CDM Phase 2 benchmarks improves identity governance while maintaining constant vigilance against cyberthreats.

The cost of failure is high for agencies that don't govern their data and identities. Leaks of sensitive federal information can permanently harm organizational credibility, citizens and work. Data and identity governance give agencies the necessary control over their assets to avoid such outcomes.

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 270,000 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 info@govloop.com.

govloop

ABOUT SAILPOINT

SailPoint enables federal agencies to confidently secure access to the Nation's most sensitive data. Recognized by Gartner, Forrester and KuppingerCole as the leading authority on identity governance and administration, SailPoint delivers modern, comprehensive identity solutions that govern access to mission-critical applications and data. Its technology provides process automations, ensures suitability, compliance and least privilege entitlement policies, enhances identity analytics, and auditing and reporting. The SailPoint solution is key component of security and compliance strategies and ensures sustainable compliance with the NIST Risk Management Framework (RMF) and Security Controls.

For more information, visit www.sailpoint.com.

SailPoint

ABOUT IMMIXGROUP

immixGroup, an Arrow company, is a value-added distributor that helps technology companies do business with the government. immixGroup enables IT manufacturers and solution providers to grow their public sector business and accelerate the sales cycle. Since 1997, immixGroup has delivered the specialized resources and expertise these companies need to increase their revenue, support their demand creators, and operate efficiently in the complex public sector IT market. Government agencies at the federal, state, and local levels trust immixGroup to provide reliable access to a wide range of enterprise software and hardware products through their preferred contracts and business partners.

immixGroup
An Arrow Company

1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop