SailPoint

SOLUTION BRIEF

A Darwinian Approach to **Reducing Government Cyber Risk**

Several key trends are creating a new wave of challenges threatening the security of sensitive and even classified government data. Fortunately for government agencies, identity governance is **evolving to counter these threats and reduce risk.**

New Trends that Identity Addresses

Expanding Definition of Users:
Attackers from the outside are now sneaking into IT networks by deploying malware and phishing tactics to compromise user credentials. Meanwhile, insiders – users with authorized access – continue to create risk by exposing data either through negligence or malicious acts. And now, there's a new concern – the adoption of robotic process automation (RPA).

These non-human users are programmed to complete a variety of repetitive tasks such as data extraction, loan disbursements, chat boxes, etc. Although RPAs have legitimate and beneficial purposes, someone with questionable intent could hack the software bot and gain access to sensitive data. This is not simply hypothesizing what can happen. In 2018, a chatbot for a major ticket distribution company was hacked and used to steal an unspecific amount of payment card data. To avoid a similar attack, government agencies must treat RPAs like human users and incorporate them into an identity governance program. In doing so, government agencies gain visibility and control of who or what gets access to sensitive data.

Rising Cloud Adoption:
Software applications are increasingly abundant in any organization. And in the federal government, those applications are increasingly in the cloud. In fact, according to a FedScoop survey, 6 in 10 federal IT executives now see cloud computing as a vital pathway to improve mission critical services.[1] Moreover, "sixty percent of federal IT leaders surveyed report that most of their agency's IT spending over the next three years will go toward a combination of cloud models, including government-only cloud services, public and commercial clouds or a hybrid approach."[1]

[1] FedScoop, *Federal IT leaders report advances in cloud adoption for critical services*

By their very nature, cloud applications are designed to be accessible from anywhere, anytime, making security uniquely challenging. By deploying SailPoint's modern, intelligent, cloud identity platform, public agencies can unify their approach to governing user access rights to applications whether on-premises or in the cloud. This approach drives consistent access policy enforcement, reducing errors in provisioning while increasing IT and operational efficiency.

SailPoint's evolutionary approach enables government agencies to reduce cybersecurity risk without having to take a leap of faith on unproven platforms.

Data Migration:
Sensitive and even classified data sitting in secure databases often migrate to less-than-secure locations and shared for legitimate reasons. For instance, someone may run nightly reports that are exported into a spreadsheet. Another user may copy and paste information into a presentation or document to update team members. In fact, Gartner estimates 80% of the world's data is found in this format and stored in files.[2] Moreover, an estimated 1 in 4 users will upload sensitive information to cloud applications (and data stores) whether to save or share.[3]

So how do you secure this ever-increasing volume of information sitting in file stores? The answer is by extending identity governance beyond systems and applications. SailPoint's best-of-breed technology enables government agencies to discover and classify sensitive data stored in files. This allows organizations to then apply consistent access controls across all applications, systems, and data – ensuring only the right people have the right access at the right time for the right reasons.

Take a Predictive Approach to Security

Cyberthreats are evolving and increasingly sophisticated. Combined with the sheer volume of users, applications, and data to manage, the role of IT and security has become extremely complex. Gathering, analyzing, and synthesizing the vast amount of identity-related data can become an unwieldy task. And based on this trajectory, it will only become more challenging. To address today's and tomorrow's challenges, SailPoint incorporates the power of artificial intelligence (AI) and machine learning (ML) capabilities to deliver a predictive approach to identity governance. This approach allows IT and security teams to leverage the vast amount of identity and event data to deliver advanced insights that recommend if access should be granted or not and how access policies should be updated to address change in the organization. This advanced governance approach also helps uncover where potential security gaps and risks exist by identifying the risky outliers amongst peer

[2] Gartner, *Organizations Will Need to Tackle Three Challenges to Curb Unstructured Data Glut and Neglect Foundational*
[3] SailPoint, *2017 Market Pulse Survey*

groups. This enables government agencies to proactively address security by monitoring for risk in real-time and anticipate how access should change. In addition, AI/ML insights can help identify low-risk activities that can be safely automated, allowing IT and security teams to focus on more high-risk and strategic matters.

Why is SailPoint an Ideal Partner?

With more than 60 government agencies already using SailPoint to manage more than 3 million identities, SailPoint is the most trusted name in identity governance. Our long record of success is the foundation upon which we build innovation, such as the infusion of AI/ML into our proven identity platform and the extension of identity to data stored in files. By taking this evolutionary approach, SailPoint enables government agencies to **reduce cybersecurity risk without having to take a leap of faith on unproven platforms.**

SailPoint's Government Pedigree

Support

- NIST 800-53 security Controls
- Implementation of the FICAM services for Identity Management
- ICAM Modernization Strategy
- FIAR and FISCAM security controls
- Protection of HVA by implementing security controls

Deployed

- At 23 CFO Act agencies to support the DHS CDM Master User Record
- DISA for identity lifecycle

Authorized

- To operate on Americas most sensitive DoD and intelligence community networks

Certified

- NIAP Common Criteria

Pursuing

- FedRamp Authorization

To learn how other federal agencies are leveraging SailPoint contact us or schedule a demonstration.

SAILPOINT: THE POWER OF IDENTITY™

sailpoint.com

SailPoint, the leader in enterprise identity management, brings the Power of Identity to customers around the world. SailPoint's open identity platform gives organizations the power to enter new markets, scale their workforces, embrace new technologies, innovate faster and compete on a global basis. As both an industry pioneer and market leader in identity governance, SailPoint delivers security, operational efficiency and compliance to enterprises with complex IT environments. SailPoint's customers are among the world's largest companies.

SM1318-1907