SailPoint

SOLUTION BRIEF

Govern and Secure Access to AWS infrastructure with **SailPoint Identity Security**

IaaS platforms such as Amazon Web Services (AWS), offer the ability to quickly stand-up new infrastructure with relative ease and an elastic consumption model provides capacity on demand – this gives organizations the ability to free up budget and increase investment opportunities. However, when establishing or migrating critical workloads to the AWS cloud platform, one thing that must not be overlooked is the need to ensure secure, compliant and efficient access to this infrastructure.

As organizations increase their cloud presence their attack surface now extends beyond the traditional perimeter. With the hundreds or thousands of users and each user having a multitude of entitlements, the potential failure existing outside of traditional security protocols is enormous. Taking an identity centered security approach to cloud infrastructure is key to reducing your cloud attack surface.

While cloud infrastructure platforms provide basic access control capabilities, access management is not enough. Cybercriminals are finding their way into these IaaS environments to infect systems with malware, steal data, hijack resources or even shut down critical services. In IDC's 2020 Cloud Security Survey 64% of organizations stated that one of their top three cloud security threats was lack of visibility into access in production environments.

SailPoint Identity Security enables enterprises to create a more secure and continuously compliant environment through governed access of AWS. By incorporating the benefits of AI and machine learning, you can be better equipped to meet the security requirements of your continuously evolving business and IT environment. Using the power of SailPoint Identity Security, you can properly secure, manage and govern your AWS cloud access as a part of your overall identity and security program.

A recent survey stated that

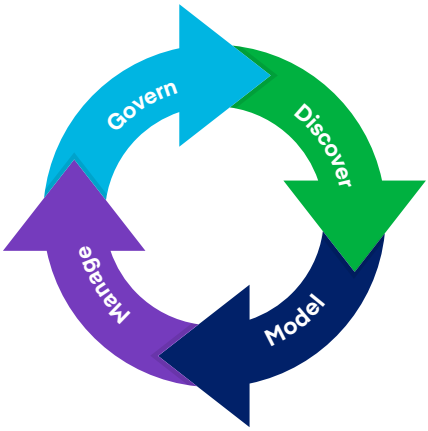
97%

of organizations experience problems managing IaaS access.[1]

[1] State of IaaS Cloud Infrastructure Security and Governance, September 2020 Dimensional Research

Discover

Discover human, non-human, cross-account and even federated across all of your AWS cloud environment on an ongoing basis. Find out how many users have access, how much access each user has and what access they aren't even using. After discovery you can view a graph of all identity and resource entitlements across your entire digital landscape including IaaS, SaaS, and on-premises applications and data.



Model

Create an identity-centric view by correlating identities to IaaS access. Use Artificial Intelligence (AI) and machine learning to visualize, compare and verify how access is distributed across job roles, location, departments, managers and apps. Model and define consistent access policies based on roles across multiple IaaS platforms.

Manage

Automate the provisioning of cloud access as users join, move within, or leave the organization. Choose from a library of several hundred pre-defined access and governance rules or guardrails that will automatically monitor and alert you to any cloud access that is not within standard policy or appears anomalous. Custom guardrails can also be created as needed to address specific business requirements. AI technology is used to monitor cloud access to alert any potential suspect behavior. Access violations are clearly described within alerts and remediation steps are provided to take action. In addition, alert data can be forwarded based on severity level via email, web hooks, or to a syslog server such as a SIEM tool.

Govern

Enable your business users to easily and accurately review and certify cloud access for both security and compliance. Control both direct and effective access to cloud resources. Make the certification process easier by using AI and machine learning to provide recommendations on whether access should be granted or removed based on risk. A centralized tamper proof, easy to use system of record provides a consistent, comprehensive view of all access across all environments for compliance and audit requirements. Historical views can be created showing how access might have been originally granted or changed over time to provide additional insight for audits. Access can also be viewed from different perspectives and filtering applied for tailored audit views.

Securing your AWS environment requires considering access and entitlements across all organizational applications, workloads and data. SailPoint Identity Security enables you to centralize visibility and reduce the risk of access in your environment. AI and machine learning automates processes and provides enhanced insight making the business more efficient and reducing costs. SailPoint ensures your AWS environment is secure and governed in the same manner as the rest of your infrastructure, increasing security and supporting compliance. For more information please visit: **https://www.sailpoint.com/integrations/amazon-web-services**.

ABOUT SAILPOINT

SailPoint is the leader in identity security for the cloud enterprise. We're committed to protecting businesses from the inherent risk that comes with providing technology access across today's diverse and remote workforce. Our identity security solutions secure and enable thousands of companies worldwide, giving our customers unmatched visibility into the entirety of their digital workforce, and ensuring that each worker has the right access to do their job – no more, no less. With SailPoint as foundational to the security of their business, our customers can provision access with confidence, protect business assets at scale and ensure compliance with certainty.

SB1718-2104