SailPoint

WHITE PAPER

Best Practices for Identity Governance **in Multi-Cloud Environments**

Get the Most from Your Multi-Cloud Environment, But Do It Securely

These days, more than three out of four businesses use multiple cloud platforms. This gives them the freedom to match the requirements of each use case to the unique strengths of each cloud platform, whether it's AWS, Azure or Google Cloud Platform.

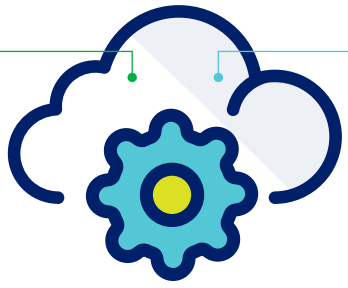
What these businesses lack, however, is a way to effectively and securely govern access across these multi-cloud environments. These challenges leave businesses open to the risks and costs of non-compliance, cyberattacks, and just plain human error.

Some may use native tools with basic identity and access management for a single platform, but this is not governance. This lack of governance also stifles productivity and growth – if users can't get the access they need when they need it, work doesn't get done.

In this White Paper, you'll learn about the best practices you can implement to get the most out of your multi-cloud environment without compromising on security: comprehensive visibility and discovery, robust protection, and tighter governance, all enabled by advanced automation technologies.

84%

of enterprises leverage the cloud[1]



78%

of enterprises use two or more platforms[1]

[1] *Rightscale 2019 state of the cloud report from Flexera*

The Four Biggest Challenges to Managing Identity in the Cloud

It's not easy to keep track of the identities of all the humans, applications and machines accessing cloud-based workloads (applications, servers, storage, databases).

But there's also another challenge to overcome in the multi-cloud environment: managing identity with respect to instances, objects, and credentials created, developed and tested in the cloud.

These often have very short life spans and may be known only to the individuals who put them there. Access to them is defined not by roles and groups but by policies that need to be managed – an activity that should not take up cycles on the part of DevOps teams.

Managing the relationships between access rights assigned to users on the one hand, and ephemeral instances and objects on the other is complicated in the case of just one cloud platform. Trying to do so in a multi-cloud environment is simply not possible given conventional tools and processes.

But failing to govern this access is both dangerous and costly, as we know from cloud-based cyberattacks and the fallout of non-compliance with regulatory requirements. There are four obstacles organizations using multi-cloud environments need to overcome.

1. **Lack of visibility.** There's no easy way to look across cloud platforms to discover who and what is out there at any given time. Understanding how they relate to each other is even more challenging – but is key to developing the right access policies.
2. **The difficulty of federated access.** Lack of visibility also impedes your ability to know who has what cloud access from your enterprise system of record, such as Active Directory.
3. **Lack of automation.** Lack of visibility has even more serious implications in a multi-cloud environment where users and workloads multiply, move and change at a much faster pace than on-premises. This makes it hard to protect privileged access to the most sensitive and valuable data and processes running in the cloud.
4. **Inability to take action.** Even if organizations could get eyes on users, workloads, and access; there's no easy way to control the quality of identity governance in multi-cloud environments.

Best practices automation of identity governance can now help organizations overcome these obstacles.

Gaining Comprehensive Visibility Across a Cloudy Landscape

Discovery of who is accessing what across a multi-cloud environment requires two things:

- A complete picture of user access by tying individual cloud access to managed identities.
- A comprehensive understanding of the underlying data access models across the different cloud platforms to fully understand all access paths between users and objects.

It's not just a question of being able to discover who and what is out there in any cloud platform used. You want to be able to discover the relationships between them. Advanced automation technologies today are enabling comprehensive visibility across the entire multi-cloud environment.

The use of dashboards, as in the realm of business intelligence, provides easy, real-time insight into what's happening across your cloud platforms.

A context-rich access graph can map access and authorization controls for every data object and privileged action in the cloud in real-time. Access graphs provide actionable information about the current state of access permissions enabling centralized management.

With an end-to-end view, it becomes possible to improve identity governance in the multi-cloud environment – especially in protecting privileged access across cloud platforms.

Cloud Vendor Security Tools: Too Many Showing Too Little

Why not just use the management tools provided by the vendors of cloud platforms, like Amazon, Microsoft and Google?

First, you would have to learn as many different sets of tools as you have platforms—and, even then, be only able to see within one platform at a time.

Management tools specific to a single cloud vendor are not identity-aware across your cloud environments. They cannot detect, for example, when multiple, separate local users belong to the same identity or not.

More importantly, these tools are focused on securing just the platform itself, not what you, the customer, are running on the platform.

As any cloud vendor will tell you, it's the customer's responsibility to secure their own workloads.

Managing Federated Access to the Cloud

A best practice recommended by cloud vendors is to leverage existing enterprise directory structures to provide federated user access to the cloud. The goal is to avoid the headache of manually maintaining the lifecycle of a separate identity for cloud users when they already have an account in your enterprise system of record, such as Active Directory.

Lack of visibility across a multi-cloud environment exponentially raises the level of difficulty in achieving this goal. You never have a complete picture of what enterprise directory groups are mapped to what cloud roles and the access those cloud roles provide. Without that end-to-end visibility, you can't effectively manage cloud access.

Seeing Through a "Lens of Identity"

Comprehensive visibility across a multi-cloud environment lets you look through an "identity lens." For example, you can know that AWS user 'test10' and GCP user 'testmanager" are actually the same identity for "Jane Doe" who may be a QA manager.

Through the lens of identity, we can see a person's full cloud footprint and how they are obtaining their cloud access, whether it is indirectly from an AD group, or directly as a local cloud user.

The kind of complete visibility and identity context previously described not only provides that higher level of visibility, but also lets you effectively grant, administer, and certify federated access.

You can detect both native access and effective access through membership in Enterprise Directory groups that are mapped to cloud roles through an identity provider.

Leveraging existing federated structures, you can also map authorization to privileged access credentials, or Access Groups. Federated credentials are protected when performing privileged access actions in addition to key-logging and screen recording.

When you can easily manage federated access in a multi-cloud environment, you can centralize and streamline access control to the cloud, as well as reduce risk by minimizing the number of local user credentials present on cloud platforms.

Protecting Privileged Access Across Cloud Platforms

Access to highly sensitive and valuable information and critical processes running on-premises can be well-managed by best of breed privileged access solutions. But in a multi-cloud environment, users and services multiply, move and change at a much faster pace--fertile ground for cyberattack and human error.

Protection of privileged access in this dynamic and complex environment needs to happen by default. Advanced automation technologies can enable this by:

- Automating the creation of secure credentials for accessing workloads using valuable and sensitive information or running business critical processes;
- Automatically obfuscating and rotating keys, secrets, and passwords to minimize risk and prevent stale credentials;
- Protecting privileged access to management consoles, SSH and RDP sessions used to access cloud platforms and infrastructure.

Leveraging these technologies creates an auditable trail of what users are doing in critical cloud environments, facilitating compliance adherence.

Tightening Identity Governance Throughout the Multi-Cloud Environment

Automation is fundamental to the success of governing access across multi-cloud environments.

Replacing manual processes in governing identity reduces the risks of human error. Automation of cloud governance also improves the productivity of those responsible for assigning and overseeing identity and access in the cloud.

It starts with automating the creation of policies and "guardrails" that govern identity in a multi-cloud environment. Many policies and guardrails for complying with the most common regulatory requirements are made available out of the box.

Monitoring of the enforcement of these policies and guidelines needs to be constant in dynamic multi-cloud environments, with the ability to quickly generate alerts when violations are detected.

Enforcing least privilege practices, including the identification of excess privileges as well as unused access, is critical to ensure that each user has the right-sized access to do their job—no more, no less.

With these capabilities in place, the reporting in response to audits and investigations become faster and more accurate.

Artificial intelligence and machine learning can further automate identity governance. Activity and usage data can be analyzed and "learned" to create or adjust policies and guardrails. Identity governance becomes self-learning and data-driven.

Finally, you need integration between the identity governance you have running in the cloud with your central identity management solution to support identity lifecycle management tasks such as certifications, access requests, advanced policy roles, audit reporting, and provisioning.

Benefits of Best Practices Identity Governance in Multi-Cloud Environments

The best practices described in this white paper give you the freedom to use as many cloud platforms as you need, fitting the right platform to the requirements of different workloads--without sacrificing security.

Advanced automation can now maximize your visibility into the multi-cloud environment, so you see everything you need to see, better protect critical assets and processes, and tighten your control over identity and access everywhere in the cloud.

The effort and risk of managing identity governance and proving compliance in the cloud can be minimized as never before, improving the productivity of everyone involved in defining and controlling access to anything running in the cloud.

The volume and velocity of the cloud grow every day. Now is the time to take advantage of the new capabilities offered by automating identity governance, so you get maximum value from your multi-cloud environment while safeguarding your organization's security.

Check Out SailPoint Cloud Governance Services

SailPoint Cloud Governance gives you a comprehensive view of access to all resources across your multi-cloud infrastructure. From a single dashboard, our AI insights help you make faster, more informed access decisions, detect potential risks and easily enforce access policies for all users.

For more information, visit us at **www.sailpoint.com/solutions/cloud-governance/.**