britive

2023 STATE OF CLOUD IDENTITIES & PRIVILEGES REPORT

Assessing Cloud Native Privileged Access Challenges & Key Recommendations

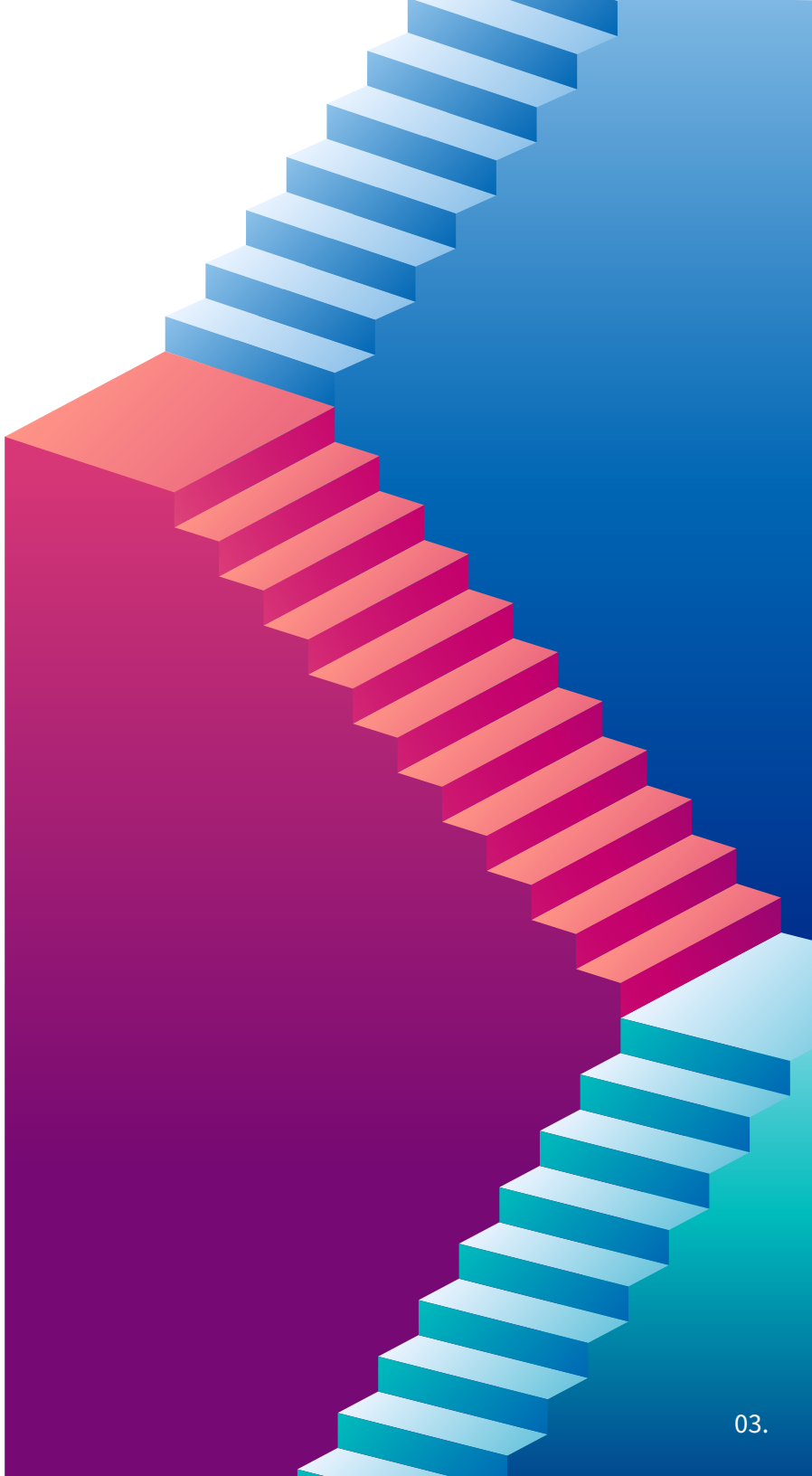
Table of Contents

Executive Summary

Businesses harness the power and scale of the cloud to innovate and expand their operations, elevate customer service, and seize a competitive edge. Doing so requires enforcing controlled access to critical cloud infrastructure, applications, and data.

To assess the state of cloud identity and privileged access, Britive surveyed over 1,000 IT and cloud operations practitioners in 2023 regarding identity and access management (IAM) and privileged access management (PAM) in the major cloud service providers (CSPs). The responses to our cloud access management survey make it clear: rapid adoption of multi-cloud environments brings with it challenges to effectively managing identities and privileges, yet many organizations have not implemented effective ephemeral cloud access.

This 2023 State of Cloud Identities and Privileges Report examines Britive's access management survey results to shed light on critical issues enterprises face in their quest for secure, scalable, and efficient multi-cloud access control. This report also provides recommendations for security, development, and cloud operations stakeholders to guide them as they seek the means to effectively secure and control identities and privileges to cross-cloud resources. The trends and challenges that emerged from the survey data are summarized on the following page, along with Britive's recommendations.



Cloud Identity Trends

- Rapid adoption of cloud infrastructure and applications has led to identity sprawl driven by development and cloud operations teams' need to spin up new cloud infrastructure and deploy code frequently.
- Thousands of permissions are exposed across the major cloud service providers with massive security and operational implications for organizations operating in multi-cloud environments.

Cloud Identity Challenges

- Organizations struggle to maintain a state of least privileged access as part of their overall security posture: just 13%[1] of companies maintain zero standing privileges regardless of the CSPs they utilize in their cloud footprint.
- Development, platform engineering and security teams are hobbled by fragmented, manual access procedures for request reviews and the granting and revocation of entitlements.
- Some organizations try to build their own cloud access tooling based on CSP-native identity frameworks—but it's costly and does not scale cross-cloud: 31%[2] of organizations cannot effectively implement just-in-time (JIT) cloud access controls without extensive development work or outside assistance.

Key Recommendations

- Eliminate static privileges and ensure least privileged access with ephemeral JIT access, reducing the risk of security breaches and insider threats.
- Enable the adoption of cloud technologies more rapidly and securely with an automated approach to controlling cloud access.
- Integrate JIT tooling with your DevOps team's tools and processes to streamline operations, reduce IT workload and eliminate over-privileged accounts consuming cloud resources, all of which saves time and resources that can be refocused on high-value initiatives.

1. Assessing the Cloud Identities & Privileged Access Management Landscape of 2023

According to the Identity Defined Security Alliance[3], a nonprofit that focuses on identity risks and facilitates community collaboration to help organizations reduce the risk of an identity-related attack, the driving forces behind the need for secure, effective, and scalable cloud access management are attributable to:

- Acceleration of cloud-native application development, including mainstream adoption of DevOps and Platform Engineering strategies and processes
- Broad adoption of cloud-hosted data platforms
- Prevalence of the virtualized workforce along with increased use of mobile devices
- Emergence of non-human, machine identities.

Unfortunately, most organizations have failed to solve the cloud access management problem in a way that balances security with operational agility. As a result, identity and access sprawl is the de-facto outcome of multi-cloud reality, leaving a wide array of privileged permissions exposed across the major CSPs with massive security and operational implications for organizations operating in multi-cloud environments.

> As more workloads shift from an on-prem world to the public cloud, how we think about protecting the perimeter must also shift from a network based to an identity-based approach. The public cloud offers an impressive array of products and services. **Ensuring both humans and machines have just the access they need to those products and services, only when they need it, becomes critically important.** Standing access simply no longer makes sense.

Thomas Rawley
Director of Cloud Architecture, Britive

Complexity and Inconsistency of Cloud Platforms Drives Privilege Sprawl

The rapid and widespread adoption of cloud computing has ushered in an era of agility and scalability for organizations. But as organizations transition to the cloud, they encounter the formidable challenge of inconsistency and complexity of identity management models that differ across individual cloud service provider platforms. Indeed, over 40,000 available permissions can be granted to identities across the major cloud CSPs[4]. Of these permissions 50% are classified as high-risk[5]. Yet, none of the major CSPs have adopted a standard access model and taxonomy for permissions that would help simplify cross-cloud identity and privileges management.

Addressing privilege sprawl, the phenomenon where users accumulate unnecessary account permissions over time, is necessary to fortify security, maintain compliance, and optimize operations in the ever-evolving cloud ecosystem. Yet DevOps teams are under constant pressure to innovate and keep their development pipelines moving to provide customers with new functionality—all of which contributes to the privilege sprawl issue. And when we consider the inconsistent and largely fragmented, manual processes for provisioning access to cloud infrastructure and apps, the result unsurprisingly is a massive over-provisioning of privileges.

This confluence of numerous permissions—including those that are high-risk—creates a situation that organizations must successfully manage if they want to protect the integrity of their data and operations cross-cloud.

2. The Pitfalls of Legacy IAM Tooling in Multi-Cloud Environments

As organizations embrace the flexibility and scalability of multi-cloud environments, they must navigate a complex maze of IAM challenges. While CSPs offer native IAM tooling tailored to their respective platforms, the incompatibility of these tools across different cloud service providers poses a significant hurdle.

Legacy IAM solutions were designed for traditional datacenters and so they struggle to keep pace with the dynamic nature of cloud environments, particularly in managing Just-in-Time access. The stakes are high: the financial and reputational impact of a breach caused by standing privileges is potentially catastrophic:

- When threat actors leverage accounts with standing privileges they gain immediate access to sensitive data, normally beyond the reach of standard users.
- Accounts with standing privileged access when taken over by attackers provide an entry into a cloud environment, lateral movement, privilege escalation, and hijacking of other accounts within the organization.

The Costly Conundrum of Native and DIY Permissioning Systems

When organizations realize that legacy IAM tooling built for datacenters will not provide the rapid yet secure access their employee base needs, they typically try to use manual processes for access requests and management using a ticketing system from request submissions by end users and status change tracking by IT and operations teams: this provides some level of automation for request oversight, but not provisioning. IT operations or security staff members must review access request tickets and then manually provision and deprovision access.

When security and operations stakeholders realize the amount of time lost to back and forth asynchronous communication using fragmented, manual processes, they consider a second option: internally design, build, deploy and maintain a “Do It Yourself (DIY)” JIT access tool based upon the various CSP-specific identity frameworks—but the pitfall here is that each CSP has a different identity framework, each of which can change over time which creates the need for software maintenance and staff time diverted by tool maintenance and end-user support.

All of this creates technical debt that will need to be addressed on an ongoing basis as the CSPs change and modify the underlying identity frameworks the organization has based its DIY JIT access tooling:

- Organizations must allocate substantial financial resources to recruiting and retaining skilled developers and identity security experts who can create and maintain these complex systems.
- The costs associated with the design, development, and rigorous testing phases can rapidly escalate, leading to budget overruns and delays. These expenses are only the tip of the iceberg, as the challenges continue well beyond the initial development phase.
- The ongoing costs associated with system maintenance, including bug fixes, security patches, and code changes required as the CSP changes its underlying identity framework and APIs over time can be substantial.
- Additionally, organizations must allocate resources for monitoring and auditing these systems to ensure they remain compliant with ever-changing industry regulations and security standards.

73% of organizations that Britive surveyed reported legacy IAM tools and **developing their own DIY access tooling** using CSP-native identity frameworks as their biggest challenge.

Comprehensive end-user support is also required for a DIY cloud access tool: building an in-house system places the onus on organizations to provide extensive support services to address user issues, manage system updates, and ensure smooth access for end-users. This entails investing in a dedicated support team, continuous training, and robust processes to handle user inquiries and resolve technical issues.

The cumulative costs of both building a DIY JIT access tool and supporting end users once the inhouse-built tool is in production are significant and divert resources away from other critical business initiatives.

Based on cost estimates by Britive, below is the cost breakdown for a typical DIY JIT tool. Building an in-house access management system may seem appealing in terms of customization, yet organizations need to consider the initial and ongoing cost to maintain and support end users using DIY JIT access tooling.

Example cost of building a DIY JIT cloud access tool:

DESCRIPTION	AMOUNT
Annual cost of three FTE software engineers for initial design, development, testing and deployment of DIY JIT tool	$525,000
Annual cost of one FTE software engineer for maintenance:	$175,000
Annual infrastructure cost per CSP to host and operate the JIT tool (In this example we are assuming 2 CSPs or $18Kx2)	$36,000
Annual cost of one FTE support engineer for end users once tool is in production:	$100,000
Cost to refactor code to support JIT access in more than one CSP ($100K per additional CSP)	$100,000
TOTAL	**$936,000**

3. Limitations of Native Access Tooling in Major Cloud Service Providers

In the realm of cloud computing, the four major CSPs—Google Cloud Platform (GCP), Microsoft Azure, Amazon Web Services (AWS), Oracle Cloud Infrastructure (OCI)—stand as pillars of innovation and scalability. These CSPs offer native tooling options to facilitate IAM within their respective ecosystems. While these native tools may seem convenient, they come with specific limitations that organizations must consider when developing a robust access management strategy.

Understanding these limitations is crucial for organizations aiming to optimize access control and security in multi-cloud environments while mitigating the potential pitfalls associated with relying solely on CSP-specific identity management solutions.

Amazon Web Services (AWS)

AWS, renowned for the breadth of its cloud computing services, has solidified its position as the premier cloud services platform. According to Britive's cloud access management survey results, 78% of organizations have embraced AWS as their cloud provider of choice. AWS's pervasive presence in the cloud landscape can be attributed partially to its proactive stance on modernizing access controls, evident in the transition from traditional IAM User setups to the more sophisticated AWS Identity Center with the incorporation of Assume Role which returns a set of temporary security credentials used to access AWS resources. These temporary credentials consist of an access key ID, a secret access key, and a security token.

However, the migration process from IAM User to Identity Center requires a substantial investment in operational resources due to the demands of automation and scalability when moving away from IAM User and adopting the AWS Identity Center.

70% of AWS survey respondents characterized their methods of gaining and revoking privileged access as “challenging.”

Creating a customized, ephemeral access system within AWS places a significant burden on an organization's resources. It's akin to purchasing a vacant plot of land instead of a move-in ready home, where the purchaser must allocate time, funds, and expertise to design and construct the entire house from the ground up: each component of this process demands meticulous planning and execution. The complexity increases when organizations operate across multiple cloud environments simultaneously.

The formidable endeavor of crafting bespoke access solutions underscores the heightened demand for a secure JIT privileged access solution is easy to set up and requires little to no maintenance. This underscores the critical need for efficient access management that can alleviate the complexities and resource drain associated with building custom access tooling for AWS.

Google Cloud Platform (GCP)

Organizations choose Google Cloud Platform (GCP) as either their sole cloud service platform or as a part of their multi-cloud environments because it is user-friendly and enables rapid application development. The flipside to ease of use and rapid development lifecycles is the risk of standing privileged access: just 6.8% of companies using GCP enforce zero standing privileges as part of their overall security posture[6].

Although some organizations do use GCP as their exclusive cloud provider, Britive's survey of GCP users found that their organizations have at least one additional cloud service platform in their development environment.

As multi-cloud usage grows, limited insight into user, group, and role privileges results in:

- Excessive privileges issued to too many identities increase an organization’s attack surface and puts critical business data at risk. For GCP users especially, gaining visibility into the privileged entitlements of their organization will strengthen security strategies and reduce cloud security risks. Britive's access management survey found that 47% of organizations have sufficient insight into privileged access in the multi-cloud, but this drops to 41% for GCP users.
- inadequate understanding and control of the user behavior in cloud platforms and applications.

Multi-cloud JIT permissioning has emerged as the new industry best practice for improving cross-cloud access provisioning and reducing privilege sprawl, but GCP does not make robust time-bound access management tooling available as a robust feature: organizations using GCP will fall behind in cloud security best practices.

Britive’s GCP study found that organizations operating in Azure and AWS were three times more likely to have implemented least privilege as part of their overall security posture than organizations operating only in GCP. These organizations require a cloud access management solution that offers multi-cloud integration and automatic, time-bound privileged access.

Oracle Cloud Infrastructure (OCI)

65% of OCI users are concerned about the attack surface of their cloud environments because of standing privileges.

OCI is a robust and feature-rich cloud environment that empowers businesses to achieve their digital transformation goals. However, when it comes to managing privileged access within OCI, many organizations struggle with the limitations of legacy tools that were designed for on-premises environments. Britive's 2023 access management survey found that 65% of OCI users are concerned about the attack surface of their cloud environments because of standing privileges[7]. Despite the prevalent concern about standing privileges, 72% of OCI users rely on native permissions tooling to grant and revoke privileged access[8].

Organizations navigating the complexity of PAM in OCI will encounter limitations when relying solely on OCI's legacy suite of IAM tooling, including Oracle Access Manager (OAM). While OAM has been a reliable solution for on-premises environments, it faces challenges in meeting the demands of a multi-cloud and OCI environment. In Britive's 2023 cloud access management study, OCI users named Ineffective Just-In-Time (JIT) Privilege Access Management as their primary challenge with Oracle Access Manager (OAM).

In sum, OCI's legacy IAM suite is the only option for access management but it was not designed to be cloud native and thus not ideal for managing cloud identities and privileges.

Integrating OCI's legacy IAM tooling with cloud-native technologies will require customization, additional components, or complex configurations. This integration effort can lead to increased complexity, longer implementation timelines, and potential risks of misconfigurations or security gaps. Given these limitations and challenges, organizations require a cloud-native approach to JIT cloud access management in OCI.

Microsoft Azure

Organizations operating in the Azure cloud ecosystem encounter a unique set of challenges when relying solely on Azure-native privileged access management tooling. While Azure offers a suite of access control tools there are complexities and limitations that can impede seamless access management and support is limited to the Azure platform and select SaaS apps.

Microsoft Entra Permissions Management (formerly CloudKnox) and Privileged Identity Management (PIM) claim to offer JIT access and monitoring, however they do not offer true ephemeral JIT access. Additionally, API support for automating administrative tasks via CI/CD pipeline integration is lacking in both Entra products. Further, Microsoft Entra Workload ID lacks multi-cloud machine identity management capabilities.

In sum, JIT access tools for Azure environments lack key functionality, limiting the number of use cases Azure's native privileged access management tooling can address. Azure's access tools are optimized for its ecosystem, making it challenging to maintain a cohesive access control strategy, especially when the need to deploy IAM tooling across other CSPs arises.

Other notable challenges with Azure's native access tooling include the intricacy of Azure's Role-Based Access Control (RBAC) system and the lack of a unified access management solution across multi-cloud environments. Azure's RBAC is an effective tool for defining fine-grained access permissions, but it demands intensive planning and execution to ensure roles align precisely with an organization's operational needs. Misconfigurations or an overly complex RBAC structure can lead to over-privileged or under-privileged users, posing significant security and compliance risks as well as potentially decreased productivity for under-privileged users.

For organizations operating in a hybrid or multi-cloud setup, managing access consistently across Azure and other cloud platforms becomes complex, resulting in operational inefficiencies, security vulnerabilities, and difficulties tracking and auditing access across an organization's entire multi-cloud environment. Consequently, organizations are increasingly exploring unified multi-cloud access management solutions to address these challenges and streamline access control in multi-cloud environments that include Azure.

4. Navigating the Journey to Secure yet Agile Multi-Cloud Access

In today's fast-paced digital landscape, the adoption of cloud computing has become more than just a trend: it's a strategic necessity. But as organizations race to harness the scalability and innovation offered by the cloud, they face a conundrum: how do they maintain a balance between rapid development and robust security? The challenges of adopting effective JIT multi-cloud access management encapsulate this struggle, where real-world breaches serve as stark reminders of what can go wrong when privilege sprawl and inefficient access processes are left unchecked.

> All of access control will **shift to focusing on the resource versus dependency on the identity.** Trying to manage static over-privileged accounts is being exposed as cumbersome, dangerous, and archaic.

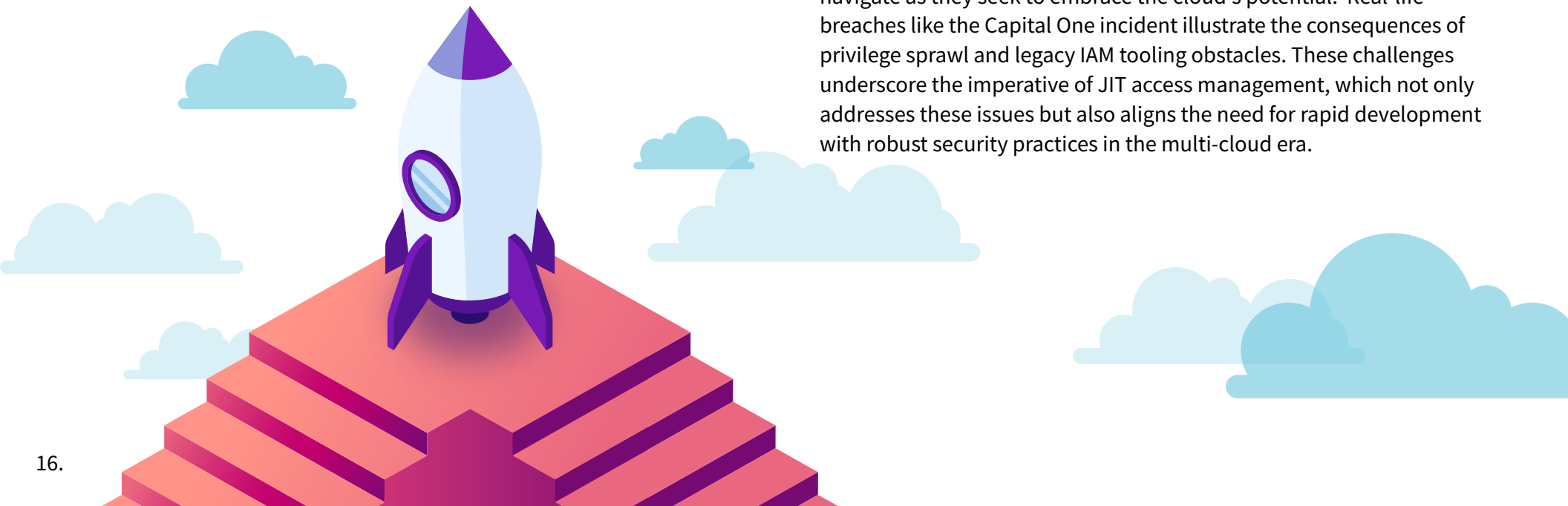
John Morton
Field CTO, Britive

Challenge 1: Privilege Sprawl in the Age of Rapid Cloud Adoption

In the quest for rapid cloud adoption, organizations often find themselves at a crossroads. On one hand, cloud resources are spun up at an astonishing pace to accelerate development cycles. But rapid provisioning of resources can inadvertently lead to privilege sprawl. The Capital One breach of 2019 stands as an example of the perils associated with privilege sprawl. In this notorious incident, an ex-employee exploited over-privileged access to exfiltrate sensitive data, exposing the vulnerabilities created by unchecked privilege accumulation. This challenge underscores the pressing need for effective JIT access management to curb privilege sprawl to prevent identity-based breaches.

Challenge 2: Rapid Cloud Adoption vs. Legacy IAM Tooling

While rapid cloud adoption is a common goal across for companies regardless of industry, the reality often presents a stark contrast. Developers, eager to leverage the cloud's capabilities for innovation, often perceive legacy IAM and PAM as barriers to rapid development. Developer perception of legacy IAM and PAM tools as blockers to rapid releases reflects the need to reconcile innovation with the need for identity and access controls—and overall hinders cloud adoption efforts. By examining the Capital One breach and others stemming from the mismanagement of identity privileges, it becomes evident that an effective JIT access management strategy can strike a balance between speed and security.



Challenge 3: Balancing Speed and Security in Development Pipelines

In the race to move at cloud speed, development and engineering teams often find themselves hampered by convoluted and fragmented IAM processes that disrupt development pipelines and inflate cloud operation costs. The friction between the need for rapid development and the necessity of secure, controlled access creates a challenging dynamic.

Organizations must optimize access management to empower development teams so they can innovate while adhering to necessary security controls. This challenge reflects the broader need for JIT access management to streamline access processes, reduce bottlenecks, and enable agile, cost-effective cloud operations.

In conclusion, the challenges of legacy IAM tooling in multi-cloud environments exemplify the complex terrain that organizations must navigate as they seek to embrace the cloud's potential. Real-life breaches like the Capital One incident illustrate the consequences of privilege sprawl and legacy IAM tooling obstacles. These challenges underscore the imperative of JIT access management, which not only addresses these issues but also aligns the need for rapid development with robust security practices in the multi-cloud era.

5. Guidance Looking Forward to 2024 and Beyond

The lessons learned from the trends and data of our 2023 cloud access management survey provide insights for the future and sets the stage for what lies ahead in 2024 and beyond. Clearly, modern JIT multi-cloud permissioning is not only a response to immediate identity-based threats but also a necessary best practice that empowers organizations to secure access to their cloud environments for the long-term. Additionally, the challenges of multi-cloud privileged access cannot be ignored:

- Organizations seek to maintain a state of least privileged access as part of their overall security posture but relatively few do, leaving their cloud infrastructure, apps and data open to identity-based attacks.
- Fragmented, manual processes access processes for request reviews and the granting and revocation of privileged access block the productivity of development, platform engineering and security teams.
- Building, maintaining, and supporting cloud access tooling based on CSP-native identity frameworks is a costly endeavor both short and long-term and does not scale across multiple cloud service providers.

As you look to help your organization overcome these challenges, look to implement JIT tooling that can be deployed quickly and works effectively to future proof your organization's cloud environments by:

- Eliminating static privileges and ensuring least privileged access with ephemeral just-in-time access, reducing the risk of security breaches and insider threats.
- Enabling the adoption of cloud technologies more rapidly and securely with an automated approach to controlling cloud access.
- Integrating with your DevOps team's tools and processes to streamline operations, reduce IT workload and eliminate over-privileged accounts consuming cloud resources, all of which saves time and resources that can be refocused on high-value initiatives.

Final Thoughts From the CEO

"As security and software builders with over 20 years of experience in the identity space, we know the challenges you face as you seek to adopt multi-cloud to innovate and build market share: we designed and built the Britive platform to provide a proactive approach to cloud access management so organizations can accelerate their growth in the cloud while safeguarding their digital infrastructure and assets against identity-based breaches and operational disruptions.

The challenges of rapid cloud expansion can be addressed with effective Just-in-Time (JIT) access that effectively provisions entitlements precisely when they are needed so you can secure identities and privileges across diverse multi-cloud environments. Realizing the business benefits of the cloud while guarding against identity-based breaches and operational disruptions can be reality and I encourage you to contact us so we can show you how."

Artyom Doghramjian

Britive, Co-Founder and CEO

Endnotes

1. Britive 2023 cloud access management survey
2. Ibid.
3. 2023 State of Identity Security Report - Identity Defined Security Alliance, www.idsalliance.org
4. 2023 State of Cloud Permissions Risk Report - Microsoft Security
5. Ibid.
6. Britive 2023 cloud access management survey
7. Ibid.
8. Ibid.

Methodology

Unless otherwise noted, the findings in this report are based on over 1,000 responses to Britive's cloud access management survey regarding privileged identity management in the major CSPs – the survey was conducted during 2023. The goal of the survey was to focus in on identity and access management as it pertains to a cloud services provider such as Amazon Web Services, Google Cloud Platform, and Oracle Cloud Infrastructure. Respondents are end users of the major cloud service providers and are on the frontlines of building, deploying and maintaining cloud infrastructure and applications. Participants were located in the United States and Europe with job titles including Site Reliability Engineer, Director of DevOps, VP Engineering and Platform Engineering Director.

About Britive

Britive is the leader in securing identities and access to cloud resources with its Cloud Identity Security Platform that empowers organizations to secure and simplify access so they can rapidly adopt cloud infrastructure, apps and data while preventing identity-based security breaches and operational disruptions. Britive's Cloud Identity Security Platform is API-based and deploys in hours, not months like legacy PAM and IAM offerings. Britive's patented technology empowers CloudOps, DevOps and security teams to eliminate the risk associated with breaches caused by over-privileged accounts. **Learn more at www.britive.com**

britive

www.britive.com