britive

Data-Driven GCP Security Strategies for Multi-Cloud Landscapes

Britive, Fall 2022

Data-Driven GCP Security Strategies for Multi-Cloud Landscapes

In the Summer of 2022, we gathered survey data from over 260 IT security professionals to better understand the current state of cloud security operations.

- 260+ professionals working at the intersection of cloud, security, and DevOps
- 50+ analysis of anonymized and aggregated cloud IaaS environments across Britive customers

Our findings confirmed industry trends: Cloud-native development is here to stay, and multi-cloud environments are on the rise. The majority of Google Cloud Platform (GCP) users are implementing one or more additional cloud environments. As organizations using GCP adapt to multi-cloud landscapes, native security controls quickly prove insufficient. To capitalize on everything GCP and other cloud and SaaS platforms have to offer, organizations need robust security tools that reduce privilege sprawl, eliminate standing permissions, and facilitate the automation and speed DevOps need to meet business objectives.

How can GCP users with multi-cloud environments seamlessly bolster their security and reduce their attack surface? By harnessing best practice security strategies that were built for cloud, provide ephemeral Just-In-Time (JIT) access controls, while protecting both human and non-human identities.

Using Zero-Trust to Knock Down Standing Privileges

Our survey showed that on average, companies have 1,300 privileged access entitlements (e.g. admin or delete controls) and an average of 26,000 total users. Bearing in mind that users aren't just humans – they can be processes, scripts and applications, too. High numbers of human and synthetic users, many with excessive, static privileges leave organizations open to attack.

Standing privileges signify security and business risks for organizations. Static access to privileged entitlements are commonplace, and most organizations struggle to eliminate (or even mitigate them).. Our data shows that GCP users are particularly vulnerable to serious exposure.

20.4% of companies using clouds other than GCP have a zero standing privilege posture.

6.8% of companies using GCP have a zero standing privilege posture.

AWS and Azure customers are **3 times more likely** to have a zero standing privilege posture than GCP customers.

The security community is starting to embrace the zero-trust principle with an increasing sense of urgency, because it helps prevent breaches by eliminating implicit trust from a system's architecture. In order to achieve a zero-trust security strategy, organizations must adopt a zero stranding privilege posture. Cloud platform users are ramping up their zero-trust models, but organizations using GCP environments are lagging behind.

The zero-trust model is wonderfully simple: when you remove trust, you reduce security risk. This strategy may be simple, but it isn't yet adopted at a high rate. According to our data, fewer than 1 in 10 organizations are currently adhering to zero standing privilege in the cloud (9.6%). Eliminating standing privilege is a strong step in the direction of adopting a zero-trust security model.

Security leaders do not know the number of standing privileges in their cloud environments. Chances are, those standing privileges are dangerously elevated and are creating security weak points.

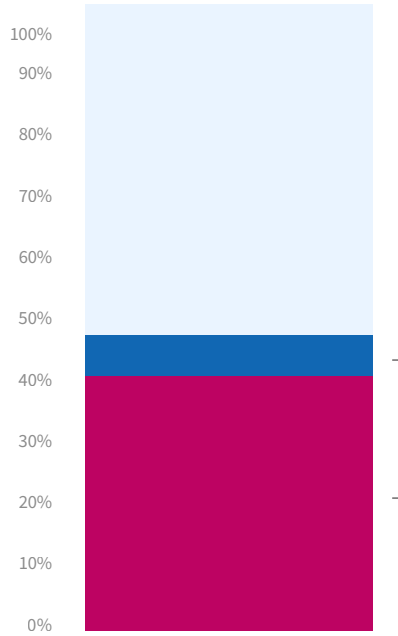
14% of security leaders have **no idea** how many standing privileges they have in the cloud

51% of organizations have static access to high-risk privileges

Gaining Visibility into Privileged Entitlements

Gaining a unified view into what's happening across different clouds is a major challenge for security leaders. It's very difficult to implement effective access controls for human and synthetic identities without insight into privileged entitlements and how they are used.

1 in 10 organizations have almost **no visibility** into privileged access in the multi-cloud



% of Organizations with Sufficient Visibility into Privileged Access in the Multi-Cloud

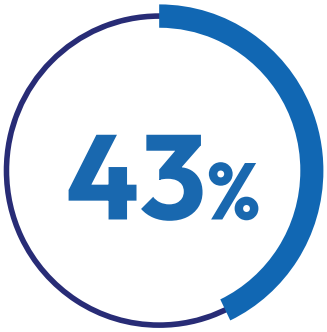
As the use of multi-cloud grows and scales, poor visibility into user, group, and role privileges results in inadequate understanding and control of the user behavior in cloud platforms and applications. Excessive privileges issued to too many identities increases an organization's attack surface and puts critical business data at risk.

47% of organizations have sufficient visibility into privileged access in the multi-cloud.

This number drops to 41% for GCP customers.

For GCP users especially, gaining visibility into the privileged entitlements of their organization will strengthen security strategies and reduce vulnerabilities in their cloud.

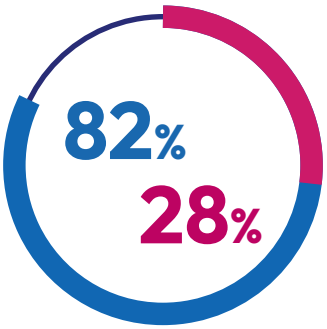
The Time Is Now for Just-In-Time (JIT) Access Controls



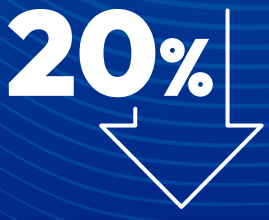
43% of organizations not currently employing JIT principles to privileged access have plans to implement it in the next 12 months

JIT access controls mitigate risks by granting and revoking privileges on a temporary, as-needed basis. Human and synthetic user requests are approved or denied based on policy, in line with the a zero standing privilege philosophy. JIT permissions expire in the minimum amount of time required to accomplish tasks, or users can manually end them sooner, which allow frictionless granted access without creating situations of over-privileged entitlement.

JIT permissioning is an excellent way to significantly reduce risk for privileged access. It is an approach that many companies are starting to adopt, or have already adopted, while many have also managed to deploy some kind of time-limited control to cloud permissions, too. However, these practices are much more achievable in single cloud environments, with the multi-cloud once again proving more difficult to secure.



82% apply some kind of time-limited controls to privileged access entitlements but **only 28%** can do it across more than one cloud environment.



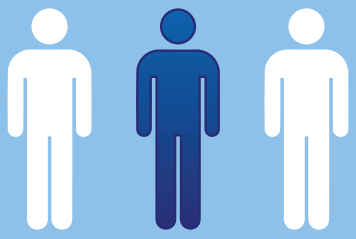
GCP customers are **20% less likely** than customers of other IaaS providers to have implemented JIT access controls.

GCP customers, particularly those building in multi-cloud environments, require a cross-cloud JIT tool that can enable ephemeral access for their human and synthetic users.

britive

Key Priorities and Strategies for Improved Multi-Cloud Security

The **#1** cloud risk concern for security leaders is having **too many standing privileges.**



1/3 of respondents listed this as their biggest concern.

This number rises to **45%** for GCP users.

The **#2** cloud risk concern for security leaders is struggling to adjust **legacy access tools** to the cloud (31%).

Top 3 Multi-Cloud Security Strategies for GCP Users:

1. Implement a Zero-Trust Model
2. Increase Visibility into Privileged Entitlements
3. Enable Just-In-Time (JIT) Access

How Britive Helps

Britive's cloud identity security platform integrates with all major IaaS, SaaS, PaaS & DaaS platforms, including Google Cloud Platform.

Learn more about Britive's security solutions for GCP users →

Increase Visibility

Identifying who has access to what is foundational to reducing the risks associated with privileged access. That is why it is essential to gain visibility across cloud environments and applications. When privileged access instances are clear and understood, teams can make decisions that enforce cloud security best practices and accelerate business priorities. Britive's unified access model provides cloud visibility and insight into misconfigurations, high-risk permissions, and unusual admin activity across your SaaS, IaaS, PaaS, and DaaS solutions.

Enable Just-In-Time (JIT) Access

The Britive platform easily integrates with your cloud services through an easy-to-deploy API. Britive mitigates risks cross-cloud by granting and revoking privileges as needed. Human and synthetic user requests are approved or denied based on policy. JIT permissions expire in the minimum amount of time required to accomplish their tasks or users can manually end them sooner eliminating the risks associated with standing privileges.

Eliminate Standing Privileges

Eliminating standing privileges is predicated on knowing where they are present. Organizations should have a plan to elevate discoverability on GCP and cross-cloud. Britive lets you monitor and manage user access, establish protocols to ensure users are not left with access if they leave the organization, and determine ways to tighten user access across cloud environments so admins can confidently grant and revoke privileges as necessary.

Request A Demo of Britive's Cloud Security Solution