The Top 5 Hidden Risks Expanding Your Cloud Infrastructure Attack Surface

In the cloud, your security is only as good as your ability to control the level of access your human and non-human identities have to your infrastructure. Since the actions these identities can take are dictated by the types of permissions you grant them, protecting against excessive permissions and quickly responding when those permissions are abused, becomes critical.

We all get that cloud makes it easy to spin up new resources, and this rapid seamlessness is the main driver for migrating to the environment. However, what we don't always take into account is the unfortunate byproduct of high automation – **permission chaos.** With over 40,000 (and growing) permissions across the key cloud platforms, it's nearly impossible to track who has what, what is being used, and on which resources.

In most organizations, there is an unfortunate and dangerous delta between permission granted and permissions used. We call that the **Cloud Permissions Gap**, and it's growing larger by the day in every cloud environment. Sufficiently addressing it means tackling the hidden risks that are creating it.

There is simply no way around it. You absolutely must work to minimize your Cloud Permissions Gap. It is an emerging attack surface that is proving to be fertile ground for both accidental and malicious permissions misuse and exploitation. The good news is that the gap is entirely avoidable – and closing it will help you achieve an ongoing least privilege policy posture throughout your cloud environment.

To help you get started on the path, we're providing intel on the top 5 hidden risks contributing to your Cloud Permissions Gap. They are:

1. Inactive Identities
2. Super Identities
3. Over-permissioned Active Identities
4. Cross-account Access
5. Anomalous Behavior

1. Inactive Identities
An inactive identity is a human or non-human user with permissions and access to cloud resources that have not been utilized for at least 90 days. For human identities, it's often because the user has left the company, changed job functions, or is no longer working on a specific project. Non-human identities, like service accounts or bots, on the other hand, usually become inactive when a proof of concept (PoC) ends or some software is decommissioned.

Regardless of the inactivity's cause, the associated identity retains a specific set of permissions that allows it to continue to perform actions—often high-risk—on critical resources within your environment. That means inactive identities pose a significant, albeit completely avoidable risk to your organization.

2. Super Identities
Super identities are human and non-human users that have been granted a super-admin role. Also referred to as a "break-glass account," they exist within virtually every organization and give users unlimited permissions and unrestricted access to all your cloud resources. The principle of least privilege recommends that super-admin accounts only be used to perform critical tasks like managing user permissions or creating or deleting databases. For all other non-critical tasks, reduced privileged administrator accounts should be used.

But that's not the practice. Most IT organizations operating in the cloud will assign these potent permissions to a broad set of identities either by mistake (e.g., a policy was changed to include all permissions) or for simple convenience (e.g., attaching a super-admin policy to a role).

Given how powerful the identities are, it's crucial you are aware of their security implications. When misused, inadvertently (e.g., mistyping a command or accidentally deleting an EC2 instance or S3 bucket) or with malicious intent, they can inflict catastrophic damage across your entire cloud infrastructure.

3. Over-permissioned Active Identities
Over-permissioned active identities are the most common hidden risk to your cloud infrastructure and the primary contributor to the Cloud Permissions Gap in any organization. They are human and non-human users with many more permissions than they need to perform their day-to-day tasks.

IT organizations continue to be overwhelmed by the proliferation of new services, roles, and permissions in the cloud. They often feel their only choice is over-provisioning an identity—mainly because it's so difficult to know or predict what permissions an identity will need and seemingly impossible to keep pace with requests. Therefore, they usually fall back on vendor-defined roles that are static by nature and broad by design. It's common and natural to err on the side of granting too many permissions in the name of productivity. After all, it's a real fear that identities won't have what they need when they need it to perform their jobs effectively. However, it's simply not an acceptable approach.

The permissions problem is compounded further when an identity finishes a project, moves to another or changes job functions. This is due to permissions rarely being re-examined for accuracy, and in most cases, a new set of permissions is assigned to identities when changes in responsibility do occur. Placing new permissions on top of existing permissions is how you get Privilege Creep (also known as "permission bloat"), which contributes to the Cloud Permissions Gap.

4. Cross-account Access
To simplify management and the need to have a different set of credentials for every environment, AWS provides IAM roles with cross-account access. Organizations leverage cross-account roles for two primary reasons: 1) Allow identities within their organization to access different environments (e.g., development, test, or production) and 2) Allow third party entities such as security tool vendors to access their account(s).

Due to the ability to create IAM roles that trust one account to assume the role in another account, an AWS account is vulnerable to attacks from other AWS accounts. Including those belonging to identities outside of your organization where you do not have any control over their environment. The inherent danger of cross-account access is when the IAM role is over-provisioned. Since these roles grant permissions to an entire account, the misconfigured permissions tied to the role can cause significant downstream effects. This creates unnecessary and powerful access to your AWS accounts by opening them to potential data exfiltration or creation and destruction of resources. Further compounding the problem is the reality that cross-account access is rarely actively maintained or revisited.

5. Anomalous Identity Behavior
Anomalous identity behavior occurs when a human or non-human identity's access pattern changes in relation to their historical activity. A good example of anomalous behavior is when an identity suddenly executes a high-risk action that they had never performed before or accessed a critical resource that they have never accessed prior. Other examples include an identity that unexpectedly logs in from a different IP address, logs in from a new or unusual geo-location, or uses a new login client to access their account.

Anomalous identity behavior is more worrisome for non-human identities because, unlike human identities that perform actions based on their intelligence within the context of the task at hand, non-human identities typically perform the same actions repetitively. So, if a non-human identity suddenly executes an action it has never performed on a resource that it has never accessed, there is a very good chance credential misuse has occurred. You should only see non-human identities performing repetitive tasks with a small number of fixed permissions. Anything beyond that signals a potential problem or danger.

Get More Info

To learn how to remediate these risks, look for future blog entries or register for our upcoming online workshop. In this free webinar, we'll examine the Five Hidden Risks that Can Expand Your Cloud Infrastructure Attack Surface. That means you'll get further insight into these exposures, in addition to solutions for all. You'll also learn how to minimize your potential for exposing your organization to this emerging and menacing cloud-native attack vector—the Cloud Permissions Gap.

In the meantime, you can uncover your cloud infrastructure risk profile by scheduling a free assessment at https://cloudknox.io/risk-assessment.

Authored by Mora Gozani and Parag Bajaria

CLOUDKNOX
333 W El Camino Real
Sunnyvale, CA 94087

www.cloudknox.io

July 23, 2020