30 Minutes of Your Time Gets You a No Cost, No Obligation Cloud Identity Risk Assessment

The Privilege Dilemma

Unprecedented levels of automation and innovation have led to an exponential growth in human and non-human identities who have, in turn, amassed tens of thousands of privileges across a growing number of platforms, devices, services etc. In effect, modern infrastructure has created "super identities" with extraordinary power that can create or destroy an entire data center with a single command.

Enterprises have gone from managing less than 100 to over 20,000 privileges across the four major cloud platforms – Amazon Web Services, Microsoft Azure, Google Cloud Platform and VMware. Of the 20,000+ privileges, over 50% are considered high-risk – if these super identities falls into the wrong hands or is accidentally misapplied, the damage can be significant.

As more enterprises move to hybrid and multi-cloud environments, over-provisioning of privileges starts to spiral out of control, leaving security and operations teams to clean up the mess. Additionally, most identities use less than 1% of their privileges to perform day-to-day operations, leaving 99% of privileges unused and wide-open to misuse or exploitation. Most enterprises are generally aware of the problem and want to fix it, but they rarely know where to start or what to do.

Their biggest pain point is visibility – they simply don't have the level of visibility required to truly understand which identities are performing what actions on their critical resources across multiple, complex and vastly different cloud operating models. Moreover, the identity teams don't have the time or expertise to keep up with the proliferation of privileges, roles, resources and services across multiple cloud platforms. It's a perfect storm.

Get to Know Your Risk

At CloudKnox, we have made it our mission to help you improve your risk posture by giving you multi-dimensional visibility and insight into *who in your environment has access to your cloud infrastructure, what operations are they authorized to execute, what actions they've taken and which resources they've impacted.*

Get Acquainted with Your Privilege Creep Index

Using CloudKnox's Privilege Creep Index, we begin the assessment by measuring your overall cloud identity risk. Updated hourly, this single metric reflects the aggregate of all high-risk privileges granted to your never-been-used identities. Once you know your risk score, you can take immediate action to reduce it.

Don't Let Inactive Identities Sneak up on You

As part of our assessment, we examine your environment for identity-related risk by looking for identities that have been inactive within the last 90 days. These inactive identities are often over-provisioned, representing a significant but avoidable risk to your cloud environment. We also provide actionable insights and recommended steps to remediate this risk.

Prune Those Pesky Privileges That Keep Creeping Up
We know that you want your active identities to be productive, but more often than not, active identities are granted many more privileges than they actually need to get their jobs done. Our assessment provides a granular look at each unique identity's granted privileges vs. used privileges. The delta not only represents a significant and avoidable risk, but also a great opportunity to right-size your active identities' privileges.

Man vs. Machine: Non-Humans Are Outnumbering Human Identities by 20:1
The risks associated with non-human identities such as service accounts and bots are inherently different then human identities and require even more rigorous oversight. Since non-human identities don't have the capability to adapt their behaviors to changing scenarios, any change in behavior such as performing a new action on a new resource may signal a potential threat. The assessment will conduct a detailed review of your non-human identities to determine the likelihood of privilege credential misuse.

Who's Handling Your Critical Cloud Resources?
This assessment also considers your risk posture through the resource lens to quickly ascertain which entities accessed critical resources and what type of actions—especially high-risk actions—were performed. CloudKnox models multiple access paths to resources by mapping all human and non-human identities, roles, groups and services that have authority to perform actions on these resources.

Your Risk Assessment Benefits
With a no cost, no fuss cloud identity risk assessment, you will be able to:

– Understand your current cloud identity risk profile

– Identify the areas of greatest risk and opportunities for mitigation

– Improve your risk profile with prescriptive recommendations

Key benefits include:

– Immediate visibility into your cloud identity risk

– Bridge the gap between security and operations teams

– Prioritize cloud security projects, budgets and resources

– Quickly improve your organization's overall cloud security posture

– Meet numerous IAM and PAM compliance requirements

About CloudKnox Security
CloudKnox Security is the only Cloud Security Platform built from the ground-up to support the monitoring and management of identities, actions, and resources across hybrid and multi-cloud environments using an Activity-based Authorization model. Through a single extensible platform, CloudKnox transforms how organizations implement the principle of least privilege and empowers security teams to proactively address accidental and malicious credential misuse by continuously detecting and mitigating the insider threat risk. CloudKnox is based in Sunnyvale, CA.

May 17, 2021

www.cloudknox.io