CLOUDKNOX

Success Story
gojek

How a Fast-Growing Cloud Company Is Taking Control of Its Permissions

In today's cloud-based economy, a company can grow quickly, add services and expand its cloud infrastructure before realizing it has lost track of the exploding number of identities and permissions that have access to its data. That situation creates a considerable risk, as over-permissioned human and machine identities create the possibility of expanding the attack surface for malicious or unintentional misuse. Additionally, inactive accounts and identity policies also provide an opportunity for attackers to exfiltrate sensitive and confidential company information.

GoJek is a good example of a company taking control of its permissions. The Indonesian-based company started in 2010 as a call center operation in Jakarta for ride-hailing services. It introduced its GoJek app in 2015 with four services, and has since become a "decacorn" in Southeast Asia, with more than 20 services (including ride-hailing, online payments, food delivery and consumer services) in five Southeast Asian countries. Between 2016 and 2019, GoJek's transactions grew by 1,000% and its app—dubbed a Super App as a single portal for anything from transportation and logistics to daily services—by then had been downloaded 170 million times.

While business was booming, GoJek's Cloud Security leaders realized developers had significantly more permissions than they were using in what had become a multi-cloud infrastructure with approximately 3,500 employees, 300 projects and 750 project owners. Additionally, the team realized that former employees' identities were still active, as well as orphan identities created as a result of multiple prior projects. They knew this would likely cause a massive security risk if it was not addressed immediately.

"Checking for inactive identities and roles, and granted versus used permissions for active users became a daily activity which consumed a significant amount of our time and left very little availability to execute on new strategic initiatives," said Sanjog Panda, GoJek's Senior Staff Information Security Engineer.

In search of a platform that could provide a comprehensive view of its entire cloud infrastructure and an efficient way to identify and right-size over-permissioned identities across the enterprise, GoJek zeroed in on CloudKnox.

Permissions Run Amok

Permissions creep—which in many cases might more accurately be called permissions sprawl—has become one of the most significant threats facing cloud infrastructures. The number of identities in cloud infrastructures has grown sevenfold in recent years, with non-human identities (such as service accounts and bots) accounting for most of that growth. And that growth is only going to accelerate.

Across the four major cloud platforms—AWS, Google Cloud Platform (GCP), Microsoft Azure and VMWare vSphere—organizations manage an average of more than 40,000 permissions. According to one study, 95% of identities are over-provisioned, and in most cases using only 2-5% of the permissions they have been granted. Along with those inactive and orphan accounts, that leaves a lot of permissions—particularly high-risk permissions—open to exploits should attackers gain entry. Verizon's 2020 Data Breach Investigations Report found that more than 80% of hacking-related breaches involved the use of lost or stolen credentials.

On the heels of the fast expansion of its business, GoJek recognized the importance of getting a tight grip on cloud infrastructure permissions management, Panda said. Yet, prior to enlisting CloudKnox, the company ran into a number of hurdles when trying to manage

identities and permissions in a multi cloud and hybrid cloud architecture. Without a single sign-on between their two clouds, AWS and GCP, or the ability to grant permissions on-demand, even managing a single user could become a complicated process that greatly impacted productivity. For example, an employee who was given access to a GoJek system still had to ask AWS for a username and password. If that person left the company, someone had to remember to delete the account—if they don't, that user still has access to AWS. Because the cloud infrastructures had to be handled separately, permissions management couldn't be centrally managed by only one team, Panda said.

Moving to CloudKnox's integrated platform gave GoJek the means to enforce least privilege principles across its multi-cloud and hybrid cloud infrastructure, eliminating over-permissioned accounts while also being able to easily grant the appropriate permissions on-demand when requested.

"Now, if I am the owner of a project and somebody asks me for a set of permissions or a pre-defined role, I can give that right away, across GCP and AWS. It helps us accelerate the overall process and makes it very efficient. My developers and project owners are very happy and we are able to maintain a robust security posture for all the identities," said Panda.

GoJek Implementation
GoJek's implementation of the CloudKnox platform currently is tied to the realignment of the company into its three major areas of services: ride-hailing, financial services and services that involve third-party merchants - each of these services are treated as separate entities of the company. The benefits are already becoming apparent. CloudKnox enables GoJek to automate their audits of project accounts, a process which previously took a week or more, and was completed sporadically. Now, they are performed weekly and the time spent generating reports "has come down to next to zero," said Panda.

CloudKnox also enables GoJek to keep a close track of its PCI score in order to identify trends. Most importantly, GoJek has been able to gain visibility into their growing infrastructure and full control over their accounts. Permissions can be added or deleted from the CloudKnox console while staying within the "permissions boundary" of only allowing the authorizations each identity actually requires. Panda said that as the implementation of CloudKnox continues across the company, GoJek will also leverage the permissions on-demand feature. Ultimately, it is the company's goal to get to a Zero Trust model of identity and access management, which will be made possible through CloudKnox's single solution to manage identities and permissions across their multi-cloud infrastructure.

About CloudKnox
CloudKnox offers a full range of automated identity management in its Cloud Infrastructure Entitlement Management (CIEM) Platform, which can be deployed in about 30 minutes and operational in a day. Its services include assessments to quickly determine an organization's IAM risk profile and reveals the "super identities" within the infrastructure, such as super admins who have access and high-risk permissions across the infrastructure, and thus the ability to inadvertently cause damage.

In addition to identifying identities and permissions, CloudKnox's Just Enough Privilege (JEP) Controller automates and simplifies the rightsizing of permissions across multiple commercial clouds, including the four major providers. The platform also delivers continuous monitoring to locate and remediate over-permissioned identities and simplifies permissions-on-demand and just-in-time permissions which can otherwise be resource-intensive. If someone leaves the company and/or their account goes unused for a while, CloudKnox's anomaly detection will notice and send an alert.

At the core of much of CloudKnox's services is its Privilege Creep Index (PCI), which aggregates information on high-risk permissions—those that could result in a serious breach—into a single metric. Once an organization knows its high-risk score, it can remediate over-permissioned identities in a matter of minutes.

May 19, 2021

www.cloudknox.io