CLOUDKNOX

Solution Brief

CloudKnox Cloud Permissions Management Platform

> **“CloudKnox offers us a unique permission management solution** that has immediately transformed the way we uncover over-provisioned identities, as well as the way we rightsize and enforce least privilege policies across our AWS environment.”
>
> ***Jon Roller***
> *Chief Information Officer*
> *Horsley Bridge Partners*

EXCESSIVE PERMISSIONS HAVE BECOME YOUR NEW ATTACK SURFACE

Cloud Infrastructure is the foundation of every enterprise today, and the ability to derive consistent value from it depends on how well you are protected from accidents, malicious insiders, and compromised credentials. Enterprises often know how vulnerable they are, but don't have the skill set or tools to adequately address the exposure. Over time, the problem becomes increasingly acute as organizations expand their cloud footprints without establishing protocols and capabilities to properly assign, manage, and monitor human and non-human identity permissions across their cloud environments. As a result, they accumulate permissions far exceeding technical and business requirements. This creates a dangerous scenario whereby the probability of an incident due to permission misuse—whether intentional or not—increases along with cloud adoption rates.

Traditional security models are expanding the threat surface

Because of the more dynamic nature of these complex cloud environments, legacy practices and protocols such as role-based access controls (RBAC) that are used to define what roles and permissions identities get access to only aggravate the problem by allowing overprovisioning to spiral out of control. Moreover, with the growth of cloud, IT and Security teams have gone from managing less than 100 permissions just a few years ago to managing an average of more than 40,000 permissions across the four major cloud platforms. Of those 40,000 permissions, more than 50% are defined as high-risk because their associated actions could cause catastrophic damage if used improperly.

A high-risk permission is defined as **any action performed by an identity or resource** that can result in any of the following:

- Data leakage
- Service disruption
- Service degradation

The problem is as simple as it is devastating: overprovisioning has become the norm, yet the typical identity needs less than 1% of its permissions to perform daily required tasks. That leaves 99% of all permissions unused and unchecked for misuse or exploitation.

CLOUDKNOX

Solution Brief

The CloudKnox Cloud Permissions Management platform was **built from the ground up to support a continuous and adaptive framework for managing identity and resource permissions.**

The **Privilege Creep Index** is a single metric that **measures your ability to implement the principle of least privilege** (PoLP) across your hybrid and multi-cloud environments.

MANAGING PERMISSIONS MUST BE DYNAMIC

The CloudKnox Cloud Permissions Management platform was built from the ground up to support a continuous and adaptive framework for managing identity and resource permissions. This risk-based decision-making approach enables your security and cloud infrastructure teams to continuously create, monitor, and enforce the principle of least privilege across their hybrid and multi-cloud deployments. This ensures every human and non-human identity, and resource that can access infrastructure, only has the permissions needed to perform their daily tasks.

Activity-based Authorization – a paradigm shift

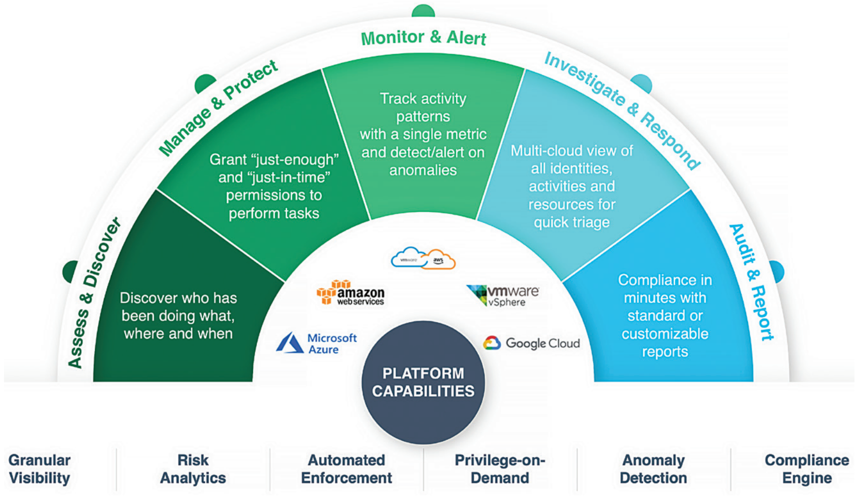
You can benefit from the only platform combining the granular visibility of real time and historical identity and resource activity with a simplified and automated enforcement mechanism needed to continuously implement and maintain a least privilege posture across hybrid and multi-cloud deployments. CloudKnox does this by abstracting out all activity across four very complex and different cloud operating models. This allows CloudKnox to deliver easily consumable data that helps you take immediate action, thereby significantly reducing your threat surface.

Discover and Assess

With a **Privilege Creep Index,** CloudKnox's **Dashboard** and **Activity Analytics** modules help you understand your risk level for your identities and resources at both the account (e.g., AWS) and individual identity levels. This single metric is a function of the number of unused high-risk permissions and the number of resources that can be accessed.

Cloud Permissions Management Platform

Continuous detection and remediation of over-provisioned identities and resources


Monitor & Alert
Manage & Protect
Investigate & Respond
Assess & Discover
Audit & Report
Track activity patterns with a single metric and detect/alert on anomalies
Grant "just-enough" and "just-in-time" permissions to perform tasks
Multi-cloud view of all identities, activities and resources for quick triage
Discover who has been doing what, where and when
Compliance in minutes with standard or customizable reports
amazon web services
vmware vSphere
Microsoft Azure
Google Cloud
PLATFORM CAPABILITIES
Granular Visibility
Risk Analytics
Automated Enforcement
Privilege-on-Demand
Anomaly Detection
Compliance Engine

The Activity Analytics module offers a multi-dimensional view into your environment by giving you the ability to see it from three perspectives: identity, action (permission), and resource. For example, you can execute an in-depth historical analysis of every identity and their activity by examining:

CloudKnox lets you take immediate action to **mitigate identity and resource risk without the heavy operational costs** associated with the manual implementation of least privilege policies.

- Permissions granted
- Permissions used
- Permissions not used
- Resources accessed

Access to real activity data helps you quickly uncover the true permissions gap by comparing permissions granted vs. permissions used—which is a critical first step to implementing least privilege policies.

From the resource perspective, you can quickly ascertain which identities accessed a specific resource and what type of actions were performed on it. And if you want to examine your environment from an action point of view, you can easily determine which permissions (e.g., aws s3 sync s3://sensitive_data_bucket) were used on a specific resource (e.g., S3 bucket). Based on this data, CloudKnox creates activity profiles for each unique identity and resource, and these profiles are then used as a baseline to monitor for, and detect, anomalous behavior.

Manage and Protect
CloudKnox lets you take immediate action to mitigate identity and resource risk without the heavy operational costs associated with the manual implementation of least privilege policies. The patented **JEP (Just-Enough-Privileges) Controller** module provides you the ability to automate the permission rightsizing process across AWS, Azure, Google Cloud, and VMware (vSphere, NSX) and VMware on AWS. The JEP controller also enables new permissions to be granted on-demand for just-in-time access to a specific cloud resource for a predetermined period. In addition, the JEP Controller includes an auto-remediation feature that allows the automated revoking of all unused permissions on a regular basis for a predetermined set of identities.

JEP Controller use cases include:

- **Creation** of least privilege custom roles based on an identity(s) and resource(s) historical activity
- **Pruning** unused permissions from an identity's or resource's profile
- **Deletion** of inactive identities or reassignment to read-only access

Monitor and Alert
CloudKnox's risk monitoring capability continuously collects the permissions and activity details of your unique identities and resources and updates your risk score on the hour. It also looks for any anomalous activity, such as an identity that suddenly performs a high-risk action, logs in from a different IP address, uses a new login client, or accesses a resource for the first time. CloudKnox then flags any deviation from the norm or suspicious behavior in your portal and sends you alerts via email or a third-party SIEM or SOAR tool.

Investigate and Respond
CloudKnox collects your security events across multiple cloud environments to create a context-rich view of identity and resource activities for analysis. Forensic reports around identities, actions, and resources support rapid investigation and comprehension of the total impact and demonstrate how best to respond. From the data, you can create, update, and export policies to drive automated least privilege response to keep your environment safe.

The CloudKnox time-to-value is immediate … you immediately gain a three-dimensional view of all your human and non-human identities, their actions, and the resources they have accessed.

333 W El Camino Real
Sunnyvale, CA 94087

www.cloudknox.io

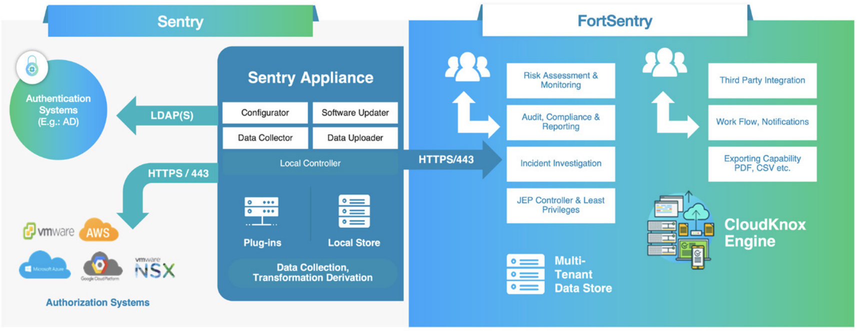
May 18, 2020

Audit and Report

You can keep ahead of the risk over-provisioning poses to your environment and demonstrate compliance to auditors immediately with both out-of-the-box and fully customizable reports. You can create and modify reports to meet the specific needs of your organization, including those that may come from industry or regional compliance mandates. You can also run reports on demand or set up a schedule to run and distribute specific reports by email.

INTEGRATED AUDIT AND COMPLIANCE ENGINE

You can leverage the **Audit and Compliance Engine** to continuously monitor cloud resources for configuration drift and regulatory violations. With hundreds of built-in policies to measure industry-standard best practices, including CIS and AWS Well-Architected Framework, as well as the ability to craft custom policies, CloudKnox captures and records a continuous historical record of your compliance posture. Moreover, you can download fixes and remediate misconfigured polices for yourself or have CloudKnox address them on your behalf.



CloudKnox Platform Architecture

TECHNOLOGY AND IMPLEMENTATION

The CloudKnox Permissions Management platform is comprised of two components: **CloudKnox FortSentry** and the **CloudKnox Sentry Virtual Appliance.** FortSentry is a multi-tenant SaaS service hosted in the cloud and represents the central portal where CloudKnox is administered. The Sentry appliance is a Linux virtual machine that collects all identity permissions and activities from each cloud platform and uploads this data to the FortSentry system.

Rapid time to value

The CloudKnox time-to-value is immediate. Once CloudKnox is installed, in an average of 30 minutes or less, it immediately begins pulling data from your cloud platform(s) via the Sentry appliance.

It typically takes 24 hours for us to pull an entire 90-day activity data set from one cloud platform such as AWS. But once the data has been exported, you immediately gain a three-dimensional view of all your human and non-human identities, their actions (permissions used), and the resources they have accessed.

Get a **free** risk assessment

Give us 30 minutes of your time, and **our team of cloud security experts will uncover your identity and resource risk profile –** in less than 24 hours.

Contact us at **https://cloudknox.io/risk-assessment/**