CloudKnox Security
Permissions Management Platform for Cloud Infrastructure

CloudKnox overview

The CloudKnox Permissions Management Platform (2020 Gartner Cool Vendor) is an entitlements management platform that protects all cloud infrastructure resources and identities by providing comprehensive visibility, automated remediation, and continuous monitoring of permissions (granted versus used) using patented Activity Based Authorization technology.

By bringing together data from every account in your company’s AWS environment, CloudKnox provides a continuous and adaptive framework for viewing, detecting, and remediating over-permissioned human and non-human identities.

Through a risk-based decision-making approach, security operations and cloud infrastructure teams can continuously create, monitor, and enforce least privilege policies across all AWS accounts in a single dashboard. This ensures that every identity that can access cloud infrastructure only have the permissions needed to perform their daily tasks and nothing more.

Benefits

**Rapid Deployment** - Deploy in 30 minutes and be operational in 1 day

**Immediate ROI** - Reduce cloud security and infrastructure operational costs by up to 80%

**Single Integrated Dashboard** - Unified cross-cloud view of all identities, actions and resources

**Comprehensive Visibility** - Gain insights into effective permissions and usage of all identities and resources

**Automated Remediation** - Automatically enforce least privilege policies by eliminating unused entitlements. Grant permissions on demand instantaneously with an integrated approval workflow.

**Continuous Monitoring** - Measure and Monitor activity and user behavior utilizing AI-ML, alert and remediate anomalies

**Integrated audit and compliance engine** - Continuous security and compliance controls & anomaly detection

Product features

**Entitlements Management**
- Comprehensive visibility into identity and resource permissions gap
- Cross account access visualization
- Automatically remediate over-permissioned identities (user, role, group, resource) to create least privileged roles/policies
- Deliver Permissions-on-Demand & Just-in-Time Permissions which are time and resource bound

**Anomaly Detection and Response**
- Detect anomalous behavior with infrastructure identities and resources
- Automated Alerts and remediation for anomalies
- Audit trail and reports

**Integrated Audit and Compliance Engine**
- Continuously monitor cloud resources for configuration drift and regulatory violations
- Measure industry-standard frameworks - CIS, NIST, PCI, AWS Well-Architected Framework and craft custom policies
- Capture and record continuous historical record of your compliance posture
- Download fixes and remediate misconfigured polices automatically
How it works

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 to pull an entire 90-day CloudTrail data. But once the data has been exported, customers can immediately gain a three-dimensional view of all their human and non-human identities, their actions (permissions used), and the resources accessed.

Differentiators

- Automatically enforce least privilege policies by eliminating unused entitlements
- Grant permissions on demand instantaneously with an integrated approval workflow
- Integrated with Identity Providers like Okta, ADFS, Ping, Azure AD to give full visibility into SAML roles access
- Only CIEM solution with enterprise customers integrated into AWS Control Tower and AWS Config
- Monitor third party access into accounts through direct and role chaining with cross account roles
What our customers are saying

"CloudKnox provided insight into identities where full administrator access was granted and gave us guidance as to help account administrators proceed in the path of least privilege access. CloudKnox also provided an easy means to create and deploy these new more restricted policies reducing workload and saving significant time."

-Jay Brothers, IAM engineer, Guidewire

Data Points

80% ROI

30 mins Deploy

24 hours Fully operational

Additional Resources

- [CloudKnox Explainer Video](#)
- [CloudKnox Risk Assessment datasheet](#)
- [CloudKnox Platform datasheet](#)
- [AWS partner page](#)

Solution available in [AWS Marketplace](#)