REPORT REPRINT

Coverage Initiation: Upstart CloudKnox looks to control 'privilege creep' for public and private cloud resources

JULY 22 2020

By Garrett Bekker, Fernando Montenegro

The vendor has developed an offering – and proprietary protocol – for analyzing and enforcing least privileged access policies for both human and machine identities across private and public cloud environments (AWS, Azure, Google Cloud Platform and VMware). CloudKnox calls it 'activity-based authorization.'

451 Research®
Now a Part of
S&P Global Market Intelligence

Introduction

For many organizations, as soon as public cloud adoption takes hold beyond initial experiments, one of the biggest security challenges is managing privileged identities and dealing with excessive permissions to cloud services and accounts. Static role-based access controls are a common way to figure out what resources an identity can access, but static roles are of limited help in the public cloud, which may have hundreds or thousands of permissions – with as few as one percent of them actually being used or necessary. This set of unused additional permissions creates a significant vulnerability that is nearly impossible to track and manage using manual techniques.

CloudKnox has developed a platform – and proprietary protocol – for analyzing and enforcing least privileged access policies for both human (e.g., employees, third-party contractors) and machine identities (e.g., service accounts, resources) across private and public cloud environments (AWS, Microsoft Azure, Google Cloud Platform and VMware). The firm calls it 'activity-based authorization.'

451 TAKE

CloudKnox was basically founded to answer four fundamental questions: How many separate identities are running across my public and private cloud environments? What are those identities entitled to do? What activities are they actually doing in practice? Which resources have they impacted or touched? These questions are surprisingly hard to answer at scale, particularly as cloud service providers continue to add more services to the mix – AWS, for example, now offers over 200 separate services. The key question for any vendor focused on providing a layer of security for cloud environments, however, is to what extent that extra layer will become part of the basic functionality of that cloud platform's offerings.

The goal, then, is to avoid obsolescence by innovating at a faster rate, and by offering cross-platform and hybrid cloud capabilities that cloud platforms alone can't provide. CloudKnox seems to be on strong footing on both counts, although the market is quickly becoming crowded and we expect more entrants to emerge. We also suspect that incumbent identity and access management (IAM), identity governance and administration (IGA) and privileged access management (PAM) providers will eventually come knocking as they look to extend their reach into the cloud.

Context

Sunnyvale, California-based CloudKnox was founded in 2016 by CEO Balaji Parimi, who previously served as VP of engineering and operations at datacenter analytics firm Cloud Physics and as an engineer at VMware. The startup's management team and backers have a strong cybersecurity pedigree, including COO Raj Mallempati, who has held executive marketing roles at Malwarebytes, MobileIron, Riverbed and VMware; and newly appointed VP of sales John Donnely, who has held executive sales leadership roles at MobileIron and Symantec, and also served as a partner at Wing Venture Capital.

CloudKnox has raised a total of $22.8m in funding, including a $10.8m round in 2018 led by ClearSky Security, Dell Technologies Capital and Foundation Capital, and a $12m round in January led by Sorenson Ventures. The company has also taken a strategic investment from Wipro Ventures as part of a partnership with Wipro Limited. Former RSA Security executive chairman and CEO Art Coviello serves as an adviser. The company has been granted patents for its Activity-Based Authorization Protocol and its ability to detect anomalous permissions misuse across hybrid multi-cloud environments.

Products

Conceptually, CloudKnox performs two basic functions: Visibility into access permissions and activity, and remediation of excessive permissions within hybrid and multi-cloud environments. This may seem straightforward on the surface, but in reality, understanding what has been granted to an identity can be hard to answer since each cloud supplier has its own IAM architecture. The differences include concepts, best practices, policy language, and more. Some of the challenges include policies that can be directly attached or inherited from groups, as well as cross-account access and role-chaining that can lead to nested roles and identities that can grant access in unintended ways, and that are difficult to fully comprehend.

To address this problem, CloudKnox pulls access entitlement records and activity logs directly from cloud suppliers, as well as identity data stored in cloud-based directories from identity providers (IDPs) like Okta, Azure Active Directory, Ping Identity and OneLogin. The vendor has developed a proprietary protocol – Activity-Based Authorization – that can analyze identities' permissions and activity from disparate authorization systems across AWS, Azure, GCP and VMWare.

CloudKnox refers to its offering as the Cloud Permissions Management Platform, the main component of which is the FortSentry console. Architecturally, customers have two deployment options for collecting the required access and identity data. The most common deployment choice is a Linux VM – the vendor's Sentry appliance – that can be installed on a customer's cloud environment (currently AWS, Azure, GCP and VMware). The second option is a full multi-tenant architecture that runs on AWS (although a single-tenant offering is available) and relies on 'agentless collection,' which essentially creates a cross-account role for each of the customer's accounts with the cloud supplier.

Sentry enumerates the machine and human identities in that environment, as well as their permissions, actions and resources they can access, and sends the data to the FortSentry console for analysis. CloudKnox claims that the initial deployment is often less than an hour, and that the historical data collection process typically takes a few hours to complete. Since the vendor starts with the collection and analysis of historical data, it claims that the time needed for tuning and training the models is reduced to less than one day.

One of the outputs of the visibility analysis is what CloudKnox dubs a 'privilege creep index' that helps firms measure their progress in terms of controlling excessive permissions. The index is a function of both the number of unused high-risk permissions and the total number of resources that an identity can access. The higher the number of unused high-risk permissions, the higher the index score. The index can also drill down into specific human and nonhuman identities to analyze their activities.

CloudKnox offers four remediation methods. The first is to create least privileged policies by looking at historical usage and adjusting permissions accordingly. The second is to perform automated removal of all permissions that are not deployed by any entity. The third method is to grant each identity with the least amount of privileges required, and only grant 'high-risk privileges' on request and after approval from a manager – and only for a defined time period, such as four hours to perform maintenance on a server. Lastly, firms can remove permissions manually.

Strategy

CloudKnox uses a two-tier indirect sales model employing both security resellers such as Guidepoint Security and Optiv as well MSSPs. Pricing is a yearly subscription based on two variables – a base platform fee for each CSP and then a variable cost based on compute resources.

Competition

CloudKnox bills itself as a cloud infrastructure security vendor, but in our view it also has some adjacencies with cloud security posture management, PAM and IGA. To the extent that it enforces least privileged, the company also arguably falls within the emerging zero-trust umbrella.

The most direct competitor for CloudKnox is likely fellow startup Ermetic, which similarly discovers all of the machine and human identities in primarily public cloud environments, as well as the privileges, actions and resources they can access, and then attempts to identify and remove excessive privileges. Sonrai Security positions itself as an identity and data governance provider for AWS, Azure, GCP and Kubernetes that can also discover and classify structured and unstructured data. Obsidian shares a similar focus on remediating excess permissions for cloud resources but is more concentrated on SaaS apps than public cloud environments. Britive offers visibility into permissions and enforces just-in-time access policies across both public cloud and SaaS uses cases.

CloudKnox could eventually vie indirectly – even if just for budget dollars – with established players with CSPM offerings such as Palo Alto Networks, Trend Micro, Sophos, Check Point, Rapid7, VMware, Qualys, Netskope, Aqua Security, Zscaler, as well as smaller firms like Turbot, DisruptOps, JupiterOne, Fugue, Threat Stack, Cavirin, Lacework, and others. While many of these vendors start with a focus on compliance benchmarks, there is increased interest in addressing user roles and permissions.

To some extent, CloudKnox's functionality overlaps with – and also potentially complements – companies in the PAM space such as CyberArk, BeyondTrust, Centrify, One Identity and Thycotic, as well as Okta, STEALTHbits, Remediant, Xton and Wallix, some of which have added functionality to address public cloud environments. IGA specialists such as SailPoint, Saviynt and Avatier could also lay claim to somewhat similar functionality, although with less direct applicability to the unique requirements of public cloud services.

SWOT Analysis

STRENGTHS

CloudKnox works across both public multi-cloud and hybrid environments, and can pull identity data from a broad range of CSPs and IDPs. In addition to discovery and visibility into permissions, the company offers multiple means of manual and automated remediation as well as multiple anomaly-detection methods.

WEAKNESSES

Although CloudKnox has a strong management team and backers, it is still an early-stage startup in a nascent, albeit promising market. The vendor is also focused primarily on public and hybrid cloud, with limited support for SaaS applications.

OPPORTUNITIES

As cloud suppliers continually add new services, the number of related permissions and machine identities should expand exponentially. And as workloads continue to migrate to public cloud, security will remain a front-burner issue for most firms. If the CSPM sector serves as any guide, vendors in this emerging category will likely become M&A fodder for larger security incumbents and IAM/PAM vendors.

THREATS

Cloud providers themselves will always pose an existential threat. CloudKnox will need to out-innovate both the cloud suppliers as well as a growing rank of would-be rivals.