Varun Khadayate

A016

B. Tech (CsBs) TY

Aim

Case study on Any one Cloud Security tool

Cloud Security refers to a set of policies, technologies, applications, and controls utilized to protect virtualized IP, data, applications, services, and the associated infrastructure of cloud computing. Most organizations are more concerned with hitting product delivery deadlines than handling development security right from the very start, often relegating security toward the end of the production schedule. The rationale behind this false assumption is that dealing with security may cause production delays. While this assumption may have been correct years ago, new tools and services that smoothly integrate into the CI/CD pipeline have matured to a point where this is no longer the case. Beyond baseless fears, the cloud infrastructure is a vast wonderland of powerful features and capabilities representing a complex weave of technologies that are impossible to secure without solutions.

There are Six types of cloud securities:

1. **CASB – Cloud Access Security Brokers**
2. **SAST – Static Application Security Testing**
3. **SASE – Secure Access Service Edge**
4. **CSPM – Cloud Security Posture Management**
5. **CWPP – Cloud Workflow Protection Platforms**
6. **CIEM – Cloud Infrastructure Entitlement Management**

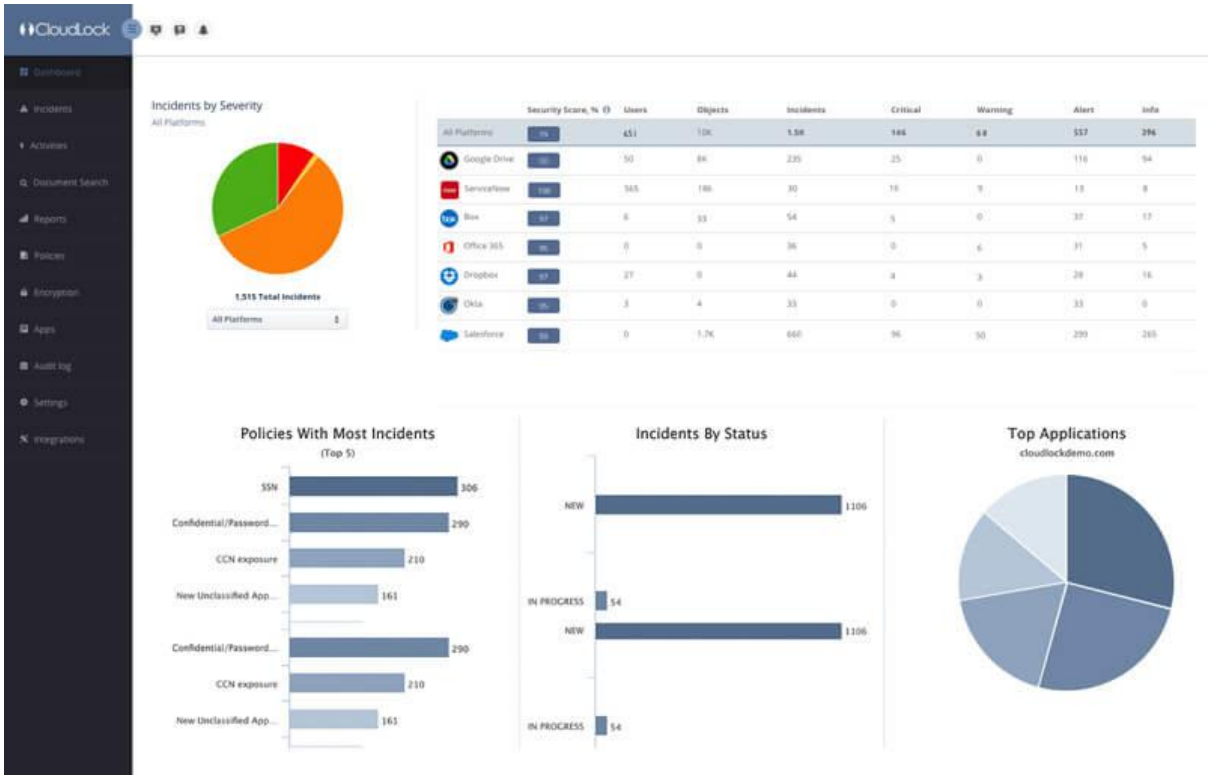
Cisco Systems Cloud lock

Cisco's Systems Cloud lock offers an enterprise focused CASB solution to safely transfer and manage users, data, and apps on the cloud.

Cloudlock is a cloud access security broker (CASB), meaning that it provides cloud protection based on User and Entity Behavior Analytics (UEBA). Cisco is known as a networking and virtualization giant; to this effect, the company has been making strategic acquisitions such as Cloudlock for the purpose of building up its Cisco Umbrella suite of security solutions. Securing the cloud is a relatively new business process. When companies started migrating their enterprise networks to the cloud a few years ago, the security concerns were still heavily focused on endpoint protection, which is no longer sufficient. These days, business owners whose data networks are managed in the cloud should consider solutions such as Cisco Cloudlock, an advanced cloud infrastructure security platform that offers identity protection, breach mitigation, malware detection, and compliance policy implementation. One of the challenges faced by cloud security software developers is that attack surfaces have become considerably large. Cisco Cloudlock addresses this challenge by means of smart API solutions that mitigate risk according to intelligence collection and policy-based security measures. The Community Trust Rating feature, for example, assigns crowdsourced security scores to cloud accounts, shared files, and websites that may have been compromised or are deemed to be suspicious. Other Cloudlock features include:

- Easy integration with major cloud apps and services such as Slack, Dropbox, Office 365, Salesforce, G-Suite, and others.
- Smart firewall powered by machine learning algorithms and community ratings.
- Full visibility of the entire network, including virtual machines, apps, accounts, endpoints, and mobile users.

Pricing for Cisco Cloudlock is based on the number of apps and users; subscription packages are available for one to three years, and free interactive demos can be arranged through the vendor.



The ecosystem is API-based and assists with organizations meeting compliance regulations while combating potential data breaches. It features app discovery, secure and synchronized security policy adoption cross-platform, and active monitoring in real-time.

Cisco Cloud lock is a cloud-native cloud access security broker (CASB) that helps you move to the cloud safely. It protects your cloud users, data, and apps. Cloud lock's simple, open, and automated approach uses APIs to manage the risks in your cloud app ecosystem. With Cloudlock you can more easily combat data breaches while meeting compliance regulations.

Features

User security

Cloudlock uses advanced machine learning algorithms to detect anomalies based on multiple factors. It also identifies activities outside allowed countries and spots actions that seem to take place at impossible speeds across distances.

Data security

Cloudlock's data loss prevention (DLP) technology continuously monitors cloud environments to detect and secure sensitive information. It provides countless out-of-the-box policies as well as highly tunable custom policies.

App security

The Cloud lock Apps Firewall discovers, and controls cloud apps connected to your corporate environment. You can see a crowd-sourced Community Trust Rating for individual apps, and you can ban or allow list them based on risk.

Featured technologies

Cisco Umbrella: Shadow IT Discovery

Cloud lock technology is now built into Cisco Umbrella to deliver App Discovery and blocking. It provides cloud app usage and risk info to enable secure cloud adoption.

Cloud lock's FedRAMP ATO

The authority to operate helps you enable secure cloud adoption across multiple platforms.

Cloud and application performance monitoring

Get end-to-end cloud monitoring with AppDynamics to help manage and visualize your critical cloud-based app performance, in real time.

Modules

Available on

Business size

L M S

Markets

- United States
- Canada
- United Kingdom
- Australia
- China
- India

Languages

- English

Features

- Multi-Cloud Management
- Procurement Management
- Service Level Agreement (SLA) Management