Cloudlock (CASB)

(Cloud Access Security Broker)

Cisco Partner

https://cs.co/1page

Cisco Cloudlock is a cloud-native Cloud Access Security Broker (CASB) that protects your cloud users, data, and apps. Cloudlock'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.

Benefits:

Reduce the risk of cloud security breaches: Cloudlock helps secure users, data, and applications in the cloud with user and entity behavior analytics, cloud DLP, applications firewall, and app discovery.

Enable compliance: Organizations need to protect their user accounts from compromise and their data from exposures and leaks.

Conversation Starters:

Users and Accounts:

- Who is accessing your cloud applications, and what are they doing?
- How do you detect a compromised account?
- Are malicious insiders extracting information?

Corporate Data:

- Do you have, or could you unknowingly have, sensitive information stored on cloud services?
- Do you have to meet regulatory requirements, such as PCI or HIPAA?
- Do you have data that is being shared inappropriately?
- How do you detect policy violations?

Applications:

- How do you monitor application usage and risk?
- Do you have any third party connected applications?
- How do you revoke risky applications?

Over 80 pre-defined Policies such as:

General:

- Email address
- IP address
- Passwords/login information

PII:

- SSN/ID numbers
- Driver license numbers
- Passport numbers

PCI:

- Credit card numbers
- Bank account numbers
- SWIFT codes

PHI:

- HIPAA
- Health identification numbers (global)
- Medical prescriptions

Use Cases:

User Entity and Behavior Analytics (UEBA): Analyze user & entity behavior (e.g. Login anomalies, upload/download behavior, geolocation, etc.) to detect account compromise and malicious insider activity to identify and protect against user threats including malicious insiders.

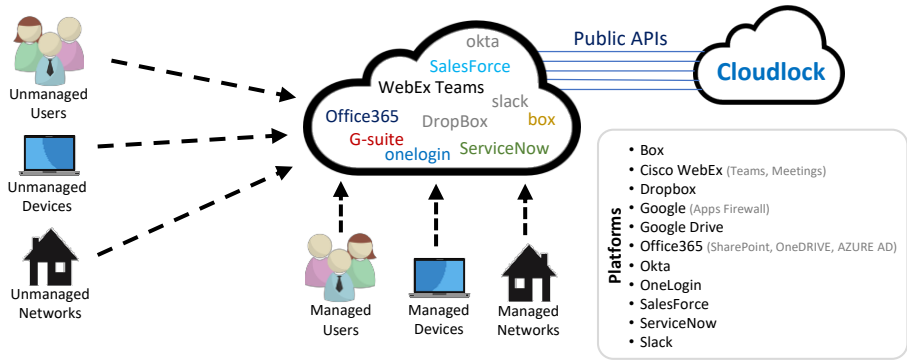
Data Loss Protection (DLP): Protect corporate data in the cloud for compliance violations and unknown vectors of risk. Continuously monitor cloud environments for sensitive data (PII, PCI etc.) and information exposure.

Application Firewall: Prevent 3rd party apps (OAuth and Shadow IT) that are authenticated to the corporate cloud from accessing sensitive cloud environment.

Geolocation: Allow or Block specific IP addresses and ranges to defend against account compromises.

Cross-Platform Security Intelligence: Aggregate and analyze activities across SaaS and PaaS platforms.

Day one defense: Gain immediate value with out-of-the-box policies for common data security concerns.



Resources:

SalesResources	Cloudlock Console	Documentation Hub
Data sheet	Cloudlock API	Cloudlock Status
Proposal Template	Cloudlock FedRAMP	Public page

Example SKUs: ***CLOUDLOCK-SUB*** | ***CLOUDLOCK-FED-SUB***