Cisco Cloudlock: Secure Cloud Data

Protect sensitive data stored in the cloud.

Discover and protect sensitive information

Mitigate increased risk of data exposure in cloud applications

Combating data leakage in the cloud is a formidable challenge given the collaborative nature of cloud environments and the ease with which they enable users to access, create, and share sensitive information. Organizations are struggling to bridge the gap between legacy data protection tools and the often limited level of visibility and control within cloud environments, particularly when accessed by external users or employees off of the corporate network.

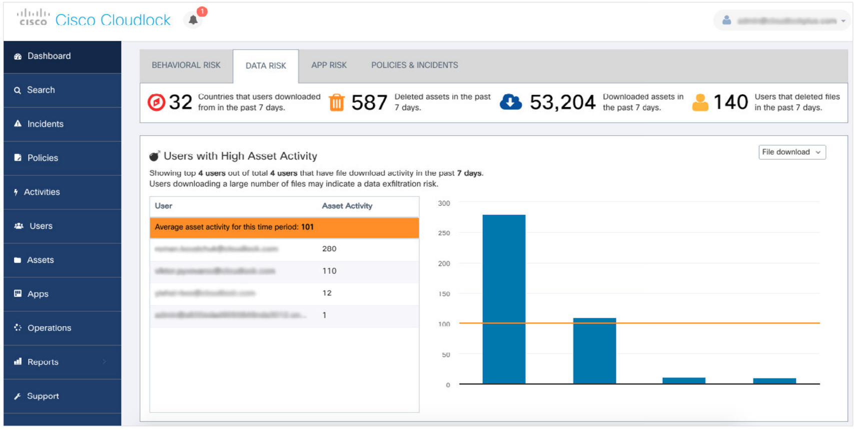
Identify sensitive data in cloud environments

Cisco Cloudlock continuously monitors cloud environments with a cloud Data Loss Prevention (DLP) engine to identify sensitive information stored in cloud environments in violation of policy. With Cisco Cloudlock, security professionals enforce out-of-the-box policies focused on common sensitive information sets, such as PCI-DSS and HIPAA compliance, as well as custom policies to identify proprietary data, such as intellectual property. Advanced capabilities such as custom regular expression (RegEx) input, threshold settings, and proximity controls ensure high true positive and low false positive rates.

Mitigate risk through automated responses

Cisco Cloudlock takes cloud DLP beyond discovery by offering configurable cross-platform automated response actions. Through an API-driven Cloud Access Security Broker (CASB) architecture, Cisco Cloudlock supports deep, integrated response workflows that leverage the native capabilities of the monitored application, such as automated field-level encryption in Saleforce.com and automated file quarantining in Box. Cisco Cloudlock enables efficient risk reduction without the resource-intensive operation of many data protection tools.

Cisco Cloudlock



32 Countries that users downloaded from in the past 7 days.

587 Deleted assets in the past 7 days.

53,204 Downloaded assets in the past 7 days.

140 Users that deleted files in the past 7 days.

Users with High Asset Activity

Showing top **4 users** out of total **4 users** that have file download activity in the past **7 days**.
Users downloading a large number of files may indicate a data exfiltration risk.

User	Asset Activity
Average asset activity for this time period: **101**	
[redacted]	280
[redacted]	110
[redacted]	12
[redacted]	1

How Cisco Cloudlock helps

- Gain visibility into and control over sensitive information stored in cloud environments
- Mitigate the risk of cloud data leakage through powerful, automated response actions when sensitive data is discovered
- Support adherence to compliance regulations within cloud applications

Functionality highlights

- **Cloud data protection:** Continuously monitor cloud environments for sensitive data and information exposure
- **Automated enforcement:** Leverage automated response workflows to efficiently mitigate risk
- **Day one defense:** Gain immediate value with out-of-the-box policies for common data security concerns
- **Advanced DLP precision:** Pinpoint proprietary sensitive information through advanced DLP functionality such as RegEx input and threshold controls

Problems we solve

Lack of visibility into sensitive data within cloud applications

An increasing amount of organizations are adopting cloud applications. The visibility of on-premises DLP systems is limited to on-network traffic and does not extend to cover cloud environments, such as Software-as-a-Service (SaaS). Additionally, given the ease with which users can distribute information in cloud environments, and their highly collaborative nature, distribution of sensitive information to external parties is easy for employees but difficult for security analysts to detect.

The cloud as a means of data exfiltration

Cybercriminals and malicious insiders can easily employ cloud services to access and exfiltrate sensitive information. Cisco Cloudlock enables security analysts to gain control of cloud applications and excessively exposed information to combat malicious behaviors.

Operation-intensive security tools challenge security team resources

Traditional data protection tools are resource-intensive, requiring a great deal of manual oversight due to excessive false positives and limited automated response. Additionally, deployment and scalability concerns demand additional security resources to achieve minimal value.

Why Cisco Cloudlock

- **Cloud Native.** Cisco Cloudlock is a frictionless, cloud-native solution that deploys in 5 minutes, delivers immediate value, and has zero impact on end users.
- **Broadest and Deepest Coverage.** Cisco Cloudlock's retroactive security analytics go back further than any of our competitors – to the beginning! Unlike proxy solutions, Cisco Cloudlock also natively covers cloud-to-cloud traffic and Cisco Cloudlock's collection of microservices can protect any app.
- **Intelligence Driven.** Cisco Cloudlock is driven by our Talos intelligence team – providing you with a security solution aggregated from billions of security events around the globe.
- **Scalable to Any Organization.** Cloudlock's cloud delivered deployment, and seamless network integration will secure organizations of any size – validated with over 750 active customers.
- **Cisco Ecosystem.** Cisco provides an integrated, architectural approach to security with rock-solid vendor viability.

Coverage:

- Microsoft Office 365
- Salesforce.com
- Box
- Dropbox
- Google G Suite
- ServiceNow
- Slack
- Webex Teams

Use cases

- Continuously monitor cloud environments for sensitive information and exposures
- Activate automated end-user notifications to educate employees and reduce future DLP violations
- Pinpoint sensitive data within cloud apps through custom and out-of-the-box DLP policies
- Enforce cross-platform automated response actions to mitigate risk rapidly
- Reduce false positives through advanced DLP capabilities such as threshold and proximity controls
- Integrate with SIEM solutions for simplified incident investigation and incorporation in broad security analysis

The Cloudlock advantage

"The biggest benefit Cloudlock provides for us is visibility into what users are doing; what they are storing up in the cloud, and being able to keep ourselves out of hot water, to be honest. We don't want news channel moments, and without Cloudlock, we would not have had nearly as good a view into what is out there and how to take action on it."

- David Duchan, Information Security Engineer, Ahold