Cisco Cloudlock

DATASHEET

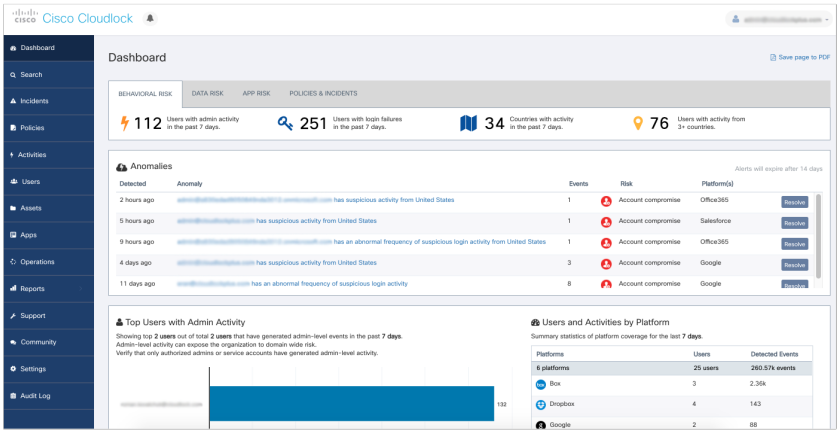
Cloud User Security

Detect Anomalies in Your Cloud User Accounts

Compromised Accounts, Malicious Insiders, and Privileged Users

Cisco Cloudlock provides cross-platform User and Entity Behavior Analytics (UEBA) for SaaS, IaaS, PaaS, and IDaaS environments. Cisco Cloudlock leverages advanced machine learning algorithms to detect anomalies based on factors such as activities outside of whitelisted countries and actions across distances at impossible speeds.

Attackers are defeating today's security controls that rely on the network perimeter, firewalls, or exclusively focus on a specific platform. Activities across platforms are not correlated, making it difficult or impossible to identify suspicious behavioral patterns. At the same time, security teams are inundated with alerts that lack priority, useful information, or context. Faced with a flood of unhelpful alerts, the legitimate security breaches get overlooked. This problem is magnified with the use of cloud applications and platforms, as organizations often have little visibility into the activities of their users in their SaaS, PaaS, IaaS, and IDaaS environments.



Problems We Solve

Compromised Accounts
Attackers are compromising cloud application accounts at astonishing rates. Targeted attacks, such as spearphishing have reached a level of sophistication where they are virtually indistinguishable from legitimate communications. In many cases, there are not any files or malicious URLs involved in an attack, rendering traditional security solutions, including anti-malware and anti-phishing tools, incapable of addressing these threats.

Malicious Insiders
As malicious insiders are unlikely to trigger typical security telemetry when performing nefarious tasks, detecting insider threats is extremely difficult. Given the ease with which malicious individuals can leverage cloud applications to access, modify, distribute, and exfiltrate sensitive information, detecting and mitigating malicious insiders is crucial.

Dangerous Privileged Account Actions
Privileged users not only have access to a high volume of sensitive data, but also have administrative rights, such as configuration settings and user provisioning within applications. As such, ensuring the integrity of privileged accounts is critical to security.

How Cisco Cloudlock Helps

- Detects compromised cloud accounts
- Identifies malicious insiders
- Monitors privileged user accounts

Functionality Highlights

- User and Entity Behavior Analytics: Analyze user and entity behavior to detect account compromis¬e and malicious insider activity
- Cross-Platform Security Intelligence: Aggregate and analyze activities across SaaS, IaaS, and PaaS platforms
- Geolocation Whitelisting and Blacklisting: Allow and block specific IP addresses and ranges to defend against account compromises

How We Do It

User and Entity Behavior Analytics
Cisco Cloudlock detects activity indicative of account compromise by correlating and analyzing usage information across SaaS, IaaS, PaaS, and IDaaS environments to identify anomalies. Additionally, through advanced machine learning, Cisco Cloudlock adaptively learns user behavior to uncover suspicious behavior patterns. Additionally, Cisco Cloudlock integrates with IDaaS solutions to analyze login behavior for the thousands of applications connected to those services.

Policy-Based Enforcement
Cisco Cloudlock identifies suspicious behavior such as a single user logging in from geographically disparate locations in a short period of time, an unusually high volume of file downloads, and access outside of typical business hours triggers. Additionally, Cisco Cloudlock enables the whitelisting and blacklisting of specific IP addresses and IP ranges to defend against account compromise. When anomalies are detected, Cisco Cloudlock enables a range of automated remediation actions, including administrative alerting, end-user notification, and even requiring step-up authentication through integrations with IDaaS solutions.

Threat Protection
Cisco Cloudlock integrates with malware detection and threat emulation services to both detect cloud-resident malware and enable automated threat response workflows, including administrative alerting, end-user notification, file quarantine, and more. Cisco Cloudlock also enables the whitelisting and blacklisting of activity from both specific geographies and IP ranges for additional security confidence.

Use Cases


Detect and respond to compromised accounts


Monitor and secure privileged accounts


Detect and respond to malicious insiders


Whitelist and blacklist access from specific geographies as well as specific IP addresses and ranges


Detect impossible velocities


Integrate with IDaaS solutions for additional behavioral visibility and response actions

Why Cisco Cloudlock

- **Superior Detection.** Cisco Cloudlock ingests and correlates data from not only SaaS applications, but also IaaS, PaaS, and IDaaS environments for superior security intelligence and incident detection.
- **Integrated Threat Detection and Remediation.** Cisco Cloudlock integrates with malware detection and threat emulations services, as well as IDaaS solutions, and SIEM solutions for comprehensive visibility, threat detection, and remediation.
- **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.
- **Smartest Intelligence.** Cisco Cloudlock has the smartest cyberintelligence and CyberLab because it has the most and best data by having the largest CASB customer base.
- **Most Scalable Platform.** Cisco Cloudlock pioneered the API approach to CASB and has proven Enterprise-scale, with over 750 paying, subscription customers.
- **Cisco Ecosystem.** Cisco provides an integrated, architectural approach to security with rock-solid vendor viability.