Cisco Cloudlock

DATASHEET

Cisco Cloudlock: Secure Cloud Apps

Shadow IT Control with Apps Firewall

Discover and Control Cloud Apps

As employees continue to embrace the phenomena of BYOD, work from anywhere, and the self-enablement of cloud apps, security leaders and practitioners alike are challenged to address a growing volume of Shadow IT.

Despite the considerable investments made in security solutions, many security teams remain ill equipped to comprehensively identify application usage and the associated risk - a critical practice to mitigate the risk of account compromise and data exfiltration.

OAuth Connected Apps: A Unique Threat Vector

Most users have seen the "Login with Google" or "Login with Microsoft" options when signing up for a new web application. But what many individuals do not understand are the security implications of such connected cloud apps. Organizations have an average of over 750 unique, user-enabled cloud apps authorized with corporate credentials and connected to corporate applications[1]. These apps are authorized through OAuth to access Google G Suite or Microsoft Azure Active Directory (AD) environments via APIs.

Due to the excessive access scopes associated with many of these apps, often including the ability to view, edit, delete, share, and download data, they create unique security and compliance challenges. Additionally, as these apps connect directly to corporate cloud apps via APIs, they are completely invisible to traditional security solutions, from on-premises devices to anti-malware and anti-phishing tools. Connected cloud applications can present risk in multiple ways:

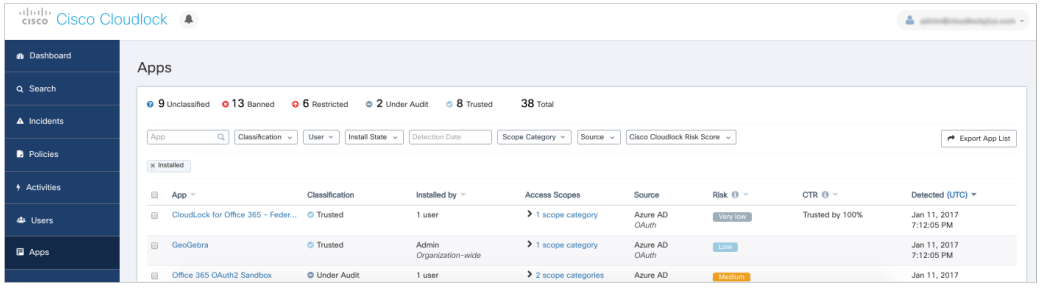
1) While benign in intent, an app may access and/or distribute sensitive information to fulfill its function,

2) An app may be counterfeit or malicious by design and aim to leverage an excessive permission set to act nefariously, or

3) While the app may be benign, the organization behind the app may be compromised, allowing the malicious actor to leverage the permissions of the app to compromise accounts as well as access and exfiltrate sensitive information.

On-Network Cloud App Usage Discovery

In addition to providing visibility into and control of OAuth connected apps, Cloudlock ingests data from firewalls and proxies, including Cisco ASA and Cisco Firepower. Cloudlock augments this raw data with cybersecurity insight, including app risk level ratings, traffic volume by application, and visibility into the most active users, to enable superior security intelligence and efficient resolution.



Data Sources

1. The 1% Who Can Take Your Organization: Cloudlock Cloud Cybersecurity Report

How Cisco Cloudlock Helps

- Gain visibility into and control over the riskiest Shadow IT in the form of user-enabled cloud apps connected to corporate systems, including Google G Suite and Microsoft Azure Active Directory (AD)*
- Enable compliance and reduce the risk of compromised accounts and sensitive data exfiltration by revoking risky apps with excessive access scopes
- Leverage cloud security intelligence and application risk insight via app risk score and peer insights such as the Community Trust Rating

*Cisco Cloudlock Apps Firewall for Microsoft Azure AD is currently in Beta

Functionality Highlights

- Pain-free 360° Visibility: The only CASB to detect and control off-network cloud app usage without agents or proxies
- Powerful App Control: Move beyond visibility with policy-based enforcement capabilities
- Efficient Investigation: Evaluate your environment with risk ratings powered by the Cloudlock CyberLab and security peers
- APIs for Immediate ROI: Enterprise-wide coverage in minutes without any impact to end-users

Problems We Solve

Connected Apps: The Cloud-to-Cloud Blind Spot
Conventional security solutions limit visibility to on-network traffic, blinding security analysts to the growing volume of cloud-to-cloud communications occurring off-network. This includes the usage of apps enabled with corporate credentials via OAuth that connect to corporate systems such as Google G Suite and Microsoft Office 365. On average, organizations have over 750 of these connected applications, each posing a risk of data exposure or account compromise.

Lack of Shadow IT Enforcement Capability
Detection is the first step in combatting Shadow IT risk, but security only improves with the ability to control cloud app risk. Cisco Cloudlock offers automated, policy-based enforcement capabilities to revoke risky applications based on their permission set and risk level.

Compliance Considerations
Organizations consistently make considerable investments in data loss prevention (DLP) technologies, yet overlook the massive data ingress and egress points represented by Shadow IT, particularly OAuth connected apps. Cisco Cloudlock extends data protection efforts through cloud app visibility and control.

Operation-Intensive Security Tools Challenge Security Team Resources
Information without context and actionable recommendations creates more work for security analysts. Cisco Cloudlock provides true security intelligence, complementing application detection capabilities with insights, including assessments of application risk and the Community Trust Rating, the peer-driven assessment score of application trustworthiness. The result? Security analysts are enabled to efficiently remediate risk and improve the security posture of the organization.

Coverage

- Cisco Cloudlock detects applications connected to Google G Suite and Microsoft Office 365.
- Cisco Cloudlock integrates with Cisco firewalls, including Cisco FirePower and Cisco ASA with FirePOWER services, as well as other firewall and proxy logs to augment on-premises Shadow IT visibility with cloud security intelligence for efficient evaluation of cloud app risk
- Cisco Cloudlock also integrates with Cisco Umbrella to ban detected applications at the DNS level for ultimate confidence and control

Use Cases

Gain visibility into cloud app usage, including apps enabled prior to CASB deployment

Reduce risk of compromised accounts, data exfiltration, and unintentional data exposure through app control

Enforce cloud app control, including off-network usage of cloud apps connected to corporate systems

Ban applications by domain at the DNS level through integration with Cisco Umbrella

Evaluate cloud app risk efficiently through cybersecurity intelligence, including the Community Trust Rating and app risk level assessments

Ingest logs from Cisco FirePower and Cisco ASA with FirePOWER Services, as well as other firewall and proxy logs, to provide additional insight on on-network cloud app usage

Automate policy-driven cloud app control, including revocation based on factors including application access scope and risk score

Integrate with SIEM solutions for simplified incident investigation and incorporation in broad security analysis

Why Cisco Cloudlock

Crowdsourced Security. Cisco Cloudlock enables efficient application security assessment through app ratings based on anonymized peer behavior.

Superior Security Intelligence. Cisco Cloudlock offers actionable cyberintelligence in the form of app risk ratings fueled by the CyberLab as well as Community Trust Ratings, the crowdsourced assessment of cloud app risk.

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.

Connected App Visibility. Only Cisco Cloudlock offers visibility into and control over the riskiest Shadow IT in the form of user-enabled cloud apps connected to corporate systems.

The Cloudlock Advantage

"Cloudlock has been a real game changer for us. It's given us a level of comfort and visibility that we just didn't have before."

- Mitchell Bailey, IT Manager, Austin Fraser