Cisco Cloudlock

DATASHEET

Automated Assessment

Uncover Your Cloud Security Risks

Cloud Users, Data, and Apps

Organizations using the cloud often have little visibility and insights into their cloud security risks. The CloudLock Automated Assessment can help. It analyzes your cloud user activities, your cloud data usage trends, and the risk of your "connected" cloud applications.

Suspicious Behavior

Cloud user accounts are targeted by hackers to gain immediate access to your organization's systems and data. "Phishing" is a commonly-used technique in which an attacker poses as a legitimate entity in an attempt to trick a user to click a malicious link or provide sensitive information to the attacker. Targeted "spearphishing" techniques are staggeringly successful and often target company executives and key IT personnel.

Detecting account compromises requires identifying the most suspicious user behavior across cloud users and applications. Have a user that logs into Salesforce from Toronto and downloads a file from Box five minutes later from Pyongyang? Do you have admin accounts with multiple login failures? With configurable policies and the latest in machine learning, the CloudLock Automated Assessment can tell you.

Data Leaks

Malicious insiders will often download massive quantities of data to take with them to future jobs or use for other purposes. This is also true of compromised accounts.

Are certain users downloading or deleting high volumes of data? Do you know which files are the most-downloaded across your organization? Do you have unexpected spikes in uploads and downloads? The CloudLock Automated Assessment can tell you.

App Risk

Have you ever seen a button on a web application that says "Login with Google" or "Login with Microsoft"? What you may not know is that by using that, you often give those apps full permissions to your account, from viewing your emails to copying and deleting your files. Now imagine that app is malicious or a legitimate app is itself hacked. This is what we call a cloud-native threat.

Your employees are authorizing these apps every day using their corporate credentials, which represents both a security and a compliance risk because data can be exfiltrated in ways completely invisible to traditional security solutions, from anti-malware to anti-phishing. Do you know the most risky apps that your users have installed? How about the users that have installed the most risky apps?

The CloudLock Automated Assessment can give you visibility into the apps that your employees have "connected" into your corporate cloud environment so that you understand your true cloud app risk.

Want to Know?

- If you have compromised cloud user accounts?
- If there are unusual trends in cloud data downloads?
- If your employees have granted permissions to risky cloud apps?

Results

- Uncover suspicious behavior
- Gain visibility into connected cloud applications