Enterprise Strategy Group | **Getting to the bigger truth.™**

ESG Lab Validation

# Cisco Cloudlock Cloud Access Security Broker (CASB) Platform

## Visibility and Control of Cloud-connected Applications

By Kerry Dolan, Senior IT Validation Analyst

November 2017

This ESG Lab Report was commissioned by Cisco and is distributed under license from ESG.

## Contents

### ESG Lab Reports

The goal of ESG Validation reports is to educate IT professionals about information technology solutions for companies of all types and sizes. ESG Validation reports are not meant to replace the evaluation process that should be conducted before making purchasing decisions, but rather to provide insight into these emerging technologies. Our objectives are to explore some of the more valuable features and functions of IT solutions, show how they can be used to solve real customer problems, and identify any areas needing improvement. The ESG Validation Team's expert third-party perspective is based on our own hands-on testing as well as on interviews with customers who use these products in production environments.

## Introduction

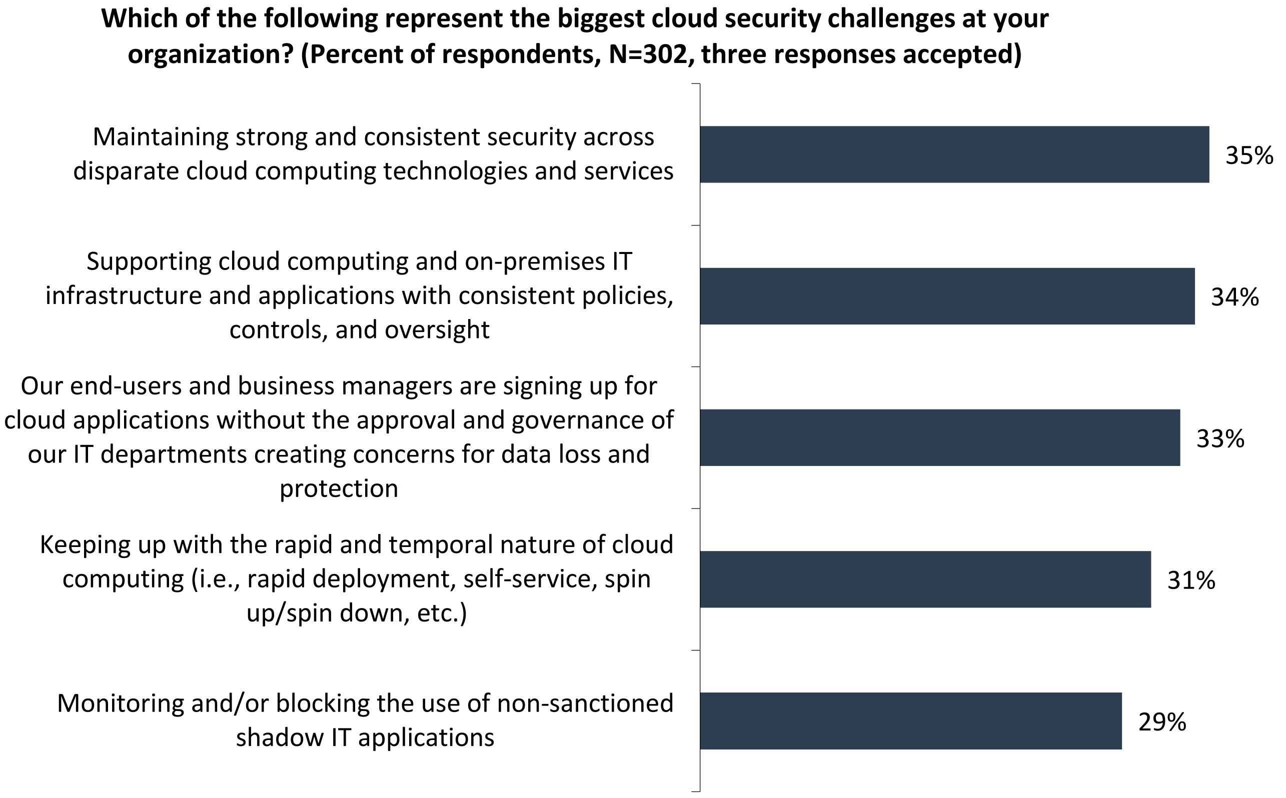
This ESG Lab report documents hands-on testing of Cisco Cloudlock, a cloud access security broker (CASB) and cloud cybersecurity solution, with a focus on the Apps Firewall, which provides visibility and protection of connected cloud applications.

### Background

Of the many recent changes to the workplace, the wide usage of cloud applications may be among the most consequential. Cloud applications such as Office 365, Salesforce, SharePoint, Google G Suite, Dropbox, and many others enhance collaboration and data sharing, make it easier for employees to work from anywhere, and empower business units with more application choices.

However, with applications, data, and user identities/credentials moving to the cloud, organizations can open themselves up to additional security risks, as users log in from public WiFi wherever they happen to be. These behaviors add vulnerability, and cloud-connected applications can create new attack vectors for malicious behavior. When respondents to an ESG research survey were asked about their biggest cloud security challenges, 35% selected the ability to maintain strong, consistent security across cloud technologies and services; 34% chose supporting cloud and on-premises infrastructure with consistent policies and controls; and 33% indicated unapproved cloud application use (what many call "shadow IT"), making these three responses the most-cited (see Figure 1).[1]

**Figure 1. Top Five Cloud Security Challenges**



*Source: Enterprise Strategy Group, 2017*

[1] Source: ESG Research Report, *The Visibility and Control Requirements of Cloud Application Security*, May 2016.

Traditional security solutions don't work well for cloud platforms; organizations struggle to get adequate visibility into cloud applications and their usage, including what data is being accessed and how it is shared. This leaves them vulnerable to both user error (such as accidentally sharing a file with external contacts) and increasingly sophisticated cyber-attacks. While protecting the network perimeter can go a long way toward securing on-premises infrastructure, the cloud provides a new attack surface. Most organizations don't have sufficient controls in place to deal with it.

### OAuth

OAuth is an open authorization standard that connects third-party applications to Internet identities, helping reduce the number of passwords for simplification and security. If you have seen a message such as, "Would you like to sign in using Google, Facebook, Salesforce, or your corporate email address?" then you have used OAuth. OAuth is a helpful tool that works effectively as long as proper protections are in place. Since many apps request the ability to view, edit, delete, share, and download user data, lack of proper oversight can result in giving more access than you want, resulting in security and compliance challenges. In addition, when these apps connect directly to corporate cloud apps such as Google G Suite and Office 365 via APIs, they are invisible to anti-malware or anti-phishing solutions.

#### *Recent Attack*

While Cloudlock has protected OAuth connections for years, many organizations remain unaware of the potential risks. A recent attack highlighted the challenges of cloud-connected applications. In May 2017, a sophisticated Google phishing attack led Gmail users to give permission to a malicious application to access their accounts, email, and contacts, spreading the attack and creating a persistent connection to each user. This attack used a real Google login page, making the request look credible, but once permission was granted, the browser was redirected to the malicious site. It should be noted that this type of attack could have used any cloud application, not just Google.

The well-publicized attack was contained quickly, and Google reports that it impacted less than 0.1% (@one million) Gmail users. It does not appear that any data other than contacts was retrieved, and there have been no reports of data deletion or ransom, so the attack caused very little damage. However, it is abundantly clear how damaging this attack could have been—the sheer number of cloud applications and users illuminates the vastness of the attack surface. This one had the appearance of an attacker "testing the waters" for a potential future attack, making it even more important for organizations to not only understand the new attack vectors that come with cloud applications and OAuth permissions, but to also take action to improve their security profiles to prevent damage.

## Cisco Cloudlock

Cisco's security division focuses on network, endpoint, and cloud security solutions. Cloud security is comprised mainly of Cisco Cloudlock, to focus on cloud and SaaS applications, which Cisco added to its portfolio with a 2016 acquisition; and Cisco Umbrella, for securing Internet access at the DNS layer, resulting from its 2015 acquisition of OpenDNS. Cloudlock is an API-based, cloud-native, CASB that provides:

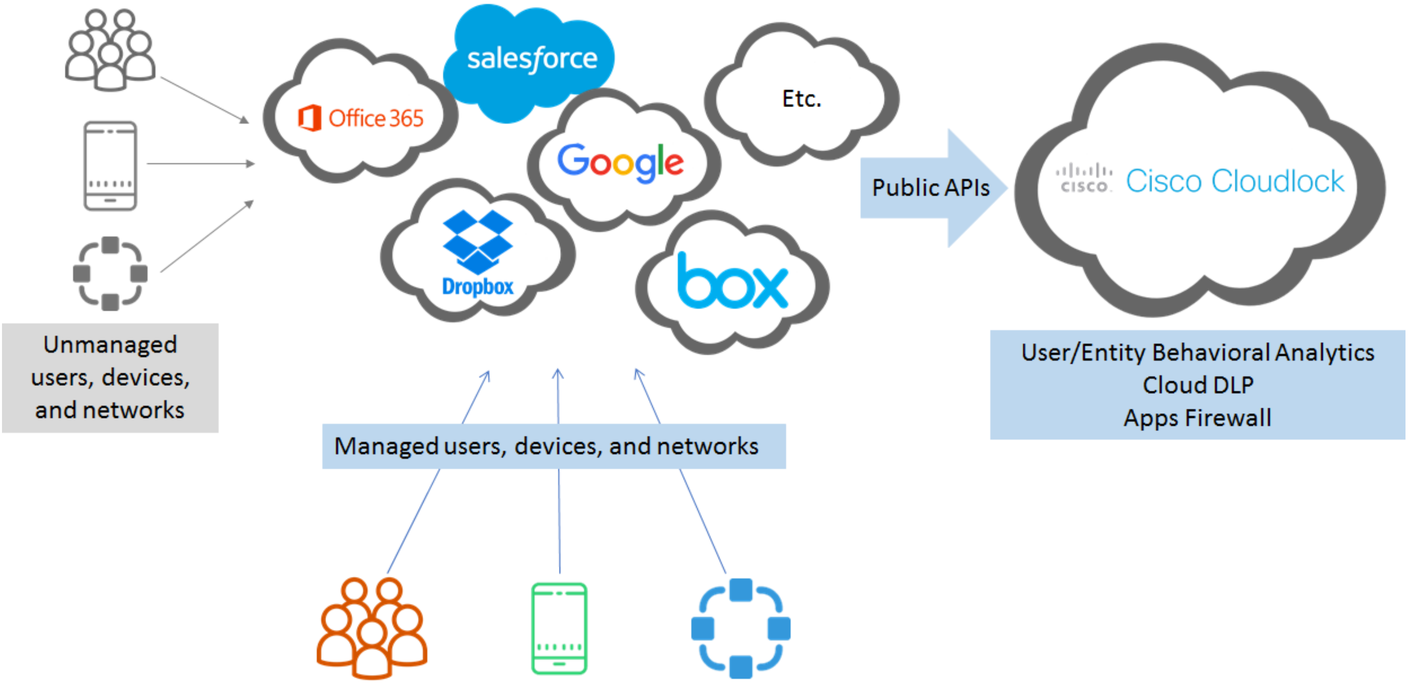
- User security via User/Entity Behavior Analytics for cloud environments—detecting insider threats and compromised accounts.
- Data security via cloud data loss prevention (DLP)—protecting sensitive data in the cloud by identifying leakage of financial, health, and other personally identifiable information.
- Application security via the Cloudlock Apps Firewall—securing connected applications, identifying cloud malware, improving security of OAuth connected apps, and providing visibility for OAuth applications and "shadow IT" to minimize vulnerability.

## Cloudlock CASB Platform

Typical security solutions operate by protecting the network perimeter, protecting traffic on the network, and managing mobile devices. These solutions are important to have in place, but they have a blind spot: cloud applications that connect with on-premises applications and data as well as with other cloud applications. Unmanaged users, devices, and networks create vulnerabilities that these solutions cannot see.

Cloudlock automatically discovers cloud applications connected to your environment, providing visibility into what applications users are connected to, and how they are using and sharing data. It helps organizations control applications by classifying and monitoring activities and revoking access when needed. Cloudlock monitors all user activities that occur in any discovered cloud application, and connects to each cloud platform's public APIs. When a user uploads a file to Dropbox, for example, Dropbox records that event and shares it with Cloudlock via API; Cloudlock can then scan the content using a pre-configured classification engine, evaluate it in the context of configured policies, identify whether a violation has occurred, and immediately respond by encrypting or quarantining the file. Integration with other tools also enables detailed forensics after an attack. Cloudlock tracks activities from managed and unmanaged users, devices, and networks.

Figure 2. Cisco Cloudlock


Office 365
salesforce
Etc.
Google
Dropbox
box
Public APIs
Cisco Cloudlock
Unmanaged users, devices, and networks
User/Entity Behavioral Analytics
Cloud DLP
Apps Firewall
Managed users, devices, and networks

*Source: Enterprise Strategy Group, 2017*

While many cloud applications offer security controls, they cannot provide the holistic view across applications from the user side; for example, Google and Dropbox may show user activities, but IT administrators cannot correlate information between them, much less across the thousands of applications that most organizations use today. Cloudlock provides that holistic view. It is an open solution, easy to integrate with existing network security, SIEM, EMM, and IAM solutions; it can also leverage the logs of other CASBs to expand visibility.

Unlike gateway-based CASB solutions, Cloudlock does not get between the users and their cloud applications. It resides in AWS, alongside other cloud applications, monitoring data in real time and at rest. As a result, Cloudlock activities do not impact performance or scalability the way proxies or gateways can. This also enables a new Cloudlock deployment to provide visibility into what data was used and how it was shared in the past, rather than only from the time of deployment, as with non-API-based CASBs.

Cloudlock is fast and easy to set up without disrupting users. It consists of a collection of microservices, such as for data classification or threat protection. Microservices are exposed through the Cloudlock UI, or through APIs to other products. The software comes with 80+ pre-defined policies that can be tailored as needed, such as to define the level of sensitivity, appropriate data proximity, data exposure, or policies by department. For example, an organization might permit cloud-based applications to store a single credit card number, but identifying hundreds of them might prompt alerts and actions. Granular policies can be created and deployed to multiple cloud applications, saving administrators from having to configure individual policies by application. Policies can be applied to users, individually or in groups, based on behaviors, locations, and IP addresses.

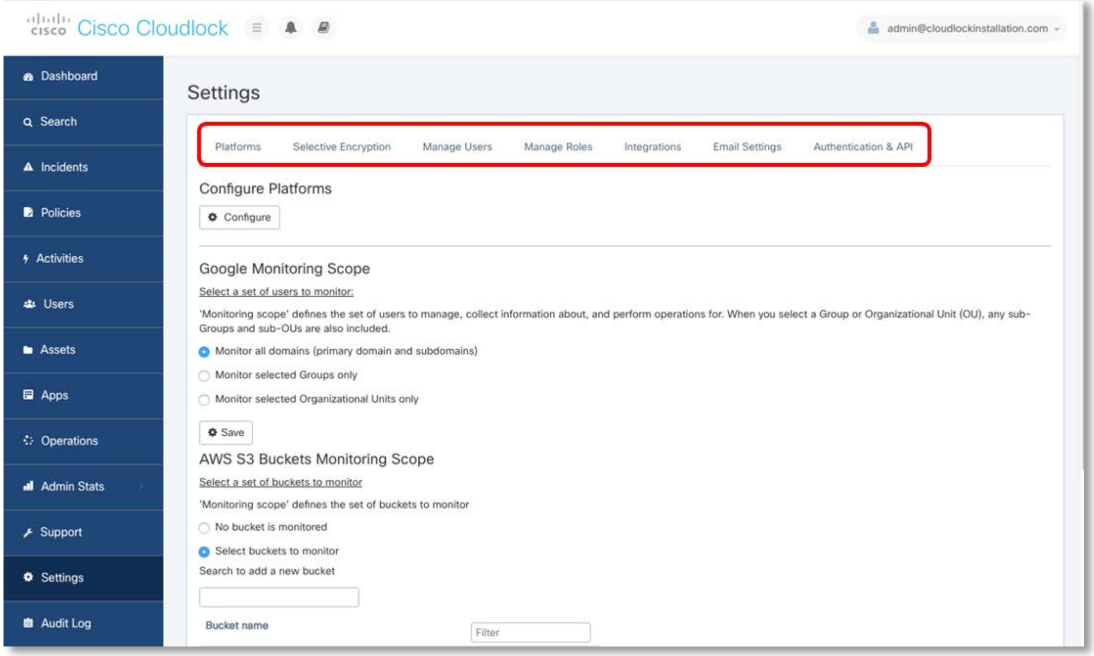
Cloudlock keeps track of user activities, and can view the logs of Office 365, Google, Dropbox, Box, Salesforce, or other cloud applications via API. Policies can be created to act automatically when events occur, such as automatically revoking an OAuth token and severing the connection for banned apps, or automatically encrypting and quarantining data, such as when a credit card number is added where it shouldn't be.

Cloudlock also provides two special features:

- ***Community Trust Rating*** (CTR), a crowd-sourced rating system for cloud applications that provides customers with additional credible information to make informed choices about what applications to approve.
- ***Cyberlab***, a division that leverages crowd-sourced data to proactively research cloud risks, investigate breaches, analyze attacks, and keep customers informed.

## ESG Lab Validation

ESG Lab performed a hands-on evaluation of Cloudlock's application security features using a demo environment. Testing focused on ease of use, visibility, and protection for connected cloud applications. The environment included cloud apps for collaboration/productivity (Office 365, Slack), file sharing (Dropbox, Box), cloud storage (Google Drive, AWS), CRM (Salesforce), IT service management (ServiceNow), and identity/single sign-on (OneLogin, Okta).



Settings

Configure Platforms

Google Monitoring Scope

Select a set of users to monitor:

'Monitoring scope' defines the set of users to manage, collect information about, and perform operations for. When you select a Group or Organizational Unit (OU), any sub-Groups and sub-OUs are also included.

● Monitor all domains (primary domain and subdomains)
○ Monitor selected Groups only
○ Monitor selected Organizational Units only

AWS S3 Buckets Monitoring Scope

Select a set of buckets to monitor

'Monitoring scope' defines the set of buckets to monitor

○ No bucket is monitored
● Select buckets to monitor

Search to add a new bucket

Bucket name

### Configuring Cloudlock

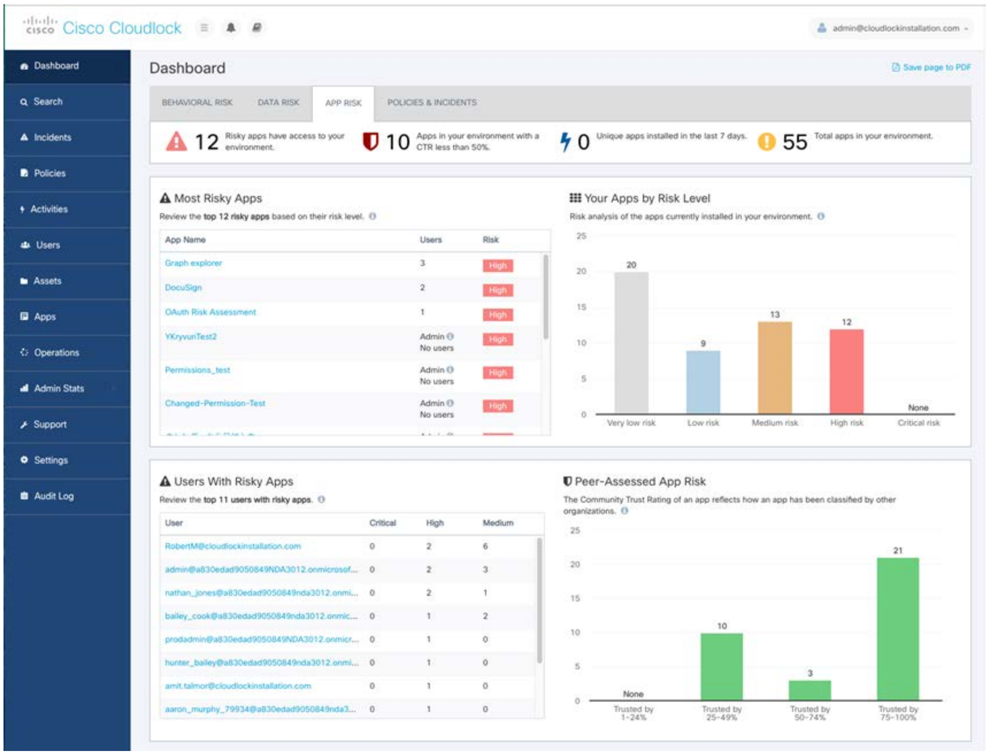
With an already deployed Cloudlock environment, ESG Lab began by exploring the configuration options. Under the Settings tab, ESG Lab could easily manage platforms, encrypt files, add and delete users and roles, manage integrations with other applications such as Cisco Umbrella DNS security, and manage SSO logins and API tokens. One important task is to configure the monitoring scope of each cloud platform, defining which users to include when tracking activities, collecting behavioral information, and executing operations. For example, Cloudlock can monitor all or selected Google domains and Organizational Units (OUs), certain AWS S3 buckets, Slack channels, and Office 365, Box, and Dropbox domains.

## Making Applications and Activities Visible

The Cloudlock dashboard offers a high-level view of what Cloudlock monitors: behaviors, data, and applications. Each tab includes a top-level report of four key statistics from the past week that might indicate a breach or data leak. These summary tabs aggregate details that can also be viewed from the menu tabs on the left.

- The *Behavioral Risk* tab shows the numbers of users with administrative activity, login failures, country activities, and activities from more than three locations. These behaviors may alert IT  to problems, such as administrative actions occurring from a user without administrative credentials, or user logins from numerous countries.
- The *Data Risk* tab shows the numbers of countries from which users downloaded data, deleted and downloaded assets, and the specific users who deleted files. If a user suddenly deletes gigabytes of data, IT needs to know and take action.
- The *App Risk* tab shows the numbers of risky apps accessing the environment, apps with a CTR of less than 50%, unique apps installed, and total apps.

These can alert administrators at a glance to potentially unsafe access to the environment. Each tab includes additional details and charts that link anomalous activities with risk levels, cloud applications, users, and locations. The Behavioral and Data Risk tabs provide charts and graphs showing trend lines, asset exposure by cloud platform or location, and details of asset activities and downloads by user. Administrators can click on graph bars, maps, and user IDs to drill down even further.



Dashboard

12 Risky apps have access to your environment.

10 Apps in your environment with a CTR less than 50%.

0 Unique apps installed in the last 7 days.

55 Total apps in your environment.

Most Risky Apps

Review the **top 12 risky apps** based on their risk level.

| App Name | Users | Risk |
|---|---|---|
| Graph explorer | 3 | High |
| DocuSign | 2 | High |
| OAuth Risk Assessment | 1 | High |
| YKryvunTest2 | Admin<br>No users | High |
| Permissions_test | Admin<br>No users | High |
| Changed-Permission-Test | Admin<br>No users | High |

Your Apps by Risk Level

Risk analysis of the apps currently installed in your environment.

Users With Risky Apps

Review the **top 11 users with risky apps.**

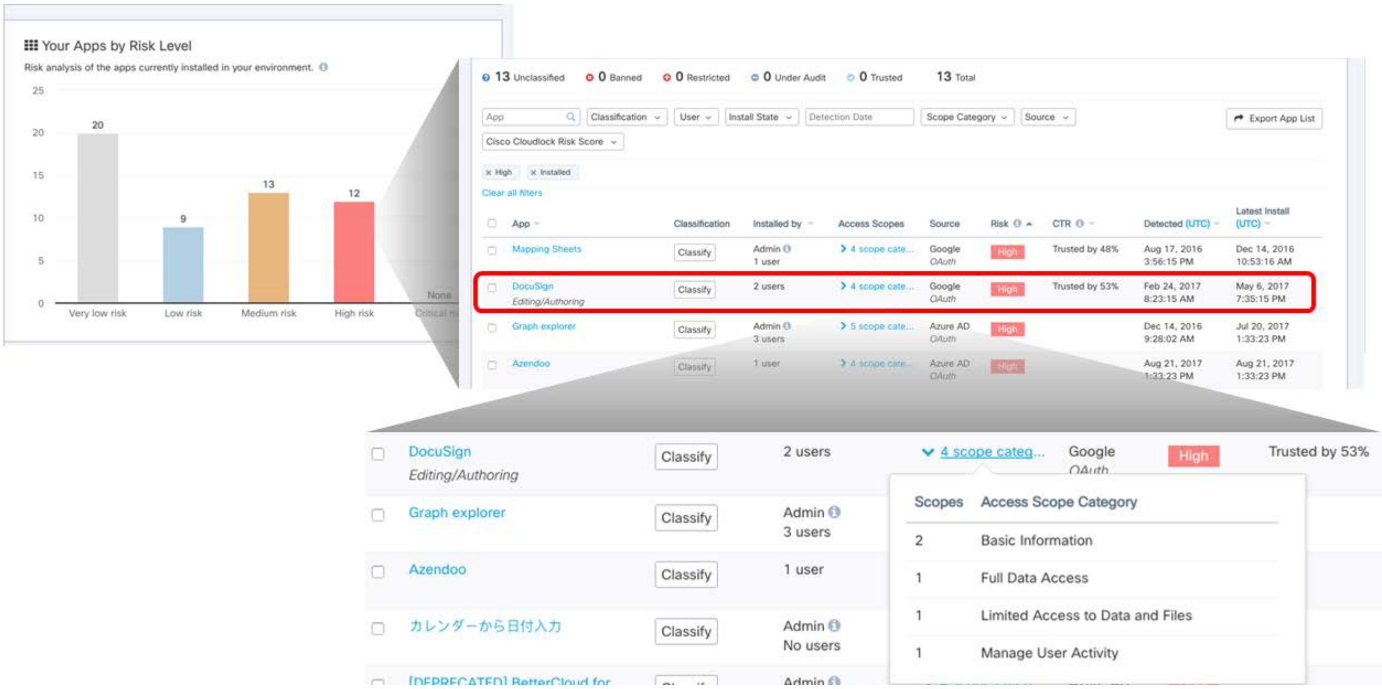
| User | Critical | High | Medium |
|---|---|---|---|
| RobertM@cloudlockinstallation.com | 0 | 2 | 6 |
| admin@a830edad9050849NDA3012.onmicrosof... | 0 | 2 | 3 |
| nathan_jones@a830edad9050849nda3012.onmi... | 0 | 2 | 1 |
| bailey_cook@a830edad9050849nda3012.onmic... | 0 | 1 | 2 |
| prodadmin@a830edad9050849NDA3012.onmicr... | 0 | 1 | 0 |
| hunter_bailey@a830edad9050849nda3012.onmi... | 0 | 1 | 0 |
| amit.talmor@cloudlockinstallation.com | 0 | 1 | 0 |
| aaron_murphy_79934@a830edad9050849nda3... | 0 | 1 | 0 |

Peer-Assessed App Risk

The Community Trust Rating of an app reflects how an app has been classified by other organizations.

The *App Risk* dashboard shows important detail for evaluating the risk levels of cloud applications. On the top left is a list of the most risky apps deployed, including the number of users and risk rating, which is generated from a combination of CTR ratings, Cyberlab analysis, the category of app, and the access scope risk. Access scopes define what data the app can access in the user environments, such as full data, contacts, and the ability to act on behalf of the user. Defining access scopes can add critical protections. Also available are a list of users with risky apps, and a chart of peer-assessed app risk leveraging the CTR, and a chronology of the number of app authorizations recently granted.

On the top right, a bar graph tracks the number of apps in each risk category; clicking on the high-risk bar (below) revealed additional details of high risk apps by date, as well as details on each app included in the category. Clicking on the app name provided lists of all application events, users, and access scopes, and clicking on the ***Classify*** button enabled reclassification of the app. Administrators can easily and quickly see what kind of information each app has access to, under the Access Scopes column. For example, ESG Lab viewed the OAuth-connected app DocuSign access scopes, which include access to basic information, full access to data, limited access to data and files, and the ability to manage user activity. These access scopes can cause problems if used maliciously, a key reason that this app is classified as High Risk.



13 Unclassified | 0 Banned | 0 Restricted | 0 Under Audit | 0 Trusted | 13 Total

App | Classification | User | Install State | Detection Date | Scope Category | Source | Export App List

Cisco Cloudlock Risk Score

× High × Installed

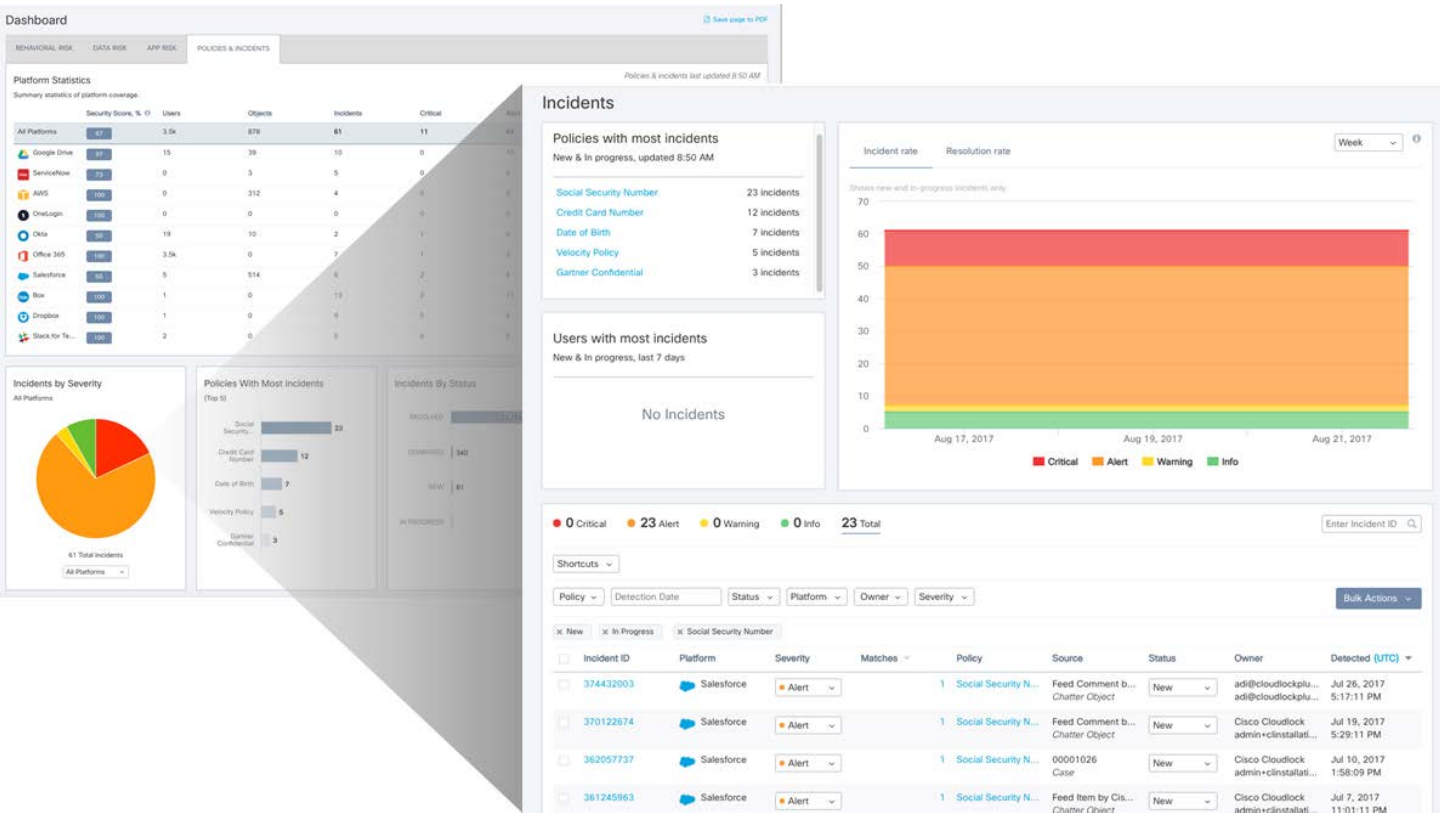
Clear all filters

| | App | Classification | Installed by | Access Scopes | Source | Risk | CTR | Detected (UTC) | Latest Install (UTC) |
|---|---|---|---|---|---|---|---|---|---|
| □ | Mapping Sheets | Classify | Admin<br>1 user | 4 scope cate... | Google<br>OAuth | High | Trusted by 48% | Aug 17, 2016<br>3:56:15 PM | Dec 14, 2016<br>10:53:16 AM |
| □ | DocuSign<br>*Editing/Authoring* | Classify | 2 users | 4 scope cate... | Google<br>OAuth | High | Trusted by 53% | Feb 24, 2017<br>8:23:15 AM | May 6, 2017<br>7:35:15 PM |
| □ | Graph explorer | Classify | Admin<br>3 users | 5 scope cate... | Azure AD<br>OAuth | High | | Dec 14, 2016<br>9:28:02 AM | Jul 20, 2017<br>1:33:23 PM |
| □ | Azendoo | Classify | 1 user | 4 scope cate... | Azure AD<br>OAuth | High | | Aug 21, 2017<br>1:33:23 PM | Aug 21, 2017<br>1:33:23 PM |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| □ | DocuSign<br>*Editing/Authoring* | Classify | 2 users | 4 scope categ... | Google<br>OAuth | High | Trusted by 53% |
| □ | Graph explorer | Classify | Admin<br>3 users | | | | |
| □ | Azendoo | Classify | 1 user | | | | |
| □ | カレンダーから日付入力 | Classify | Admin<br>No users | | | | |
| □ | [DEPRECATED] BetterCloud for | | Admin | | | | |

| Scopes | Access Scope Category |
|---|---|
| 2 | Basic Information |
| 1 | Full Data Access |
| 1 | Limited Access to Data and Files |
| 1 | Manage User Activity |

The final dashboard we viewed was for ***Policies & Incidents***. Each cloud platform is listed, along with a security score and the numbers of users of that platform; objects; incidents; critical issues; alerts; etc. A chart of ***Incidents by Severity*** can be filtered by cloud platform; clicking in the pie chart enables administrators to view incidents based on the policy breached. When ESG Lab clicked on the pie chart, a new view showed incidents by policy (below). There were 23 incidents related to the Social Security Number policy, 12 for the Credit Card Number policy, etc. A list of users with the most incidents is also available. A chart in the upper right can show data by either the level of incident (critical, alert, warning, or info), or by resolution rate. All incidents are listed at the bottom, and can be sorted by policy, status, platform, owner, or severity. The source of the incident is shown as well as owners, incident status, and time of detection.



Incidents

Policies with most incidents
New & In progress, updated 8:50 AM

| | |
|---|---|
| Social Security Number | 23 incidents |
| Credit Card Number | 12 incidents |
| Date of Birth | 7 incidents |
| Velocity Policy | 5 incidents |
| Gartner Confidential | 3 incidents |

Users with most incidents
New & In progress, last 7 days

No Incidents

● 0 Critical ● 23 Alert ● 0 Warning ● 0 Info 23 Total

Enter Incident ID

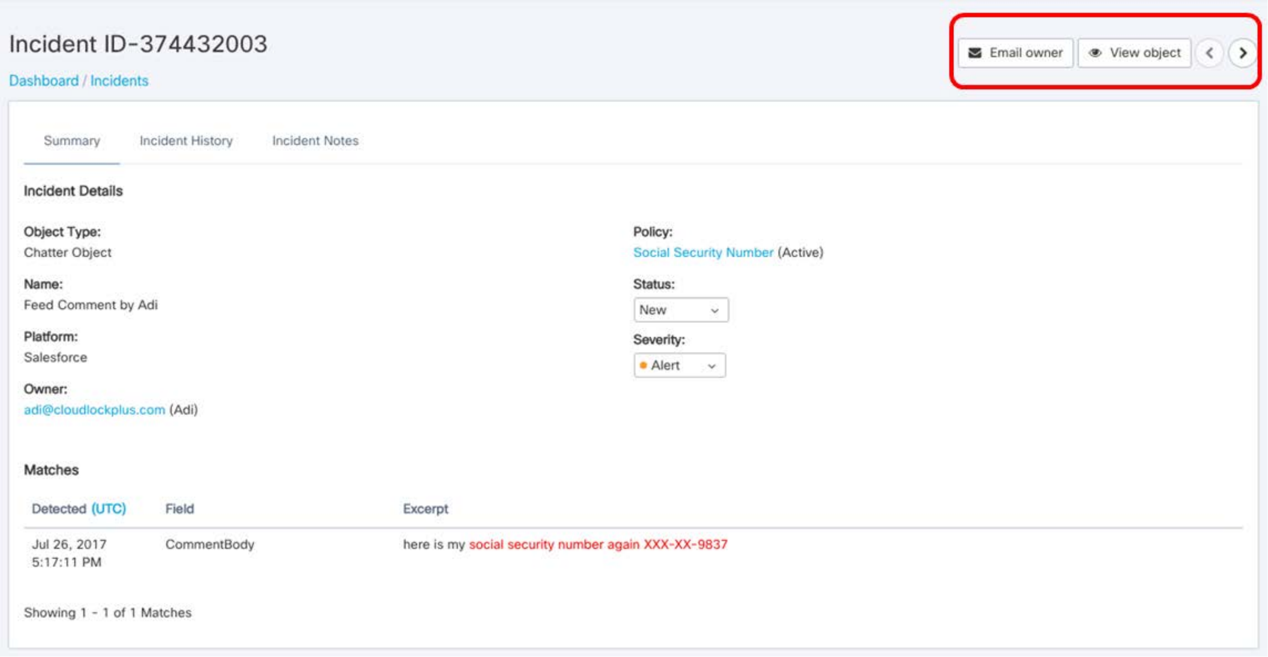
Shortcuts

Policy | Detection Date | Status | Platform | Owner | Severity | Bulk Actions

× New × In Progress × Social Security Number

| Incident ID | Platform | Severity | Matches | Policy | Source | Status | Owner | Detected (UTC) |
|---|---|---|---|---|---|---|---|---|
| 374432003 | Salesforce | ● Alert | 1 | Social Security N... | Feed Comment b...<br>*Chatter Object* | New | adi@cloudlockplu...<br>adi@cloudlockplu... | Jul 26, 2017<br>5:17:11 PM |
| 370122674 | Salesforce | ● Alert | 1 | Social Security N... | Feed Comment b...<br>*Chatter Object* | New | Cisco Cloudlock<br>admin+clinstallati... | Jul 19, 2017<br>5:29:11 PM |
| 362057737 | Salesforce | ● Alert | 1 | Social Security N... | 00001026<br>*Case* | New | Cisco Cloudlock<br>admin+clinstallati... | Jul 10, 2017<br>1:58:09 PM |
| 361245963 | Salesforce | ● Alert | 1 | Social Security N... | Feed Item by Cis...<br>*Chatter Object* | New | Cisco Cloudlock<br>admin+clinstallati... | Jul 7, 2017<br>11:01:11 PM |

We clicked on incident *ID-374432003*, which brought up details and a history of a violation of a social security number policy. A button in the upper right enables administrators to email the incident owner, and also to view the object that prompted the incident. Making incident details immediately viewable enables IT to check with users and take action immediately if needed.



Incident ID-374432003

Dashboard / Incidents

Incident Details

**Object Type:** Chatter Object

**Name:** Feed Comment by Adi

**Platform:** Salesforce

**Owner:** adi@cloudlockplus.com (Adi)

**Policy:** Social Security Number (Active)

**Status:** New

**Severity:** ● Alert

Matches

| Detected (UTC) | Field | Excerpt |
|---|---|---|
| Jul 26, 2017<br>5:17:11 PM | CommentBody | here is my social security number again XXX-XX-9837 |

Showing 1 - 1 of 1 Matches

## Why This Matters

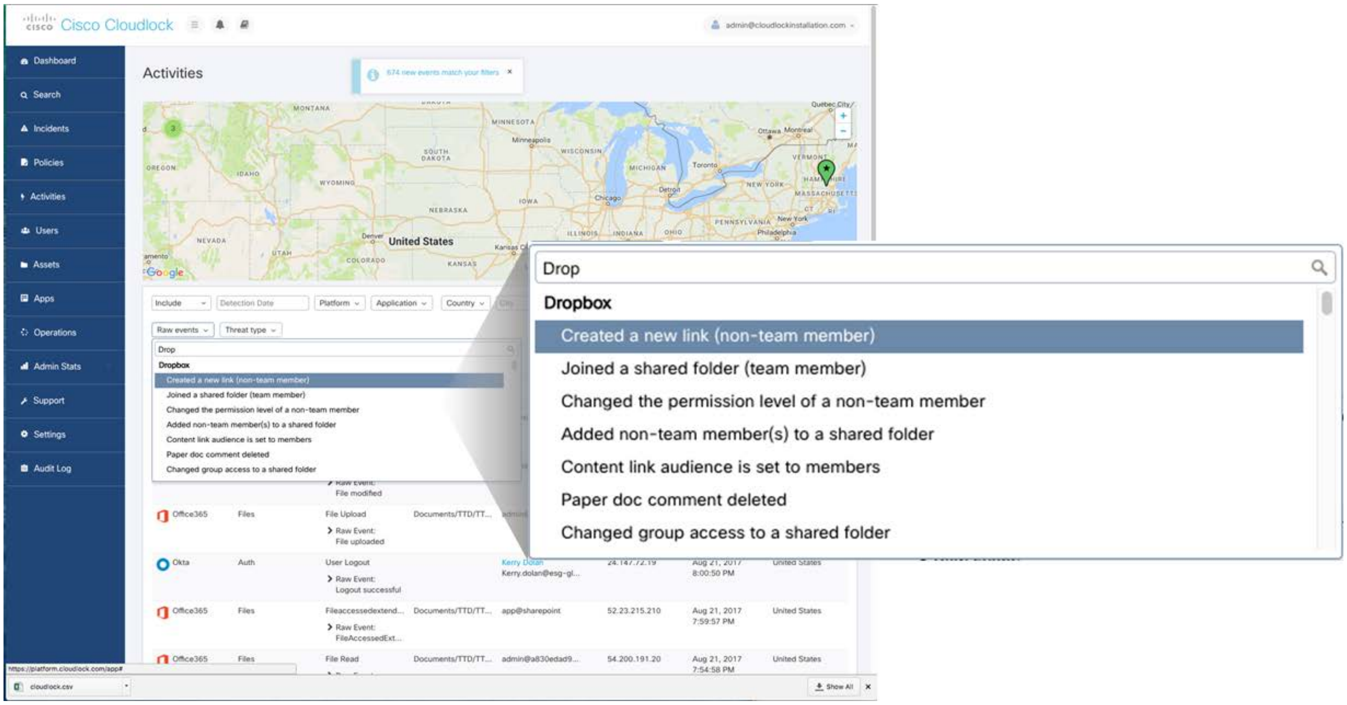
In recent ESG research with midmarket and enterprise organizations, 69% of respondents reported that they are currently using SaaS, and another 15% are planning to do so.[2] Cloud applications have become a major part of business. But traditional security solutions that focus on network activities cannot see what's happening with these applications, much less manage their access and security.

Email and DNS security solutions generally operate based on volume—IT is alerted to potential problems by unusual bursts of activity. But what happens if it's a "low and slow" attack? An OAuth attack targeting a privileged user—such as a C-level executive or high-level IT administrator—won't be detected by these methods. Organizations need a solution that looks at which users are accessing which applications, and how they are using and sharing data.

ESG Lab validated the ease of viewing cloud application usage details using Cisco Cloudlock to assess behavior, data, and application risks. The dashboard views aggregate important details that can alert IT to potential problems and enable them to take immediate action.

### Menus and Actions

Cloudlock provides flexible navigation options so that administrators can monitor and manage tasks by incident, policy, activity, user, asset, or application. For example, using the ***Activities*** menu, ESG Lab viewed all activities occurring in the U.S. for all cloud platforms; with one click we also exported the details to a .csv file. Activities can be viewed by platform, application, location, user, IP address, event type, raw events, or threat types. The figure below shows activities on all platforms in use, and the map shows the location of the request (with the star) as well as the number of activities in a given location. ESG Lab demonstrated the ability to select a specific event from a specific cloud platform to view, in this case the drop-down list of Dropbox events. Cloudlock provides the ability to monitor many types of activities, such as unexpectedly large data downloads, logins by users in unexpected locations, etc., that can alert administrators to potential breaches.


Cisco Cloudlock
admin@cloudlockinstallation.com
Dashboard
Search
Incidents
Policies
Activities
Users
Assets
Apps
Operations
Admin Stats
Support
Settings
Audit Log
Activities
674 new events match your filters
United States
Include
Detection Date
Platform
Application
Country
Raw events
Threat type
Drop
Dropbox
Created a new link (non-team member)
Joined a shared folder (team member)
Changed the permission level of a non-team member
Added non-team member(s) to a shared folder
Content link audience is set to members
Paper doc comment deleted
Changed group access to a shared folder
https://platform.cloudlock.com/app#
cloudlock.csv
Show All

Raw Event: File modified

Office365 Files File Upload Documents/TTD/TT... admin...
Raw Event: File uploaded

Okta Auth User Logout Kerry Dolan Kerry.dolan@esg-gl... 24.147.72.19 Aug 21, 2017 8:00:50 PM United States
Raw Event: Logout successful

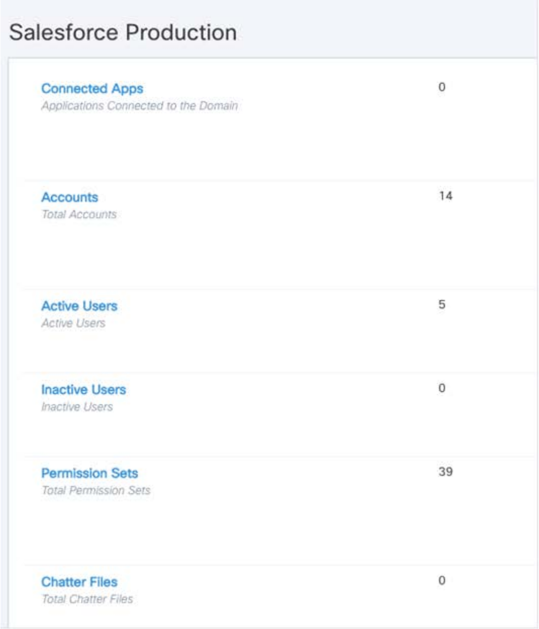
Office365 Files Fileaccessedextend... Documents/TTD/TT... app@sharepoint 52.23.215.210 Aug 21, 2017 7:59:57 PM United States
Raw Event: FileAccessedExt...

Office365 Files File Read Documents/TTD/TT... admin@a830edad9... 54.200.191.20 Aug 21, 2017 7:54:58 PM United States

[2] Source: ESG Research Report, *Public Cloud Computing Trends*, April 2017.

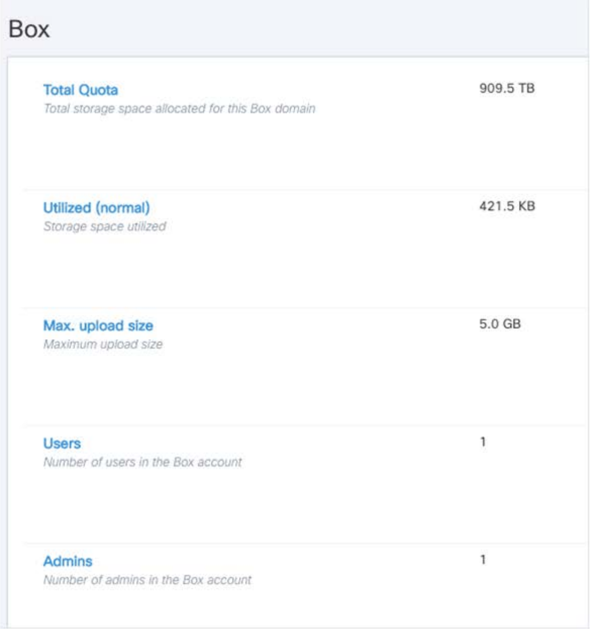
## Details Provided by Cloud Platform APIs

A key feature of Cisco Cloudlock is the API connection that enables Cloudlock to display details gathered directly from each cloud platform. Cloudlock can include whatever details each cloud platform makes available through APIs. For example, Salesforce provides details on connected apps, accounts, users, permissions, Chatter, opportunities, leads, etc.; Box APIs provide storage utilization details including total storage quota, storage utilized, maximum upload size, number of users, etc. These enable administrators to keep track of users and activities in the context of each application, enabling a more complete picture of application usage that supports better security.



Salesforce Production

| | |
|---|---|
| Connected Apps<br>Applications Connected to the Domain | 0 |
| Accounts<br>Total Accounts | 14 |
| Active Users<br>Active Users | 5 |
| Inactive Users<br>Inactive Users | 0 |
| Permission Sets<br>Total Permission Sets | 39 |
| Chatter Files<br>Total Chatter Files | 0 |



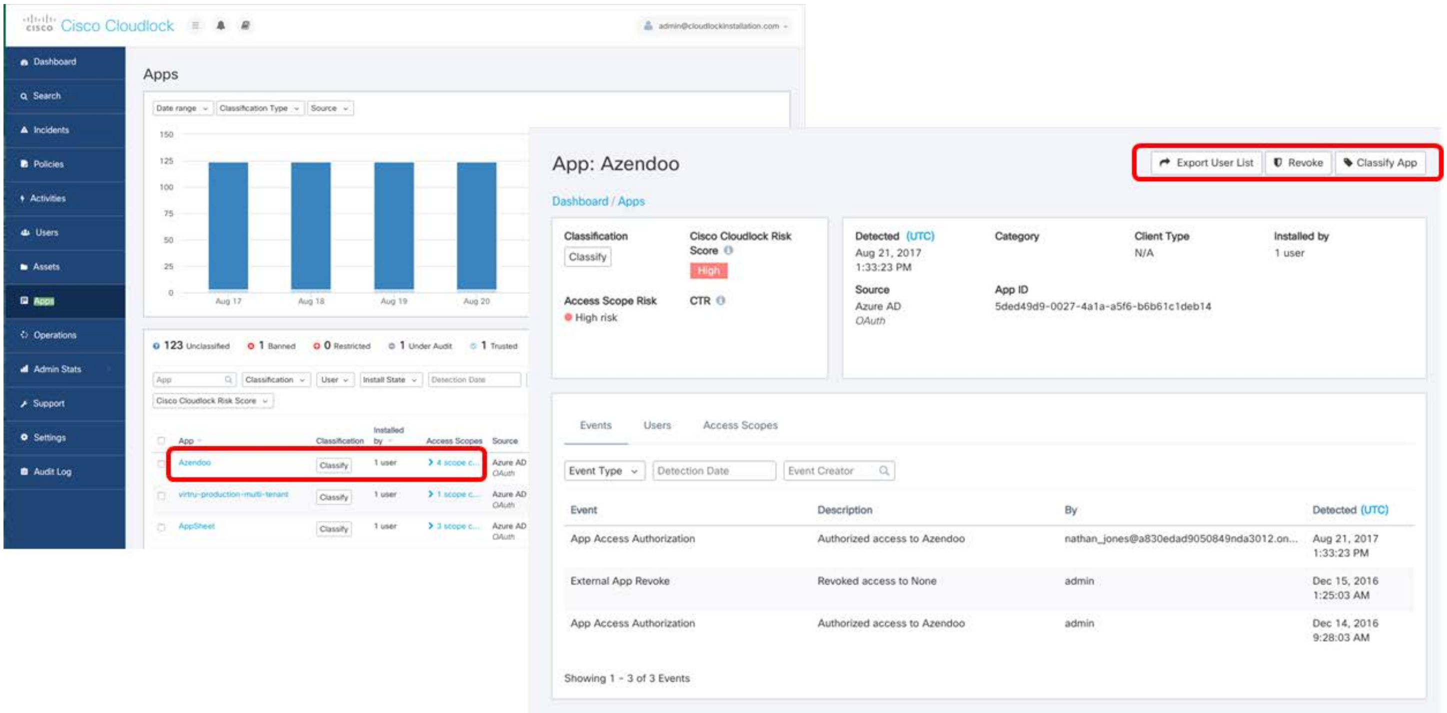
Box

| | |
|---|---|
| Total Quota<br>Total storage space allocated for this Box domain | 909.5 TB |
| Utilized (normal)<br>Storage space utilized | 421.5 KB |
| Max. upload size<br>Maximum upload size | 5.0 GB |
| Users<br>Number of users in the Box account | 1 |
| Admins<br>Number of admins in the Box account | 1 |

## Viewing and Managing by Application

Cloudlock enables organizations to better understand how applications are being used, and their associated risks. Administrators can view applications being used in each organization, often bringing to light "shadow IT" applications of which IT has no knowledge. With this visibility, organizations can select which cloud apps to keep and which are too risky. They can also permit application usage by user or department, instead of banning apps completely. Cloudlock ingests data from firewalls and proxies such as Cisco ASA and Cisco Firepower, and augments this with cybersecurity insight such as risk ratings, traffic volumes, and most active users, to help organizations understand and remediate risks.

The *Apps* tab provides details for each application including classification (trusted, banned, etc.) risk level, number of users, access scopes, and when the app was detected. Drilling down on each app, organizations can view every event that has occurred with that app, when, and which users were involved.



123 Unclassified · 1 Banned · 0 Restricted · 1 Under Audit · 1 Trusted

| App | Classification | Installed by | Access Scopes | Source |
|---|---|---|---|---|
| Azendoo | Classify | 1 user | 4 scope c... | Azure AD<br>OAuth |
| virtru-production-multi-tenant | Classify | 1 user | 1 scope c... | Azure AD<br>OAuth |
| AppSheet | Classify | 1 user | 3 scope c... | Azure AD<br>OAuth |

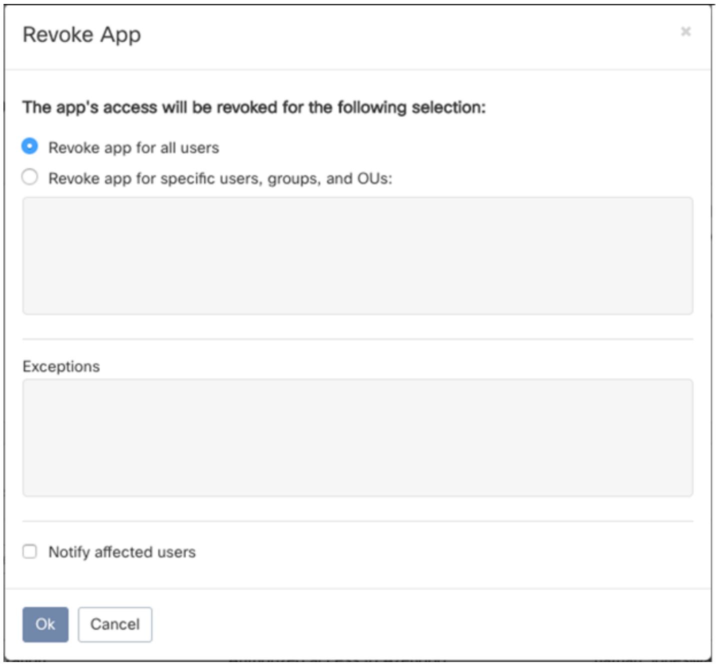
App: Azendoo

Classification: Classify
Cisco Cloudlock Risk Score: High
Access Scope Risk: High risk
CTR
Detected (UTC): Aug 21, 2017 1:33:23 PM
Category
Client Type: N/A
Installed by: 1 user
Source: Azure AD *OAuth*
App ID: 5ded49d9-0027-4a1a-a5f6-b6b61c1deb14

| Event | Description | By | Detected (UTC) |
|---|---|---|---|
| App Access Authorization | Authorized access to Azendoo | nathan_jones@a830edad9050849nda3012.on... | Aug 21, 2017<br>1:33:23 PM |
| External App Revoke | Revoked access to None | admin | Dec 15, 2016<br>1:25:03 AM |
| App Access Authorization | Authorized access to Azendoo | admin | Dec 14, 2016<br>9:28:03 AM |

Showing 1 - 3 of 3 Events

One of administrators' first tasks when deploying Cloudlock is to classify their apps as trusted, banned, restricted, or under audit. This can be done in groups of applications, such as banning all applications with a low CTR score or that require too wide an access scope. When apps are classified as banned, OAuth tokens are revoked and connections are severed. When new apps are discovered, they can be automatically classified based on these details. The figure above shows the Apps main screen on the left; on the right is a the drill-down view into the OAuth-connected app Azendoo. Classification, risk, and event details are provided, and administrators can take actions: export a list of users, revoke the OAuth token, or classify the app. The figure at right shows the ***Revoke App*** dialog box.



The app's access will be revoked for the following selection:

● Revoke app for all users
○ Revoke app for specific users, groups, and OUs:

Exceptions

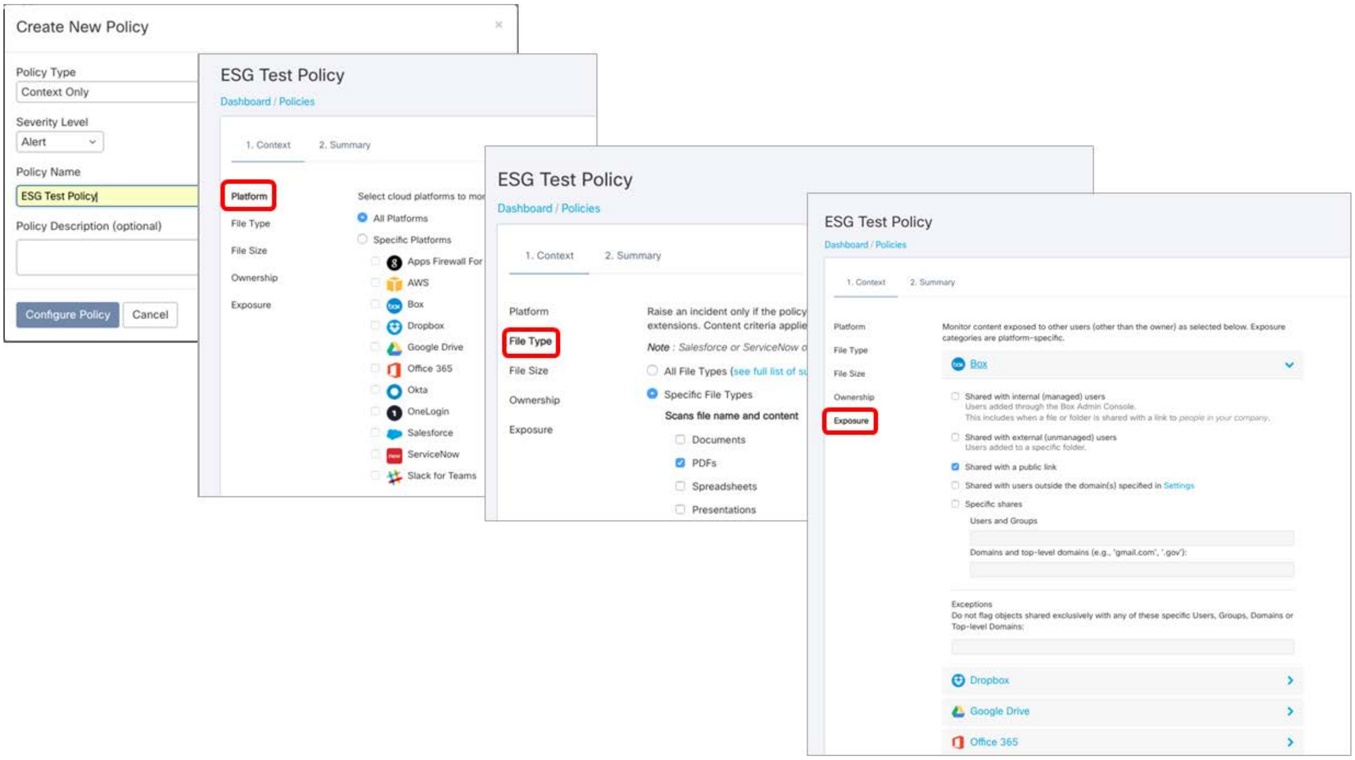
□ Notify affected users

## Creating Policies to Automate Security

Policies are a powerful tool for protection from risky applications, data exposures, and user behaviors. Cloudlock includes 80+ policies out of the box, and organizations can create their own. Policies can be created and pushed out to multiple cloud platforms, saving IT from having to create individual policies for each cloud. An organization might want to whitelist some applications and ban the rest, or ban applications with a certain level of access. For example, ESG Lab could edit the Risky Access Scopes policy so that any app requesting full data access would be automatically banned, and notification would be sent to the user.

While many policies come pre-configured and can be edited, administrators can easily create their own policies. ESG Lab created a policy that would monitor all cloud platforms for any PDF files that were being shared with public links; this type of policy makes administrators aware of potential data exposure.

From the Policies main page, we clicked the ***Add a Policy*** button, and created a new policy, selecting the ***Alert*** severity level. On the ***Platform*** screen, we chose to monitor all cloud platforms; on the ***File Types*** screen we selected PDFs, with no file size defined; and on the ***Ownership*** screen, applied the policy to all users. Other options included specifying users to monitor, or specifying user or group exceptions that would not be monitored for this policy. Using the ***Exposure*** screen, we configured for each cloud platform the ***Shared with public link*** parameter. A summary page enabled us to review the policy before saving the changes. Once we clicked ***Save All Changes***, the policy appeared in the main list.



Create New Policy

Policy Type: Context Only

Severity Level: Alert

Policy Name: ESG Test Policy

Policy Description (optional)

ESG Test Policy

Select cloud platforms to mo

● All Platforms

○ Specific Platforms

□ Apps Firewall For

□ AWS

□ Box

□ Dropbox

□ Google Drive

□ Office 365

□ Okta

□ OneLogin

□ Salesforce

□ ServiceNow

□ Slack for Teams

ESG Test Policy

Raise an incident only if the policy extensions. Content criteria applie

*Note* : *Salesforce or ServiceNow o*

○ All File Types (see full list of su

● Specific File Types

Scans file name and content

□ Documents

☑ PDFs

□ Spreadsheets

□ Presentations

ESG Test Policy

Monitor content exposed to other users (other than the owner) as selected below. Exposure categories are platform-specific.

Box

□ Shared with internal (managed) users
Users added through the Box Admin Console.
This includes when a file or folder is shared with a link to *people in your company*.

□ Shared with external (unmanaged) users
Users added to a specific folder.

☑ Shared with a public link

□ Shared with users outside the domain(s) specified in Settings

□ Specific shares

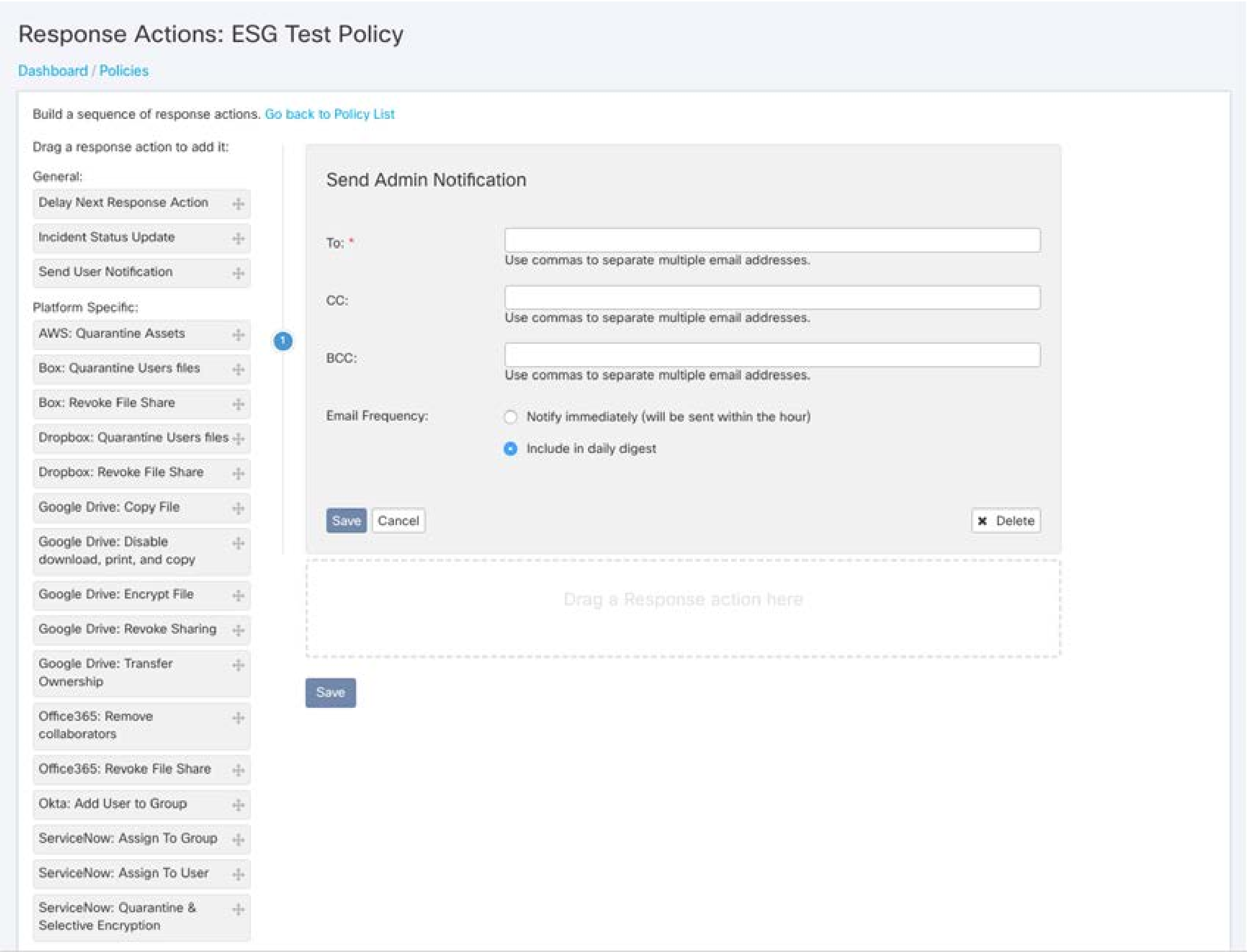
Users and Groups

Domains and top-level domains (e.g., 'gmail.com', '.gov'):

Exceptions
Do not flag objects shared exclusively with any of these specific Users, Groups, Domains or Top-level Domains:

Next, we added general and platform-specific response actions to the policy by clicking the ***Create*** button in the response actions column. This automates what happens when the policy is violated. We selected several response actions by dragging them into the spaces on the right, including sending a notification to administrators, which could be immediate or daily, and sending a notification to the user as a reminder not to share content with public links. The full user notification email can be created right there in the policy, including a header with an image, text, and a footer; an automatically generated table in the notification would show the user the specific method of policy breach, such as the file name and type, and the number of times the policy had been breached.

In addition, individual cloud platforms offer specific response action options. File sharing platforms such as Box, Dropbox, and Google Drive offer the option to remove file shares and quarantine users or assets, disable the ability to download, print, or copy, etc. These make it easy to automatically protect organizations from malicious operations. The final response action we added was to update the status to ***Resolved***. Once the policy is violated, administrators are alerted, the user is alerted, and the incident will show up as "resolved" in the incident list. A notification informed us that the workflow had been completed successfully. The policy can be deactivated, edited, or reactivated from the Policies page.



Response Actions: ESG Test Policy

Dashboard / Policies

Build a sequence of response actions. Go back to Policy List

Drag a response action to add it:

General:

- Delay Next Response Action
- Incident Status Update
- Send User Notification

Platform Specific:

- AWS: Quarantine Assets
- Box: Quarantine Users files
- Box: Revoke File Share
- Dropbox: Quarantine Users files
- Dropbox: Revoke File Share
- Google Drive: Copy File
- Google Drive: Disable download, print, and copy
- Google Drive: Encrypt File
- Google Drive: Revoke Sharing
- Google Drive: Transfer Ownership
- Office365: Remove collaborators
- Office365: Revoke File Share
- Okta: Add User to Group
- ServiceNow: Assign To Group
- ServiceNow: Assign To User
- ServiceNow: Quarantine & Selective Encryption

1

Send Admin Notification

To: *
Use commas to separate multiple email addresses.

CC:
Use commas to separate multiple email addresses.

BCC:
Use commas to separate multiple email addresses.

Email Frequency:
○ Notify immediately (will be sent within the hour)
● Include in daily digest

## Why This Matters

As cloud applications and shadow IT add risk to corporate environments, ESG research respondents are looking to CASB solutions to improve visibility and control. IT administrators cannot control what they cannot see, making better visibility a key priority. In our survey, 66% of respondents reported currently using CASB in their organizations, with another 16% engaged in proof-of-concept projects.[3] They indicated that they are looking to discover what cloud applications are in use, identify risks associated with those applications, gain control over which users can access which applications, and add more granular data loss prevention requirements.

ESG Lab validated that Cisco Cloudlock policies and workflows enable visibility and control across multiple cloud platforms, alerting administrators to anomalous behaviors, as well as enabling automatic protections as users explore new cloud applications. This provides organizations with a safety mechanism regarding applications, data, and users. They can be immediately aware of what applications are being used; understand OAuth-generated inter-cloud activities; identify compromised user accounts; and discover data exposures.

The power of Cisco Cloudlock is the ability to centrally monitor and control cloud application vulnerabilities across an organization. If you have 1,000  applications, it difficult to not only view all that's going on, but also create the policies required for security. The Cloudlock framework simplifies visibility and control across an organization's entire environment, enabling superior security.

[3] Source: ESG Research Report, *The Visibility and Control Requirements of Cloud Application Security*, May 2016.

## The Bigger Truth

The daily life of today's knowledge worker includes multiple devices and applications, including many in the cloud: for productivity (i.e., Office 365, Google Docs); file sharing (i.e., Box, Dropbox); customer relationship management (i.e., Salesforce); contracts management (i.e., DocuSign); and many other services. As they can work from a laptop or smartphone from any location, employees are constantly using cloud applications and sharing their identities and personal credentials in the cloud, increasing the cyber threat attack surface.

Since employees can access consumer applications from any location, they feel entitled to the same frictionless access at work. And why shouldn't they? As a side effect, however, IT no longer has complete control of the data and identity environment, and that can seriously complicate security. Add to this scenario the fact that security built for on-premises data and infrastructures may not adequately protect cloud applications, and you begin to see the struggle with which organizations and IT departments are faced.

The reality is that more attacks are originating in the cloud. While the May 2017 Google attack is over, organizations should expect that other attacks are constantly in play. If you don't assume you're under attack from hackers, you will be woefully underprepared. Just ask Sony, or HBO, the DNC, or the French election authorities, Merck, Cadbury, Ukrainian ATMs. . . you get the picture.

While some breaches are malicious, others are innocent, resulting from employees finding cloud applications to help them do their jobs. So-called "shadow IT" is often just employees looking for a way to streamline their processes to get more done; similarly, OAuth is a useful credentialing tool that simply needs additional protection. Neither of these is a bad thing—but IT needs to know about them and provide proper cloud application security.

It makes sense, then, that 86% of ESG research respondents say that their cloud security spending will increase in the next year. Forty-two percent said they plan to purchase CASB products to improve the policy environment and oversight of cloud applications, making it the second most-cited action that organizations plan to take in the next 12-24 months regarding cloud security, after investing in cloud security skills development.[4]

But all CASBs are not the same. ESG Lab validated that the Cisco Cloudlock API-based CASB can help organizations improve user, data, and application security. It makes shadow IT and cloud applications visible so that IT can better protect the environment. Cloudlock can encrypt cloud data, detect malware payloads, provide granular control of user access to sensitive data, set policies and alerts, detect anomalous activity, and revoke application permissions. It is easy to deploy and doesn't use proxies, making it faster to deploy and eliminating any impact on application performance. Cisco Cloudlock brings cloud-connected applications into full view so they can be properly used with full security.

[4] Ibid.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.

ESG

**Enterprise Strategy Group** is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com contact@esg-global.com P. 508.482.0188