

# Cloud App Security

Bring visibility, control, and protection for your cloud apps

More and more organizations are adopting SaaS apps, not only to reduce costs but also to unlock competitive advantages such as improved time to market and better collaboration. Even if your company does not use cloud applications, your employees probably do. According to research, more than 80 percent of employees\* admit to using non-approved SaaS apps in their jobs.




With this fast transition to cloud apps, we know you may be concerned about storing corporate data in the cloud and how to make it accessible to users anywhere without comprehensive visibility, auditing, or controls. Legacy security solutions are not designed to protect data in SaaS applications. Traditional network security solutions, such as firewalls and IPS, don't offer visibility into the transactions that are unique to each application and traffic off-premises, including how data is being used and stored. Classic controls fail to provide protection for cloud apps as they monitor only a small subset of cloud traffic and have limited understanding of app-level activities.

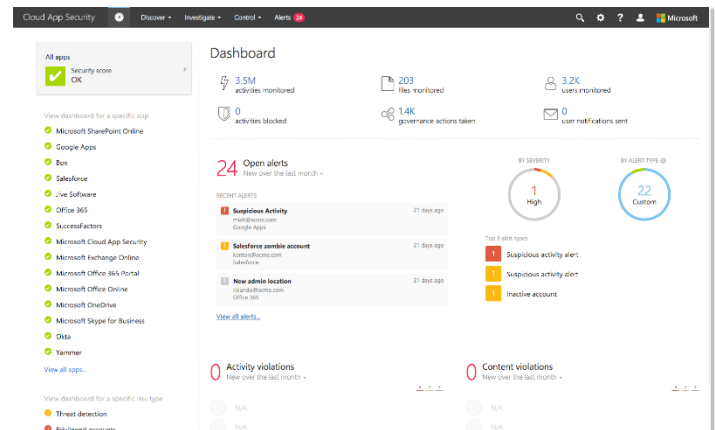
So how can you maintain visibility, control, and protection of your cloud apps? We have your solution: Microsoft Cloud App Security is a comprehensive service that provides deeper visibility, comprehensive controls, and improved protection for your cloud applications. Cloud App Security is designed to help you extend the visibility, auditing, and control you have on-premises to your cloud applications.

So how can you maintain visibility, control, and protection of your cloud apps? We have your solution:

Microsoft Cloud App Security is a comprehensive service that provides deeper visibility, comprehensive controls, and improved protection for your cloud applications. Cloud App Security is designed to help you extend the visibility, auditing, and control you have on-premises to your cloud applications.

## What does Cloud App Security provide?

|   |   |
|---|---|
|  <p><b>Discovery</b></p>         | <p>It all starts with discovery. Cloud App Security identifies all cloud applications in your network—from all devices—and provides risk scoring and ongoing risk assessment and analytics. No agents required: information is collected from your firewalls and proxies to give you complete visibility and context for cloud usage and shadow IT.</p> |
|  <p><b>Data control</b></p>      | <p>Approving an application to be used is not enough. With special focus on sanctioned apps, you can set granular controls and policies for data sharing and DLP. You shape your cloud environment using out-of-the box and custom policies.</p>  |
|  <p><b>Threat protection</b></p> | <p>Cloud App Security provides threat protection for your cloud applications that's enhanced with vast Microsoft threat intelligence and research. Identify high-risk usage, security incidents, and detect abnormal user behavior to prevent threats.</p>  |



\*<http://www.computing.co.uk/ctg/news/2321750/more-than-80-per-cent-of-employees-use-non-approved-saas-apps-report>

# Key features



## Discovery Risk assessment

Cloud App Security not only discovers 13,000 cloud applications in use, but also provides a risk score by evaluating each discovered service against more than 60 parameters: evaluating the service provider, security mechanisms, and compliance certifications. These details help determine and assess the credibility and reliability of each cloud service discovered, represented by a risk score. Cloud App Security gives you the tools to perform a total risk assessment for each service, based on a combination of risk score and usage.

| Name                              | Traffic  | Upload  | Transactions | Score  | Users | IP addresses | Last seen (UTC) |
|-----------------------------------|----------|---------|--------------|--------|-------|--------------|-----------------|
| 31 all apps                       |          |         |              |        |       |              |                 |
| 15 sanctioned apps                |          |         |              |        |       |              |                 |
| 0 unsanctioned apps               |          |         |              |        |       |              |                 |
| 16 other apps                     |          |         |              |        |       |              |                 |
| Caplio                            | 193.9 MB | 5.8 GB  | 99           | Yellow | 96    | 20           | Feb 22, 2016    |
| Google Apps Collaboration         | 78.5 GB  | 4.7 GB  | 21.0         | Green  | 5     | 9            | Mar 15, 2016    |
| ANIX Collaboration                | 79.4 MB  | -       | 10           | Yellow | 3     | 0            | Jan 30, 2016    |
| Do Project management             | 1.3 KB   | 402.0 B | 3            | Yellow | 2     | 2            | Feb 20, 2016    |
| The Web Pro Converter             | 146.7 KB | 18.6 GB | 2            | Yellow | 2     | 2            | Feb 22, 2016    |
| VIX Social network                | 17.4 MB  | -       | 4            | Yellow | 2     | 0            | Jan 26, 2016    |
| YouTube Content sharing           | 8.8 KB   | 2.6 GB  | 26           | Green  | 2     | 2            | Jan 30, 2016    |
| Acronis Collaboration             | 45.5 KB  | 48.8 GB | 1            | Yellow | 1     | 1            | Feb 7, 2016     |
| Atlassian Jira Project management | 45.5 KB  | 48.8 GB | 1            | Green  | 1     | 1            | Feb 10, 2016    |
| Box Cloud storage                 | 96.7 KB  | 9.8 GB  | 1            | Green  | 1     | 1            | Feb 28, 2016    |

## Powerful reporting and analytics

Discovering which applications are in use across an organization is just the first step in making sure sensitive corporate data is protected. Understanding use cases, identifying top users, and determining the risk associated with each application are all important components to understanding an organization’s overall risk posture. With Cloud App Security, we provide ongoing risk detection, analytics, and powerful reporting on users, usage patterns, upload/download traffic, and transactions so that you can identify anomalies right away.



## Data control Policy setting and enforcement

Granular-control security policies can be built easily. You can use out-of-the-box policies or build and customize your own. Every insight is actionable, allowing you to remediate with a single click or implement data sharing and granular usage policies.

| Name  | Count         | Severity | Risk category | Action      | Modified     |
|---|---------------|----------|---------------|-------------|--------------|
| PCI COMPLIANCE: Publicly shared files with credit card info | 2 matches     | Red      | Compliance    | Open alerts | Jul 20, 2015 |
| User login from a non-managed IP address                    | 0 open alerts | Red      | —             | Open alerts | Mar 8, 2016  |
| Account Discovery Policy                                    | 0 open alerts | Red      | —             | Open alerts | Mar 8, 2016  |
| Users shared by a single user                               | 0 open alerts | Red      | —             | Open alerts | Mar 14, 2016 |
| Testing   | 0 open alerts | Blue     | —             | Open alerts | Mar 14, 2016 |
| Denies for file   | 0 open alerts | Blue     | —             | Open alerts | Mar 17, 2016 |

## DLP and Data Sharing Control

You can govern data in the cloud, such as files that are stored in cloud drives, as attachments, or within cloud application fields. Use pre-defined fields or extend existing enterprise DLP policies to your SaaS applications. Dynamic reports can run on DLP violations, sensitive file sharing, and data-sharing violations. Data control in the cloud helps you comply with regulatory mandates such as PCI, HIPPA, and more.



## Threat protection User behavioral analytics

Cloud App Security helps you to stay ahead of attackers. You can identify anomalies in your cloud usage that may be indicative of a data breach. Cloud App Security advanced machine learning heuristics learn how each user interacts with each SaaS application and, through behavioral analysis, assesses the risks in each transaction. This includes simultaneous logins from two countries, the sudden download of terabytes of data, or multiple failed login attempts that may signify a brute force attack.

| App                       | Location        | Severity | Date        |
|---------------------------|-----------------|----------|-------------|
| Suspicious Activity       | Google Apps     | Red      | 21 days ago |
| New admin location        | Office 365      | Blue     | 21 days ago |
| Customer email account    | Salesforce      | Blue     | 21 days ago |
| General Anomaly Detection | Exchange Online | Blue     | 21 days ago |
| Suspicious Activity       | Google Apps     | Blue     | 21 days ago |
| Suspicious Activity       | Google Apps     | Blue     | 21 days ago |
| Suspicious Activity       | Google Apps     | Blue     | 21 days ago |

## Why you'll love Cloud App Security



### Shadow IT discovery— no agents required

The discovery feature identifies more than 13,000 apps that are being used and assesses risk—no agents required—Cloud App Security collects information from firewalls and proxies.



### Granular controls for your sanctioned apps

Special focus and comprehensive controls for your sanctioned apps help you set policies and enforce them—from data sharing to DLP and data security. We've committed to supporting third-party cloud apps as well as Microsoft cloud apps.



### Enterprise-grade and easy

Cloud App Security is scalable, non-intrusive, and integrates with the enterprise cloud framework. It provides a simple deployment and management process. You can integrate with your existing SIEM, IAM, SSO, and analytical solutions.



### Enhanced threat protection with Microsoft intelligent security graph

Anomaly detection draws from Microsoft's vast amount of threat intelligence and security research data. Cloud App Security benefits from Microsoft's holistic, agile security platform, and is informed by insights from our intelligent security graph.



### Builds on broader Microsoft platform

Our solutions work together to deliver a holistic, agile security platform. Cloud App Security is not a point solution: it is a key part of our vision and is enhanced with insights from our other Microsoft security solutions.

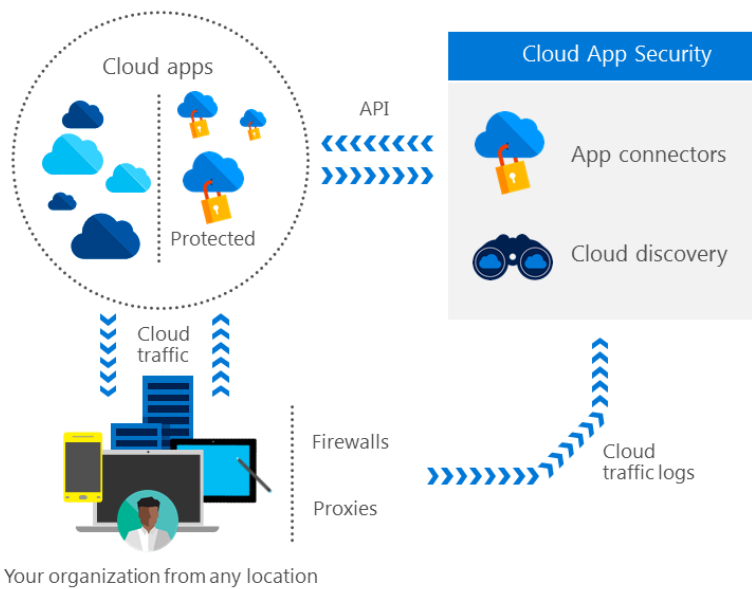


### Office 365 Deep integration with Office

Cloud App Security integrates deeply with Office. It provides new advanced security management and transparency capabilities for Office 365.

*"At Box, we believe in a modern content management and collaboration experience where information can move easily and securely between individuals and organizations and across devices and applications. By working closely with Microsoft Cloud App Security, we're providing businesses with stronger controls and deeper visibility around their cloud apps, and protecting against unwanted access to critical business content."* Roger Murff, Vice President of Technology Partnerships at Box

### How does it work?



#### Discovery

Cloud discovery uses your traffic logs to discover and analyze which cloud apps are in use. You can manually upload log files for analysis from your firewalls and proxies, or you can choose automatic upload.

#### Sanctioning and un-sanctioning

Cloud App Security enables you to sanction/block apps in your organization, using the Cloud app catalog.

The Cloud app catalog rates risk for your cloud apps based on regulatory certifications, industry standards, and best practices. You can then customize the scores and the weights of various parameters to your organization's needs. Based on these scores, Cloud App Security lets

you know how risky the app is, according to over 50 risk factors that might affect your environment.

#### App connectors

App connectors leverage APIs provided by various cloud app providers to enable the Cloud App Security cloud to integrate with other cloud apps and extend control and protection. This enables Cloud App Security to pull information directly out of cloud apps for analysis.

In order to connect an app and extend protection, the app administrator authorizes Cloud App Security to access the app, and then Cloud App Security queries the app for activity logs and scans data, accounts, and cloud content. Cloud App Security can then enforce policies, detect threats, and provide governance actions for resolving issues.

#### Policy setting

Policies allow you to define the way you want your users to behave in the cloud. They enable you to detect risky behavior, violations or suspicious data points, and activities in your cloud environment, and, if required, to integrate remediation processes to achieve complete risk mitigation. There are multiple types of policies that correlate to the different types of information you want to gather about your cloud environment and the types of remediation actions you may want to take.