Enhancing threat detection at Microsoft using Microsoft Cloud App Security

More employees than ever before are accessing and using cloud apps for work purposes. As apps are moving to the cloud, Microsoft IT has an ongoing need to ensure that corporate data is both accessible and secure. We’ve begun deploying Microsoft Cloud App Security to enable the discovery of cloud apps that are in use from within our environment. Cloud App Security also provides enhanced threat detection and protection, and it enables us to shape our cloud environment by setting granular controls or custom policies. It does this by drawing from the vast amount of threat intelligence and security research data that has already been gathered by Microsoft, and it's informed by insights from the Microsoft intelligent security graph.

Business challenge: Traditional security solutions weren’t designed to protect data in cloud apps

Before the deployment of Cloud App Security, we didn’t have any behavioral analytics coverage to help us identify potential threats for cloud apps. There wasn’t an easy way to discover all of the cloud apps used within the corporate network, to create app risk profiles, or to monitor normal and anomalous user and administrator activity, device and user agents, and activity types.

Legacy security solutions weren’t designed to protect data in cloud apps. And traditional network security solutions—such as firewalls—don’t offer visibility into the transactions that are unique to each application. They also don’t provide visibility into off-premises traffic, including how data is being used and stored.

We needed the ability to proactively discover the various cloud apps that are currently in use, and the ability to create alerting policies that provide threat detection and data control to Microsoft Office 365 and other sanctioned cloud apps. Having this information would help us to protect the company by understanding normal versus anomalous sign-in activities and processes. We needed an enterprise solution that we could easily integrate into our existing monitoring systems and infrastructure.

Deploying Microsoft Cloud App Security

Cloud App Security is a generally available subscription service. It’s scalable, agentless (requiring no client installation), and runs in the background with no impact to end users. It integrates with our current security information and event management, identity and access management, single sign-on, and analytical solutions.

We deployed the first phase of Cloud App Security in a pilot program that includes coverage for several firewalls within our infrastructure. Our goals included:

- Gaining a better understanding about the use of cloud apps and the related risks.
- Discovering cloud systems and solutions within our environment that have been built and/or are being used without our explicit organizational approval (shadow IT).
- Identifying the use cases that would help us to monitor for patterns of anomalous activities, such as a suspicious pattern for failed sign-in attempts or a privileged activity being attempted by a non-privileged user.

During this phase, we focused our efforts on deploying a few key capability areas of Cloud App Security:

- **Discovery.** Cloud App Security identifies all cloud apps on the network—from all devices. It provides risk scoring and ongoing risk assessment and analytics. Information is collected from firewalls and proxies to provide visibility and context for cloud usage and shadow IT.
Data control. We can create granular policies that provide threat detection, data loss prevention (DLP), and data control to Office 365 and other sanctioned cloud apps.

Threat detection. Cloud App Security provides threat detection for cloud apps that’s enhanced with Microsoft threat intelligence and research.

As early adopters of Cloud App Security, we worked closely with the product group to validate enterprise functionality and provide feedback about how Cloud App Security was helping us address our common security questions as defined in our User and Entity Behavior Analytics (UEBA) scenarios. Some of the user behaviors that we monitored for included:

- Sign-ins from two countries or regions that represent an impossible journey.
- Large data downloads.
- Multiple failed sign-in attempts that may indicate a brute force attack.

Discovery

Discovering which apps are in use across an organization is the first step in making sure sensitive corporate data is protected. Cloud Discovery uses uploaded traffic logs (manually or automatically) to discover and analyze which cloud apps are in use. After we subscribed to Cloud App Security, we used a fairly simple deployment and configuration process to set up the discovery infrastructure in our environment. Through Cloud Discovery, we’ve gained visibility into apps, activities, users, data, and files in our cloud environment, as well as third-party apps that are connected to the cloud.

To deploy Cloud Discovery, we first needed to select the firewalls we wanted to use during the pilot. From within our environment, we chose eight firewall servers that supported a high volume of traffic. After we determined which of the firewalls we wanted to include, we started collecting the transaction logs of the network traffic passing through each firewall from on-premises devices to sanctioned and unsanctioned apps. The transactions were gathered on a traffic log collector and fed into the Cloud App Security log collector. The Cloud App Security log collector runs on a Microsoft Azure virtual machine and automates log uploads to our Cloud App Security portal.

![Figure 1. Components of the Microsoft IT and Microsoft Cloud App Security discovery infrastructures](image)

Cloud Discovery discovers the 13,000+ cloud apps within the apps catalog—and it provides a risk score to each. The Microsoft Cloud App Security engineering research team determined the risk scores by evaluating each discovered service against more than 60 parameters—including evaluating the service provider, security mechanisms, and compliance certifications. These details help us determine and assess the credibility and reliability of each discovered cloud application, and to customize the scores and the weights of various parameters to meet our needs.

Discovery dashboard

The Cloud Discovery dashboard provides insight into how cloud apps are being used in the organization—it’s an at-a-glance overview of the kinds of apps that are being used, open alerts, and the risk levels of apps in the
organization. The dashboard provides options for filtering and drilling down into data, so we can generate specific views based on what we are interested in looking at.

![Dashboard Screenshot](image)

**Figure 2.** Discovered apps in the Cloud Discovery dashboard in the Cloud App Security portal

**Sanctioning apps**

Cloud App Security provides the information and tools that we need to be able to perform a total risk assessment for each service, based on a combination of risk score and usage. By using Cloud App Security, we can sanction and/or block apps in our organization, using the cloud application catalog. Sanctioned apps have API connectors turned on and their application data is fed into the Cloud App Security big data stores and machine learning that are integrated with the Microsoft intelligent security graph. In our current deployment phase, Office 365, Microsoft SharePoint Online, Microsoft OneDrive for Business, Microsoft Exchange Online, and Azure Active Directory have been sanctioned.

**App connectors**

App connectors use APIs provided by various cloud app providers to enable Cloud App Security 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.

To connect an app and extend protection, the app administrator authorizes Cloud App Security to access the app. After that, Cloud App Security continuously 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.

**Data control**

The Cloud App Security portal includes a **Control** tab that we can use to create alerting policies that provide threat detection and data control to Office 365 and other sanctioned cloud apps. We use policies to define the way we want employees to behave in the cloud. They enable the detection of risky behavior, violations, or suspicious data points and activities. You can use out-of-the-box policies or create your own by using templates.

In this first phase of the deployment, we’ve created custom alerting policies to help us better detect risks. Although we haven’t yet started taking action on these policies in the production environment, we’re looking forward to integrating remediation processes and implementing data sharing and granular usage policies.

We’re in the planning stages of implementing DLP controls for our sanctioned apps. Using DLP and data-sharing controls, we’ll be able to use Cloud App Security to govern data in the cloud, including files that are stored in cloud drives, as attachments, or within cloud application fields.

**Threat detection using the Cloud App Security portal**

Cloud App Security uses advanced machine learning heuristics to learn how each user interacts with each cloud application and, through behavioral analysis, assesses the risks in each transaction. A benefit of using machine learning heuristics is that the more we use Cloud App Security, the better it gets at helping us to identify and assess risks. The Cloud App Security portal has views and tools that help us visualize overall cloud health and quickly identify anomalies in cloud usage that may indicate a data breach.
Cloud App Security dashboard

The Cloud App Security general dashboard gives us an overview of open alerts, activity violations, content violations, an activity map that plots the geographical origin of user activity, and connected app usage trends in our environment.

Figure 3. Cloud App Security portal main dashboard
The dashboard displays the results of ongoing risk detection and analytics, and it provides powerful reporting on users, usage patterns, and transactions to help us quickly identify anomalies. We check the dashboard regularly to see what new alerts were triggered and use the available information to help us determine how to handle them.

![Cloud App Security Anomaly Detection alert detail page](image)

**Figure 4. Cloud App Security Anomaly Detection alert detail page**

**Investigate**

After connecting Cloud App Security to Office 365, we began using the activity log in the **Investigate** tab to learn about and investigate our Office 365 environment. The tools provide us deeper visibility and advanced search queries that are crucial for investigating security incidents related to Office 365. The new insights and tools available to us in the Cloud App Security portal have made it easier than ever to gain a deeper understanding of our cloud environment and to perform deep-dive investigations when there are alerts and issues.

To help us investigate, the following dashboards are available for each individual sanctioned app that has an API connector configured:

- **Application dashboard—overall.** This provides an overview of application usage per location, usage graphs per number of users.
- **Application dashboard—insights.** This provides an analysis of data stored in the app, broken down by files type and file sharing level.
- **User dashboard.** This provides a complete overview of the user profile in the cloud, including groups, locations, recent activities, related alerts, and browsers used.
Using investigation tools
The Investigate tab in the Cloud App Security portal includes several analytic tools:

- **Activity logs.** We use these to check what users and what devices are accessing an app and from where. We can filter the logs by app and see IP ranges, failed log-ins, and admin activity.

- **Accounts.** We use these to determine whether there are accounts that haven’t been active in a particular service for a long time. We haven’t yet implemented enforcement, but when we do, we’ll be able to revoke licenses or permissions to services, view specific users, and require specific users to perform multi-factor authentication.

When we select an application listed on the Investigate tab, an app dashboard opens—it gives us additional tools that let us drill down into very specific app information to gain additional insights.

![Image of activity log accessed by selecting an app listed in the Investigate tab in the Cloud App Security portal](image)

**Figure 5.** An activity log accessed by selecting an app listed in the Investigate tab in the Cloud App Security portal

**Reporting**
We have a variety of the built-in reports that we can use to see what’s really going on in our cloud. Built-in reports have aggregated views for investigation and help us adjust our alerting policies. For example, by using the IP addresses report, we can find IP addresses that are used in different locations by multiple Office 365 accounts that we are investigating. We can also customize reports based on our reporting needs.

**Benefits**
Cloud App Security isn’t a single-point solution—but it is a key part of our holistic, agile security platform, and it’s enhanced with insights from other Microsoft security solutions. Cloud App Security has helped Microsoft security and monitoring teams increase monitoring and understand activities required to streamline operations.

Discovery in Cloud App Security has helped us identify the cloud apps that are being used and compare their usage and benefits to their risk profiles. It has also helped us identify odd traffic patterns and the effectiveness of firewall rules on production traffic flows.
The Cloud App Security portal, with its intuitive dashboards, helped us gain deeper visibility into Office 365 cloud apps, how our users use those apps, and the threats they face.

For more information

Microsoft IT

http://www.Microsoft.com/ITShowcase

Cloud App Security: