Microsoft Cloud App Security

Bring visibility, control, and protection to your cloud apps

Microsoft Cloud App Security provides a comprehensive, intelligent security solution that brings visibility, real-time control, and security to your cloud applications.

More and more organizations are adopting SaaS apps, not only to reduce costs but also to unlock competitive advantages such as faster time to market and improved collaboration. Even if your company hasn't embraced cloud applications, however, your employees are probably using them.

Discover and get risk assessment

Identify cloud apps on your network, gain visibility into shadow IT, and get risk assessments and ongoing analytics.

Control access in real time

Manage and limit cloud app access based on conditions and session context, including user identity, device, and location.

Protect your information

Get granular control over data and use built-in or custom policies for data sharing and data loss prevention.

Detect threats

Identify high-risk usage and detect unusual behavior using Microsoft threat intelligence and research.

According to our own telemetry, the average organization has more than 25 different cloud storage apps and more than 40 collaboration apps routinely used by its employees. The fast transition to cloud apps may leave you concerned about storing corporate data in the cloud apps.

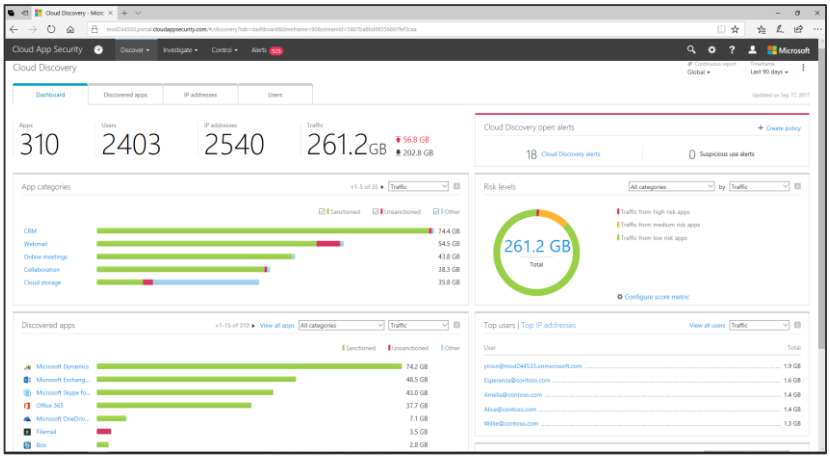
Today, data travels to many locations – across devices, apps, cloud services and on-premises. It is important to gain visibility and control of data in cloud apps, given the increasing number of cybersecurity attacks and compliance requirements with key regulations.

Microsoft Cloud App Security is a CASB (Cloud Access Security Broker) that can help you bring the protection you have on-premises to your cloud apps, gaining comprehensive visibility, auditing capabilities, and granular controls to help ensure your sensitive data stays safe.

Discovery and risk assessment

Deep visibility

Identifying cloud apps on your network and gaining visibility into Shadow IT is a first step in securing cloud apps. Cloud App Security recognizes more than 15,000 cloud apps—no agents required. It also evaluates the risk of these apps based on more than 60 parameters, including Multi-factor authentication support, IP address restriction, and regulatory compliance. The risk score can help you decide whether to sanction the app.



Powerful reporting and analytics

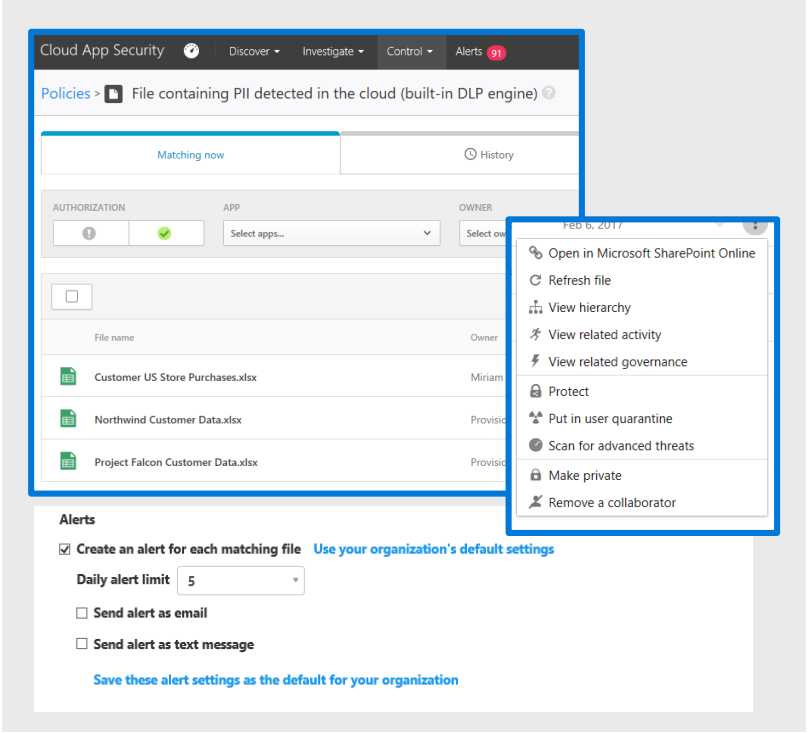
On-going risk detection and details on users, abnormal usage patterns, upload/download traffic and transactions can help you identify anomalies right away. For example, Cloud App Security sends an alert if a user sends a large amount of data to a risky app, and so you can take appropriate action immediately. Data and log anonymization help protect user privacy.

Use Cloud App Security to apply policies to apps from Microsoft or other vendors, such as Box, Dropbox, Salesforce, and more.

Information protection

Data loss prevention (DLP)

Cloud App Security enables granular control policies and powerful, single-click remediation, including document quarantine and sharing restrictions. You can apply policies—out of the box or customized—to apps from Microsoft or other vendors, such as Box, Dropbox, Salesforce, and more. Cloud App Security can scan and classify files in the cloud, and apply Azure Information Protection labels for protection—including encryption.



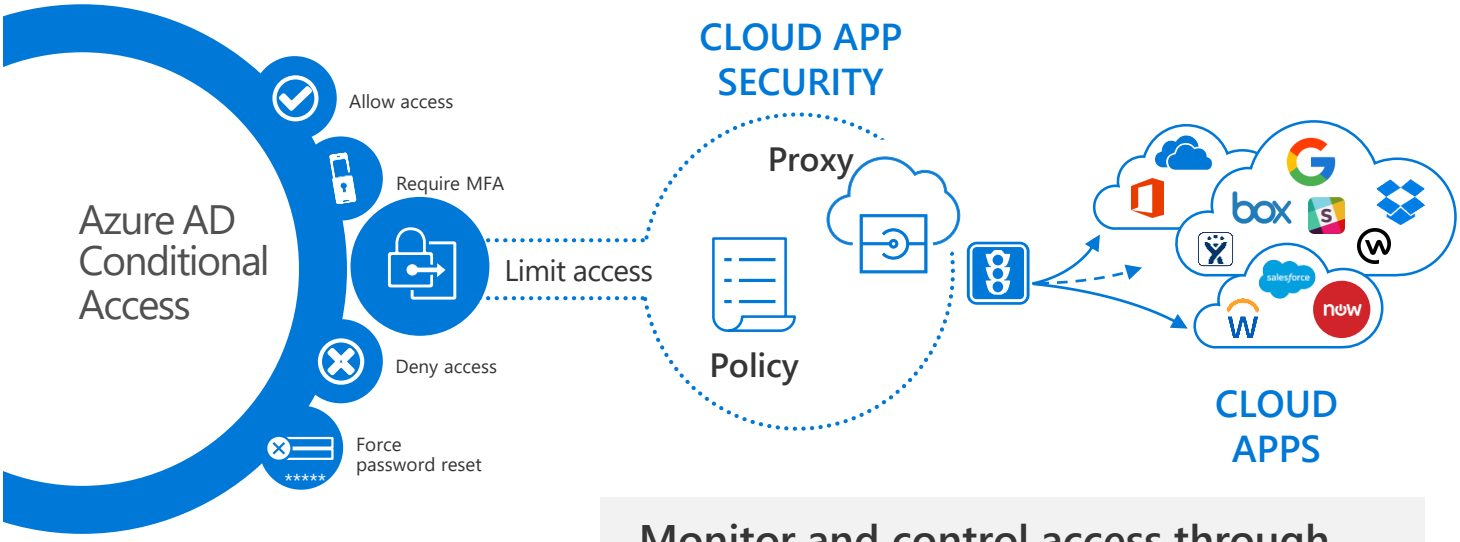
Compliance

Cloud App Security supports your compliance journey with regulatory mandates such as Payment Card Industry (PCI), Health Insurance Accountability and Portability Act (HIPAA), Sarbanes-Oxley (SOX), General Data Protection Regulation (GDPR), and others. Cloud App Security factors compliance with regulations into the risk assessment score for each app, and helps you further control and protect sensitive files through policies and governance.

Conditional access

Real-time monitoring and control

Uniquely integrated with Azure AD Conditional Access, Cloud App Security can help you limit activities performed within user sessions in SaaS apps based on user identity, location, device state, and detected sign-in risk level. For example, you can allow access to SaaS apps but protect downloads from unfamiliar locations, or block downloads of sensitive documents from unmanaged devices.

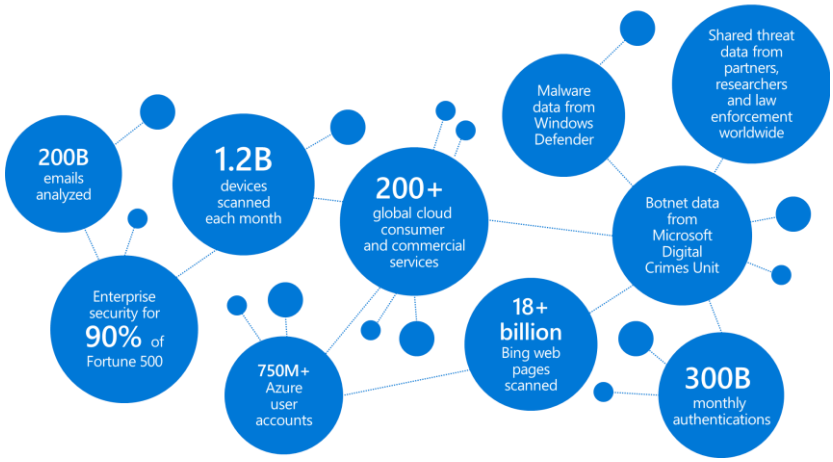


Monitor and control access through integration with Azure Active Directory.

Threat detection

Behavioral analytics

Cloud App Security helps identify anomalies in cloud usage that may indicate a data breach by leveraging the vast Microsoft threat intelligence data. It learns how each user interacts with each SaaS app and, through behavioral analytics, assesses the risks in each transaction. These include simultaneous logins from two different continents, the sudden download of terabytes of data, or multiple failed login attempts that may signify a brute force attack.



Mitigation of ransomware attacks

Cloud App Security threat detection offers a built-in policy template to detect potential ransomware activity, for example, by searching for unique file extensions. Using this template, you can specify governance actions to suspend suspect users and prevent further encryption of the user's files.

Integration with existing SIEM and DLP solutions

Through integration with your SIEM and DLP solutions, Cloud App Security helps preserve your familiar workflow. It enables a consistent policy across on-premises and cloud activities, while automating security procedures to better protect your cloud applications.

FIRST AMERICAN
EQUIPMENT FINANCE
A City National Bank Company

"Securing our data in the cloud is critical to maintaining our success. Microsoft Cloud App Security protects our users an data by providing us with alerts and information on unusual application and user activity, so we can determine if it's malicious or authorized or not."

—**Chris Thibault**, Lead Systems Engineer,
First American Equipment Finance

box

"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**, VP of Technology Partnerships,
Box

Hewlett Packard Enterprise

"The growing use of cloud applications at Hewlett Packard Enterprise creates some interesting challenges for us since we have traditionally secured applications within internal datacenters.

Microsoft Cloud App Security has given us a key capability to secure and provide insight into cloud applications so we can make the move to the cloud without compromising the visibility and control we have come to expect."

—**Andy Radle**, Cloud Security Architect,
Hewlett Packard Enterprise

Get a free trial of Cloud App Security, or get help with your deployment through Microsoft's FastTrack service.

Learn more at www.cloudappsecurity.com

Microsoft