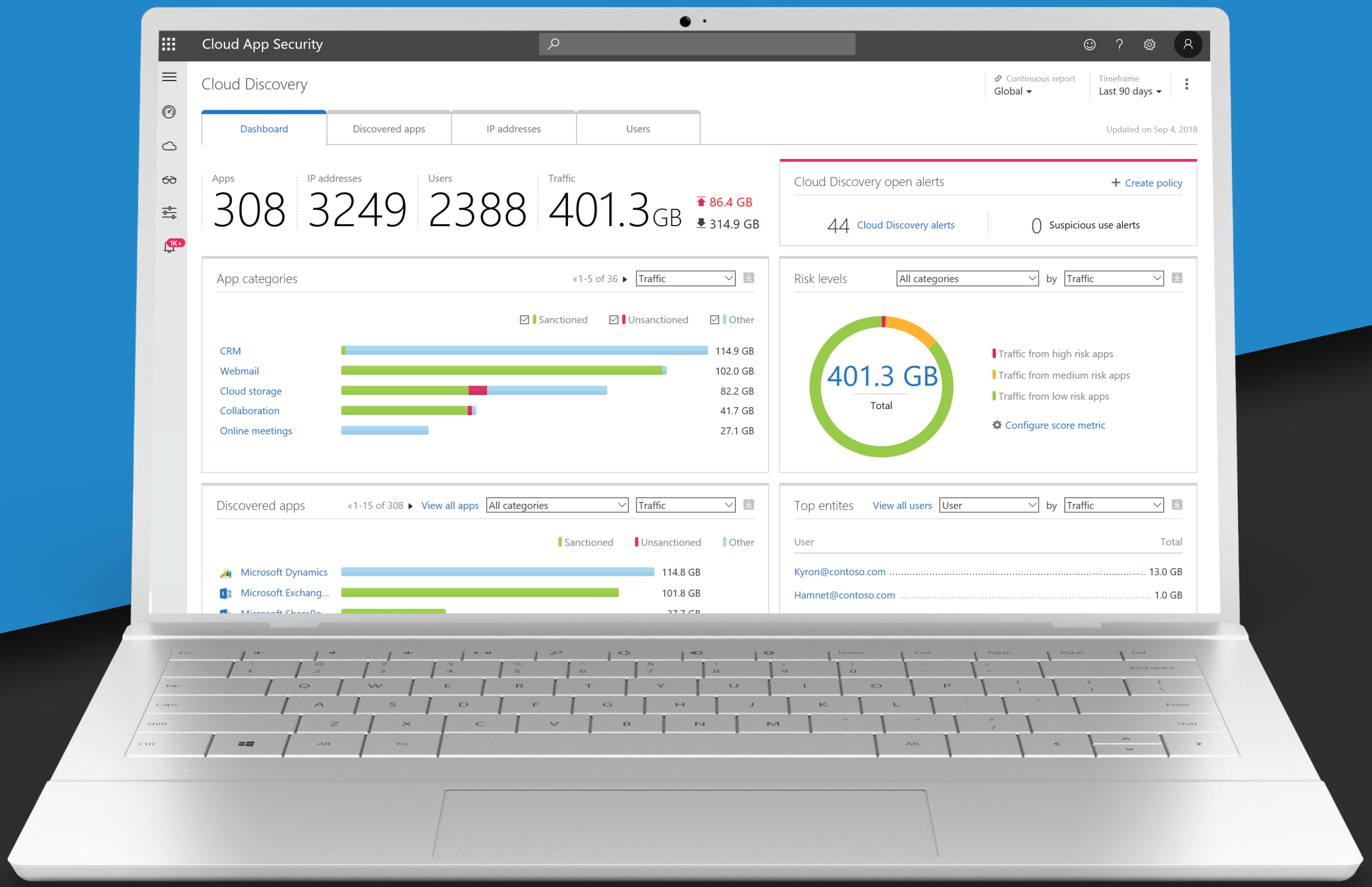
Microsoft Cloud App Security

A uniquely integrated Cloud Access Security Broker



Cloud App Security

Cloud Discovery

Continuous report: Global

Timeframe: Last 90 days

Dashboard | Discovered apps | IP addresses | Users

Updated on Sep 4, 2018

Apps	IP addresses	Users	Traffic
308	3249	2388	401.3GB (↑ 86.4 GB, ↓ 314.9 GB)

Cloud Discovery open alerts + Create policy

44 Cloud Discovery alerts

0 Suspicious use alerts

App categories ◂1-5 of 36 ▸ Traffic

☑ Sanctioned ☑ Unsanctioned ☑ Other

CRM	114.9 GB
Webmail	102.0 GB
Cloud storage	82.2 GB
Collaboration	41.7 GB
Online meetings	27.1 GB

Risk levels All categories by Traffic

401.3 GB Total

Traffic from high risk apps

Traffic from medium risk apps

Traffic from low risk apps

Configure score metric

Discovered apps ◂1-15 of 308 ▸ View all apps All categories Traffic

Sanctioned Unsanctioned Other

Microsoft Dynamics	114.8 GB
Microsoft Exchang...	101.8 GB

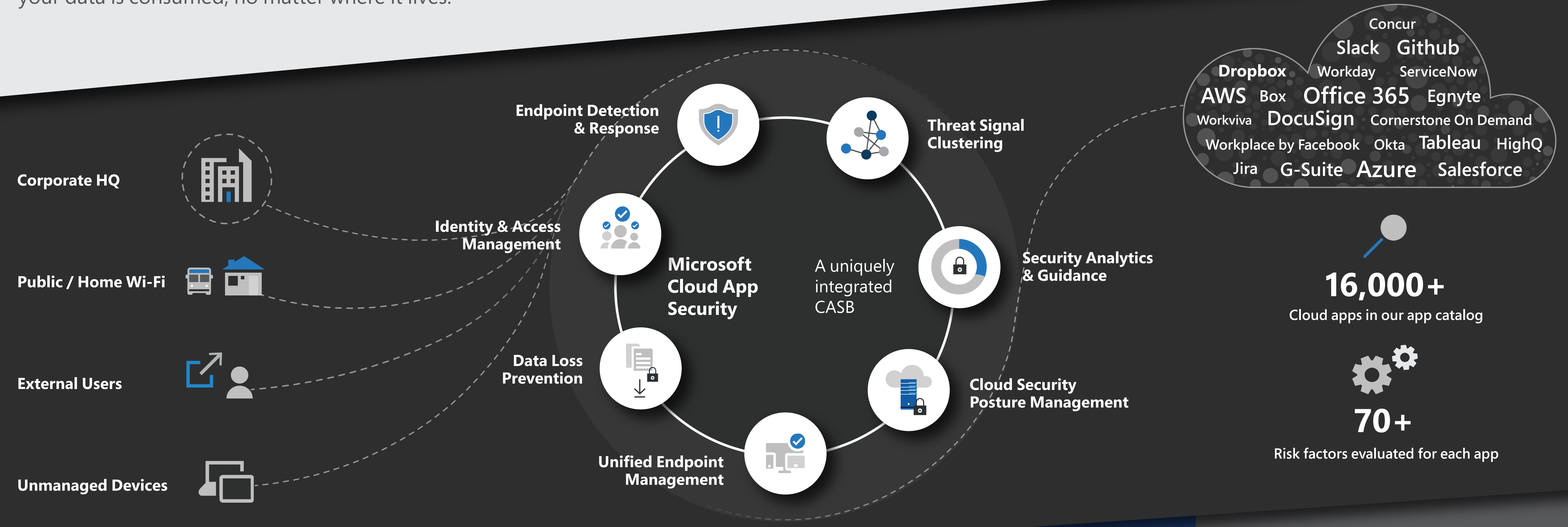
Top entites View all users User by Traffic

User	Total
Kyron@contoso.com	13.0 GB
Hamnet@contoso.com	1.0 GB

Microsoft

Microsoft Cloud App Security

Powered by native integrations with industry-leading security and identity solutions including Azure Active Directory, Intune, and Azure Information Protection – gain visibility into all your cloud apps and services leveraging sophisticated analytics to identify and combat cyberthreats. Control how your data is consumed, no matter where it lives.



Corporate HQ

Public / Home Wi-Fi

External Users

Unmanaged Devices

Endpoint Detection & Response

Threat Signal Clustering

Identity & Access Management

Microsoft Cloud App Security

A uniquely integrated CASB

Security Analytics & Guidance

Data Loss Prevention

Cloud Security Posture Management

Unified Endpoint Management

Concur
Slack Github
Dropbox Workday ServiceNow
AWS Box Office 365 Egnyte
Workviva DocuSign Cornerstone On Demand
Workplace by Facebook Okta Tableau HighQ
Jira G-Suite Azure Salesforce

16,000+
Cloud apps in our app catalog

70+
Risk factors evaluated for each app

Shadow IT Discovery

Identify and manage the cloud apps used by your organization – in and beyond the corporate network.

Information Protection

Understand, classify and protect sensitive information when it travels in- and outside of your organization with automated processes and real-time controls.

Threat Protection

Detect unusual behavior across your cloud apps to identify ransomware, compromised users or rogue applications, analyze high-risk usage and remediate automatically to limit the risk to your organization.

Compliance Assessment

Assess the compliance of your organization's apps against regulatory requirements such as GDPR, industry and legal standards and common security controls.

Shadow IT Discovery

Discover the cloud apps used in your organization.

Assess risk and business readiness of your apps against >70 risk factors including regulatory and industry standards.

Govern discovered apps by sanctioning, onboarding them to Azure AD or blocking them on your network.

Discover and control use of Shadow IT

On average more than 1,100 cloud applications are used by enterprises today, of which 61% are not sanctioned by IT. This results in duplicate capabilities, apps not meeting compliance standards or posing a security risk to the organization without any IT oversight.

Discovery identifies current cloud apps, provides risk assessments and ongoing analytics and lifecycle management capabilities to control the use.

Discovery of apps

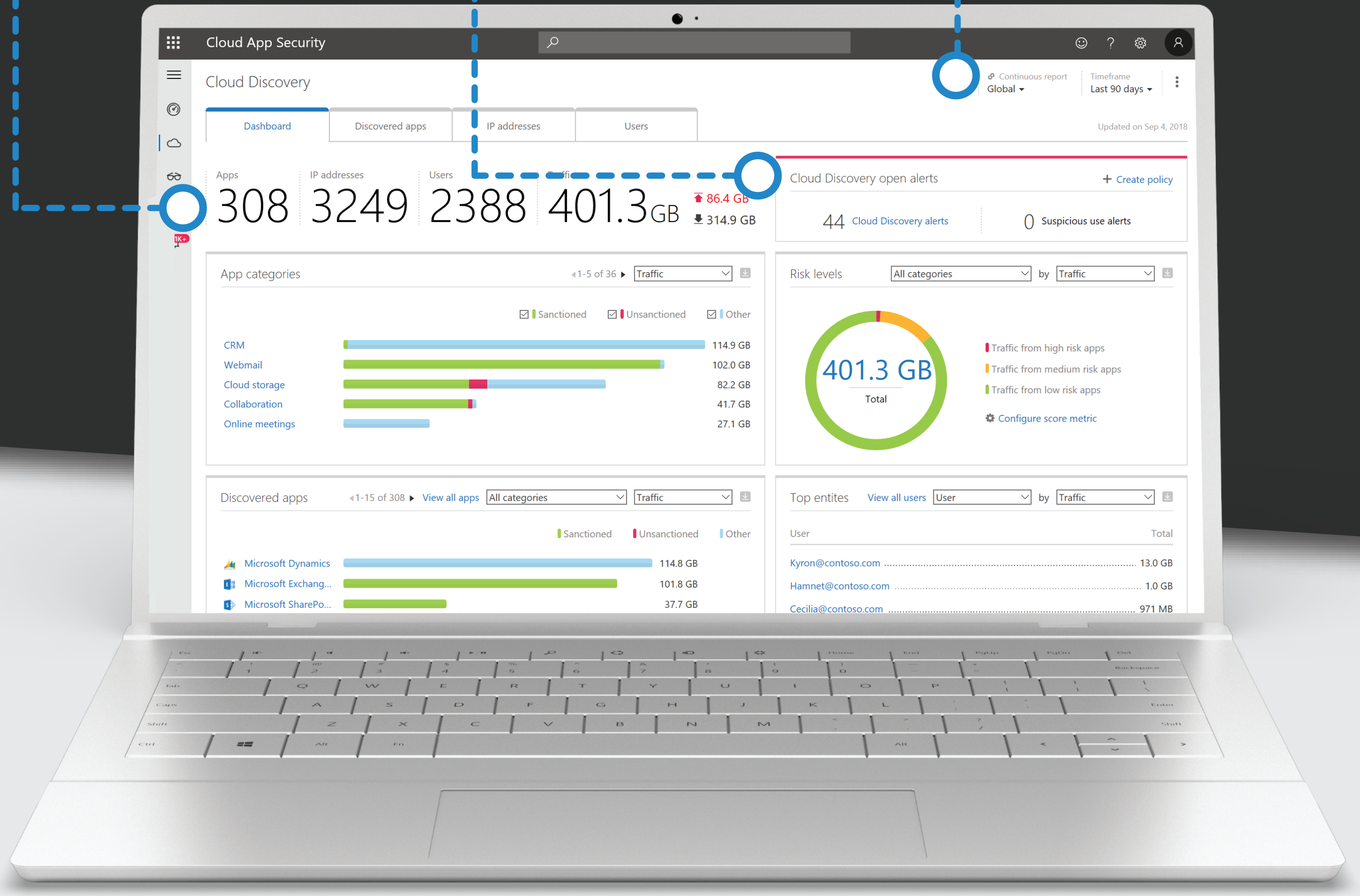
Get granular details about the usage of each discovered cloud app in your organization and dive deep into app categories, IP addresses, users and machines.

Out of the box alerts

Get notified when new risky or high volume apps are discovered so you can evaluate and govern their usage.

Executive reporting

High level overview of key findings and recommendations on how to improve visibility into, and control over, Shadow IT in your organization.



Continuous report: Global

Timeframe: Last 90 days

Updated on Sep 4, 2018

Apps	IP addresses	Users	Traffic
308	3249	2388	401.3 GB 86.4 GB 314.9 GB

Cloud Discovery open alerts + Create policy

44 Cloud Discovery alerts

0 Suspicious use alerts

App categories ◂1-5 of 36 ▸ Traffic

☑ Sanctioned ☑ Unsanctioned ☑ Other

CRM	114.9 GB
Webmail	102.0 GB
Cloud storage	82.2 GB
Collaboration	41.7 GB
Online meetings	27.1 GB

Risk levels All categories by Traffic

401.3 GB Total

Traffic from high risk apps

Traffic from medium risk apps

Traffic from low risk apps

Configure score metric

Discovered apps ◂1-15 of 308 ▸ View all apps All categories Traffic

Sanctioned Unsanctioned Other

Microsoft Dynamics	114.8 GB
Microsoft Exchang...	101.8 GB
Microsoft SharePo...	37.7 GB

Top entites View all users User by Traffic

User	Total
Kyron@contoso.com	13.0 GB
Hamnet@contoso.com	1.0 GB
Cecilia@contoso.com	971 MB

Seamless integrations to enhance and customize Discovery

Windows Defender ATP

The agent extends Discovery beyond your organization's network and enables machine-based Discovery regardless of the access point.

Azure Active Directory

Easily onboard discovered apps to Azure Active Directory (AAD) to enable managed authentication and SSO.

Leading SWG providers

Secure Web Gateway integrations allow inline app Discovery and the enforcement of governance actions.

Information Protection

Identify information at risk of exposure and remediate immediately with admin controls including quarantine, revoking privileges or notifying the owner.

Classify, label and protect sensitive information when it is stored in or newly uploaded to cloud apps.

Control and monitor user sessions in real-time to prevent data exfiltration in low-trust scenarios, such as sessions from external users.

Automated governance

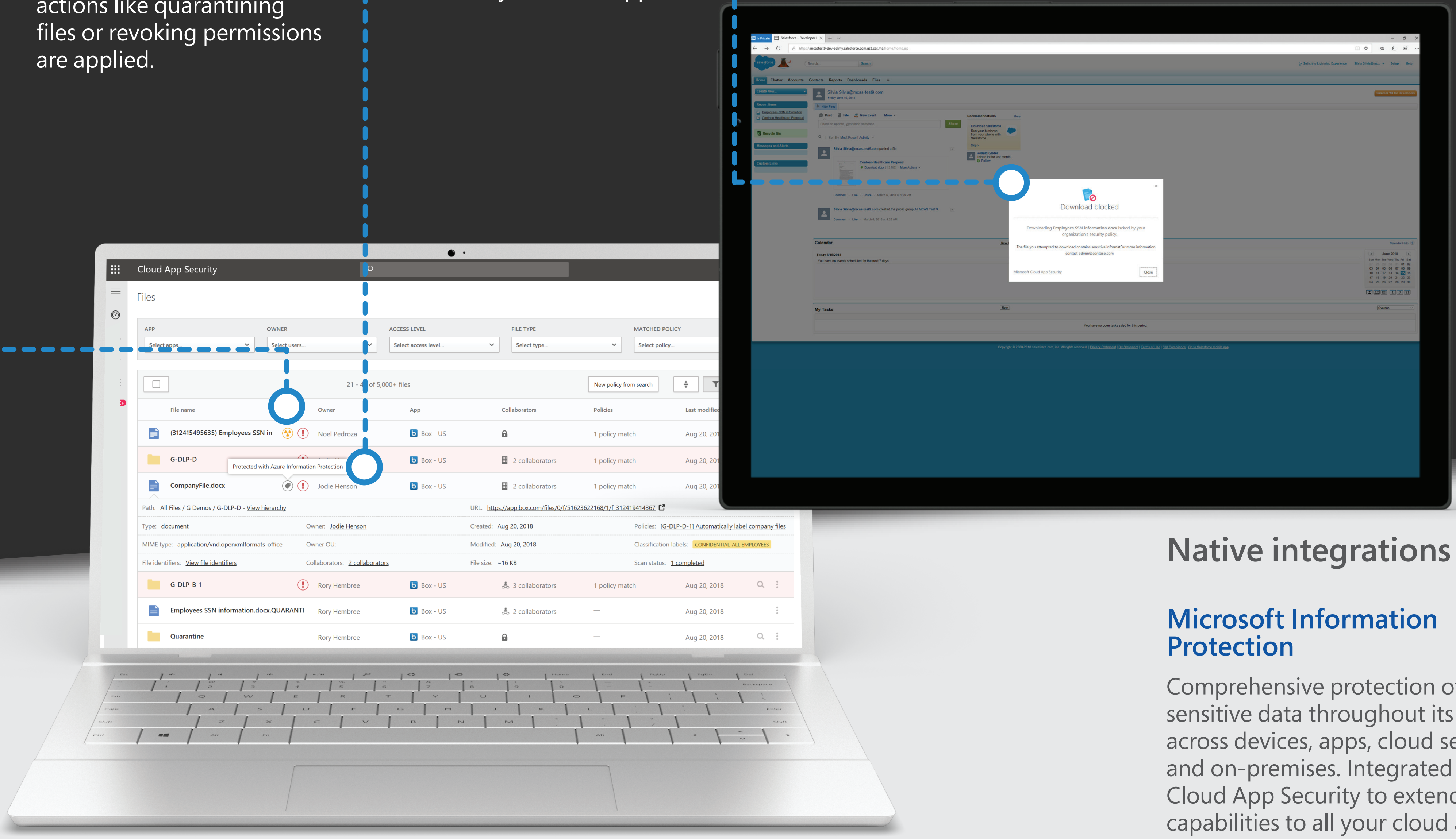
When policy violations occur, automatic governance actions like quarantining files or revoking permissions are applied.

Automatic labeling

When sensitive files are detected, AIP labels will automatically be applied across your cloud apps.

Control user sessions in real-time

Monitor and control risky user sessions in real- time and prevent data exfiltration.



Cloud App Security

Files

APP	OWNER	ACCESS LEVEL	FILE TYPE	MATCHED POLICY
Select apps...	Select users...	Select access level...	Select type...	Select policy...

21 - 4 of 5,000+ files

New policy from search

File name	Owner	App	Collaborators	Policies	Last modified
(312415495635) Employees SSN in	Noel Pedroza	Box - US		1 policy match	Aug 20, 201
G-DLP-D		Box - US	2 collaborators	1 policy match	Aug 20, 201
CompanyFile.docx	Jodie Henson	Box - US	2 collaborators	1 policy match	Aug 20, 201
G-DLP-B-1	Rory Hembree	Box - US	3 collaborators	1 policy match	Aug 20, 2018
Employees SSN information.docx.QUARANTI	Rory Hembree	Box - US	2 collaborators	—	Aug 20, 2018
Quarantine	Rory Hembree	Box - US		—	Aug 20, 2018

Protected with Azure Information Protection

Path: All Files / G Demos / G-DLP-D - View hierarchy
URL: https://app.box.com/files/0/f/51623622168/1/f_312419414367

Type: document
Owner: Jodie Henson
Created: Aug 20, 2018
Policies: [G-DLP-D-1] Automatically label company files
MIME type: application/vnd.openxmlformats-office
Owner OU: —
Modified: Aug 20, 2018
Classification labels: CONFIDENTIAL-ALL EMPLOYEES
File identifiers: View file identifiers
Collaborators: 2 collaborators
File size: ~16 KB
Scan status: 1 completed

Download blocked

Downloading **Employees SSN information.docx** iscked by your organization's security policy.

The file you attempted to download contains sensitive informatFor more information contact admin@contoso.com

Microsoft Cloud App Security

Close

Protect your data when it travels outside of your organization

To maximize the impact of information, it needs to be ubiquitous to help people and businesses succeed. With data being on the move, the risk for exposure increases, as sensitive data is overshared inside or even outside of the organization.

Microsoft Cloud App Security enables you to identify your sensitive data across cloud apps, monitor when it is shared with risky environments and take necessary governance actions by classifying, labeling and protecting existing and new data in your environment.

Native integrations powering a unique information protection approach

Microsoft Information Protection

Comprehensive protection of sensitive data throughout its lifecycle across devices, apps, cloud services and on-premises. Integrated with Cloud App Security to extend the capabilities to all your cloud apps.

Conditional Access

Automated access control for accessing cloud apps, based on conditions you define. MCAS extends these controls into the user's session to allow for real-time monitoring and granular control of any app with MCAS.

Intune

Managing mobile productivity securely and in a unified way. Leveraged to differentiate managed from unmanaged devices and apply necessary session controls.

Threat Protection

Detect insider threats and compromised accounts with sophisticated end user behavioral analytics (UEBA).

Identify and mitigate malware activities, including ransomware and other advanced cyberattacks.

Be alerted when rouge applications or overprivileged O-auth apps access your data and configure automatic remediation.

Protect against cyberthreats and anomalies

Moving to the cloud presents a new threat vector for organizations. Attacks can introduce ransomware, compromised user accounts perform malicious activities, and overprivileged O-auth apps can gain access to sensitive data or privileged accounts.

Accelerate the safe adoption of cloud apps and limit the impact to your organization by leveraging sophisticated behavioral analytics, built-in detections and automatic remediation capabilities, informed by one of the industry's largest set of threat signals.

Session investigation

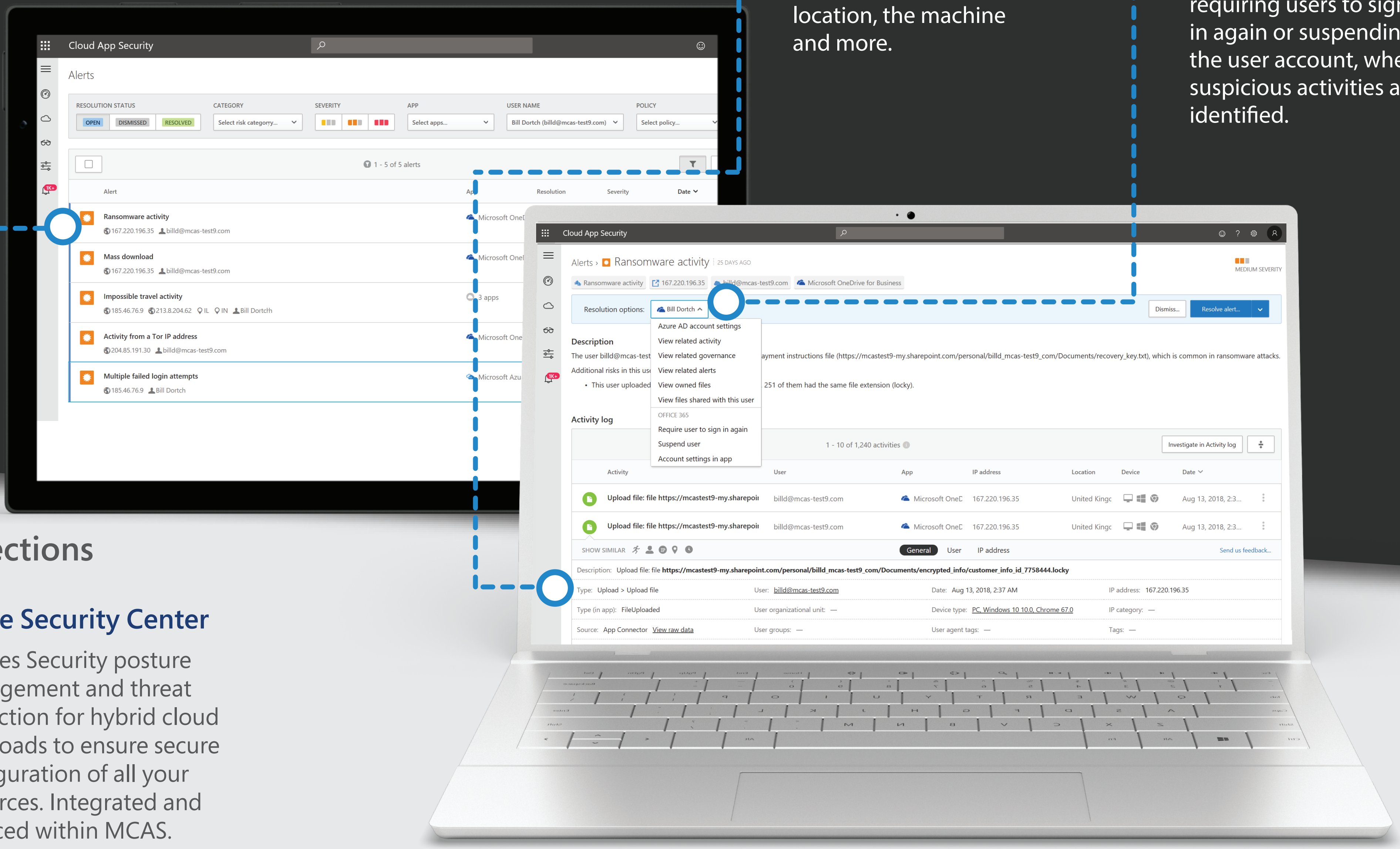
Understand the context of multiple activities of a user across various apps, to detect patterns and identify compromised accounts.

Dive into the details

Investigate the individual files and locations that are affected with additional details about IP address, location, the machine and more.

Remediation

Apply governance actions, such as requiring users to sign in again or suspending the user account, when suspicious activities are identified.



Ransomware activity
167.220.196.35 billd@mcas-test9.com — Microsoft OneI

Mass download
167.220.196.35 billd@mcas-test9.com — Microsoft OneI

Impossible travel activity
185.46.76.9 213.8.204.62 IL IN Bill Dortch — 3 apps

Activity from a Tor IP address
204.85.191.30 billd@mcas-test9.com — Microsoft One

Multiple failed login attempts
185.46.76.9 Bill Dortch — Microsoft Azu

Description

The user billd@mcas-test ayment instructions file (https://mcastest9-my.sharepoint.com/personal/billd_mcas-test9_com/Documents/recovery_key.txt), which is common in ransomware attacks.

Additional risks in this use

- This user uploaded 251 of them had the same file extension (locky).

Activity log

1 - 10 of 1,240 activities

Activity	User	App	IP address	Location	Device	Date
Upload file: file https://mcastest9-my.sharepoi	billd@mcas-test9.com	Microsoft OneD	167.220.196.35	United Kingc		Aug 13, 2018, 2:3...
Upload file: file https://mcastest9-my.sharepoi	billd@mcas-test9.com	Microsoft OneD	167.220.196.35	United Kingc		Aug 13, 2018, 2:3...

Description: Upload file: file **https://mcastest9-my.sharepoint.com/personal/billd_mcas-test9_com/Documents/encrypted_info/customer_info_id_7758444.locky**

Type: Upload > Upload file
User: billd@mcas-test9.com
Date: Aug 13, 2018, 2:37 AM
IP address: 167.220.196.35
Type (in app): FileUploaded
User organizational unit: —
Device type: PC, Windows 10 10.0, Chrome 67.0
IP category: —
Source: App Connector View raw data
User groups: —
User agent tags: —
Tags: —

Advanced Threat Intelligence - enabling sophisticated detections

Intelligent Security Graph

A platform powering Microsoft security products and services by using advanced analytics to link threat intelligence and security signals. Microsoft operates global services at a massive scale with billions of security signals that MCAS leverages to power its Threat Detection.

Secure Score

Visibility into your Microsoft security position and provides an overview of which security features are available to reduce risk. MCAS feeds into the overall scoring and helps you protect your environment of cloud apps.

Azure Security Center

Enables Security posture management and threat protection for hybrid cloud workloads to ensure secure configuration of all your resources. Integrated and surfaced within MCAS.

Compliance Assessment

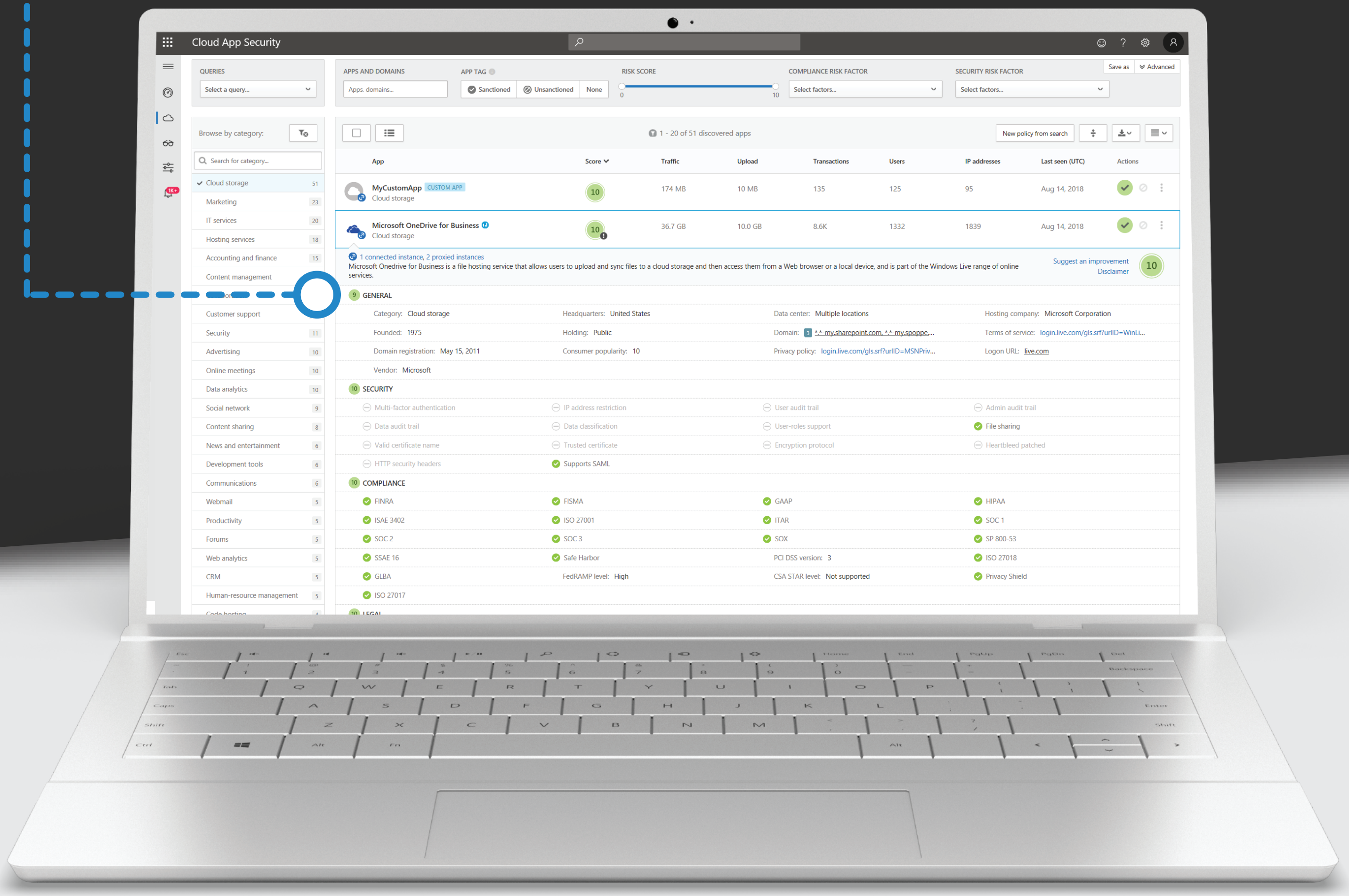
Assess if your cloud apps meet your industry's compliance requirements.

Validate GDPR and other regulatory compliance.

Protect sensitive data when it is uploaded to the cloud or shared in- and outside of your organization.

Evaluate your apps

Leverage >70 factors spanning security standards, compliance and legal.



Cloud App Security

✓ Cloud storage	51
Marketing	23
IT services	20
Hosting services	18
Accounting and finance	15
Content management	
Customer support	
Security	11
Advertising	10
Online meetings	10
Data analytics	10
Social network	9
Content sharing	8
News and entertainment	6
Development tools	6
Communications	6
Webmail	5
Productivity	5
Forums	5
Web analytics	5
CRM	5
Human-resource management	5
Code hosting	4

1 - 20 of 51 discovered apps

App	Score	Traffic	Upload	Transactions	Users	IP addresses	Last seen (UTC)	Actions
MyCustomApp CUSTOM APP Cloud storage	10	174 MB	10 MB	135	125	95	Aug 14, 2018	✓
Microsoft OneDrive for Business Cloud storage	10	36.7 GB	10.0 GB	8.6K	1332	1839	Aug 14, 2018	✓

1 connected instance, 2 proxied instances

Microsoft Onedrive for Business is a file hosting service that allows users to upload and sync files to a cloud storage and then access them from a Web browser or a local device, and is part of the Windows Live range of online services.

Suggest an improvement
Disclaimer
10

9 GENERAL

Category: Cloud storage
Headquarters: United States
Data center: Multiple locations
Hosting company: Microsoft Corporation
Founded: 1975
Holding: Public
Domain: 3 *.*-my.sharepoint.com, *.*-my.spoppe....
Terms of service: login.live.com/gls.srf?urlID=WinLi...
Domain registration: May 15, 2011
Consumer popularity: 10
Privacy policy: login.live.com/gls.srf?urlID=MSNPriv...
Logon URL: live.com
Vendor: Microsoft

10 SECURITY

⊖ Multi-factor authentication
⊖ IP address restriction
⊖ User audit trail
⊖ Admin audit trail
⊖ Data audit trail
⊖ Data classification
⊖ User-roles support
✓ File sharing
⊖ Valid certificate name
⊖ Trusted certificate
⊖ Encryption protocol
⊖ Heartbleed patched
⊖ HTTP security headers
✓ Supports SAML

10 COMPLIANCE

✓ FINRA
✓ FISMA
✓ GAAP
✓ HIPAA
✓ ISAE 3402
✓ ISO 27001
✓ ITAR
✓ SOC 1
✓ SOC 2
✓ SOC 3
✓ SOX
✓ SP 800-53
✓ SSAE 16
✓ Safe Harbor
PCI DSS version: 3
✓ ISO 27018
✓ GLBA
FedRAMP level: High
CSA STAR level: Not supported
✓ Privacy Shield
✓ ISO 27017

10 LEGAL

Assess the compliance of your cloud apps

Most organizations must comply with a set of regulations, governed by the industry and country they operate in. These dictate how organizations must manage, view, and control their data.

Microsoft Cloud App Security sources from a catalog of more than 16,000 cloud apps to discover the apps used in your environment and leverages >70 different parameters to assign a risk score to each one. These risk factors span general information, security, compliance and legal, and enable you to assess whether any given app meets the compliance requirements for your organization.

Powerful, built-in queries allow you to filter for specific requirements such as GDPR or FedRAMP, to tailor the discovery experience to your specific needs.

Get started on your compliance journey

1

Discover your cloud apps

Get started with discovery to understand which cloud apps are being used in your organization.

2

Assess their compliance

Leverage more than 70 risk factors to understand whether the discovered cloud apps meet your organization's requirements.

3

Control sensitive data

Create labels and file policies to identify and automatically protect sensitive information across your ecosystem of cloud apps.

Learn more about Microsoft Cloud App Security
aka.ms/mcas

Technical documentation
aka.ms/mcastech

Get a free 90-day trial
aka.ms/mcastrial

Questions? Connect with us on Tech Community!
aka.ms/mcascommunity