Microsoft Defender for Cloud Apps

Identify and combat cyberthreats across your cloud apps and services using Microsoft Defender for Cloud Apps

Workshop contents

P2	Introduction
P3	About Slalom
P6	About Microsoft Defender for Cloud Apps
P13	Our Approach
P15	Next Steps

About Slalom

WHAT WE DO

Slalom is a purpose-led, global business and technology consulting company.

From strategy to implementation, our approach is fiercely human. We deeply understand our customers–and their customers–to deliver practical, end-to-end solutions that drive meaningful impact.

Microsoft & Slalom achieve more together.

Our business was built on Microsoft, and for nearly two decades, we've delivered innovation together. It starts with our shared purpose: realizing greater impact through collaboration and enabling every person and organization on the planet to achieve more.

We're partnering with change-making clients to shape the future around Microsoft technology—that's because as we look to the next two decades and beyond, we know the future will be built on Microsoft, too.

slalom | Microsoft

Microsoft Gold Partner

2022 US Analytics Partner of the Year

350+
Microsoft clients served in 2021

53
Microsoft Partner Awards

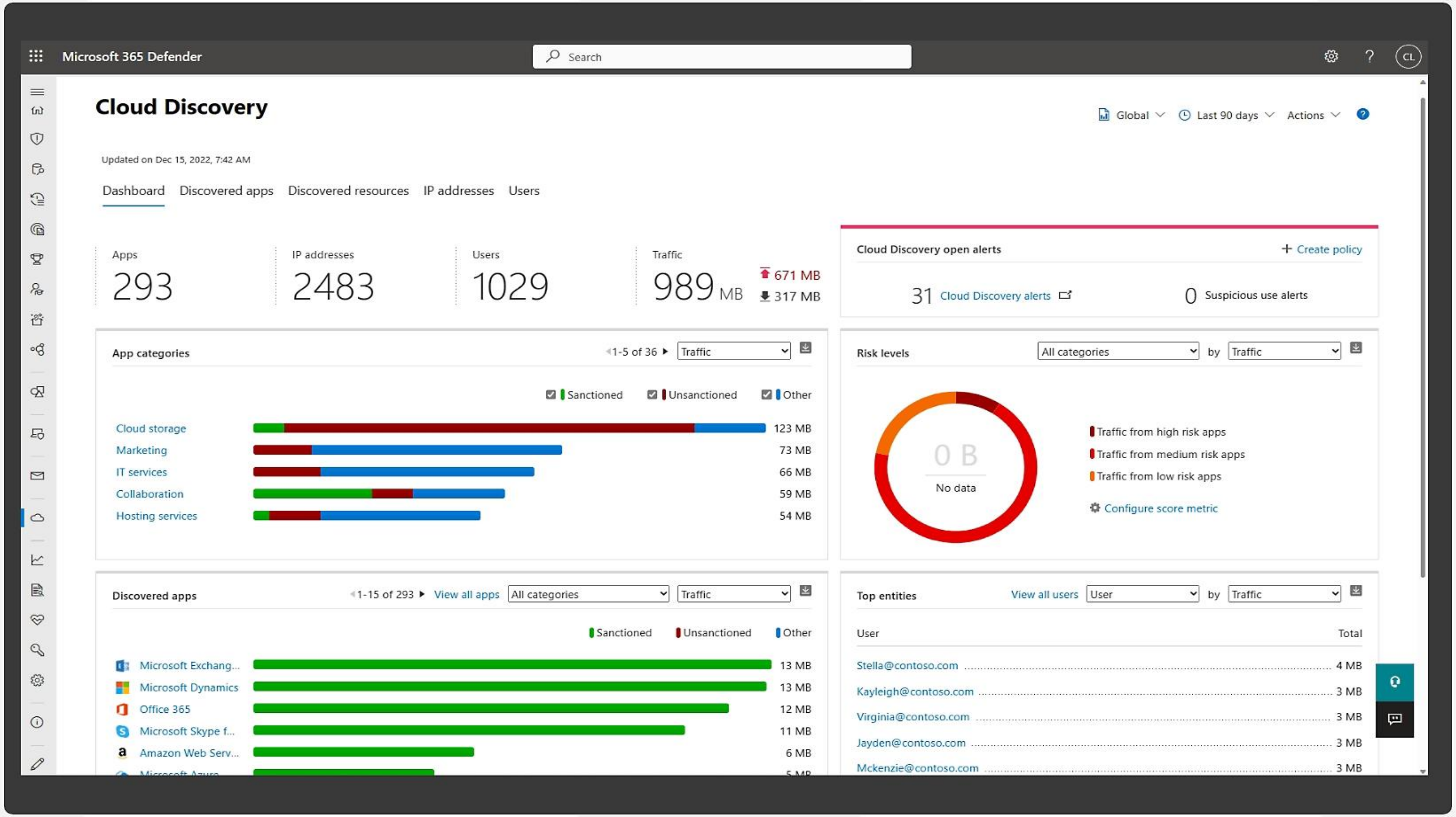
Microsoft Solutions

- Cloud architecture and migration
- Product engineering
- Enterprise application strategy and deployment
- Artificial Intelligence and machine learning
- Data architecture
- DevOps
- Data visualization and storytelling

Microsoft Defender for Cloud Apps ensures holistic coverage for cloud apps by combining SaaS security posture management, data loss prevention, app to app protection, and integrated threat protection:

- Discovery and control the use of Shadow IT
- Integrate threat protection with SIEM and XDR across the Microsoft 365 Platform
- Gain insight into the behavior of SaaS applications and Microsoft 365 application

oft



Microsoft 365 Defender

Search

Cloud Discovery

Global · Last 90 days · Actions

Updated on Dec 15, 2022, 7:42 AM

Dashboard | Discovered apps | Discovered resources | IP addresses | Users

Apps	IP addresses	Users	Traffic
293	2483	1029	989 MB 671 MB 317 MB

Cloud Discovery open alerts

+ Create policy

31 Cloud Discovery alerts

0 Suspicious use alerts

App categories

1-5 of 36 · Traffic

☑ Sanctioned ☑ Unsanctioned ☑ Other

Cloud storage	123 MB
Marketing	73 MB
IT services	66 MB
Collaboration	59 MB
Hosting services	54 MB

Risk levels

All categories by Traffic

0 B

No data

Traffic from high risk apps

Traffic from medium risk apps

Traffic from low risk apps

Configure score metric

Discovered apps

1-15 of 293 · View all apps · All categories · Traffic

Sanctioned · Unsanctioned · Other

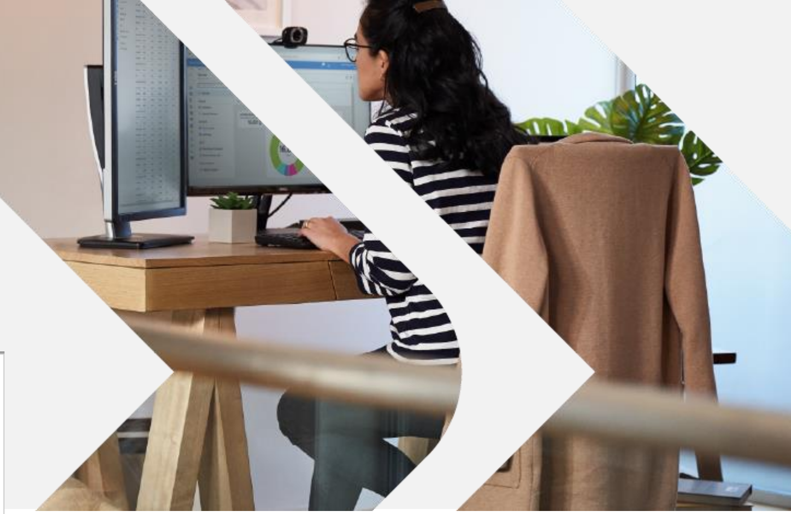
Microsoft Exchang...	13 MB
Microsoft Dynamics	13 MB
Office 365	12 MB
Microsoft Skype f...	11 MB
Amazon Web Serv...	6 MB
Microsoft Azure	5 MB

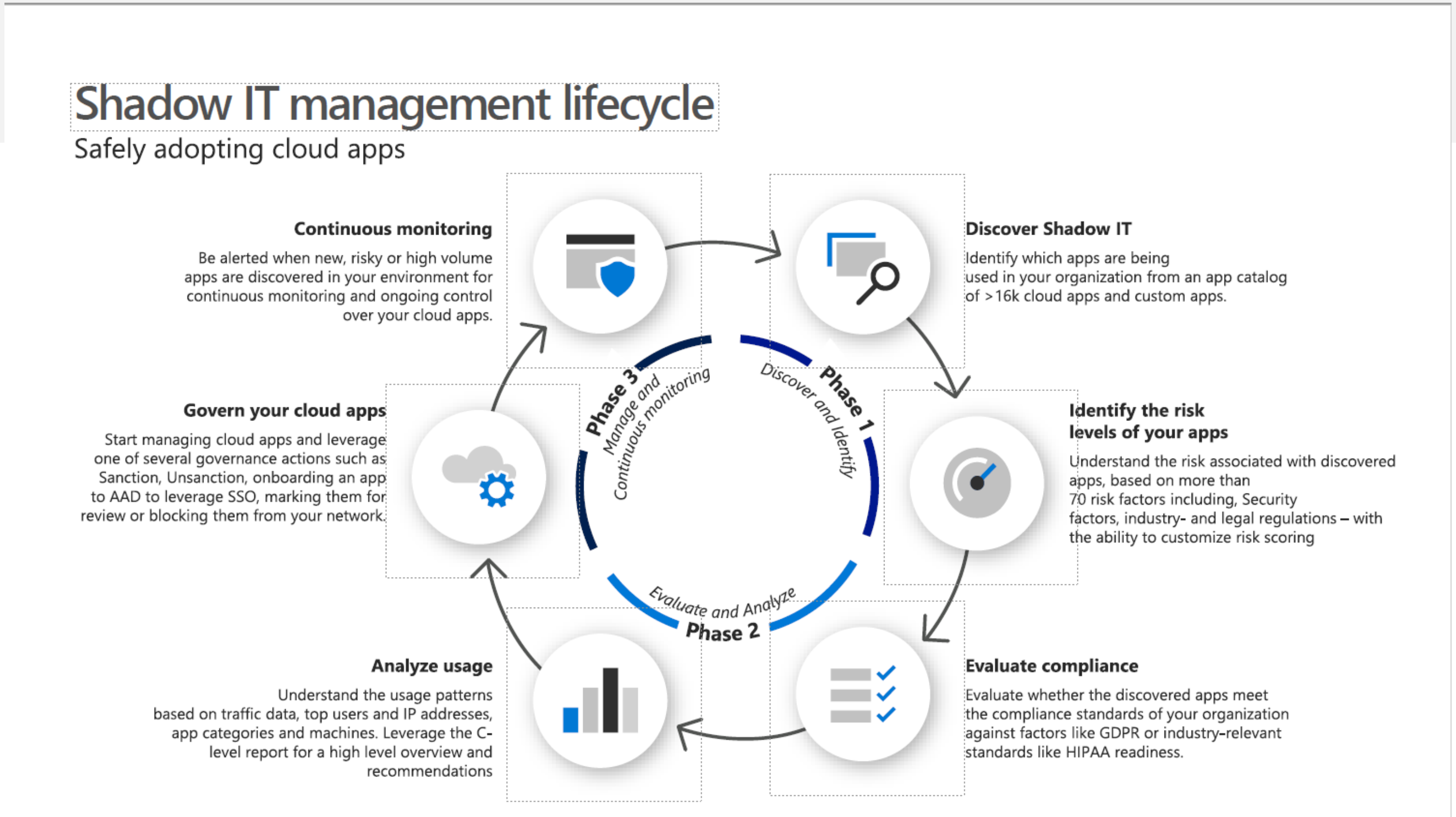
Top entities

View all users · User by Traffic

User	Total
Stella@contoso.com	4 MB
Kayleigh@contoso.com	3 MB
Virginia@contoso.com	3 MB
Jayden@contoso.com	3 MB
Mckenzie@contoso.com	3 MB

Reveal and explore Shadow IT in your organization





Shadow IT management lifecycle

Safely adopting cloud apps

Continuous monitoring

Be alerted when new, risky or high volume apps are discovered in your environment for continuous monitoring and ongoing control over your cloud apps.

Discover Shadow IT

Identify which apps are being used in your organization from an app catalog of >16k cloud apps and custom apps.

Govern your cloud apps

Start managing cloud apps and leverage one of several governance actions such as Sanction, Unsanction, onboarding an app to AAD to leverage SSO, marking them for review or blocking them from your network.

Identify the risk levels of your apps

Understand the risk associated with discovered apps, based on more than 70 risk factors including, Security factors, industry- and legal regulations – with the ability to customize risk scoring

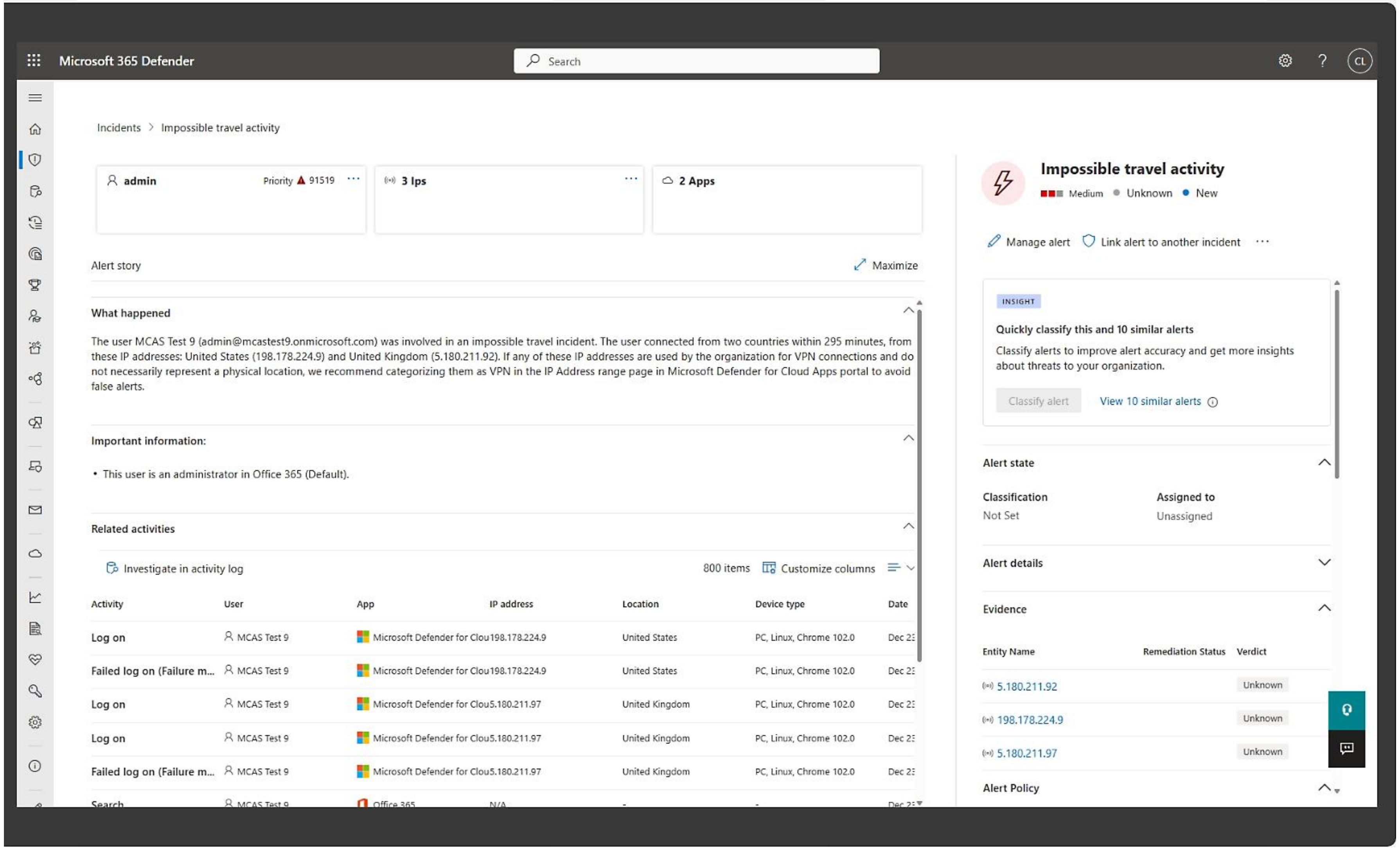
Analyze usage

Understand the usage patterns based on traffic data, top users and IP addresses, app categories and machines. Leverage the C-level report for a high level overview and recommendations

Evaluate compliance

Evaluate whether the discovered apps meet the compliance standards of your organization against factors like GDPR or industry-relevant standards like HIPAA readiness.

Protect against threats using advanced hunting in Microsoft 365 Defender



What happened

The user MCAS Test 9 (admin@mcastest9.onmicrosoft.com) was involved in an impossible travel incident. The user connected from two countries within 295 minutes, from these IP addresses: United States (198.178.224.9) and United Kingdom (5.180.211.92). If any of these IP addresses are used by the organization for VPN connections and do not necessarily represent a physical location, we recommend categorizing them as VPN in the IP Address range page in Microsoft Defender for Cloud Apps portal to avoid false alerts.

Important information:

- This user is an administrator in Office 365 (Default).

Related activities

Activity	User	App	IP address	Location	Device type	Date
Log on	MCAS Test 9	Microsoft Defender for Clou	198.178.224.9	United States	PC, Linux, Chrome 102.0	Dec 2
Failed log on (Failure m...	MCAS Test 9	Microsoft Defender for Clou	198.178.224.9	United States	PC, Linux, Chrome 102.0	Dec 2
Log on	MCAS Test 9	Microsoft Defender for Clou	5.180.211.97	United Kingdom	PC, Linux, Chrome 102.0	Dec 2
Log on	MCAS Test 9	Microsoft Defender for Clou	5.180.211.97	United Kingdom	PC, Linux, Chrome 102.0	Dec 2
Failed log on (Failure m...	MCAS Test 9	Microsoft Defender for Clou	5.180.211.97	United Kingdom	PC, Linux, Chrome 102.0	Dec 2
Search	MCAS Test 9	Office 365	N/A	-	-	Dec 2

Impossible travel activity

Quickly classify this and 10 similar alerts

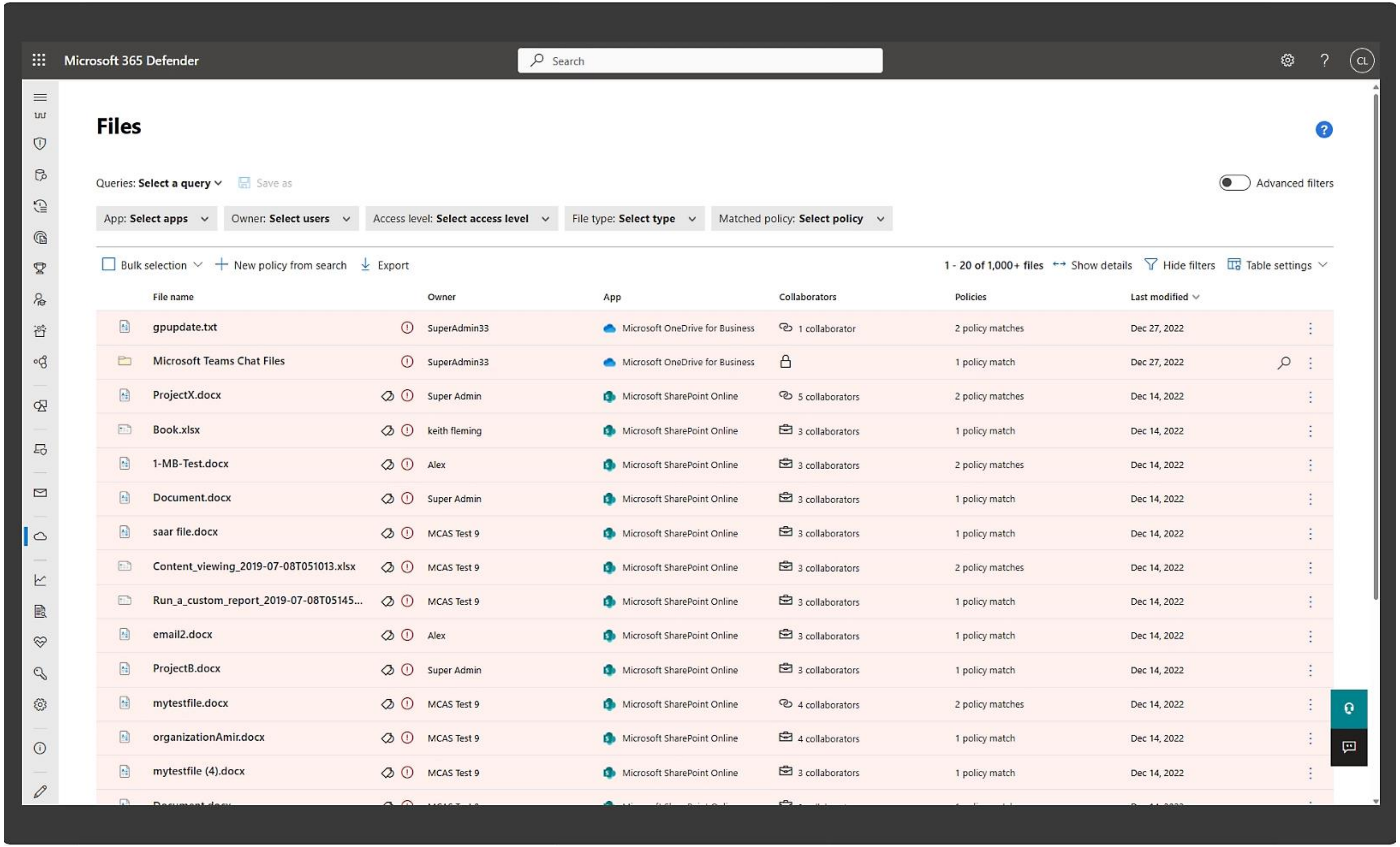
Classify alerts to improve alert accuracy and get more insights about threats to your organization.

Classification: Not Set

Assigned to: Unassigned

Entity Name	Remediation Status	Verdict
5.180.211.92		Unknown
198.178.224.9		Unknown
5.180.211.97		Unknown

Protect sensitive information across all apps



Microsoft 365 Defender

Search

Files

Queries: **Select a query** Save as

Advanced filters

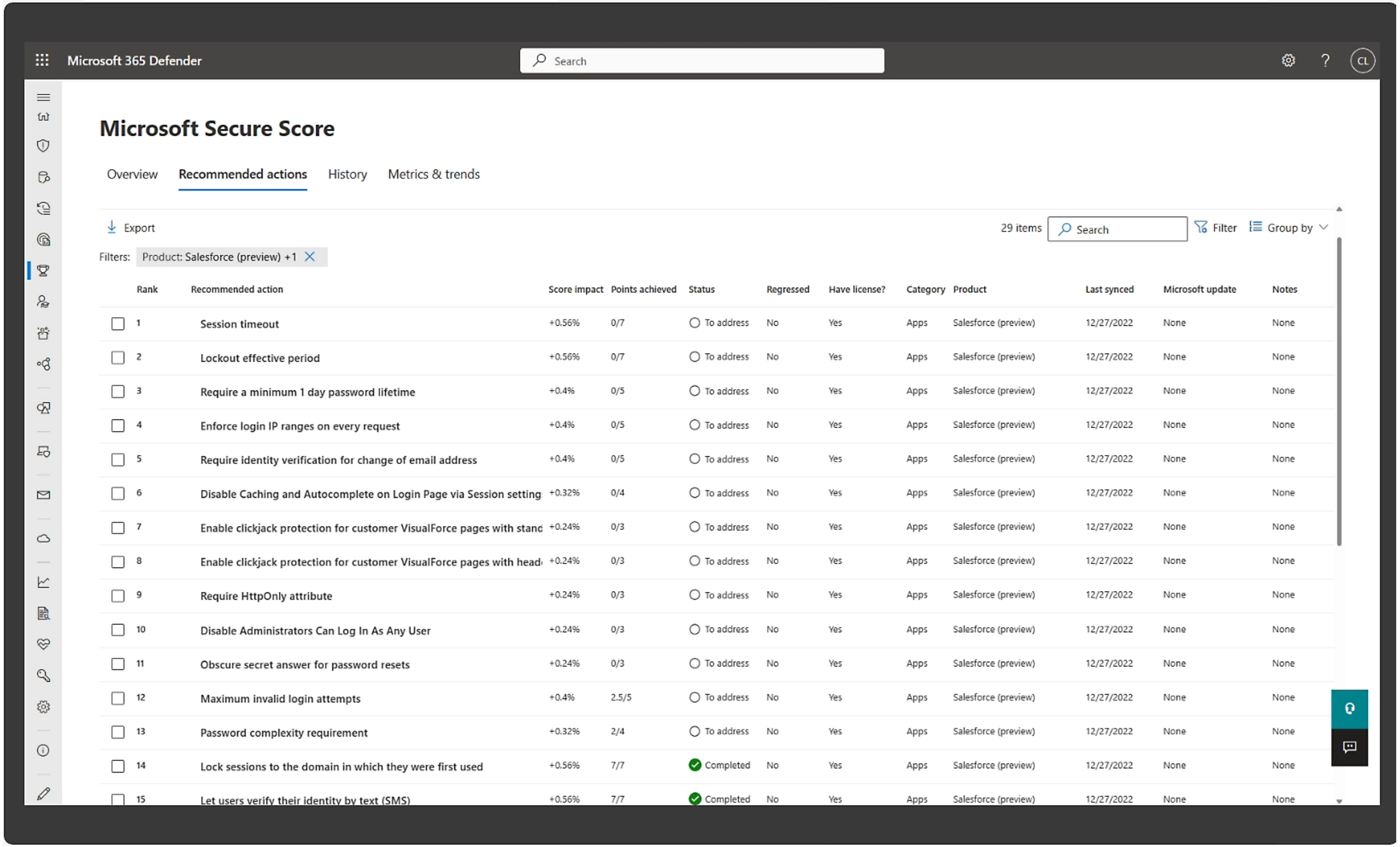
App: **Select apps** | Owner: **Select users** | Access level: **Select access level** | File type: **Select type** | Matched policy: **Select policy**

□ Bulk selection | + New policy from search | Export

1 - 20 of 1,000+ files | Show details | Hide filters | Table settings

File name	Owner	App	Collaborators	Policies	Last modified
gpupdate.txt	SuperAdmin33	Microsoft OneDrive for Business	1 collaborator	2 policy matches	Dec 27, 2022
Microsoft Teams Chat Files	SuperAdmin33	Microsoft OneDrive for Business		1 policy match	Dec 27, 2022
ProjectX.docx	Super Admin	Microsoft SharePoint Online	5 collaborators	2 policy matches	Dec 14, 2022
Book.xlsx	keith fleming	Microsoft SharePoint Online	3 collaborators	1 policy match	Dec 14, 2022
1-MB-Test.docx	Alex	Microsoft SharePoint Online	3 collaborators	2 policy matches	Dec 14, 2022
Document.docx	Super Admin	Microsoft SharePoint Online	3 collaborators	1 policy match	Dec 14, 2022
saar file.docx	MCAS Test 9	Microsoft SharePoint Online	3 collaborators	1 policy match	Dec 14, 2022
Content_viewing_2019-07-08T051013.xlsx	MCAS Test 9	Microsoft SharePoint Online	3 collaborators	2 policy matches	Dec 14, 2022
Run_a_custom_report_2019-07-08T05145...	MCAS Test 9	Microsoft SharePoint Online	3 collaborators	1 policy match	Dec 14, 2022
email2.docx	Alex	Microsoft SharePoint Online	3 collaborators	1 policy match	Dec 14, 2022
ProjectB.docx	Super Admin	Microsoft SharePoint Online	3 collaborators	1 policy match	Dec 14, 2022
mytestfile.docx	MCAS Test 9	Microsoft SharePoint Online	4 collaborators	2 policy matches	Dec 14, 2022
organizationAmir.docx	MCAS Test 9	Microsoft SharePoint Online	4 collaborators	1 policy match	Dec 14, 2022
mytestfile (4).docx	MCAS Test 9	Microsoft SharePoint Online	3 collaborators	1 policy match	Dec 14, 2022
Document.docx	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Manage your SaaS app security posture

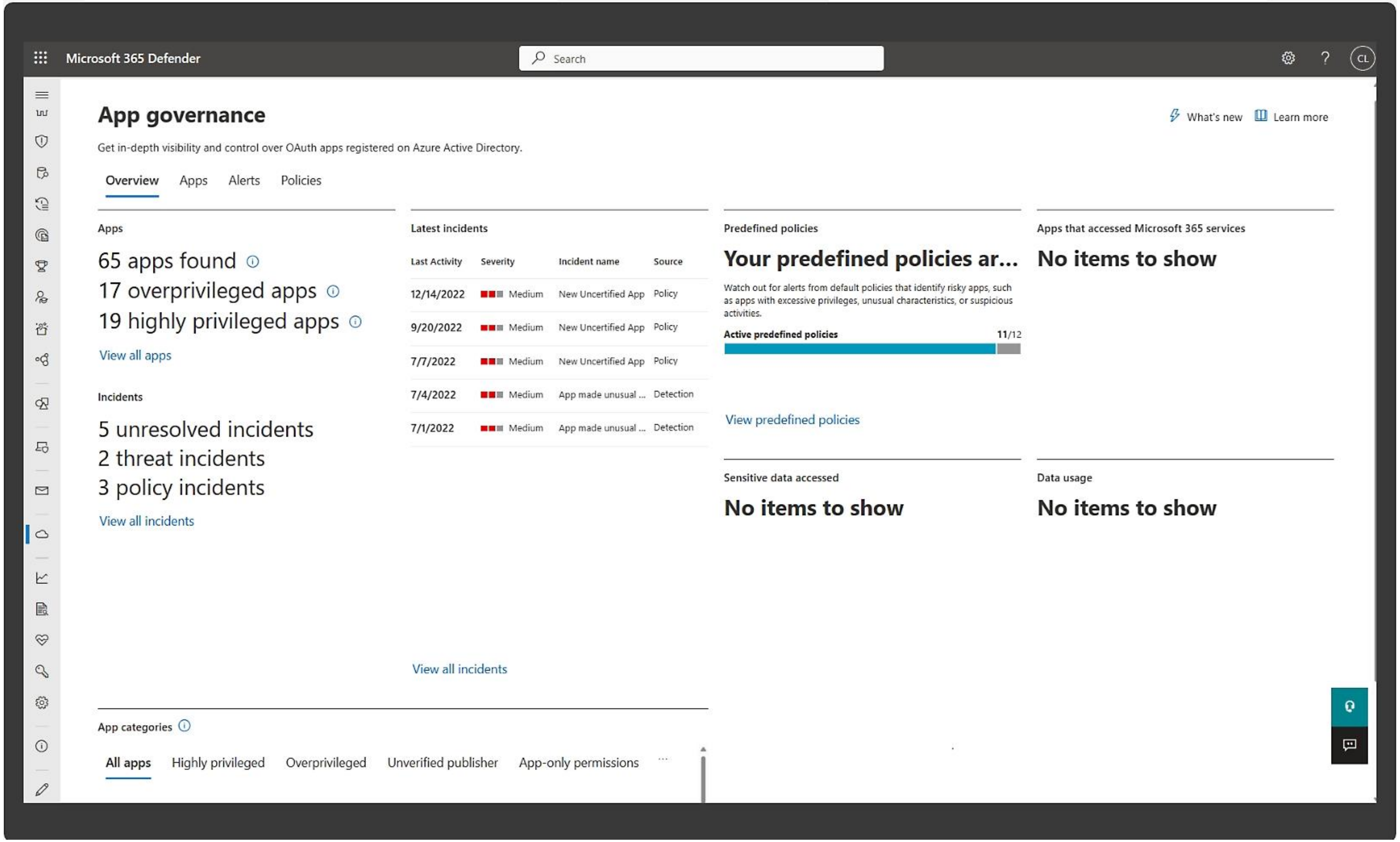


Microsoft Secure Score

Filters: Product: Salesforce (preview) +1 ✕

	Rank	Recommended action	Score impact	Points achieved	Status	Regressed	Have license?	Category	Product	Last synced	Microsoft update	Notes
□	1	Session timeout	+0.56%	0/7	○ To address	No	Yes	Apps	Salesforce (preview)	12/27/2022	None	None
□	2	Lockout effective period	+0.56%	0/7	○ To address	No	Yes	Apps	Salesforce (preview)	12/27/2022	None	None
□	3	Require a minimum 1 day password lifetime	+0.4%	0/5	○ To address	No	Yes	Apps	Salesforce (preview)	12/27/2022	None	None
□	4	Enforce login IP ranges on every request	+0.4%	0/5	○ To address	No	Yes	Apps	Salesforce (preview)	12/27/2022	None	None
□	5	Require identity verification for change of email address	+0.4%	0/5	○ To address	No	Yes	Apps	Salesforce (preview)	12/27/2022	None	None
□	6	Disable Caching and Autocomplete on Login Page via Session setting	+0.32%	0/4	○ To address	No	Yes	Apps	Salesforce (preview)	12/27/2022	None	None
□	7	Enable clickjack protection for customer VisualForce pages with stand	+0.24%	0/3	○ To address	No	Yes	Apps	Salesforce (preview)	12/27/2022	None	None
□	8	Enable clickjack protection for customer VisualForce pages with head	+0.24%	0/3	○ To address	No	Yes	Apps	Salesforce (preview)	12/27/2022	None	None
□	9	Require HttpOnly attribute	+0.24%	0/3	○ To address	No	Yes	Apps	Salesforce (preview)	12/27/2022	None	None
□	10	Disable Administrators Can Log In As Any User	+0.24%	0/3	○ To address	No	Yes	Apps	Salesforce (preview)	12/27/2022	None	None
□	11	Obscure secret answer for password resets	+0.24%	0/3	○ To address	No	Yes	Apps	Salesforce (preview)	12/27/2022	None	None
□	12	Maximum invalid login attempts	+0.4%	2.5/5	○ To address	No	Yes	Apps	Salesforce (preview)	12/27/2022	None	None
□	13	Password complexity requirement	+0.32%	2/4	○ To address	No	Yes	Apps	Salesforce (preview)	12/27/2022	None	None
□	14	Lock sessions to the domain in which they were first used	+0.56%	7/7	✓ Completed	No	Yes	Apps	Salesforce (preview)	12/27/2022	None	None
□	15	Let users verify their identity by text (SMS)	+0.56%	7/7	✓ Completed	No	Yes	Apps	Salesforce (preview)	12/27/2022	None	None

Evaluate Application Governance across SaaS workloads



App governance

Get in-depth visibility and control over OAuth apps registered on Azure Active Directory.

Apps

65 apps found

17 overprivileged apps

19 highly privileged apps

View all apps

Incidents

5 unresolved incidents

2 threat incidents

3 policy incidents

View all incidents

Latest incidents

Last Activity	Severity	Incident name	Source
12/14/2022	Medium	New Uncertified App	Policy
9/20/2022	Medium	New Uncertified App	Policy
7/7/2022	Medium	New Uncertified App	Policy
7/4/2022	Medium	App made unusual ...	Detection
7/1/2022	Medium	App made unusual ...	Detection

View all incidents

Predefined policies

Your predefined policies ar...

Watch out for alerts from default policies that identify risky apps, such as apps with excessive privileges, unusual characteristics, or suspicious activities.

Active predefined policies 11/12

View predefined policies

Apps that accessed Microsoft 365 services

No items to show

Sensitive data accessed

No items to show

Data usage

No items to show

App categories

Our Approach

Technology that empowers your business

Security in harmony with your business

People First

We aren't just here to implement technology; we are here to implement technology that works for you.

We work alongside your teams to bring business process and technology together.

Impactful Delivery

Leverage our industry and product expertise to quickly navigate everchanging compliance and regulatory requirements

Enable flexibility with solutions and policies tailored to your unique needs

Long Term Planning

Set you up for a successful future, drive meaningful impact, and limit business disruption.

What’s next for you?

Connect with us to schedule a:

- 1:1 Demo for you and your team
- Proof of concept in your environment
- Customized Strategy Session
- Requirements Gathering and Implementation Roadmap

slalom | Microsoft