

Post Ignite Security Recap

Microsoft Security

Beau Faull – Technology Specialist



Dave Caddick – Security Specialist



Jeff Beckitt – Technology Specialist





Acknowledgement of Country

We wish to acknowledge the traditional custodians of the land we are meeting on, the Whadjuk people of the Noongar nation, and pay respect to Elders past and present.

We recognise and respect their cultural heritage, beliefs and relationship with the land, as well as acknowledge the contribution they make to the life of this city and this region.





Who is Microsoft Ignite for?

[IT Professionals](#)[IT Decision Makers](#)[Security Professionals](#)[Data Professionals](#)[Developers](#)

Defend against threats by learning to use AI solutions to investigate and gain visibility faster.
Follow our curated session recommendations below to connect with security product experts about the innovations that can help you more effectively protect your organization.

Security strategist

Leverage AI and Microsoft Security solutions to strengthen your threat defense strategy.

[Explore security strategist sessions >](#)

Security architect

Fortify your device, application, and data security posture by learning about new integrations, use cases, and solutions.

[Explore security architect sessions >](#)

Security practitioner

Increase your organization's ability to find elusive security vulnerabilities with demonstrations and new solutions.

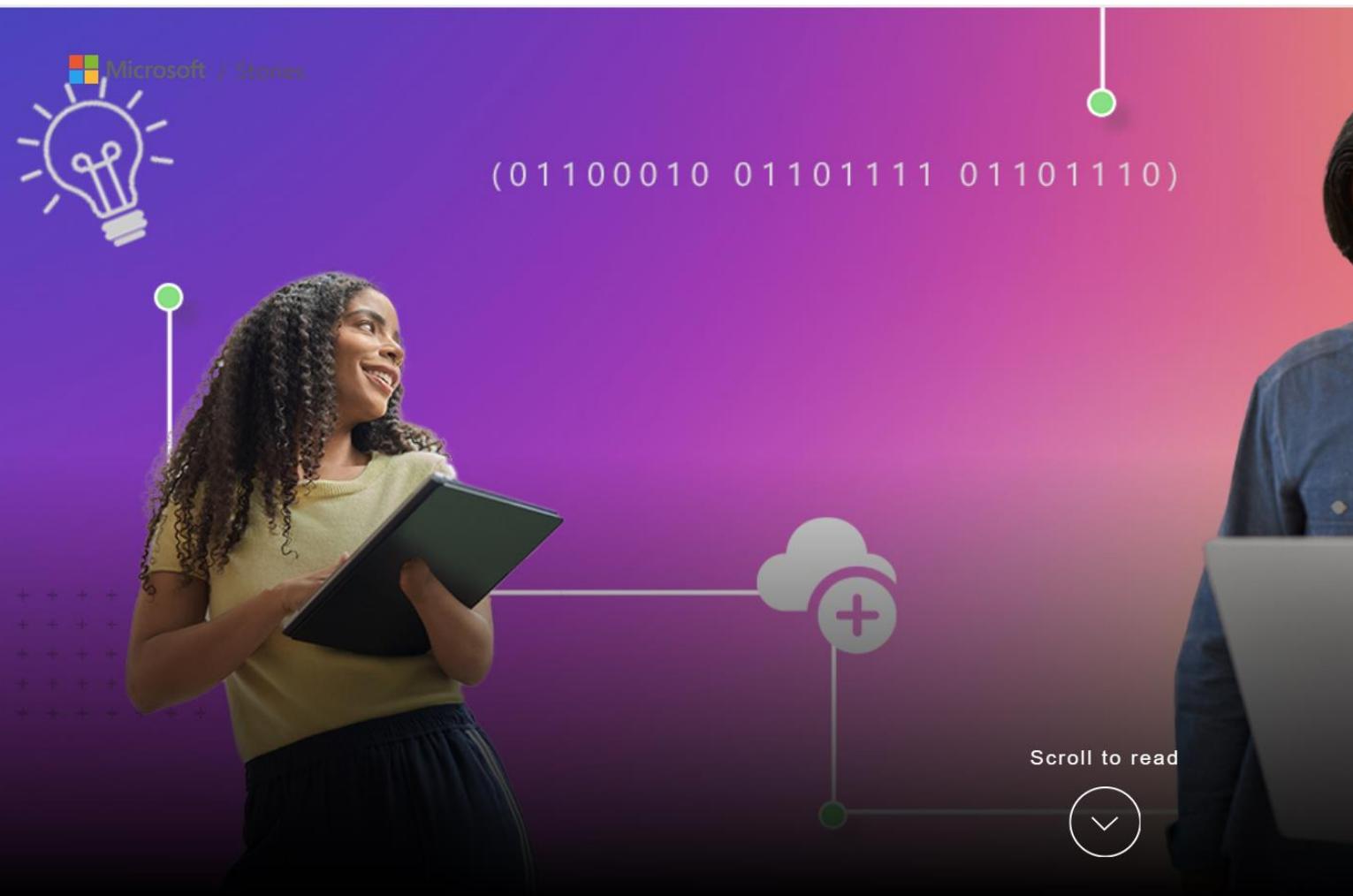
[Explore security architect sessions >](#)

Learn from Microsoft and partners



Ask me anything about Microsoft Ignite...





(01100010 01101111 01101110)

Scroll to read



MICROSOFT IGNITE BOOK OF NEWS

November 15 - 17, 2023

Table of Contents



Introduction ▾

1. Azure

- 1.1. Azure AI Services ▾
- 1.2. Azure Compute ▾
- 1.3. Azure Confidential Computing ▾
- 1.4. Azure Data ▾
- 1.5. Azure Infrastructure ▾
- 1.6. Azure Management & Operations ▾

2. Developer

- 2.1. Developer Community ▾
- 2.2. Developer Tools & DevOps ▾

3. Edge

- 3.1. Edge ▾

4. Microsoft 365

- 4.1. Microsoft 365 Apps & Services ▾
- 4.2. Microsoft Teams ▾
- 4.3. Microsoft Viva ▾



Picture in picture

Microsoft Ignite

0:02 / 1:02:31



Full Keynote: Satya Nadella at Microsoft Ignite 2023

Microsoft
1.26M subscribers

Subscribe

2K



Share

Download

Save



All

From Microsoft

Cloud computing

Cor >

How Security Copilot works

How Microsoft Security Copilot

Microsoft Ignite 2023



[Official Microsoft Blog >](#)

AI transformation and the technology driving change



[Book of News >](#)

A complete guide to all the news announced at this year's event



[Read the story >](#)

Microsoft aims to meet AI demand with systems approach to chips



[Event details >](#)

Get more information on this Nov. 15-16 event



[Press pack >](#)

Photos, transcripts and more will be added throughout the event

The opening keynote in 2 minutes

Keynote Highlights: Satya Nadella at Microsoft Ignite 2023

Copy link



Get on the list for Microsoft Ignite

Be the first to know when the event is happening. Save the date and be among industry leaders who are ready to help you find solutions to the industry's challenges.

[Get notified](#)

Relive the highlights and catch up on sessions

Learn about the latest AI innovations, build upon your skills, and access all the learning opportunities from this year's event.

[Stream on-demand sessions now >](#)

What sessions cover security copilot





Get on the list for Microsoft Ignite

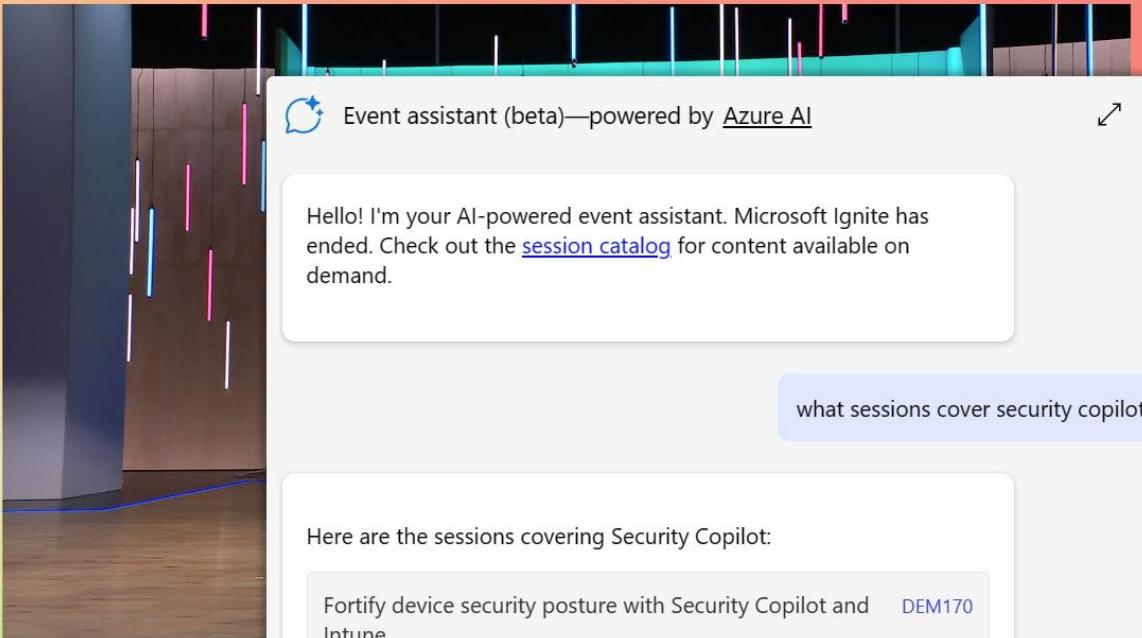
Be the first to know when the event is happening. Save the date and be among industry leaders who are ready to help you find solutions to the industry's challenges.

Get notified

Relive the highlights and catch up on sessions

Learn about the latest AI innovations, build upon your skills, and access all the learning opportunities from this year's event.

Stream on-demand sessions now >



Event assistant (beta)—powered by [Azure AI](#)

Hello! I'm your AI-powered event assistant. Microsoft Ignite has ended. Check out the [session catalog](#) for content available on demand.

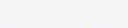
[what sessions cover security copilot](#)

Here are the sessions covering Security Copilot:

Fortify device security posture with Security Copilot and Intune [DEM170](#)

Ravi Ashok, Scott Duffy

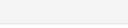
Nov 16 07:30 AM to 07:45 AM, Level 5, Hub, Demo Theater
3



Microsoft Security Copilot: Going Beyond Security Operations [DEM172](#)

Ryan Munsch

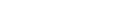
Nov 17 03:30 AM to 03:45 AM, Level 5, Hub, Demo Theater
3



Security Copilot mechanics [Studio08](#)

Jeremy Chapman, Ryan Munsch

Nov 17 06:29 AM to 06:33 AM



Ask me anything about Microsoft Ignite...



[Back to Schedule](#)[My event](#) •

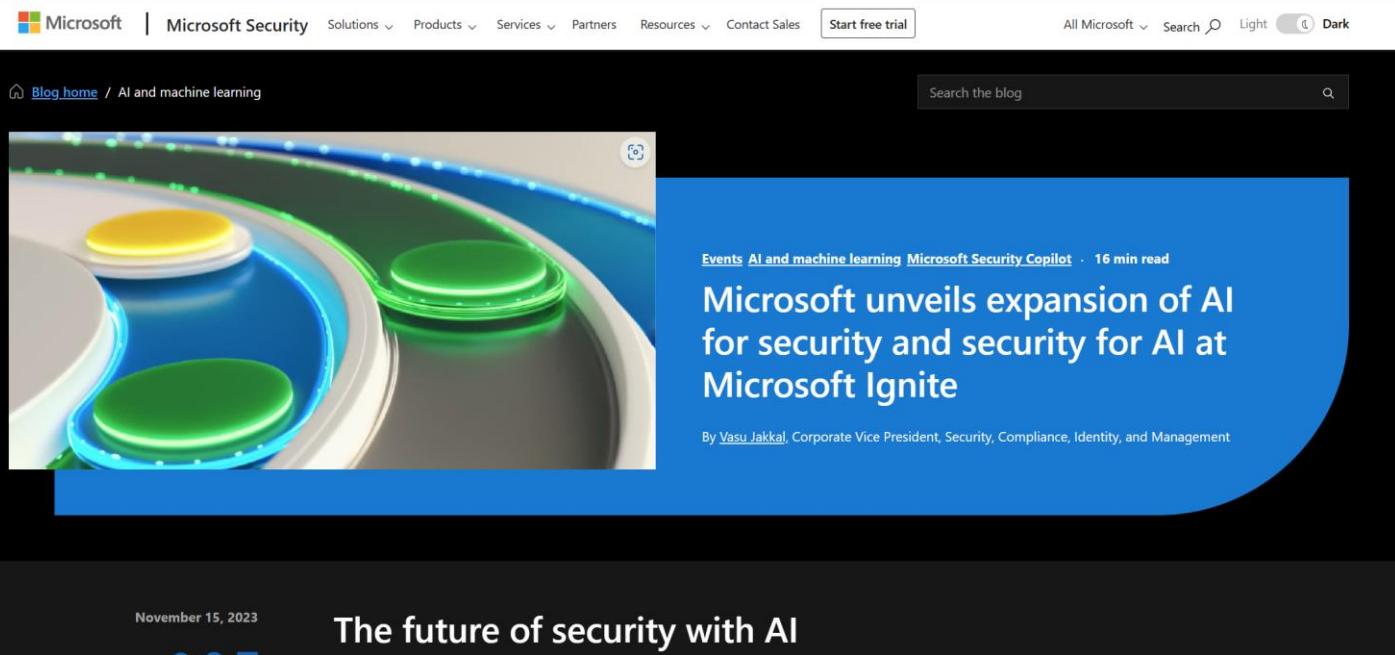
The Future of Security with AI

Friday, November 17 | 2:15 AM - 3:00 AM Australian Western Standard Time Duration 45 minutes

On Demand Keynote In Seattle + Online Will Be Recorded

Speakers:  Charlie Bell | Microsoft  Vasu Jakkal | Microsoft  Sherrod DeGrippo | Microsoft  Scott Woodgate | Microsoft

While the new era of AI presents unprecedented opportunities to elevate human potential, it also ushers in a new set of unknowns and risks. In this session, Charlie Bell and Vasu Jakkal will share how Microsoft is delivering AI for security with Security Copilot, and how we are enabling organizations to secure and govern AI with new capabilities.



[Blog home](#) / [AI and machine learning](#)

Events [AI and machine learning](#) [Microsoft Security Copilot](#) · 16 min read

Microsoft unveils expansion of AI for security and security for AI at Microsoft Ignite

By [Vasu Jakkal](#), Corporate Vice President, Security, Compliance, Identity, and Management

November 15, 2023

The future of security with AI



Security



XDR + SIEM + AI



Key announcements

Unified Security Operations Platform

The power of Microsoft Sentinel, Defender XDR and Security Copilot are now available in a unified experience

- A single view of security operations
- One place to view and prioritize incidents
- One place to hunt for threats
- One place to manage threat response

Added features

- Analyst experience is enriched with AI-powered guidance
- Security Copilot embedded experience
- Automatic attack disruption extends to SAP biz apps
- SOC optimizations to improve coverage and reduce costs

Microsoft Sentinel: A modern approach to security operations <https://bit.ly/40qlzN0>

Microsoft Ignite Sessions | Featured Partners | Blog | News and announcements | Support

Back to sessions

Microsoft Sentinel: A modern approach to security operations

Friday, November 17 | 8:00 AM - 8:45 AM Australian Western Standard Time Duration 45 minutes

Breakout In Seattle + Online

Speakers:  Preeti Krishna | Microsoft  Scott Woodgate | Microsoft

Remove from schedule Remove from backpack

This will conflict with another session in your schedule

Recommended next step: Microsoft Learn Collection

Resources

Ask me anything about Microsoft Ignite...

For more information: <https://aka.ms/UnifiedSIEMXDR>

XDR + SIEM + AI



Key announcements

Microsoft Defender for Cloud signal joining Microsoft Defender XDR

Customers now get a single XDR investigation experience across all end user assets and entire cloud infrastructure

- Holistic view across workspace and cloud infrastructure
- Uncover entire attack story in a single incident
- Visibility across Azure, AWS, and GCP environments
- Enables faster, more efficient threat hunting – all in one place

New deception techniques in Defender for Endpoint

New deception capabilities in Microsoft Defender for Endpoint give customers early-stage, high-fidelity signals of malicious activity to stop lateral movement

- Uses AI to automatically generate & disperse decoys and lures at scale
- Triggers automatic attack disruption for ransomware even faster
- Defender for Endpoint P2 customers will get immediate access at no added cost

For more information: <https://aka.ms/UnifiedSIEMXDR>

The screenshot shows a Microsoft Tech Community blog post. The URL is <https://aka.ms/MDEignite2023>. The post is titled "Microsoft Security Tech Accelerator" and was published on Dec 06 2023, 07:00 AM - 12:00 PM (PST) by Microsoft Tech Community. It has 14.6K views. The main content discusses how endpoints remain critical entryways for adversaries and how Microsoft Defender for Endpoint's built-in deception capability can help detect and respond to threats earlier. The post includes sections for Co-Authors (Evald Markinzon), Version history (Last update Nov 16 2023 06:20 PM, updated by Kim Kischel), and Labels (attack disruption, Deception, decoys, EDR).

XDR + SIEM + AI

Additional Announcements



Tier 1 announcements

Microsoft Defender XDR + Microsoft Sentinel

Unified Security Operations Platform, early access ~100 customers

Unified SIEM + XDR incidents for better workflow and better results

Security Copilot embedded experience

Automatic attack disruption, expands to include SAP data

SOC optimizations to improve coverage and reduce costs

Microsoft Defender XDR

Microsoft Defender XDR rename, public preview

Microsoft Defender for Cloud signal into Microsoft Defender XDR, public preview

Microsoft Defender for Endpoint

Deception techniques with attack disruption, public preview

Microsoft Sentinel

SOC optimizations to improve coverage and reduce costs, private preview



Tier 2 announcements

Microsoft Defender for Endpoint

Simplified security settings management experience, GA

Streamlined device connectivity experience, public preview

Windows Subsystem for Linux (WSL) support, public preview

Microsoft Defender for Cloud Apps

Discovery and management for over 400 generative AI apps, public preview

Microsoft Sentinel

New Splunk migration tools to simplify and accelerate migration to Sentinel, private preview in January

Microsoft Defender for IoT – Enterprise IoT security

E5 and E5 Security customers get Enterprise IoT security coverage for up to 5 IoT devices per eligible user license at no additional cost

Field Call to Action

Watch Ignite sessions

Wednesday November 15th

11:45am PST

[Discussion – Microsoft Defender for Endpoint with product experts](#)

4:00pm PST

[Breakout – Unifying XDR+SIEM: A new era in security operations](#)

4:00pm PST

[Discussion – Microsoft Sentinel Unleashed: Ask us anything](#)

5:00pm PST

[Breakout – The power of Microsoft's XDR: they attempted, we disrupted](#)

Thursday November 16th

4:00pm PST

[Breakout – Microsoft Sentinel: A modern approach to security operations](#)

Unified Security Operations Platform

The screenshot shows the Microsoft Defender Incident Queue interface. At the top, there's a navigation bar with icons for Home, Dashboards, and Security Copilot. Below the navigation bar is a search bar labeled "Search". The main area is titled "Incident Queue" and displays a table of 35 items. The table has columns for "Incident name", "Incident ID", "Tags", "Severity", "Categories", "Impacted assets", and "Service Sources". Each row represents a different incident, such as "SAP financial process manipulation attack disrupted" or "Multi-stage incident involving Initial access & Exfiltration". The "Service Sources" column highlights "Defender XDR, Microsoft Sentinel" for several incidents, while others like "Microsoft Defender for Office" and "Microsoft Defender for Cloud" are also listed. The "Tags" column often includes labels like "Attack disruption", "Contoso", "Subscription Theft", "AiTM attack", etc.

Incident name	Incident ID	Tags	Severity	Categories	Impacted assets	Service Sources
SAP financial process manipulation attack disrupted	2356358	Attack disruption +2	High	Initial access, Execution, Suspicious activity	Jonathan Wolcott 2 Devices SAP-01	Defender XDR, Microsoft Sentinel
Multi-stage incident involving Initial access & Exfiltration	2356634	Contoso +2	Medium	Initial access, Execution, Persistence, Defense	Mona Kane contoso-mona.pc	Defender XDR, Microsoft Data Loss Prevention
Account enumeration reconnaissance on one endpoint	2356521		Medium	Discovery	Robin Counts cont-robin.pc	Defender XDR, Defender for Identity
Initial access attempt in Office	2356963		Medium	Initial access	cecil.folk@contoso.com	Microsoft Defender for Office
Account enumeration reconnaissance on one endpoint	2355343		Low	Initial access	Robin Counts cont-robin.pc	Defender XDR, Defender for Identity
IaaS Resource Abuse	2351237	Subscription Theft	Medium	Initial access, Execution, Persistence, Defense	contoso-VM01	Microsoft Defender for Cloud
Attack using AiTM phishing (attack disruption)	2355678	AiTM attack +2	High	Initial access	Katri Ahokas cont-katri.pc	Defender XDR
Indicator 20.96.16.175 of type ipAddress was found. on...	2356323	Contoso	Medium	Initial access	Tim Deboer contoso_VM02	Microsoft Sentinel
Unusual addition of credentials to an OAuth app invol...	2356398	Contoso	Medium	Initial access	Carlos Slattery SkyScanner	Defender XDR, Defender for cloud Apps
Multi-stage incident involving Discovery & Lateral mo...	2352347		Low	Initial access	Cecil Folk cont-cecil.pc	Defender XDR
Account enumeration reconnaissance on one endpoint	2356562	Contoso	Medium	Discovery, Lateral movement	Colin Ballinger cont-colin.pc	Defender XDR

Defender for Cloud integration with Defender XDR

Incidents > Multi-stage incident involving Initial access & Credential access including Ransomware on multiple endpoints reported by multiple sources

Multi-stage incident involving Initial access & Credential access...

Security Copilot

Ask Defender Experts

Comments and history

Generate incident report

This information is limited because of your current permission. Contact a global administrator to change your permissions.

Attack story

Recommended actions (38)

Alerts (10)

Assets (15)

Investigations (2)

Evidence and Response (19)

Summary

Similar incidents

Alerts

0/10 Active alerts

Unpin all

Show all

Oct 24, 2023 6:47 PM • Resolved
Suspicious URL clicked

parkcity-
win11h.parkcity.alpineskihouse.co
biancap



Oct 24, 2023 6:50 PM • Resolved
**A potentially malicious URL click
was detected**

Bianca Pisani



Oct 24, 2023 7:21 PM • Resolved
**Azure Resource Manager operation
from suspicious proxy IP address**

4 Cloud Resources



Oct 24, 2023 7:21 PM • Resolved
**Access from a TOR exit node to a
key vault**

2 Cloud Resources



Oct 24, 2023 11:58 PM • Resolved
Malicious IP address

Backup Admin (parkcity)



Oct 25, 2023 12:03 AM • Resolved
Activity from a Tor IP address

Backup Admin (Parkcity)



Incident graph

Layout

Group similar nodes



Multi-stage incident involving Initial access & Credential access including Ransomware on multiple endpoints reported by multiple sources

High Resolved

Ransomware Credential Phish 20231025 +1

Manage incident

RECOMMENDATIONS

Phishing Incident response playbook

View phishing investigation and response recommended steps for this incident

Open phishing playbook

RECOMMENDATIONS

Ransomware Incident response playbook

Automated Attack Disruption

Microsoft Defender | https://defender.microsoft.com

Contoso | Microsoft Defender

Incidents > SAP financial process manipulation attack disrupted

SAP financial process manipulation attack disrupted

High Active Attack disruption Chain event detection

Alert story Alerts (13) Assets (7) Evidence & Response (4)

Alerts Layout Group by

13/13 Active alerts Unpin all Show all

- Jun 06, 2023 2:41 AM | Active A potentially malicious URL click was detected ✉️ jonathan.wolcott@contoso.com
- Jun 06, 2023 2:42 AM | Active Suspicious URL clicked 💻 cont-jonathan.pc ✉️ Jonathan Wolcott
- Jun 06, 2023 2:43 AM | Active Zscaler - phishing URL click detected ✉️ Jonathan Wolcott
- Jun 06, 2023 2:45 AM | Active Unfamiliar sign-in properties ✉️ Jonathan Wolcott
- Jun 06, 2023 2:43 AM | Active SAP - Login from unexpected network ✉️ Jonathan Wolcott 💻 SAP-01 💻 SAP-01-Host
- Jun 06, 2023 4:44 AM | Active SAP - cognitive tables direct access by dialog/REC 💻 SAP-01-Host

Information

Incident details

- Incident ID: 2356358
- Assigned to: Unassigned
- Classification: Not set
- Categories: Credential access, Initial access, Persistence, Discovery, Collection, Impact
- First activity: Aug 01, 2023 4:22 AM
- Last activity: Aug 01, 2023 4:22 AM

Impacted assets

- Devices: cont-jonathan.pc (Risk score: High), SAP-01-Host (Risk score: High)
- Users: Jonathan Wolcott (Investigation priority: High)
- Mailboxes: jonathan.wolcott@contoso.com

Security Copilot

SAP financial fraud attack

User Jonathan Wolcott operating on cont-jonathan.pc received a phishing email titled "Contoso bonus" with a malicious URL. They clicked the URL and their credentials were stolen. Using these stolen credentials the attacker signed in from IP 107.189.30.22 to ...

See more

AI generated. Verify for accuracy.

Recommended actions

Aug 01, 2023 2:41 AM

All (7) Unfinished

Triage

Active

Is this also a true positive incident?

3 similar incidents in your org were classified as true positive as BEC financial fraud multi stage attack.

Classify as 3 similar alerts

Contain

Completed

User 'Jonathan Wolcott' was suspended by attack disruption



Advanced Hunting

The screenshot shows the Microsoft Defender Advanced Hunting interface. On the left, there's a sidebar with various monitoring and alerting services like Microsoft Defender, AWS CloudTrail, AWS GuardDuty, and Azure Monitor for VMs. The main area displays a query editor with a schema dropdown, a search bar, and a query pane containing the following M365QL code:

```
let domains = dynamic(['someDomain.com', 'someDomain.com', 'someDomain.com']);
search in ( EmailUrlInfo, UrlClickEvents, DeviceNetworkEvents, DeviceFileEvents, DeviceEvents, BehaviorEntities)
Timestamp between (ago(180d) .. now())
and (RemoteUrl in (['domains'])
or FileOriginUrl in (['domains'])
or FileOriginReferrerUrl in (['domains'])
or Url in (['domains']))
and ActionType == "ConnectionSuccess"
| project $table, Timestamp, ActionType, DeviceId, DeviceName, RemoteUrl, InitiatingProcessFileName, RemoteIP, RemotePort,
InitiatingProcessSHA1, InitiatingProcessAccountName
```

The results section shows two items found:

Timestamp (UTC)	Table	Action type	DeviceID	DeviceName	Remote URL	Remote port
Aug 01, 2023 3:36 AM	DeviceNetworkEvent	ConnectionSuccess	6873-0r76899871...	karla.d-pc	intranet-host.cc	433
Aug 01, 2023 3:36 AM	DeviceNetworkEvent	ConnectionSuccess	6873-0r76899871...	karla.d-pc	intranet-host.cc	433

On the right, there's a Security Copilot panel with a generated query:

```
let domains = dynamic(['someDomain.com', 'someDomain.com', 'someDomain.com']);
search in ( EmailUrlInfo, UrlClickEvents, DeviceNetworkEvents, DeviceFileEvents, DeviceEvents, BehaviorEntities)
Timestamp between (ago(180d) .. now())
and (RemoteUrl in (['domains'])
or FileOriginUrl in (['domains'])
or FileOriginReferrerUrl in (['domains'])
or Url in (['domains']))
and ActionType == "ConnectionSuccess"
| project $table, Timestamp, ActionType, DeviceId, DeviceName, RemoteUrl, InitiatingProcessFileName, RemoteIP, RemotePort,
InitiatingProcessSHA1, InitiatingProcessAccountName
```

The panel also includes a note: "AI generated. Verify for accuracy." and a button to "Show only successful connections". At the bottom, it says "Here's a query you can add to find what you need:".

SOC Optimisation

Azure Portal x + https://ms.portal.azure.com Microsoft Azure Search resources, services and docs Sherrod DeGrippo CONTOSO

Home > Microsoft Sentinel

Microsoft Sentinel - SOC optimization

Selected workspace: Contoso WS

Search Refresh

General

- Overview
- Logs
- News & guides
- Search

Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks
- Entity behavior
- Threat intelligence
- MITRE ATT&CK (Preview)
- SOC optimization (Preview)**

Optimizations status

2 TB Ingested data over last 3 months See all use cases status click here

Optimization type: All

Overview Completed Dismissed

Low usage of StorageBlobLogs table

This table hasn't been used by analytic rules or detections for the last 30 days.

Value

By adding our recommended analytic rule(s), you can utilize this table better and improve your threat...

More details

Data value | Creation date Nov 15, 2023 12:32 PM

Coverage improvement against ERP (SAP) Financial Process Manipulation

We discovered that you can improve your coverage against ERP (SAP) Financial Process Manipulation...

Value

Improve your coverage against ERP (SAP) Financial Process Manipulation attacks.

More details

Coverage optimization | Creation date Nov 14, 2023 6:05 PM

Table Perf might only be used for monitoring

We have observed that this table has been used only by Azure Monitor for the last 30 days.

Value

If this table isn't used for security scenarios, save money by moving it to a non-security workspace.

More details

Data value | Creation date Nov 13, 2023 6:32 PM

Low usage of AADNonInteractiveSignInLogs table

This table hasn't been used by analytic rules or detections for the the last 30 days.

Value

By adding our recommended analytic rule(s), you can utilize this table better and improve your threat...

More details

Data value | Creation date Nov 13, 2023 2:41 AM

Table ContainerLog wasn't queried in the last 30 days

We have observed there hasn't been usage of the data in the table for a while.

Value

If the table isn't used for security detections, compliance...

Coverage improvement against Adversary in the middle (AiTM)

We discovered that you can improve your coverage against Adversary in the middle (AiTM) attacks.

Value

SOC Optimisation

The screenshot shows the Microsoft Sentinel - SOC optimization page in the Azure Portal. The top navigation bar includes the Azure logo, user profile (Sherrod DeGrippo, CONTOSO), and a search bar. The main header is "Microsoft Azure" and the sub-header is "Home > Microsoft Sentinel".

General sidebar:

- Overview
- Logs
- News & guides
- Search

Threat management sidebar:

- Incidents
- Workbooks
- Hunting
- Notebooks
- Entity behavior
- Threat intelligence
- MITRE ATT&CK (Preview)
- SOC optimization (Preview)**

Content management sidebar:

- Content hub
- Repositories
- Community

Configuration sidebar:

- Workspace manager (Preview)
- Data connectors
- Analytics

Microsoft Sentinel - SOC optimization page:

- 2 TB** Ingested data over last 3 months
- See all use cases status click here**
- Optimizations status**: Active (6), Completed (3), Dismissed (2)
- Overview**, **Completed**, **Dismissed**
- Search** and **Optimization type: All**
- Low usage of StorageBlobLogs table**: 1 out of 2 suggestions. This table hasn't been used by analytic rules or detections for the last 30 days. Value: By adding our recommended analytic rule(s), you can utilize this table better and improve your threat... [More details](#)
- Coverage improvement against ERP (SAP) Financial Process Manipulation**: We discovered that you can improve your coverage against ERP (SAP) Financial Process Manipulation... Value: Improve your coverage against ERP (SAP) Financial Process Manipulation attacks. [More details](#)
- Table Perf might only be used for Azure Monitor**: 1 out of 2 suggestions. We have observed that this table hasn't been used by analytic rules or detections for the last 30 days. Value: If this table isn't used for security detections, move it to a non-security workspace. [More details](#)
- Table ContainerLog wasn't queried in the last 30 days**: 1 out of 2 suggestions. We have observed there hasn't been usage of the data in the table for a while. Value: If the table isn't used for security detections, compliance or other reasons, save money by changing the current... [More details](#)
- Coverage improvement against Adversary in the middle (AiTM)**: We discovered that you can improve your coverage against Adversary in the middle (AiTM) attacks. Value: Improve your coverage against Adversary in the middle (AiTM) attacks. [More details](#)

Low usage of StorageBlobLogs table (Details):

- Complete** **Dismiss** **Provide feedback**
- Optimization is calculated every 24 hours | Last update Nov 15, 2023
- Description**: This table hasn't been used by analytic rules or detections for the last 30 days.
- Type**: Data value
- Suggestion 01 - Enhance protection by adding analytic rules**
 - Value**: By adding our recommended analytic rule(s), you can utilize this table better and improve your threat protection.
 - Action**: Go to Content hub and review the suggested analytic rules to activate. [Go to Content hub](#)
- Suggestion 02 - Save money by changing data plan**
 - Value**: If this table isn't used for security detections or advanced queries, save money by changing the ingestion plan.
 - Action**: Move this table to basic logs. Basic logs has KQL and retention limitations, please refer to the documentation.
 - Data ingestion (Last 3 Month)**: Table is 15% percent of all workspace data

Monitoring Shadow AI

Cloud app catalog



Filters:

Advanced filters

Apps: Apps... App tag ⓘ: Sanctioned Unsanctioned None Risk score: 0 10 Compliance risk factor: Select factors

Security risk factor: Select factors

Browse by category:



413

Bulk selection

+ New policy from search

1 - 20 of 413 apps

Show details

Table settings

generative ai

✓ Generative AI

App

Risk s... ↓

Actions



Microsoft Bing Chat
Generative AI

10



Microsoft Designer
Generative AI

10



Amazon Polly
Generative AI

10



DialogFlow
Generative AI

10



Adobe Firefly
Generative AI

10



Google Bard
Generative AI

9



Monitoring Shadow AI

Cloud app catalog



Filters:

Advanced filters

Apps: Apps...

App tag ⓘ:

Sanctioned

Unsanctioned

None

Risk score: 0 2

Compliance risk factor: Select factors

Security risk factor: Select factors

Bulk selection

Browse by category:



generative ai

✓ Generative AI

16

Bulk selection

+ New policy from search

1 - 16 of 16 apps

↔ Show details

Table settings

App	Risk s... ↑	Actions
Peoplegeist Generative AI	1	<input checked="" type="checkbox"/> <input type="checkbox"/>
SEOContentMachine Generative AI	2	<input checked="" type="checkbox"/> <input type="checkbox"/>
Qualifier Generative AI	2	<input checked="" type="checkbox"/> <input type="checkbox"/>
Localio Generative AI	2	<input checked="" type="checkbox"/> <input type="checkbox"/>
GetGenie Generative AI	2	<input checked="" type="checkbox"/> <input type="checkbox"/>
SpeechVid Generative AI	2	<input checked="" type="checkbox"/> <input type="checkbox"/>

Cloud Security

Comprehensive cloud-native application protection enhancements in Defender for Cloud



Key announcements

Proactive risk analysis and mitigation with CSPM

Integrated insights from Entra Permissions Management (CIEM)

- Centralized view of Permissions Creep Index
- Drive least privilege access controls for cloud resources
- Get proactive attack path analysis to expose vulnerabilities across Azure, AWS, and GCP

Proactive attack path analysis across clouds and faster mitigation with embedded AI

- Security admins can match critical risks to new MITRE framework mapping
- New attack path analysis engine optimized to identify more complex and sophisticated attack patterns, such as cross-cloud attack paths
- New ServiceNow integration to use existing system to automate and respond
- Assisted risk analysis and faster remediation with Security Copilot integration

The screenshot shows a Microsoft Ignite session page. At the top, there's a navigation bar with links for Microsoft, Microsoft Ignite, Sessions, Featured Partners, Blog, News and announcements, and Support. On the right, it shows 'All Microsoft' and 'Hi Jeff Beckitt'. Below the navigation, the session title is 'Boost multicloud security with a comprehensive code to cloud strategy'. It's listed as a 'Breakout' session in Seattle + Online on Friday, November 17, from 3:45 AM to 4:30 AM Australian Western Standard Time, lasting 45 minutes. Two speakers are listed: Saeema Begum and Yuri Diogenes, both from Microsoft. To the right, there's a video player showing a man with a beard and glasses speaking. A sidebar on the right includes buttons for 'Remove from schedule' and 'Remove from backpack', a note about conflicts, a 'Recommended next step' section for 'Microsoft Learn Collection', a 'Resources' section, and a feedback box asking 'Ask me anything about Microsoft Ignite...'. There are also icons for a microphone, a video camera, and closed captions.



For more information: <https://aka.ms/DefenderforCloud/Ignite23>

Cloud Security

Comprehensive cloud-native application protection enhancements in Defender for Cloud



Key announcements

Unified DevOps security insights across GitHub, Azure DevOps and GitLab

DevOps security insights part of Defender CSPM

- Deep visibility into application security posture across GitHub, Azure DevOps and GitLab (preview) within Defender for Cloud
- DevOps insights now included in Defender CSPM, Defender for DevOps (Preview) retired
- New code to cloud remediation workflows drive better collaboration between DevOps and security teams to trace and fix security issues in code, integrated with GitHub Advanced Security

Extended container and API coverage and enhanced workload protection for SOC

- Integrated with Defender XDR for a unified SOC
- New container security enhancements- support for Amazon EKS and Google EKS clusters in contextual graph, Agentless vulnerability assessments GA
- Defender for APIs GA: visibility of business-critical APIs, prioritize vulnerability fixes, and quickly detect active real-time threats published in Azure API Mgmt

For more information: <https://aka.ms/DefenderforCloud/Ignite23>

<https://aka.ms/DefenderforCloud/Ignite23>

The screenshot shows a Microsoft Tech Community blog post. The header includes the Microsoft logo, a search bar, and a sign-in link. The main title is "Microsoft Security Tech Accelerator" with a date of Dec 06 2023, 07:00 AM - 12:00 PM (PST). Below the title, the URL is https://aka.ms/DefenderforCloud/Ignite23. The post content is titled "Announcing new CNAPP capabilities in Defender for Cloud" by Vlad Korsunsky, published on Nov 15 2023 at 07:58 AM, with 4,745 views. It discusses the challenges of cloud computing and the emergence of CNAPP. The sidebar features "Co-Authors" (Vlad Korsunsky, Mona Thaker), "Version history" (last updated Nov 16 2023 at 10:58 AM by Mona Thaker), and "Labels" (Cloud Security, Cloud Security Posture Management, Threat Protection, Workload Protection).

Cloud Security

Additional Announcements



Tier 1 announcements

Microsoft Defender for Cloud

Security Copilot in Defender for Cloud, early access private preview

Defender CSPM

Unified insights from Entra Permissions Management (CIEM), public preview

Integrated DevOps security insights across GitHub, Azure DevOps, and GitLab, GA

Improved container security across multicloud environments, public preview

Proactive attack path analysis across clouds and faster mitigation, public preview

Defender CSPM capabilities for GCP, GA



Tier 2 announcements

Microsoft Defender for Cloud

Defender for APIs

Improved API security posture, GA

Data security dashboard, GA

Microsoft Defender External Attack Surface Management

EASM skills in Security Copilot to identify and analyze external risks, early access private preview

Attack Path Analysis in Defender CSPM

Microsoft Azure Search resources, services and docs Sherrod DeGrippo WOODGROVE

Home > Microsoft Defender for Cloud | Attack path analysis

Internet exposed GCP VM Instance with critical vulnerabilities allows lateral movement to AWS S3 Bucket with sensitive data

Showing 85 subscriptions

Learn more Guides & Feedback

High Severity 1 Recommendations 24 Hours Freshness interval

Description
Attacker with network access to the GCP VM Instance can exploit the vulnerabilities, gain code execution, move laterally to the AWS S3 bucket and steal the sensitive data.
[See more](#)

Attack story
1. Resolve all recommendations associated with the attack path
2. Apply additional security best practices to reduce risk:
Harden the internet exposure to the minimum needed

Resource types
GCP VM instance (1)
AWS S3 Bucket (1)
[See more](#)

Risk factors
SENSITIVE DATA EXPOSURE LATERAL MOVEMENT

MITRE ATT&CK® tactics

Discovery [Read more](#)
Cloud Storage Object Discovery (T1619)

Attack path instance Remediation

The diagram illustrates the attack path between two cloud environments:

- Attack Path:** Internet → GCP VM Instance (attackworkstation) → AWS IAM User (user_1) → AWS S3 Bucket (s3_bucket_324).
- Relationships:** The GCP VM Instance contains the AWS IAM User, which has permissions to the AWS S3 Bucket.
- Intermediate Components:** The GCP VM Instance connects to a Default Load Balancer, which in turn routes traffic to two IP addresses (20.221.212.202). These IP addresses route traffic to a VPC (vpc1), which then routes traffic to the GCP VM Instance.

Annotations indicate that the GCP VM Instance and the AWS IAM User are both exposed to the Internet, contributing to the high severity of the vulnerability.

Defender for Cloud integration with Security Copilot

The screenshot shows the Microsoft Azure interface with the 'Microsoft Defender for Cloud | Recommendations' page open. A specific recommendation is displayed: 'S3 Block Public Access setting should be enabled at the bucket level'. The recommendation is categorized as 'Critical' with a 'aws-s3-contosohotel' resource and 'Unassigned' status.

Description: This control checks whether S3 buckets have bucket-level public access blocks applied. This control fails if any of the following settings are set to false: ignorePublicAcls*, blockPublicPolicy*, blockPublicAcls*, restrictPublicBuckets*. Block Public Access at the S3 bucket level provides controls to ensure that objects never have public access. Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, or both. Unless you intend to have your S3 buckets publicly accessible, you should configure the bucket level Amazon S3 Block Public Access feature.

Attack paths: 3; **Scope:** AWS DSCP M; **Additional instances:** 24

Last change date: 5/5/2023; **Owner:** Unassigned; **Due date:** -

Risk factors: Sensitive data, Exposure to the Internet

Tactics & techniques: A horizontal timeline showing various threat stages, with 'Discovery' highlighted.

Discovery: Read more; **Cloud Storage Object Discovery:** T1619

Take action: Map, Remediate, Assign owner and set due date, Exempt, Workflow automation, Trigger logic app

Remediate: After the process completes, it may take up to 6 Hours until your resources move to the 'healthy resources' tab. Note: For information on how to remove public access at a bucket level, see [Blocking public access to your Amazon S3 storage](#) in the Amazon S3 User Guide.

Assign owner and set due date: Create assignment

Exempt: If the recommendations doesn't represent a threat or the threat is mitigated using other tools, you can exempt it for this specific resource. Exempted resources appear as not applicable and do not affect secure score.

Workflow automation: Set a logic app which you would like to trigger with this security recommendation. Trigger logic app

Security Copilot: Overview (Aug 01, 2023 2:41 AM)

The security recommendation for the resource, contoso-s3-bucket3, is to activate the S3 block public access setting at the bucket level. This action is vital to prevent unauthorized access to your data.

By blocking public access at the S3 bucket level, you ensure that objects never have public access, regardless of access control lists (ACLs), bucket policies, or both.

Addressing this recommendation will eliminate three potential attack paths and reduce the risk factors associated with sensitive data and internet exposure. Enhancing security measures is crucial for safeguarding sensitive data within aws-s3-bucket3.

AI generated. Verify for accuracy.

How to remediate the recommendation?

- Log in to your AWS account using the AWS CLI
- Run the following command to enable the S3 Block Public Access settings for the specific bucket:

```
CLI
aws s3api put-public-access-block \
--bucket aws-s3-contosohotel \
--public-access-block-configuration
"BlockPublicAcls" = true,
```

Defender CSPM in Action - YouTube

The image shows a screenshot of a YouTube video player. The video is titled "Defender CSPM in Action - YouTube". The main content area features a man with a shaved head, wearing a dark blue button-down shirt, standing behind a podium. To his right is a large screen displaying a Microsoft Mechanics slide with the title "Microsoft Mechanics" and the subtitle "Visualize future attacks". The slide shows a diagram of a network flow from a "main-source AWS S3 Bucket" through the "Internet" to a "QoL" endpoint. A shield icon indicates a security concern. Below the slide, the text "Adwait Joshi" and "Senior Director Cloud Security" is displayed, along with a blue circular icon containing a gear and puzzle piece symbol. The YouTube interface includes a search bar at the top, a subscribe button with 317K subscribers, and various video controls like play, volume, and download. The video progress bar shows 0:04 / 9:27. The video description at the bottom reads "Predict future security incidents! Cloud Security Posture Management with Microsoft Defender".

YouTube AU

Search

Microsoft Mechanics

Visualize future attacks

Adwait Joshi

Senior Director Cloud Security

0:04 / 9:27 • Cloud Security Posture Management in Defender for Cloud >

Download

Microsoft Mechanics

Subscribed 317K subscribers

102

Share

Download

Clip

All From Microsoft Mechanics Microsoft Cor >

The new Microsoft Defender Microsoft Defender XDR, ...

Security Copilot, Threat Intelligence, Services



Ignite highlights:

- Security Copilot private preview of new use cases & 1st party integrations
- MDTI free experience in Defender XDR, vulnerability profiles, detonation intelligence
- Defender Experts for XDR new enhancements and Teams app



Key announcements

Security Copilot new use cases and 1st party integrations

Private preview of generative AI capabilities for customers across identity management, data protection, compliance, and device management

• Identity management – Microsoft Entra

Discover overprivileged access, generate access review for incidents, generate and describe access policies and identify gaps, and evaluate licensing across solutions

• Device management – Microsoft Intune

Enable IT admins to generate device policies and simulate their outcomes, gather device information for forensics, and configure devices with best practices from similar deployments.

• Data security and compliance – Microsoft Purview

Identify data impacted and users involved in security incidents, generate summary of DLP and insider risks, generate contextual summary of compliance matches and review sets, and generate keyword query language from natural language prompt.

• Cloud security posture management – Defender EASM and Defender for Cloud

Simplify EASM risk assessment and manage cloud security posture more efficiently. Quickly discover potential attack paths using natural language queries, get mitigation guidance.

• Unified security operations platform – Microsoft Defender XDR + Sentinel

Accelerating incident response with guided investigation, rapid aggregation of evidence across numerous data sources, and advanced capabilities such as malware analysis

For more information: <https://aka.ms/IgniteFY24SecurityBlogPost>

The Future of Security with AI <https://bit.ly/49qOyp1>

The screenshot shows the Microsoft Ignite website interface. At the top, there's a navigation bar with links for Microsoft, Microsoft Ignite, Sessions, Featured Partners, Blog, News and announcements, and Support. On the right, it shows 'All Microsoft' and 'Hi Jeff Beckett'. Below the navigation, a banner for the session 'The Future of Security with AI' is displayed, along with the date (Friday, November 17), time (2:15 AM - 3:00 AM Australian Western Standard Time), duration (45 minutes), and a 'Duration 45 minutes' note. It also lists the speakers: Charlie Bell (Microsoft), Vasu Jakkal (Microsoft), Sherrod DeGrippo (Microsoft), and Scott Woodgate (Microsoft). The main content area shows two speakers on stage: a man in a dark suit and a woman in a colorful dress. A large play button is overlaid on the video feed. To the right, there are buttons for 'Remove from schedule' and 'Remove from backpack'. Below the video, there's a sidebar with 'Recommended next step' (Microsoft Learn Collection) and 'Resources' (Download Video, Download Transcript). At the bottom, there's a feedback box asking 'Ask me anything about Microsoft Ignite...' and a page number '29'.

Security Copilot, Threat Intelligence, Services



Ignite highlights:

- Security Copilot private preview of new use cases & 1st party integrations
- MDTI free experience in Defender XDR, vulnerability profiles, detonation intelligence
- Defender Experts for XDR new enhancements and Teams app



Key announcements

Microsoft Defender Threat Intelligence

- MDTI free experience available to any Microsoft Defender XDR customer
- Vulnerability profiles – provide intelligence on customer's most critical exposures so they can prioritize and plan action
- Detonation intelligence – enables customers to search and contextualize threats to quickly understand a malicious file or URL.
- MDTI integration with Security Copilot – instantly summarize content to provide crucial situational awareness for security teams

Microsoft Defender Experts for XDR

- New managed response enhancements provide API integration for 3rd party SIEM, more visibility into actions taken on customers' behalf, and new exclusions capability
- Onboarding and reporting enhancements – self-service readiness assessment to expedite onboarding, actionable insights highlighting most targeted users/devices and new homepage experience
- New Teams app for Defender Experts for XDR will notify customers if they need to take action to remediate a threat. Customers can chat directly with experts through the app

For more information: <https://aka.ms/DefenderExpertsforXDR/Ignite23>

MDTI: Now Anyone Can Tap Into Game-Changing Threat Intelligence <https://bit.ly/49Dz55l>

MDTI: Now Anyone Can Tap Into Game-Changing Threat Intelligence

Thursday, November 16 | 5:30 AM - 6:15 AM Australian Western Standard Time Duration 45 minutes

Speakers: Yaniv Shasha | Microsoft Sherrod DeGrippo | Microsoft

Microsoft Ignite

Remove from schedule Remove from backpack

Recommended next step Microsoft Learn Collection

Resources

Ask me anything about Microsoft Ignite...

Security Copilot, Threat Intelligence, Services

Additional Announcements



Tier 1 announcements

Security Copilot new use cases and 1st party integrations

Identity management – Microsoft Entra

Discover overprivileged access, generate access review for incidents, generate and describe access policies and identify gaps in them, and evaluate licensing across solutions

Device management – Microsoft Intune

Enable IT admins to generate device policies and simulate their outcomes, gather device information for forensics, and configure devices with best practices from similar deployments.

Data security and compliance – Microsoft Purview

Identify data impacted and users involved in security incidents, generate summary of DLP and insider risks, generate contextual summary of compliance matches and review sets, and generate keyword query language from natural language prompt.

Cloud security posture management (Defender EASM and Defender for Cloud)

Simplify EASM risk assessment and manage cloud security posture more efficiently. Quickly discover potential attack paths using natural language queries, get mitigation guidance.

Embedded experience in the unified security operation platform (SIEM+XDR)

accelerating incident response with guided investigation, rapid aggregation of evidence across numerous data sources, and advanced capabilities such as malware analysis



Tier 2 announcements

Microsoft Defender Threat Intelligence

- MDTI free experience available to any Microsoft Defender XDR customer
- Vulnerability profiles – provides intelligence on customer's most critical exposures so they can prioritize and plan action
- Detonation intelligence – enables customers to search and contextualize threats. Quickly understand a malicious file or URL
- MDTI integration with Security Copilot – instantly summarize content to provide crucial situational awareness for security teams

Microsoft Defender Experts for XDR

- New managed response enhancements to provide more visibility into actions taken on their behalf and improve response time, API integration for 3rd party SIEM
- Onboarding and reporting enhancements – self-service readiness assessment for Defender configurations, actionable insights highlighting most targeted users/devices
- Teams app for Defender Experts for XDR will notify customers if they need to take action to remediate a threat. Customers can chat directly with experts through the app

For more information – call to action

Watch Ignite sessions

Wednesday November 15th

10:25am PST

[Keynote - The future of Security with AI](#)

1:30pm PST

[Discussion – MDTI: Now anyone can tap into game-changing threat intelligence](#)

Friday November 17th

11:45am PST

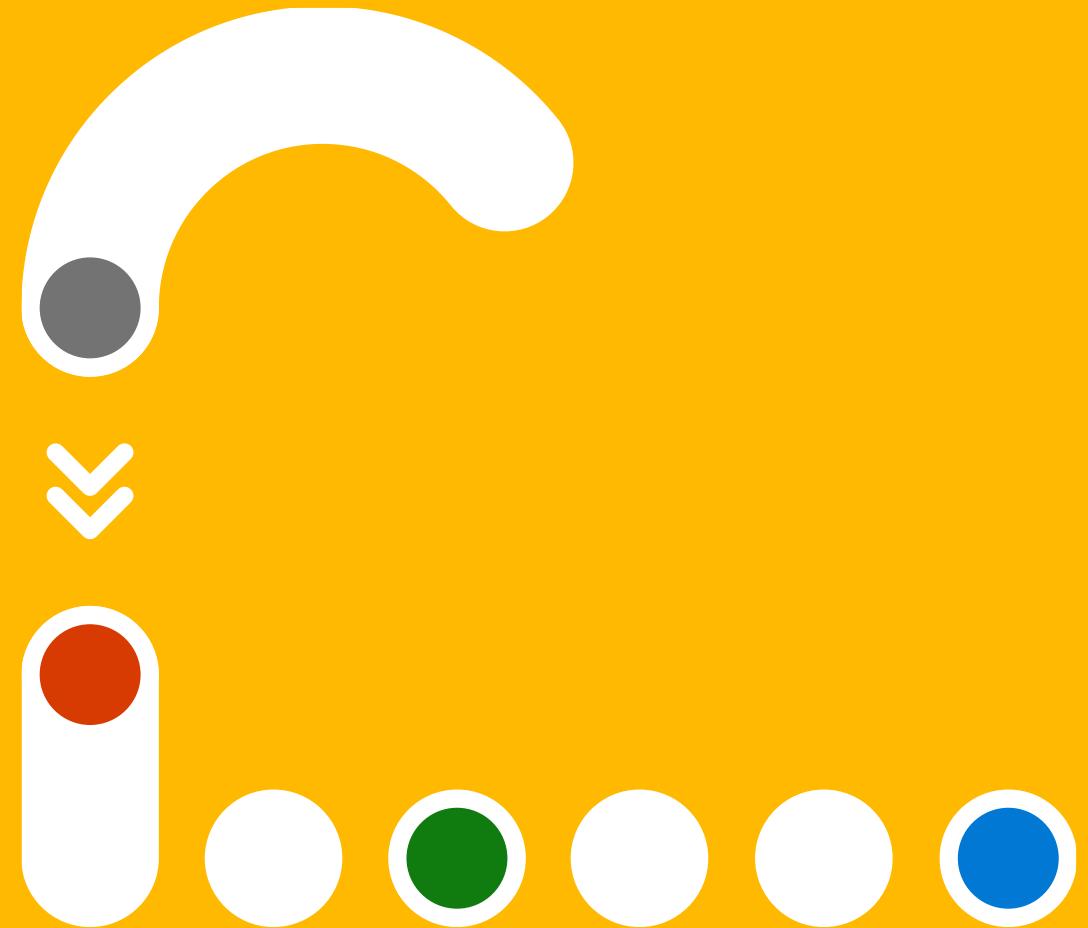
[Breakout – This year in threats: Microsoft's global fight against APTs](#)

10:15am PST

[Breakout – New era threat actor: A year battling Octo Tempest](#)

[On-demand – Jumpstart your SOC with Microsoft Defender Experts for XDR](#)

Data Security, Compliance and Privacy



Data Security, Compliance and Privacy

Securing AI with Microsoft Purview

The screenshot displays the Microsoft Purview dashboard, which integrates various security and compliance services. It includes:

- Policy compliance:** Shows an overall compliance score of 56% and highlights the "Least compliant subscriptions" as Microsoft Azure Internal Consumption at 56%.
- Resource health monitoring:** Provides a summary of issues across Compute & apps (9), Data & storage (12), Networking (1), and Identity & access (1).
- Security alerts over time:** A chart showing zero security alerts from 15 Sun to 29 Sun.
- Most prevalent recommendations:** Lists three items: "Endpoint Protection not installed" (1 VM), "Apply disk encryption" (1 VM), and "Designate more than one owner" (1 subscription).
- New - App Service threat detection (preview):** A note stating that Security Center now monitors App Service applications for malicious activities like vulnerability scanning, malicious login attempts, and management interfaces.

Securing AI with Microsoft Purview



Ignite highlights:

Microsoft Purview helps secure and govern data in AI

- Insights into generative AI usage and activity over time
- Securing data in generative AI prompts and responses (Copilot for M365, 100+ common consumer AI apps such as ChatGPT, Bard, Dall-E etc.)
- Compliance controls for M365 Copilot to easily meet business and regulatory requirements



Key announcements

Purview AI hub to provide visibility into AI activity, including total number of users using AI and the sensitive data flowing into AI prompts – for Copilot for M365 and commonly used third-part AI applications.

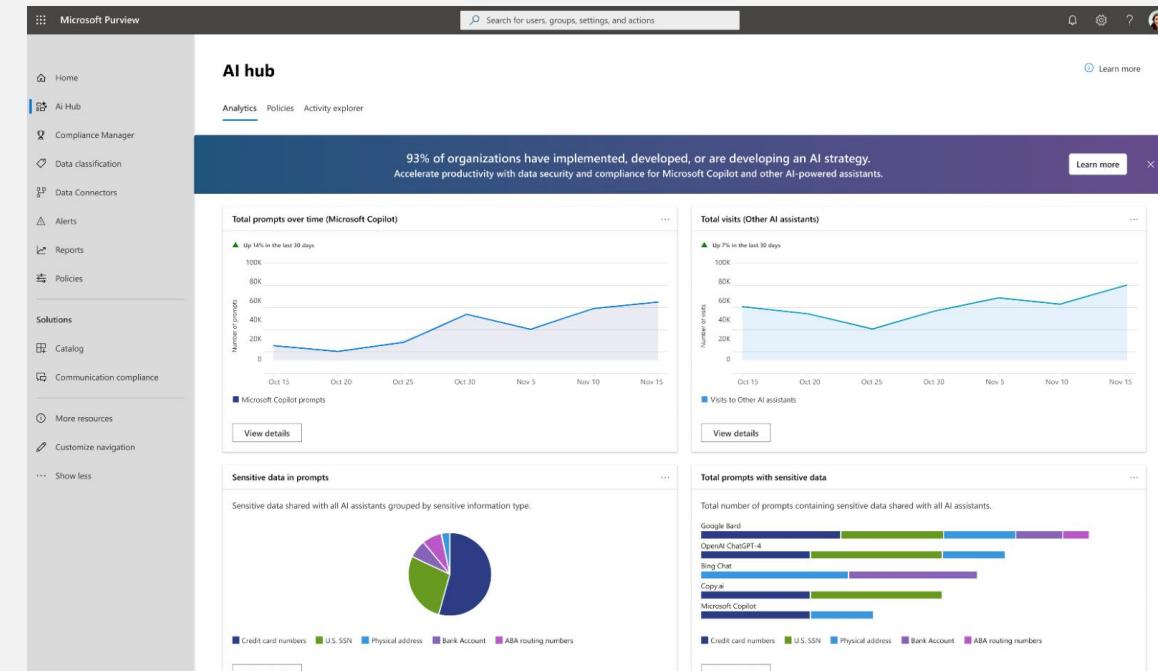
Policies to secure data in AI prompts and responses.

M365 Copilot understand and honors sensitivity labels and the permissions that come with it. Copilot generated content, both in chat and draft mode, inherit the most protective sensitivity labels from referenced files.

- Prevent users from pasting sensitive information and uploading sensitive documents to around 100 consumer AI applications such as Bard, ChatGPT and more on supported browsers.

Compliance controls for M365 Copilot including:

- Capture Copilot interactions with Audit (users, time, docs accessed etc.)
- Preserve, collect, and analyze Copilot interactions for investigations and litigations with eDiscovery
- Retention and deletion policies for Copilot interactions with Data Lifecycle Management
- Detecting business or regulatory violations in Copilot interactions with Communication Compliance



For more information: aka.ms/PurviewAI/Blog

Securing AI with Microsoft Purview

Ignite announcements



Tier 1 announcements



Tier 2 announcements

AI hub in Microsoft Purview (private preview)

Gain aggregated insights into generative AI activity in your organization, including Microsoft Copilot for M365 as 100 commonly uses consumer generative AI such as Bard, ChatGPT, and more

Secure data in M365 Copilot (GA)

- M365 Copilot understand and honors sensitivity labels and the permissions that come with it. Copilot will not summarize content from docs if users have only VIEW rights.
- M365 Copilot will inherit the sensitivity label from referenced files. If more than one file is referenced in Copilot chat or draft mode, Copilot will apply the most protective label to the conversation and to the generated output

Prevent data loss in consumer AI (public preview)

Prevent users from pasting sensitive information or uploading sensitive document to consumer AI such as ChatGPT, Bard, etc. Additionally, leverage Adaptive Protection to make your DLP policies dynamic and apply stricter restrictions for elevated risk users and allow low risk users to maintain productivity.

Detect regulatory or business violation in Copilot interactions (GA)

Extending the detection analysis in Communication Compliance to help identify risky communication within Copilot prompt and responses. This capability will allow an investigator, with relevant permissions, to examine and check Copilot interactions that have been flagged as potentially containing inappropriate or confidential data leaks

Audit Copilot interactions (GA)

Audit and understand when a user requests assistance from Copilot, and what assets are affected by the response using Microsoft Purview Audit.

Discover Copilot interactions for investigations (GA)

Identify, preserve, and collect relevant data for litigation, investigations, audits, or inquiries with Microsoft Purview eDiscovery.

Managing retention and deletion policies for Copilot interactions (GA)

Copilot for Microsoft 365 interactions are now included in the Microsoft Teams chats location. Any previously configured retention policies for Teams chats now automatically include user prompts and responses to and from Copilot for Microsoft 365

Security Copilot in Purview



Policy compliance

Overall compliance: 56% | Least compliant subscriptions: Microsoft Azure Internal Consumption 56%

Show policy compliance of your environment >

Resource health monitoring

- 9 Compute & apps
- 12 Data & storage
- 1 Networking
- 1 Identity & access

Security alerts over time

No security alerts

HIGH SEVERITY 0

LOW SEVERITY 0

New - App Service threat detection (preview)

Cloud icon: Security Center now monitors your App Service applications for malicious activities such as vulnerability scanning, malicious login attempts, management interfaces and more.

Learn more >

Purview + Security Copilot



Ignite highlights:

- Data risk and user risk surfaced in Security Copilot standalone experience
- Gain comprehensive summary of DLP alerts
- Gain comprehensive summary of insider risk alerts
- Gain contextual summary of communication risks
- Gain contextual summary of evidence collected in review sets
- Generate keyword query language from natural language prompt



Key announcements

Enhance the SOC team's ability to understand an incident end to end with **consolidated insights across Defender, Sentinel, Purview, Entra, and Intune in Security Copilot** (private preview)

Expedite complex data security, compliance, and legal investigations with **AI-powered summarization capabilities and natural language queries** (private preview)

The screenshot displays the Microsoft Security Copilot interface. On the left, there's a sidebar with navigation links like Home, Overview, Reports, Alerts, Policies, Explorers, Classifiers, and Scans. The main area shows two cards: one for 'Show me any risky activities from this user in the past 30 days' and another for 'Can you share all the files this user worked on or accessed in last 7 days?'. Below these cards, there's a 'Data Loss Prevention' section with a table showing file names, file locations, and actions taken. To the right, there's a 'Alerts' section with a list of policy matches for documents in SharePoint, and a detailed view of a specific alert for a document named 'Q2-Customer Data.xlsx'.

For more information: aka.ms/SecurityCopilot/Purviewblog

Purview + Copilot

Additional Announcements



Tier 1 announcements

Microsoft Purview capabilities in Security Copilot (private preview)

- With Microsoft Purview capabilities in Security Copilot, you gain data and user risk insights, helping to identify the source of an attack and sensitive data that may be at risk.

Gain comprehensive summary of DLP alerts (private preview)

- Gain comprehensive summary of DLP alert, including the attributed policy rules, data at risk and user risk insights from Insider Risk Management.

Gain comprehensive summary of insider risk alerts (private preview)

- Gain comprehensive summary of Insider Risk Management alerts to gain context into user intent and pinpoint specific dates for risky activities.



Tier 2 announcements

Gain contextual summary of Communication Compliance risks (private preview)

- Gain contextual summary of communication violations containing lengthy content like meeting transcripts or group chats. This content is evaluated against compliance regulations or corporate policies.

Gain contextual summary of evidence collected in eDiscovery review sets (private preview)

- Gain quick summary of documents included in an eDiscovery review set to help you save time and conduct investigations more efficiently.

Natural language to keyword query language in eDiscovery (private preview)

- Enable analysts to provide a search prompt in natural language which is then translated into keyword query language to help speed up investigation and drive more accurate results.

Expanding Data Protection (Multi Cloud)



Ignite highlights:

- Unified data map enables integration and classification across the data estate
- Unified portal for securing and governing your data
- Gain visibility across your data estate
- Extend protections across structured and unstructured data
- Detect risks across clouds and 3rd party apps



Key announcements

Secure, govern, and manage compliance of data end-to-end with integrated solutions built on a **unified data map, classification service, and portal** (public preview)

Gain visibility and protect your diverse data estate, **structured or unstructured, across Azure and AWS** with industry-leading classification and labeling capabilities (gated preview)

Extend data protections across structured and unstructured data types including **Azure SQL, ADLS, and Amazon S3** buckets (gated preview)

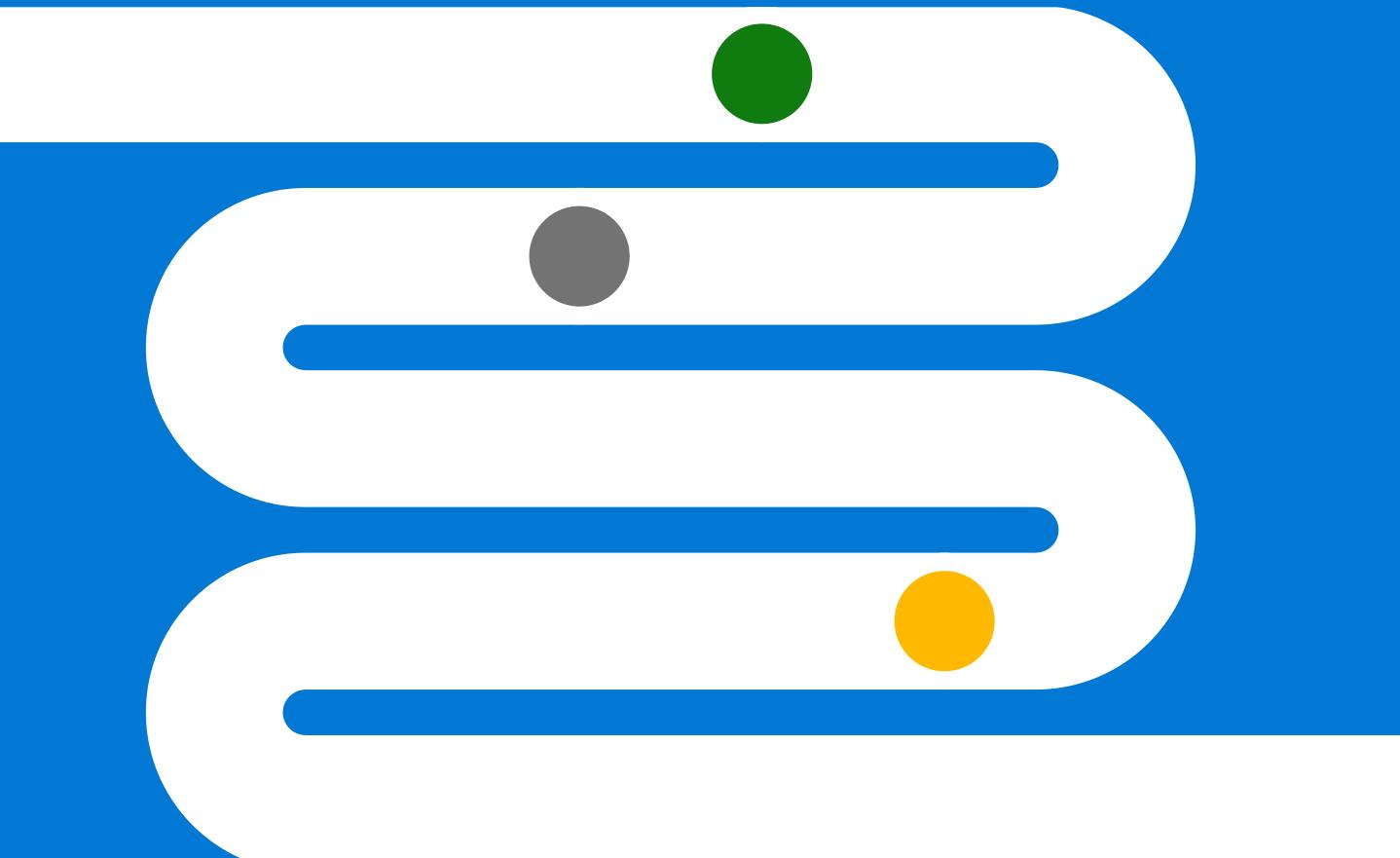
Detect critical insider risks in clouds **AWS, Azure**, and SaaS applications, including **Box, Dropbox, Google Drive, and GitHub** with ready-to-use indicators (gated preview)

The screenshot displays the Microsoft Purview portal interface. At the top, there's a navigation bar with a search bar and a link to 'New Microsoft Purview portal'. Below the header, a main banner reads 'Protect assets across your multicloud data estate with Microsoft Purview' with a sub-instruction 'Register and scan your data sources, and protect your sensitive information wherever the data lives.' To the right of the banner, three service cards are shown: 'Microsoft 365' (Protection detected), 'Microsoft Fabric' (Registered), and 'Microsoft Azure' (Registered). Below the banner, there's a section titled 'Pick up where you left off' with links to 'Discover your data' (Search Data Catalog, Recent searches: customer, address, 2023 sales), 'Recently accessed' (Product.docx, CustomerTable, Customertax, AnalyticsDashboard), and 'Know your data' (Top platforms with data: Microsoft 365, Azure, Fabric, AWS; Top 3 sensitive info types by platform: Full names, Email address, Patient ID). A legend at the bottom right identifies the colors for different platforms: Microsoft 365 (blue), Azure (light blue), Fabric (green), and AWS (orange).



For more information: aka.ms/PurviewExpandingHorizons

Identity



Entra + Security Copilot



Ignite highlights:

- Entra skills now available in Security Copilot Early Access Program
- Assisted risk investigation embedded experience in Entra - private preview
- Assisted sign-in troubleshooting embedded experience in Entra - private preview
- Assisted workflow creation embedded experience in Entra - private preview



Key announcements

- **Enable SOC teams** to discover high risk users, overprivileged access, and suspicious sign-ins that aid in a security incident investigation.
- **Enable IT Admins** to troubleshoot daily identity tasks such as why a sign-in required multi-factor authentication (MFA).
- Ask about users, groups, sign-ins, and permissions then instantly get a risk summary and recommended guidance for each identity at risk.
- Create a Lifecycle Workflow to streamline the process of creating and issuing user credentials and access rights.

The screenshot displays two side-by-side interfaces. The left interface is 'Microsoft Security Copilot (Preview)' and the right is 'Security Copilot (Preview)'. Both show a user profile for 'Adriana Giorgi' with a timestamp of 'March 16, 3:55 PM'. The Microsoft interface shows a 'Tell me about security incident 33778' section with a summary: 'Based on the provided data, the user Vik Verma (vikverm@woodgrove.ms) was previously considered risky. However, their risk level is currently set to "None" as the risk has been remediated. The remediation action taken was a secured password reset performed by the user. The risk state is now "Remediated". The risk detail states "User performed a secured password reset." The risk information was last updated on 2022-10-10T06:20:15.315357Z.' It includes buttons for 'Confirm', 'Off-target', and 'Report'. The right interface shows a 'Why was Adriana Giorgi prompted for MFA?' section with a detailed list of findings: 'Adriana Giorgi was prompted for Multifactor Authentication (MFA) due to enforcement of certain Conditional Access policies during their sign-in attempt. Here are the details: • The sign-in attempt was made on November 14, 2023 at 7:56:30 UTC. • The application used was "M365 Admin Center". • The IP address for the sign-in was 167.220.101.17. • The sign-in was interactive and was done using the Edge browser. • The device used was not compliant and not managed. • The location of the sign-in attempt was Redmond, Washington, USA.' Below this, it lists applied Conditional Access policies: 'The following Conditional Access policies were applied 1. CA01 - TOU - All Contoso (and Guest) Users - This policy was successfully enforced. The conditions satisfied were the application and the users. 2. CA20 - Admin reminders - This policy was successfully enforced. The conditions satisfied were the application and the users. 3. CA01 - MFA - All Apps - All Users - Do not change - Policy is monitored - This policy was successfully enforced. The conditions satisfied were the application and the users.' A note at the bottom states: 'There were other policies that were not applied or not enabled during this sign-in attempt. If you need more details about these policies or any other information, feel free to ask.' The bottom of the right interface shows a prompt: 'What is the MFA requirement policy? Are other users impacted?' and a button 'I want to ...'.

For more information: <https://aka.ms/Entra/Ignite23>

Security Service Edge (SSE)



Ignite highlights:

- Microsoft Entra Internet Access for all internet, SaaS, and Microsoft 365 applications and resources – public preview
- Microsoft Entra Private Access additional capabilities – public preview



Key announcements

Internet Access capabilities:

- **Universal Conditional Access** - extend adaptive access controls universally to rely on Conditional Access to any network destination like an external website, or non-federated SaaS applications without a need to change these applications.
- **Token Theft protection** - for Entra ID apps through compliant network check in Conditional Access to protect Microsoft Entra-integrated cloud applications against token theft.
- **Context aware SWG** - restrict end user access to unsafe and non-compliant content with web content filtering (URL, FQDN, web category) and make internet filtering policies more succinct, readable, and comprehensive, by leveraging the rich user, device, and location awareness of Conditional Access.

For more information: <https://aka.ms/Entra/Ignite23>

Secure access in the AI era: What's new in Microsoft Entra <https://bit.ly/49hOR5s>

Microsoft | Microsoft Ignite Sessions | Featured Partners | Blog | News and announcements | Support | All Microsoft | Hi Jeff Beckitt | My event

Secure access in the AI era: What's new in Microsoft Entra

Thursday, November 16 | 5:30 AM - 6:15 AM Australian Western Standard Time Duration 45 minutes

Back to sessions

Breakout In Seattle + Online

Speakers: Joy Chik | Microsoft Jade DSouza | Microsoft John Savill | Microsoft

Remove from schedule Remove from backpack

This will conflict with another session in your schedule

Recommended next step: Microsoft Learn Collection

Resources

Download Video Download Slides Download Transcript

Ask me anything about Microsoft Ignite... Microsoft Preview Azure AD Is

Security Service Edge (SSE)



Ignite highlights:

- Microsoft Entra Internet Access for all internet, SaaS, and Microsoft 365 applications and resources – public preview
- Microsoft Entra Private Access additional capabilities – public preview



Key announcements

Private Access capabilities:

- **VPN replacement** – adding User Datagram Protocol (UDP) and private Domain Name System (DNS) will enable a seamless transition from traditional Virtual Private Network (VPN) deployments to a fully ready, identity-centric Zero Trust Network Access (ZTNA) solution.
- **MFA to all on-prem apps** – provide modern authentication methods, such as Multi-Factor Authentication (MFA), to secure access to all private applications and resources. This applies to any application, located anywhere, for both remote and on-premises users.

For more information: <https://aka.ms/Entra/Ignite23>

Unified Conditional Access controls: Identity & Security Service Edge <https://bit.ly/47jqL8E>

Microsoft | Microsoft Ignite Sessions | Featured Partners | Blog | News and announcements | Support | All Microsoft | Hi Jeff Beckett | My event

< Back to sessions

Unified Conditional Access controls: Identity & Security Service Edge

Thursday, November 16 | 6:45 AM - 7:30 AM Australian Western Standard Time Duration 45 minutes

Discussion In Seattle + Online

Speakers: Abdi Saeedabadi | Microsoft Ashish Jain | Microsoft Yair Tor | Microsoft Nitika Gupta | Microsoft

Remove from schedule Remove from backpack

This will conflict with another session in your schedule

Discussion | Unified Conditional Access controls: Identity & Security Service Edge

Abdi Saeedabadi
Senior Product Marketing Manager
Security Service Edge (SSE)
<https://www.linkedin.com/in/asaeed/>

Recommended next step

Microsoft Learn Collection

Resources

Ask me anything about Microsoft Ignite... ▶

For more information - call to action

1

- ✓ Watch Entra Ignite Sessions:
 - **BRK297H** - Secure access in the AI era: What's new in Microsoft Entra
 - **BRK264H** - Accelerate your Zero Trust journey with unified access controls
 - **DIS663H** - Unified Conditional Access controls: Identity & Security Service Edge
- **PRT084** - Share your feedback on Microsoft's Security Service Edge solution
- **OD02** - Bringing Passkey into your Passwordless Journey

2

- ✓ Ignite Entra announcement blog
 - <https://aka.ms/Entra/Ignite23>

Entra ID (formerly Azure AD)



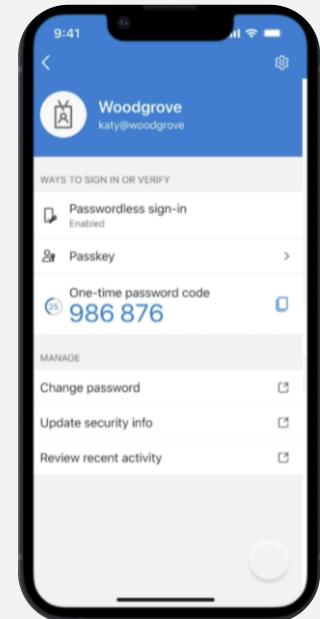
Ignite highlights:

- Microsoft-managed Conditional Access policies - public preview
- Certificate Based Authentication (CBA) - public preview
- Passkeys managed by the Microsoft Authenticator app - public preview



Key announcements

- **Microsoft-managed Conditional Access policies** - Microsoft will automatically enroll customers into Conditional Access policies based on their risk signals, current usage, and licensing. The policies will enhance their security posture and reduce the complexity of managing conditional access.
- **Microsoft Entra Certificate based Authentication (CBA)** - several new features that enable customers to customize authentication policies based on certificates, resource type, and user group. Customers now have more control and flexibility to choose certificate strength for different users, combine CBA with other methods for multi-factor or step-up authentication.
- **Microsoft Authenticator**: Microsoft Entra ID users will be able to sign in with passkeys that are managed by the Microsoft Authenticator app. By using passkeys, customers will have a free, phishing-resistant credential based on open standards and ensuring access to the latest security enhancements that will be added to the FIDO standard in the coming years.



For more information: <https://aka.ms/Entra/Ignite23>

Permissions Management



Ignite Highlights

- Permissions Management integration with Microsoft Defender for Cloud (MDC) – public preview
- Permissions Management integration with ServiceNow – GA



Tier 2 announcements

Integration with Microsoft Defender for Cloud

- Provides an efficient way to consolidate insights into other cloud security posture information on a single interface.
- Customers receive actionable recommendations for addressing permissions risks in the MDC dashboard
- Gain a centralized view of the Permissions Creep Index, facilitating the enforcement of least privilege access for cloud resources across Azure, Amazon Web Services, and Google Cloud Platform.



Tier 2 announcements

Integration with ServiceNow

- Customers can request time-bound, on-demand permissions for multicloud environments (Azure, AWS, GCP) via the ServiceNow portal.
- Helps organizations enhance their Zero Trust posture by enforcing the principle of least privilege for multi-cloud permissions and streamlines access permission requests within existing ServiceNow approval workflows.

For more information - call to action

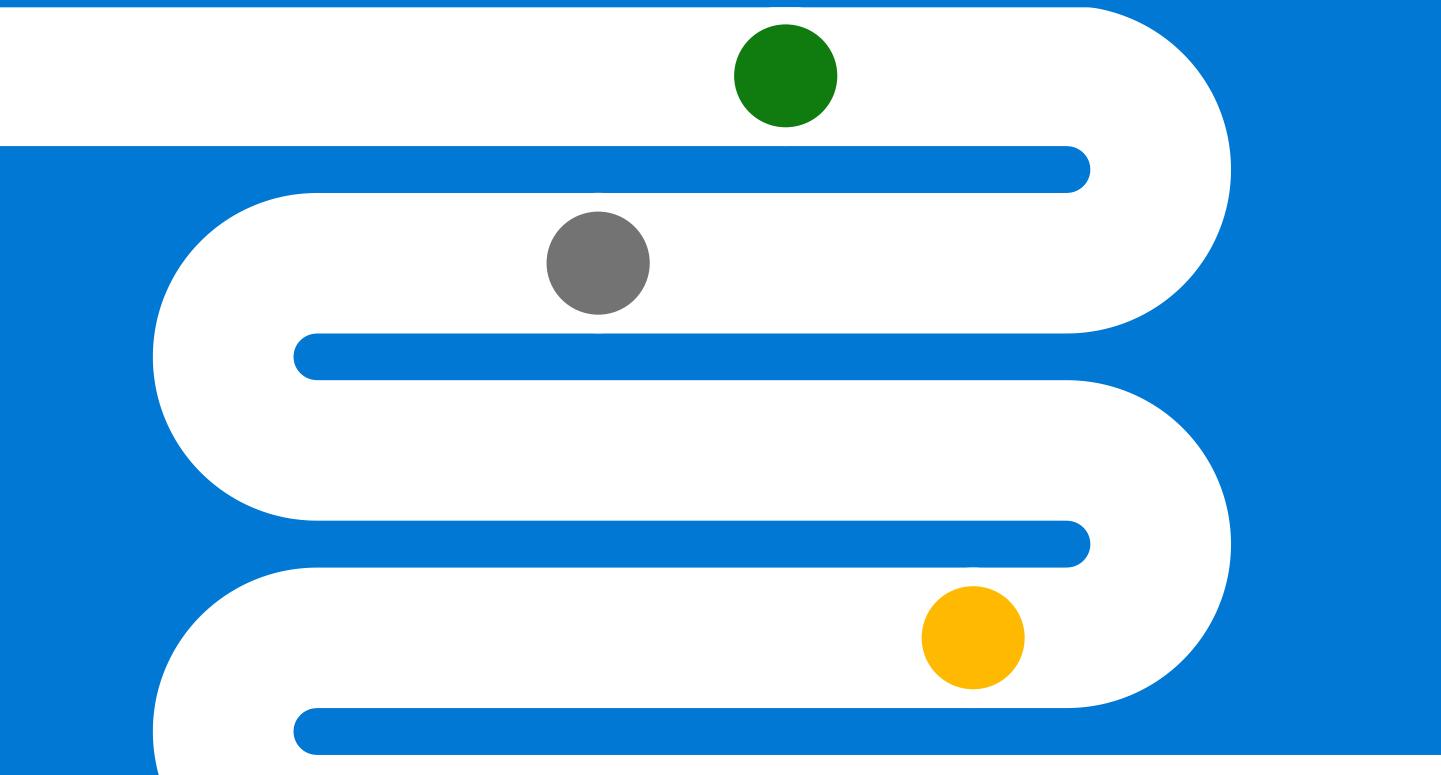
1

- ✓ **Watch Entra Ignite Sessions:**
 - **BRK297H** - Secure access in the AI era: What's new in Microsoft Entra
 - **BRK264H** - Accelerate your Zero Trust journey with unified access controls
 - **DIS663H** - Unified Conditional Access controls: Identity & Security Service Edge
- **PRT084** - Share your feedback on Microsoft's Security Service Edge solution
- **OD02** - Bringing Passkey into your Passwordless Journey

2

- ✓ **Learn more about Permissions Management**
 - <http://aka.ms/PermissionsManagementDefenderforCloud>
 - <http://aka.ms/ServiceNowPoD>

Management



Intune Announcements



Ignite highlights:

- Security Copilot integration with Microsoft Intune
- New solutions as part of Intune Suite
- Intune and Windows: More secure together



Key announcements

Security Copilot embedded experience in Intune

- Map settings and configurations with intelligent policy creation and AI assisted what-if analysis.
- Swiftly respond to threats with full device context and automated compliance checks.
- Summarize root cause, impact and remediate with ease
- Translate business requirements into recommended and compliant configurations using natural language
- Private preview for select customer in the EAP

For more information: <https://aka.ms/Intune/Ignite2023>

Fortified security and simplicity come together with Microsoft Intune

The screenshot shows a Microsoft Ignite session page. At the top, there's a navigation bar with links for Microsoft, Microsoft Ignite, Sessions, Featured Partners, Blog, News and announcements, and Support. On the right, it shows 'All Microsoft' and 'Hi Jeff Beckitt'. Below the navigation, a large title reads 'Fortified security and simplicity come together with Microsoft Intune'. Underneath the title, it says 'Friday, November 17 | 9:15 AM - 10:00 AM Australian Western Standard Time Duration 45 minutes'. It indicates the session is a 'Breakout' and 'In Seattle + Online'. The speakers listed are Dilip Radhakrishnan, Jason Roszak, Archana Devi Sunder Rajan, and Sangeetha Visweswaran, all from Microsoft. To the right, there's a video player showing two speakers, a woman and a man, sitting at a table. On the far right, there are buttons for 'Remove from schedule' and 'Remove from backpack', a note about conflicts, and a sidebar with 'Recommended next step' (Microsoft Learn Collection) and 'Resources'.

Intune Announcements

Ignite highlights:

- Security Copilot integration with Microsoft Intune
- New solutions as part of Intune Suite
- Intune and Windows: More secure together



Key announcements

New Intune Suite Solutions - February 2024 GA

- Microsoft Intune Enterprise Application Management
- Microsoft Intune Advanced Analytics
- Microsoft Cloud PKI

For more information: <https://aka.ms/Intune/Ignite2023News>

The screenshot shows a Microsoft Ignite session page. At the top, there's a navigation bar with links for Microsoft, Microsoft Ignite, Sessions, Featured Partners, Blog, News and announcements, and Support. A user profile for 'Jeff Beckitt' is shown on the right. Below the navigation, the session title is 'Modern management innovation shaping endpoint security'. It includes details like the date (Thursday, November 16), time (6:45 AM - 7:30 AM Australian Western Standard Time), duration (45 minutes), and location (Breakout, In Seattle + Online). The speakers listed are Ramya Chitrakar, Steve Dispensa, and Jeff Pinkston. On the right side of the page, there are buttons for 'Remove from schedule' and 'Remove from backpack', and a note about conflicts. A sidebar on the right suggests a 'Recommended next step' to 'Microsoft Learn Collection' and lists 'Resources'. At the bottom, there's a feedback bar asking 'Ask me anything about Microsoft Ignite...'.

Intune Announcements (All)

Additional Announcements



Key announcements

Intune and Windows: More secure together

- Local Admin Password Service (LAPS) now Cloud-enabled
- MAM for BYO-Windows devices in GA
- Microsoft Tunnel capacity expands to 20K Devices
- Config refresh overwrites policy changes to stay secure
- New Windows security baseline to apply
- Windows hardware-backed attestation report enhanced
- Export / Import Settings Catalog policies
- Windows Subsystem for Linux now Intune-configurable

For more information: <https://aka.ms/IntuneWN2310>

The screenshot shows a Microsoft Ignite session page. The title is "Modern management innovation shaping endpoint security". It was held on Thursday, November 16, from 6:45 AM to 7:30 AM Australian Western Standard Time, lasting 45 minutes. The session is marked as a "Breakout" and "In Seattle + Online". Three speakers are listed: Ramya Chitrakar, Steve Dispensa, and Jeff Pinkston, all from Microsoft. A video player shows two speakers on stage. To the right, there are buttons for "Remove from schedule" and "Remove from backpack", a note about conflicts, a "Recommended next step" section for "Microsoft Learn Collection", and a "Resources" section. At the bottom, there's a "Ask me anything about Microsoft Ignite..." button.

For more information – call to action

1

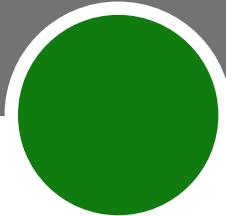
✓ **Watch Intune Ignite Sessions:**

- BRK295H - Modern management innovation shaping endpoint security
- BRK263H - Fortified security and simplicity come together with Microsoft Intune
- BRK252H - Future of Windows that is AI-enabled and Cloud-powered

2

✓ **Join us Nov. 27-30 for the [Windows and Intune Technical Takeoff](#) – digital, live event.**

Session List



👉 Security sessions - Level 300:

- The power of Microsoft's XDR: they attempted, we disrupted <https://bit.ly/3FNVsXR>
- Boost multicloud security with a comprehensive code to cloud strategy <https://bit.ly/3MwKTME>
- Accelerate your Zero Trust journey with unified access controls <https://bit.ly/474Fo02>
- Beyond traditional DLP: Comprehensive and AI-powered data security <https://bit.ly/47oZPEH>
- Microsoft Sentinel: A modern approach to security operations <https://bit.ly/40qlzN0>
- Fortified security and simplicity come together with Microsoft Intune <https://bit.ly/3QKv3Aq>
- Making end to end security real <https://bit.ly/3FPoV3S>

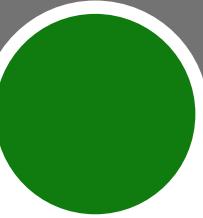
Session List



👉 Security sessions - Level 200:

- The Future of Security with AI <https://bit.ly/49qOyp1>
- How we secure the Microsoft estate <https://bit.ly/46YmZlx>
- Learn Live: Threat detection with Microsoft Sentinel analytics <https://bit.ly/40urr9d>
- Technical Foundations of Secure AI Q&A <https://bit.ly/3QvMhAo>
- Secure access in the AI era: What's new in Microsoft Entra <https://bit.ly/49hOR5s>
- MDTI: Now Anyone Can Tap Into Game-Changing Threat Intelligence <https://bit.ly/49Dz55l>
- Modern management innovation shaping endpoint security <https://bit.ly/3SqThkD>
- Unified Conditional Access controls: Identity & Security Service Edge <https://bit.ly/47jqL8E>
- Unifying XDR + SIEM: A new era in SecOps <https://bit.ly/3u6d7aL>
- Microsoft Sentinel Unleashed: Ask us anything about your favorite SIEM <https://bit.ly/49t0O8K>
- Preventing loss of sensitive data: Microsoft Purview DLP Q&A <https://bit.ly/3SvHilD>
- Secure and govern your data in the era of AI <https://bit.ly/3u1TNLI>

Session List



👉 Security sessions - Level 200:

- Discussing Microsoft Defender for Endpoint with product experts <https://bit.ly/3FUCiPX>
- Boosting ID Protection Amid Sophisticated Attacks <https://bit.ly/49jL2gl>
- Security for AI: Prepare, protect, and defend in the AI era <https://bit.ly/3MxgjSY>
- The AI effect: how are organizations securing the use of Generative AI <https://bit.ly/46YIIA8>
- Accelerate risk assessment and incident investigation with AI <https://bit.ly/40swMO8>
- Bringing Passkey into your Passwordless Journey <https://bit.ly/47334Sc>
- Effortless Application Migration Using Microsoft Entra ID <https://bit.ly/474cDjW>
- How Microsoft Purview helps you protect your data <https://bit.ly/49rxUpu>
- Jumpstart your SOC with Microsoft Defender Experts for XDR <https://bit.ly/47lqaDp>
- Making Zero Trust real: End to end security architecture and guidance <https://bit.ly/40pszuB>
- Protect your entire data estate across multiple clouds <https://bit.ly/3swQyvf>



Thank you

Microsoft Ignite