Microsoft

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.

Microsoft

South West Aboriginal Land & Sea Council

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 >

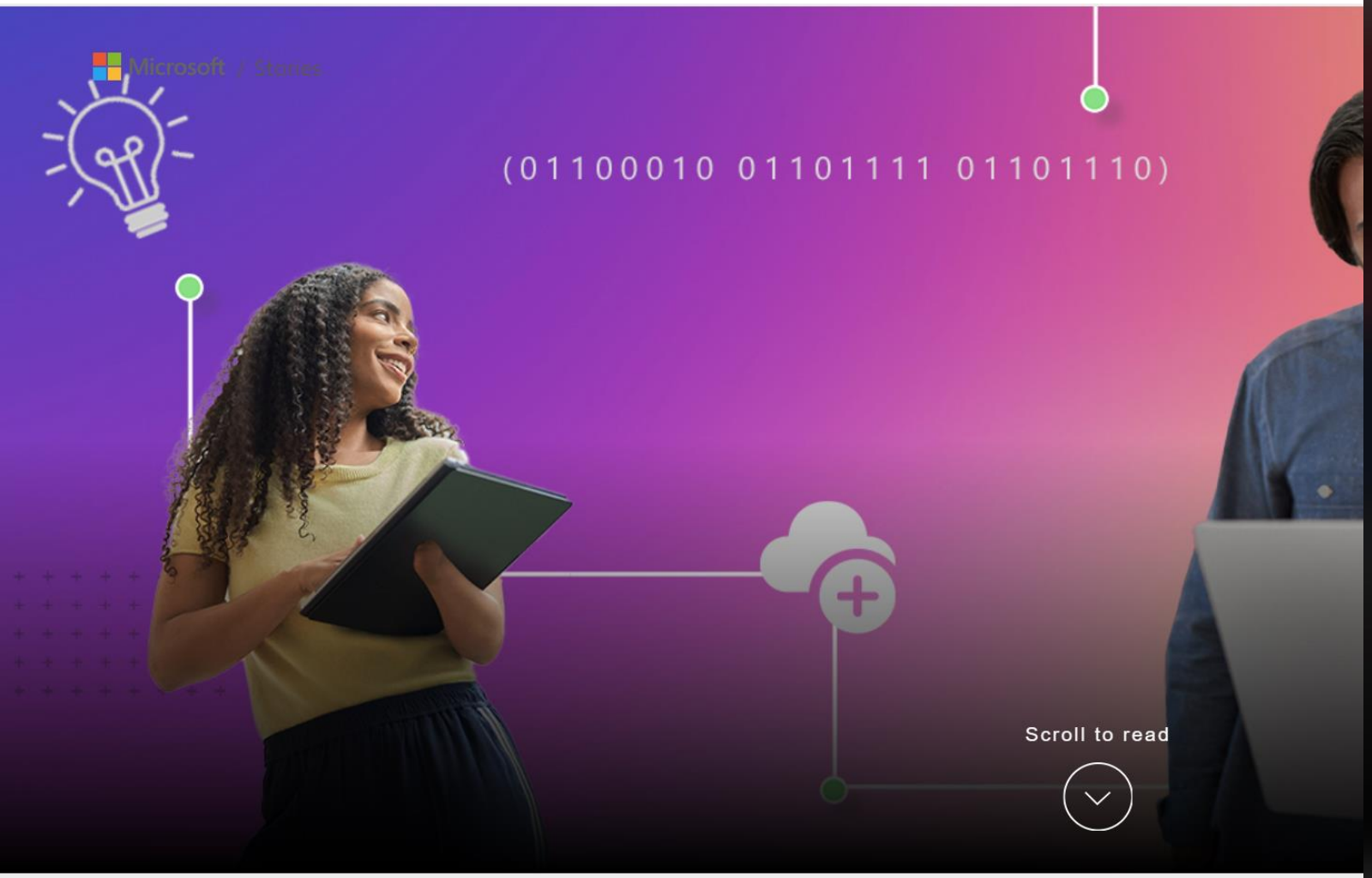
Security practitioner

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...

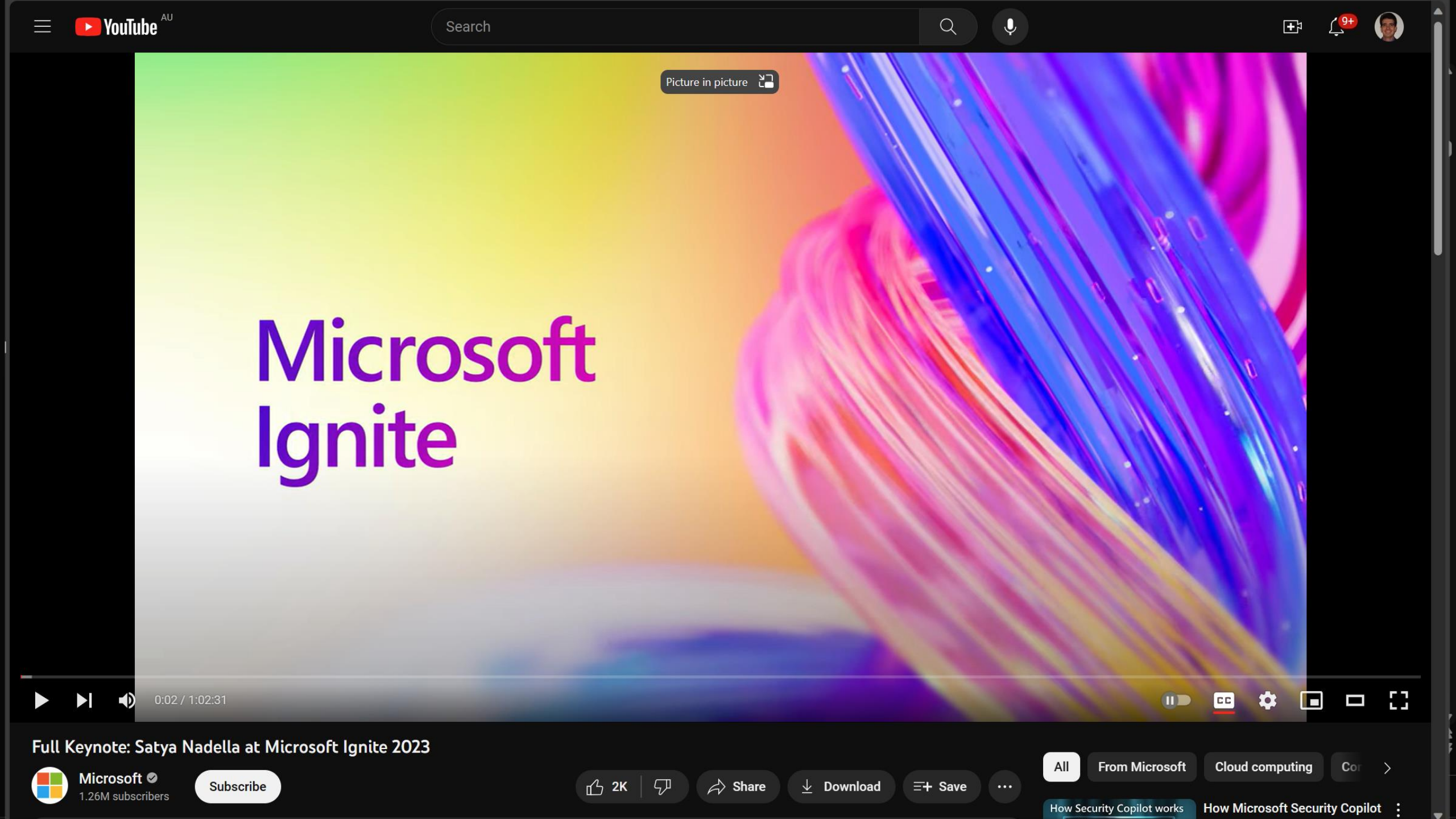


MICROSOFT IGNITE

BOOK OF NEWS

November 15 - 17, 2023

Table of Contents



Full Keynote: Satya Nadella at Microsoft Ignite 2023

Microsoft
1.26M subscribers

Subscribe

2K

Share

Download

Save

All

From Microsoft

Cloud computing

How Security Copilot works

How Microsoft Security Copilot

Microsoft Ignite 2023

Official Microsoft Blog >
AI transformation and the technology driving change

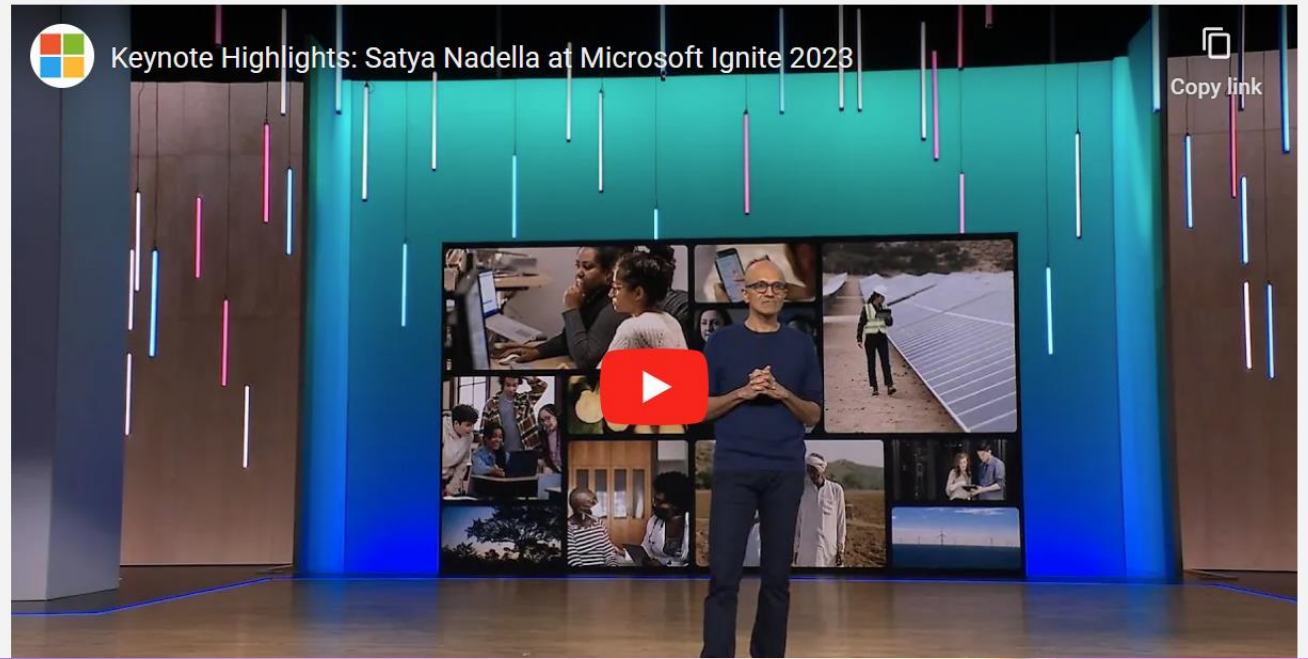
Book of News >
A complete guide to all the news announced at this year's event

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

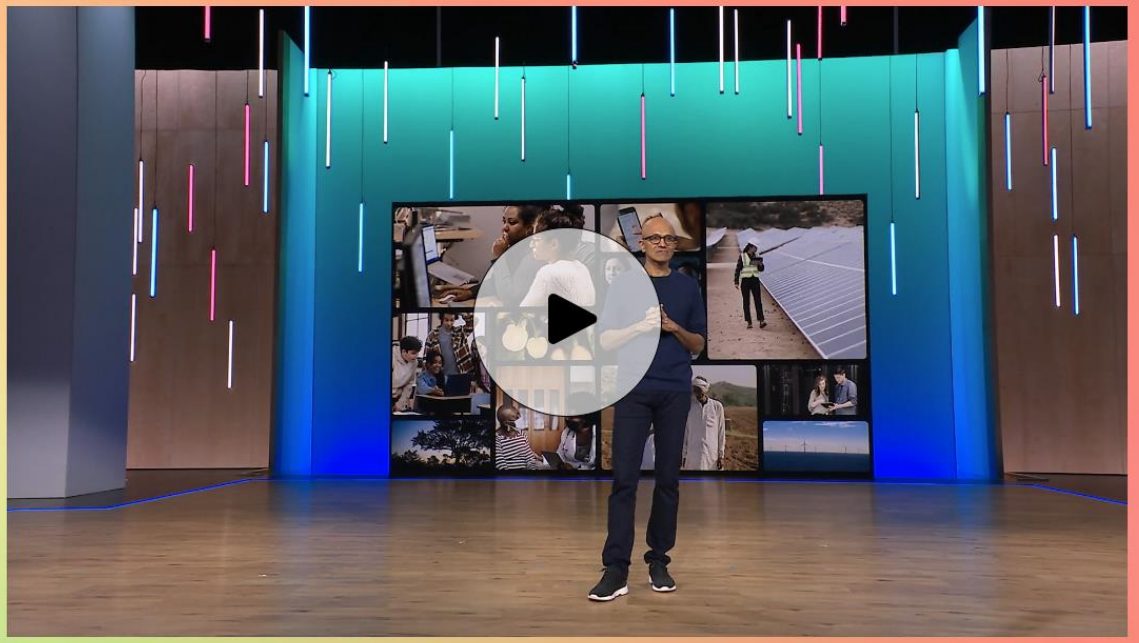
The opening keynote in 2 minutes



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.

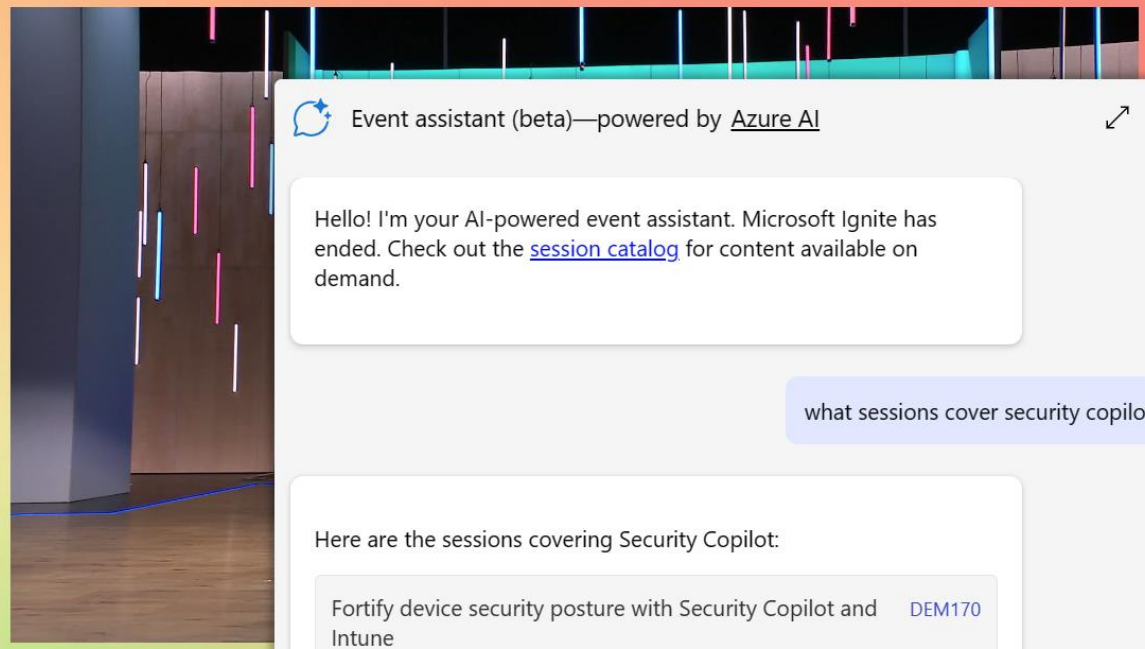
Stream on-demand sessions now >

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



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 Duffey
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...

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 >




Back to Schedule

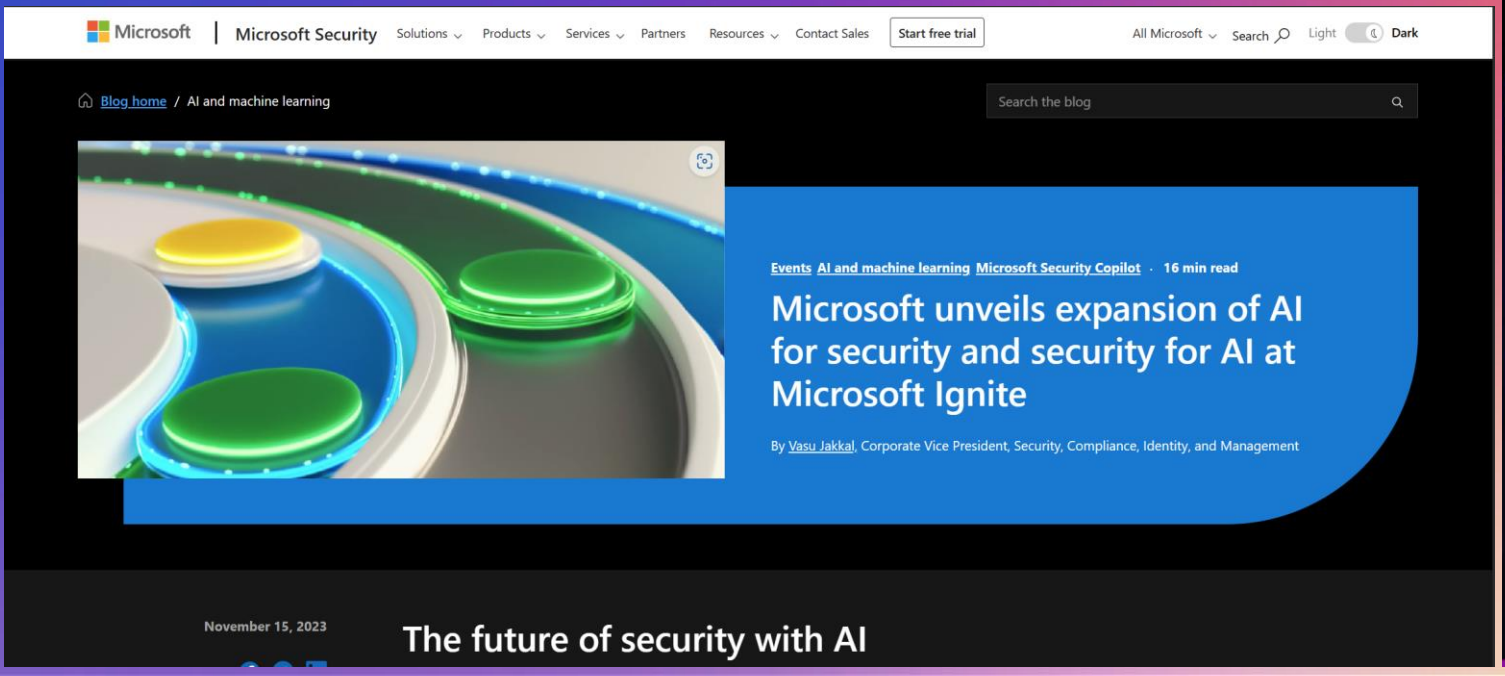
The Future of Security with AI

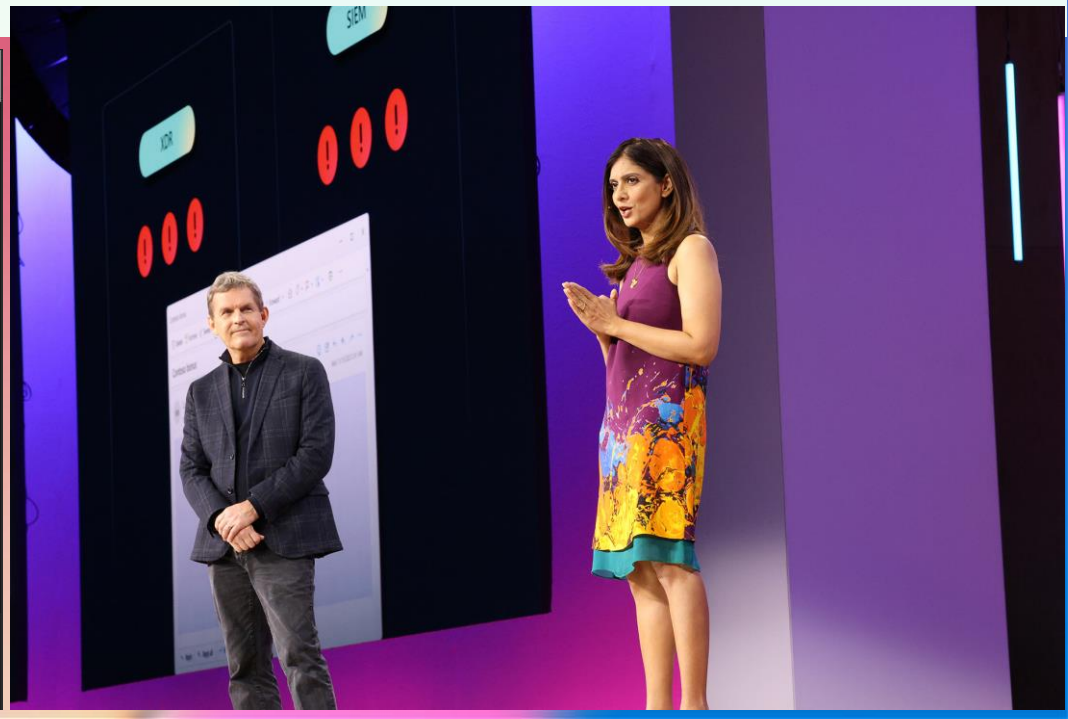
Friday, November 17 | 2:15 AM - 3:00 AM Australian Western Standard Time Duration 45 minutes

On Demand | Keynote | In Seattle + Online | Will Be Recorded

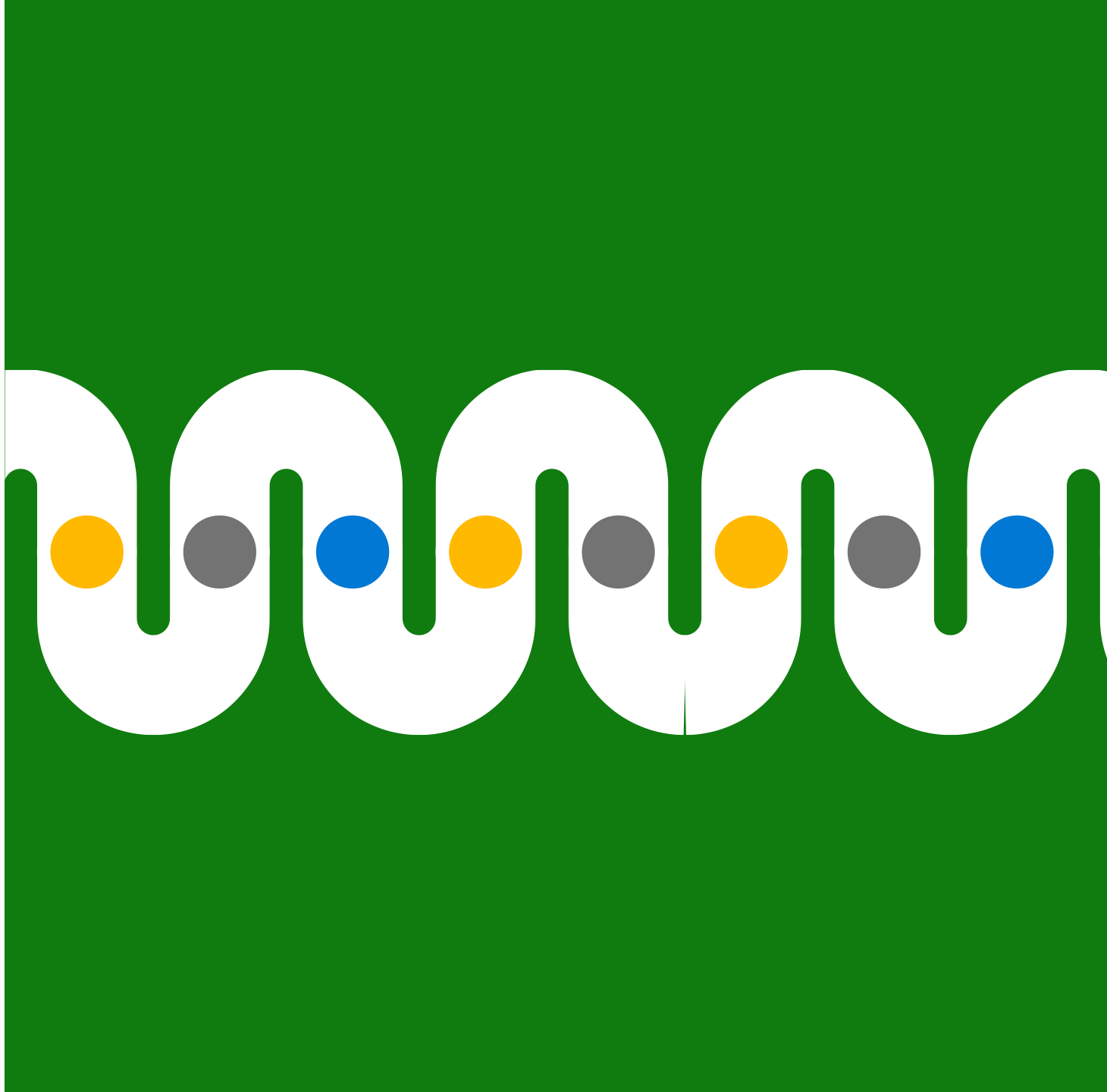
Speakers: Charlie Bell | Microsoft; Vasu Jakkal | Microsoft; Sherrod DeGrippo | Microsoft; Scott Woodgate | Microsoft

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.





Security



XDR + SIEM + AI

Key announcements

Unified Security Operations Platform

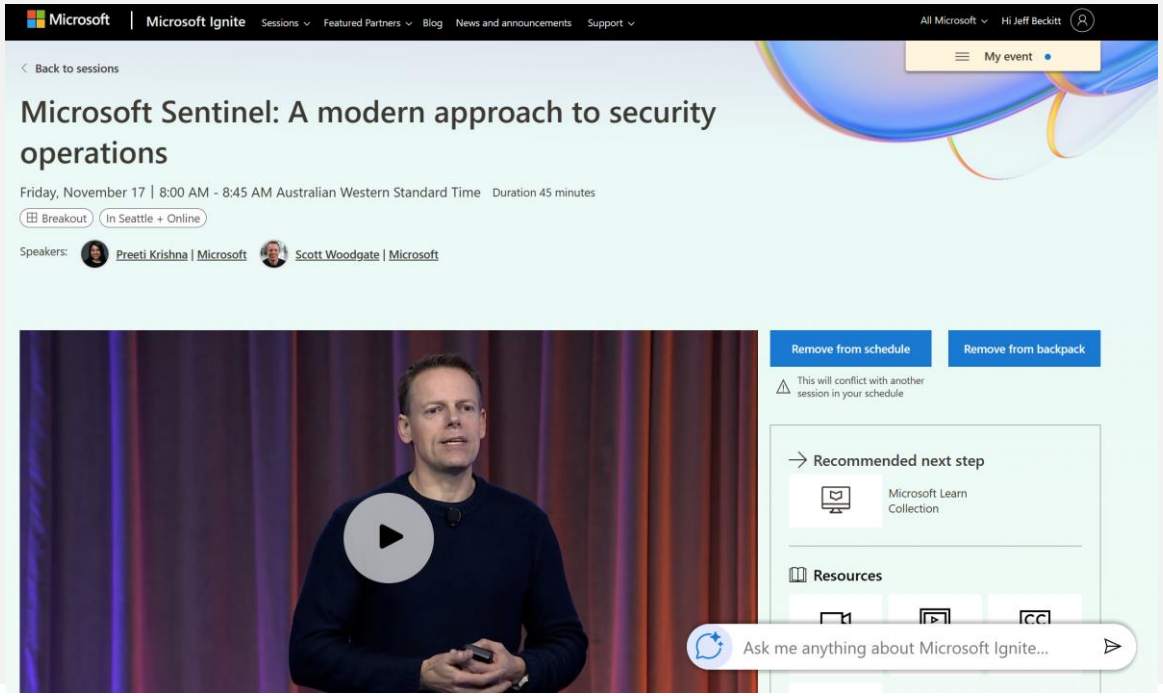
The power of Microsoft Sentinel, Defender XDR and Security Copilot are now available in a unified experience

- 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/40qIzN0



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

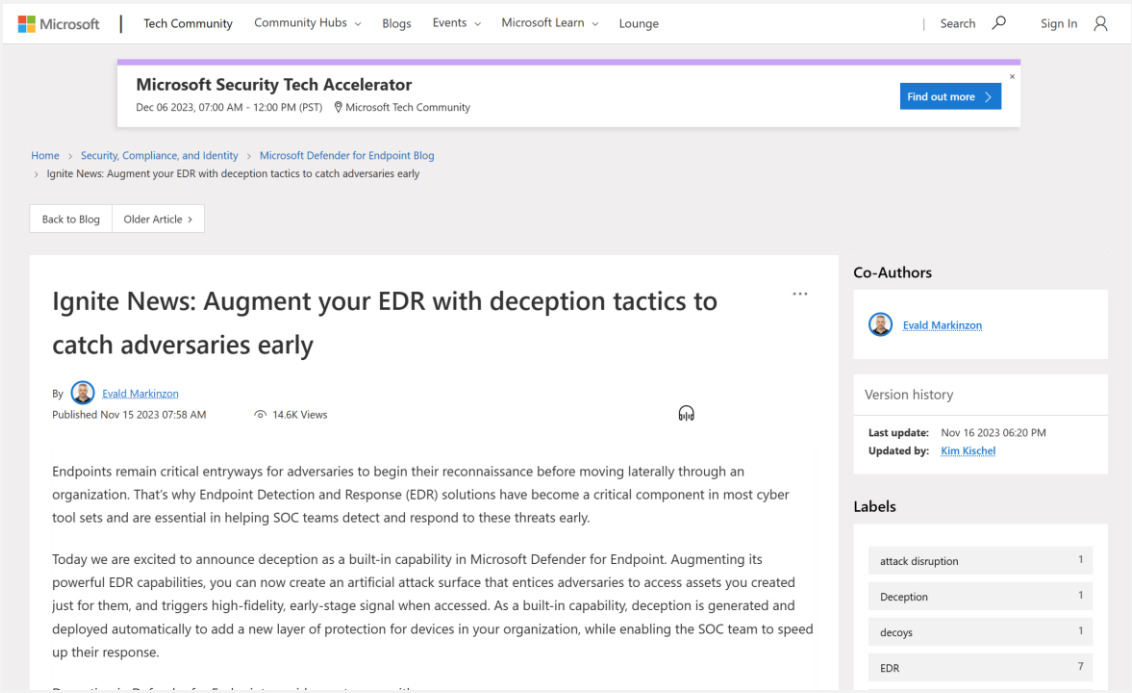
New deception techniques in Defender for Endpoint

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

https://aka.ms/MDEIgnite2023



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 eIoT 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

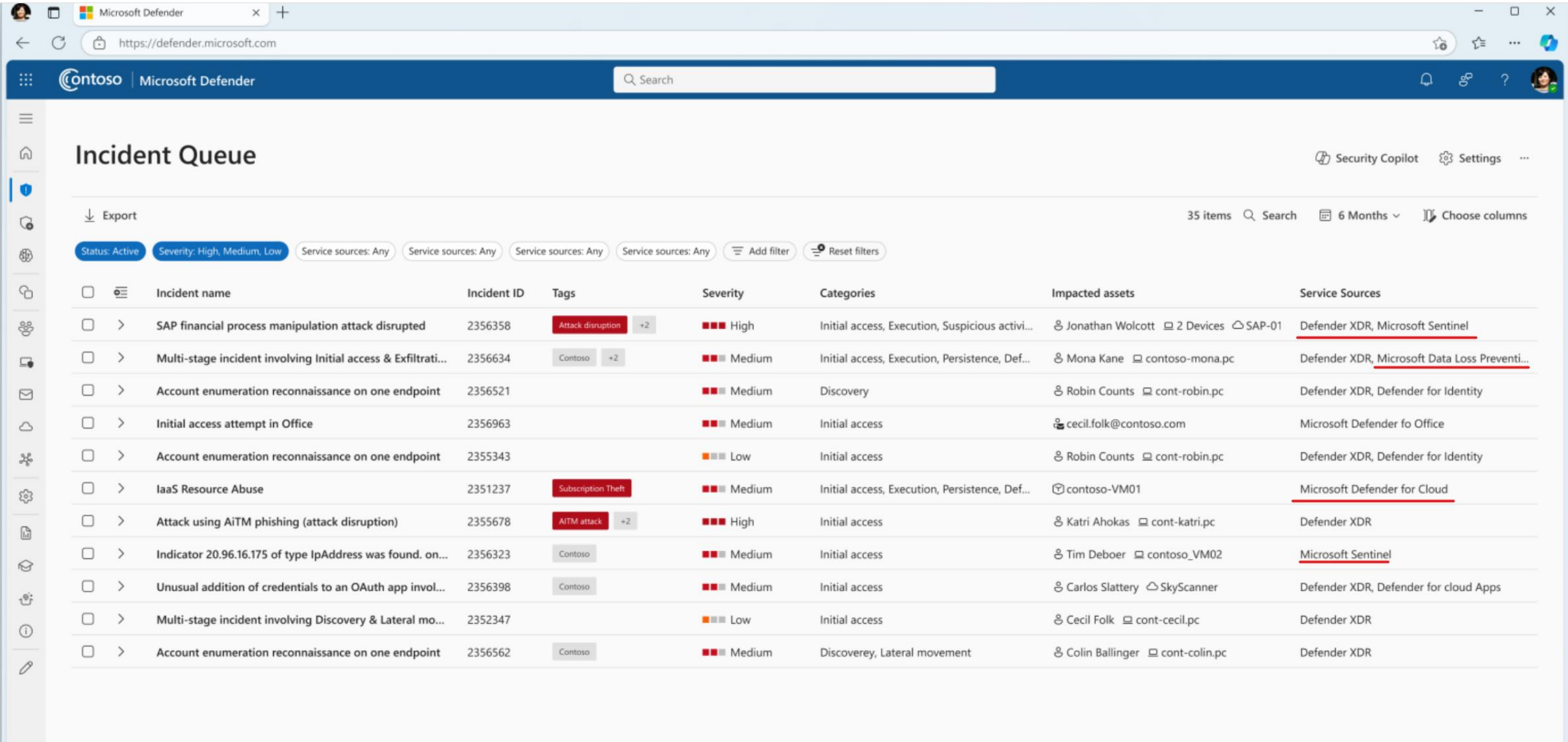
Breakout – The power of Microsoft's XDR: they attempted, we disrupted

Thursday November 16th

4:00pm PST

Breakout – Microsoft Sentinel: A modern approach to security operations

Unified Security Operations Platform



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 | Bianca Pisani

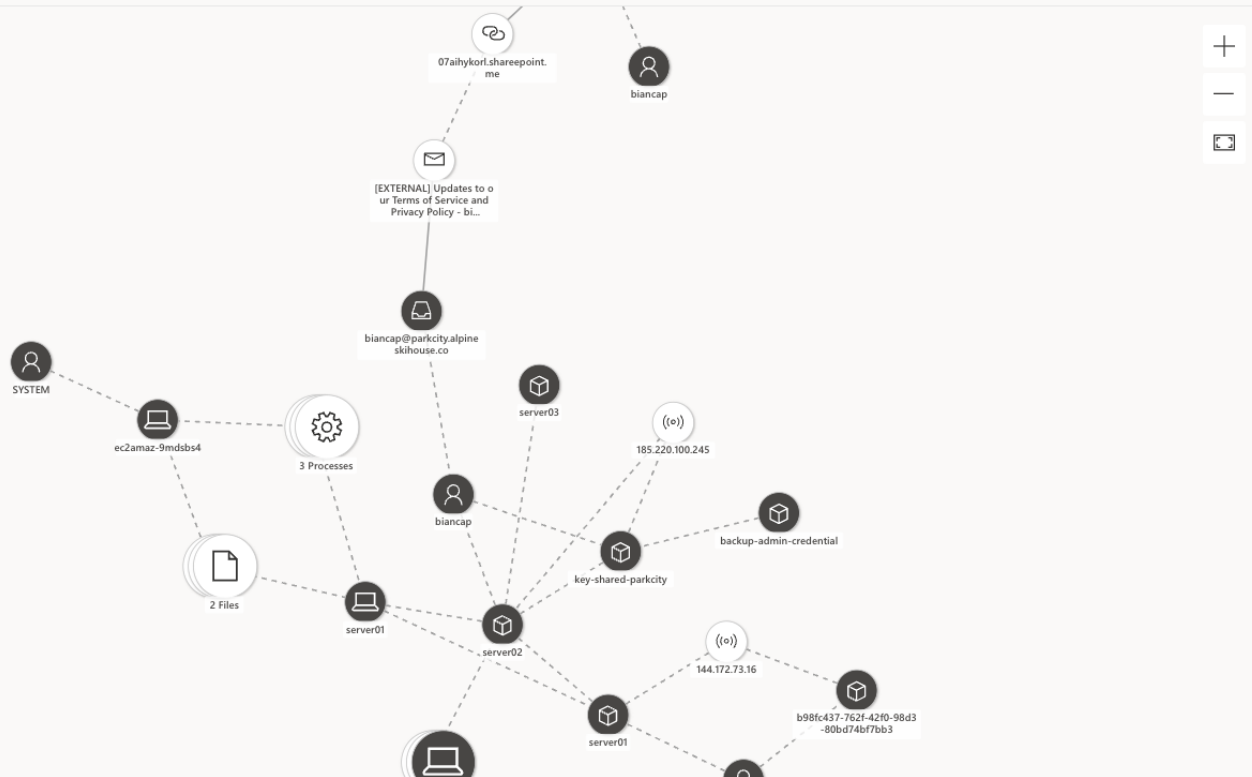
Oct 24, 2023 7:21 PM ● Resolved
Azure Resource Manager operation from suspicious proxy IP address
4 Cloud Resources

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

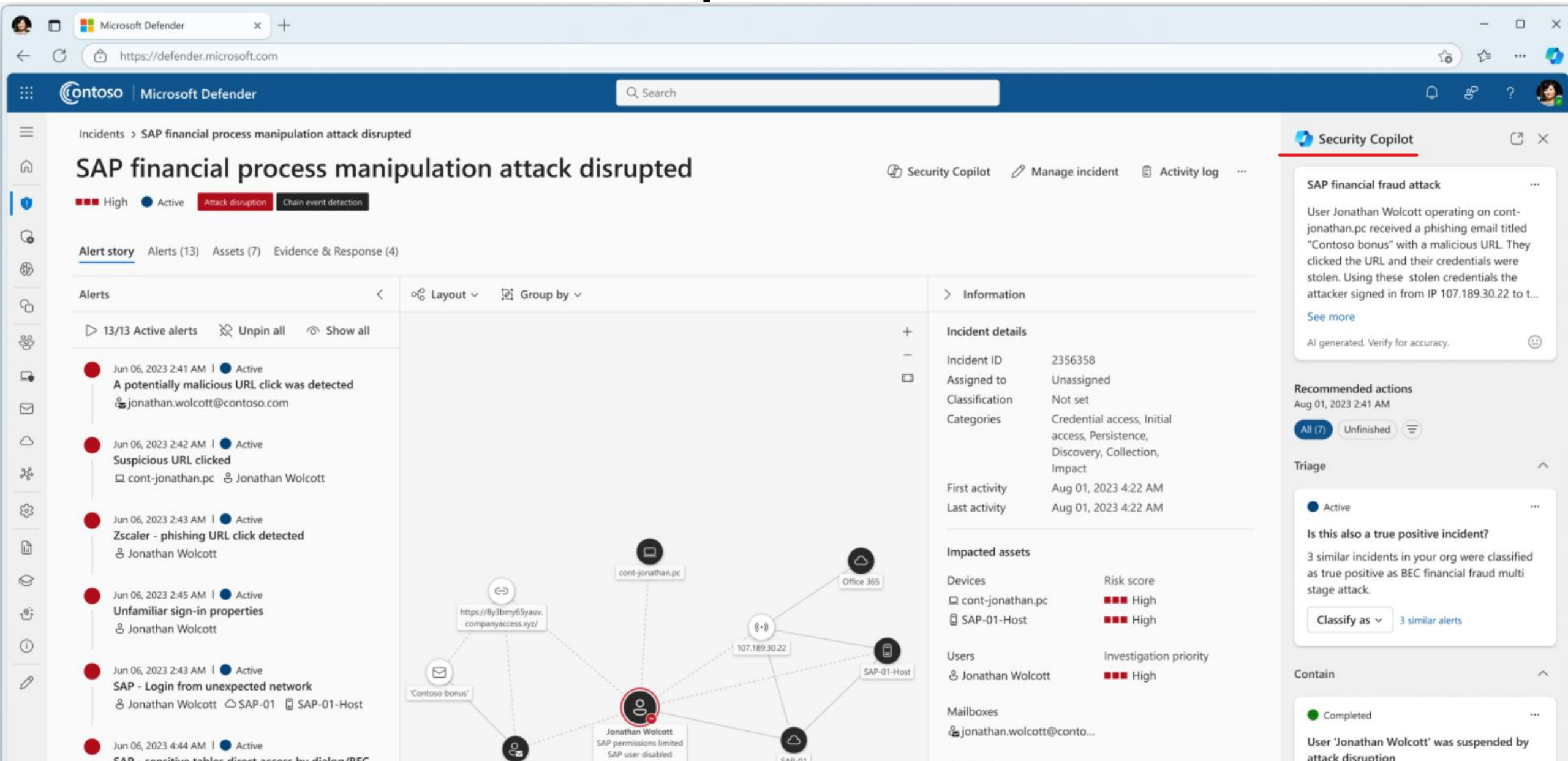
View phishing investigation and response recommended steps for this incident

Open phishing playbook

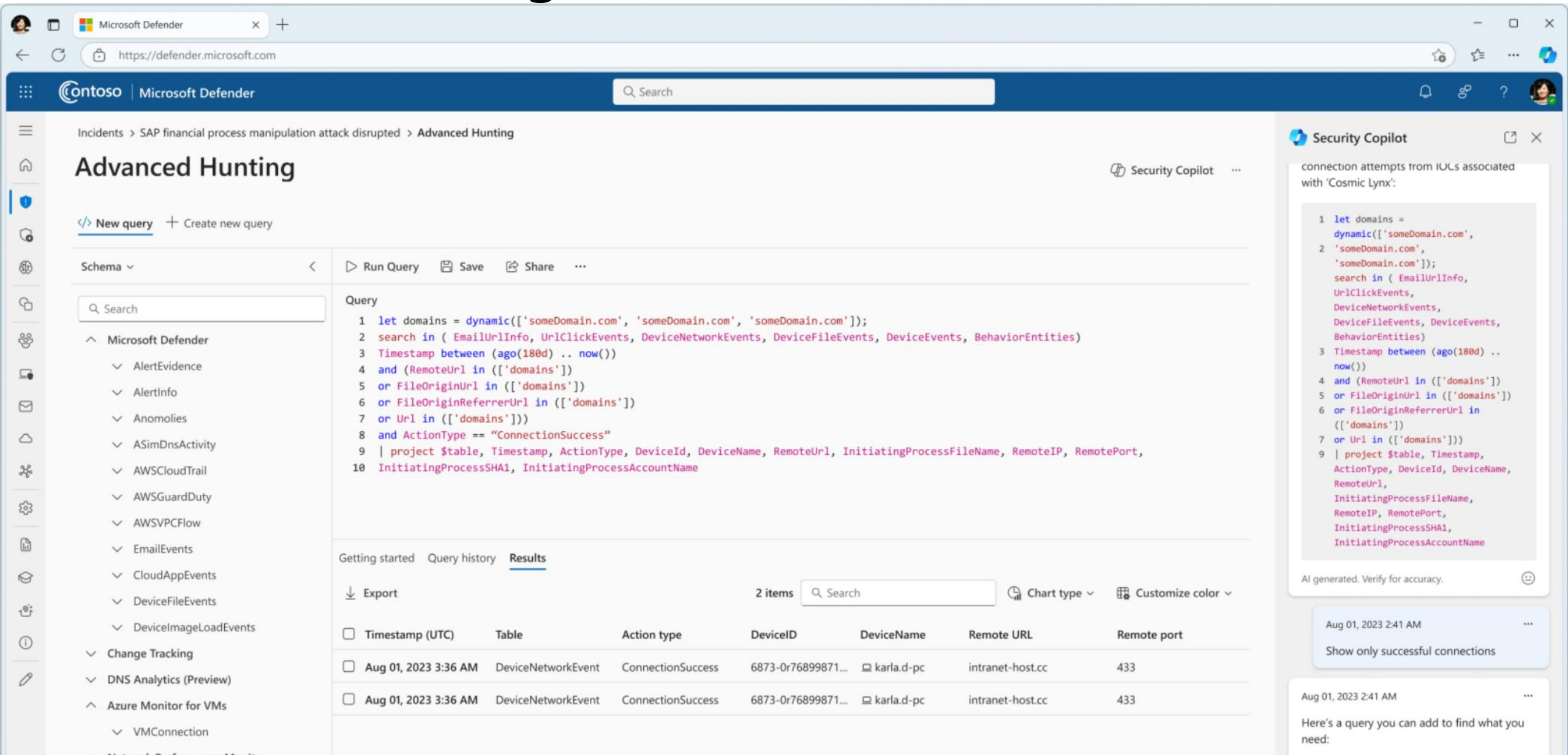
RECOMMENDATIONS

Ransomware Incident response playbook

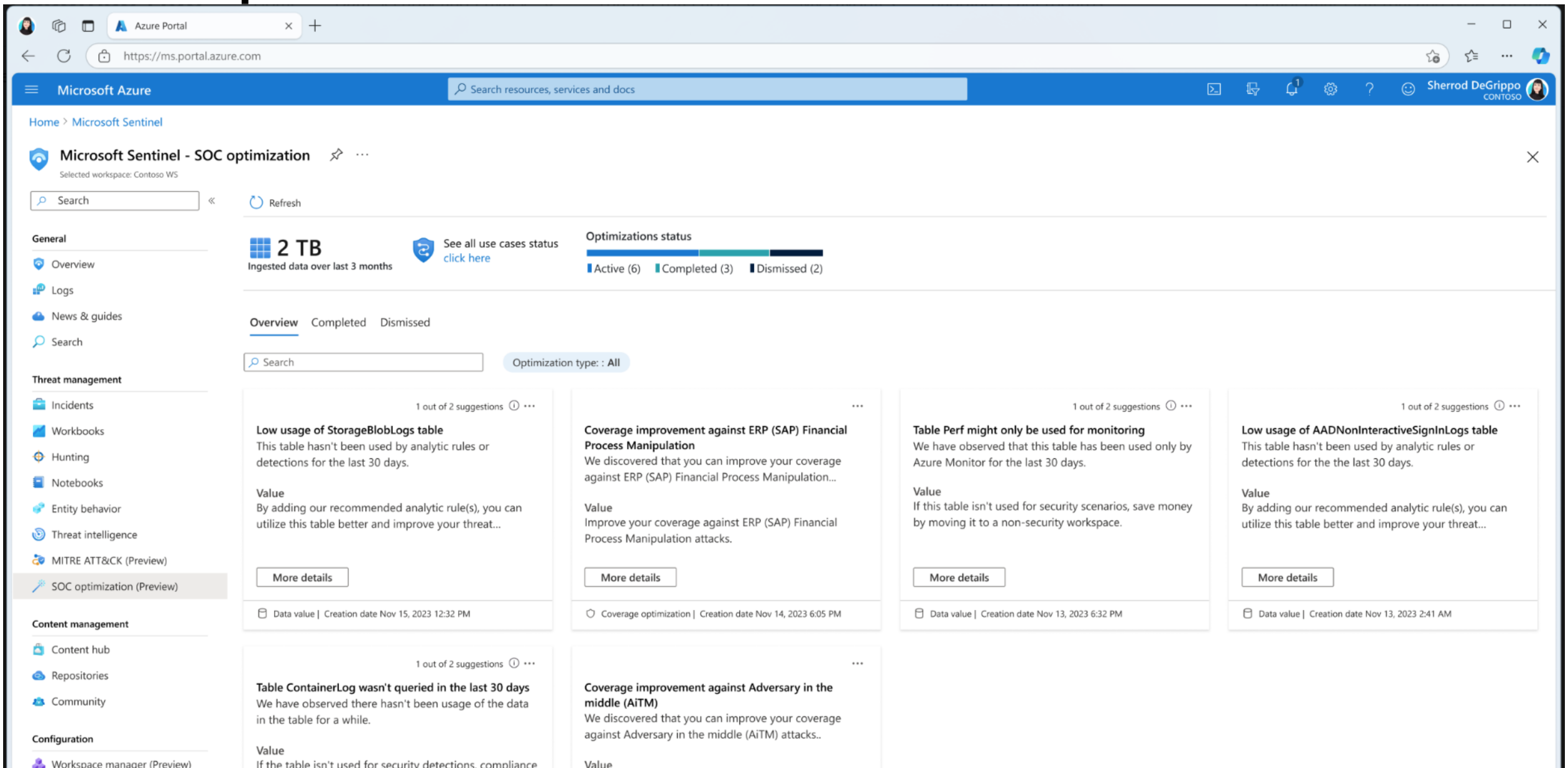
Automated Attack Disruption



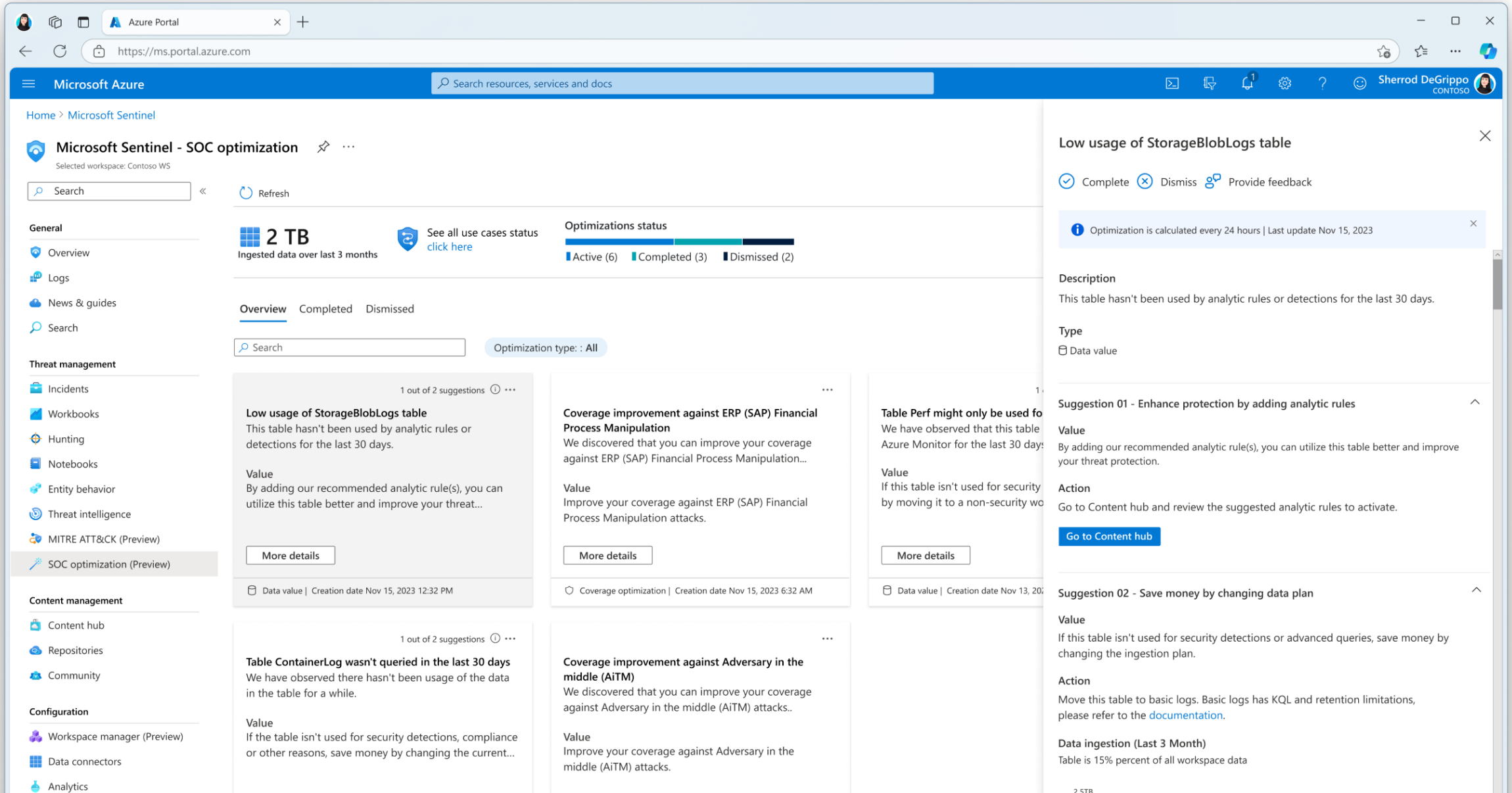
Advanced Hunting



SOC Optimisation



SOC Optimisation



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:

generative ai

✓ Generative AI 413

Bulk selection | New policy from search | 1 - 20 of 413 apps | Show details | Table settings

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	
SEOContentMachine Generative AI	2	
Qualifier Generative AI	2	
Localio Generative AI	2	
GetGenie Generative AI	2	
SpeechVid Generative AI	2	

Cloud Security

Comprehensive cloud-native application protection enhancements in Defender for Cloud

Key announcements

Proactive risk analysis and mitigation with CSPM

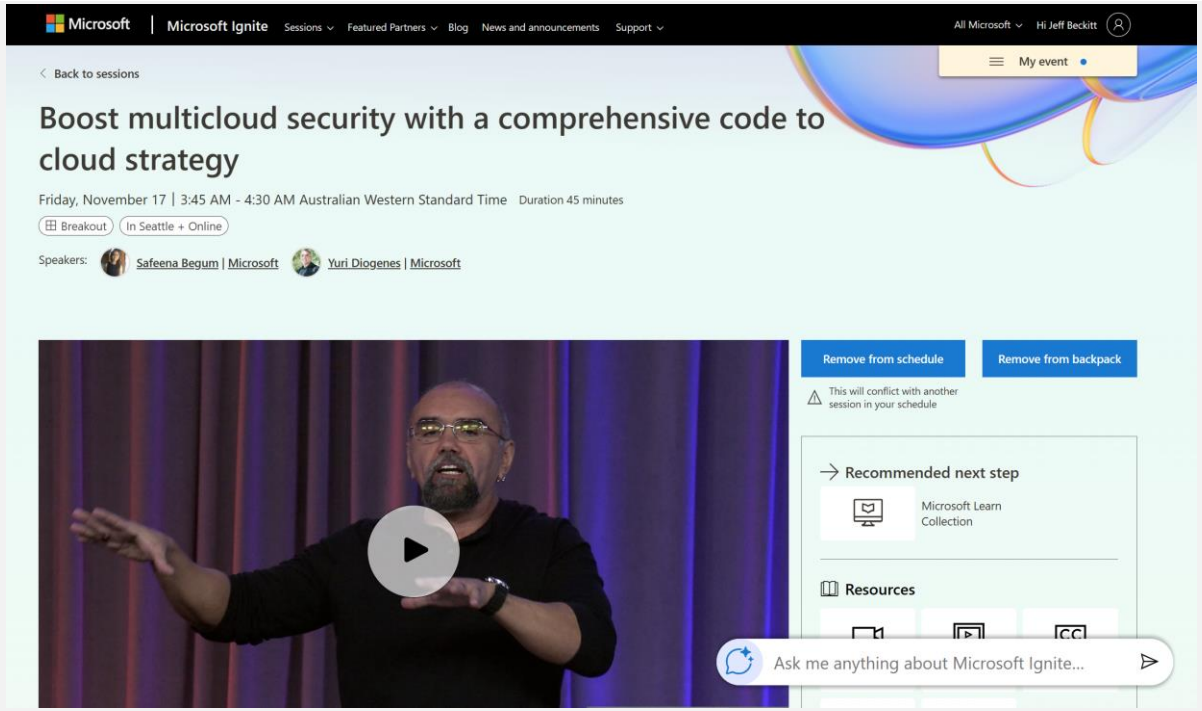
Integrated insights from Entra Permissions Management (CIEM)

- 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

Boost multicloud security with a comprehensive code to cloud strategy https://bit.ly/3MwKTME



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

Cloud Security

Comprehensive cloud-native application protection enhancements in Defender for Cloud

Key announcements

https://aka.ms/DefenderforCloud/Ignite2023

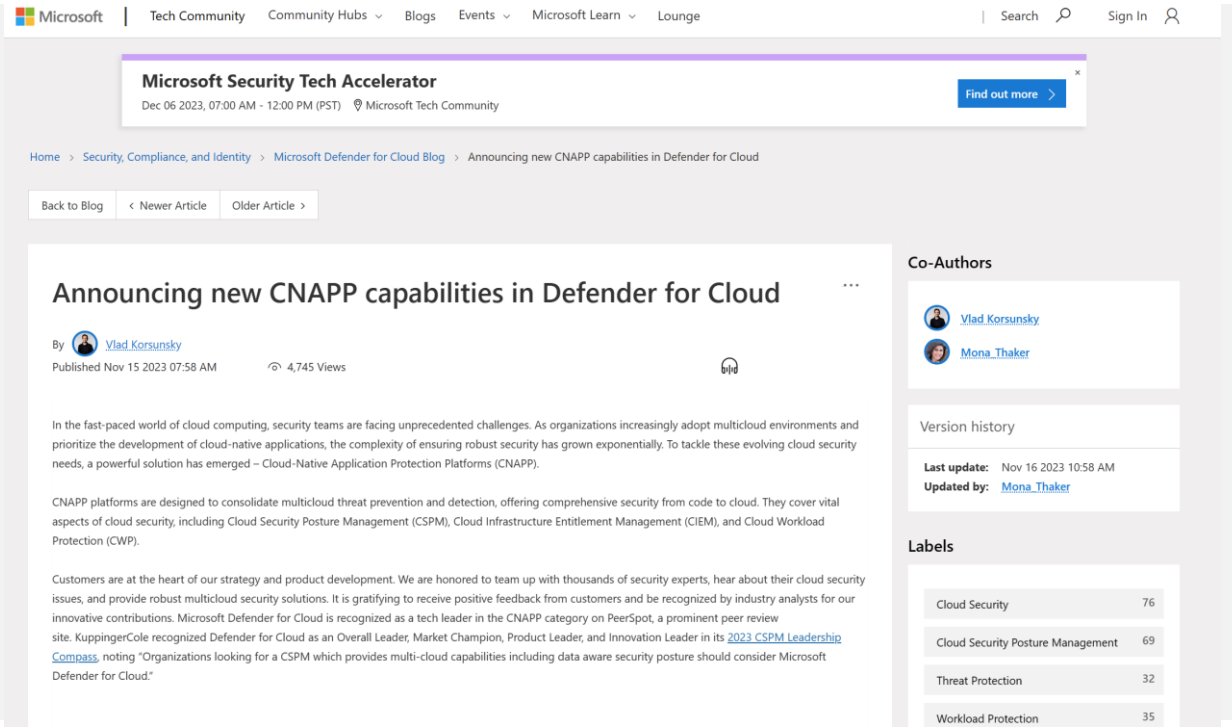
Unified DevOps security insights across GitHub, Azure DevOps and GitLab

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

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

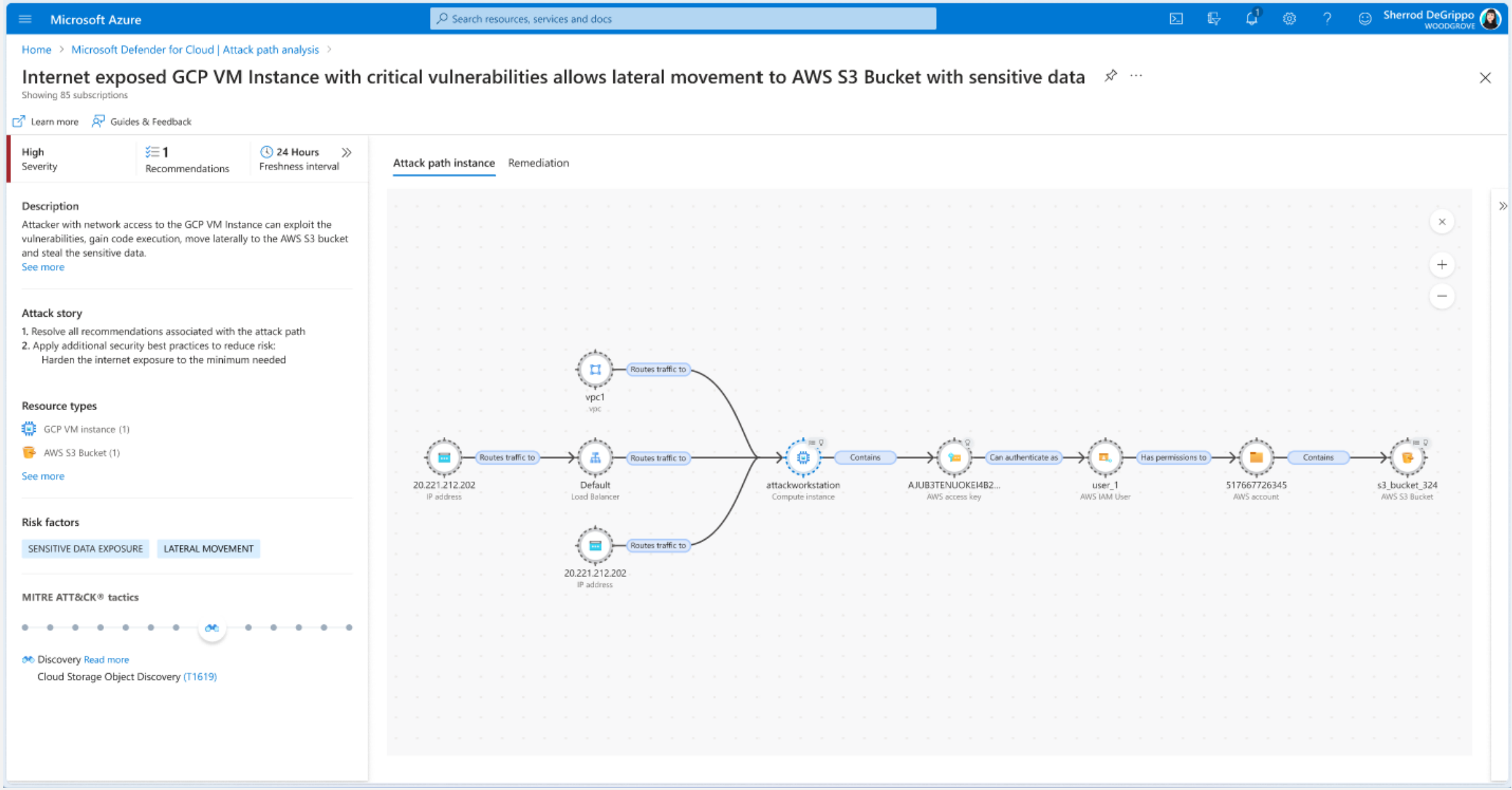
Improved API security posture, GA

Data security dashboard, GA

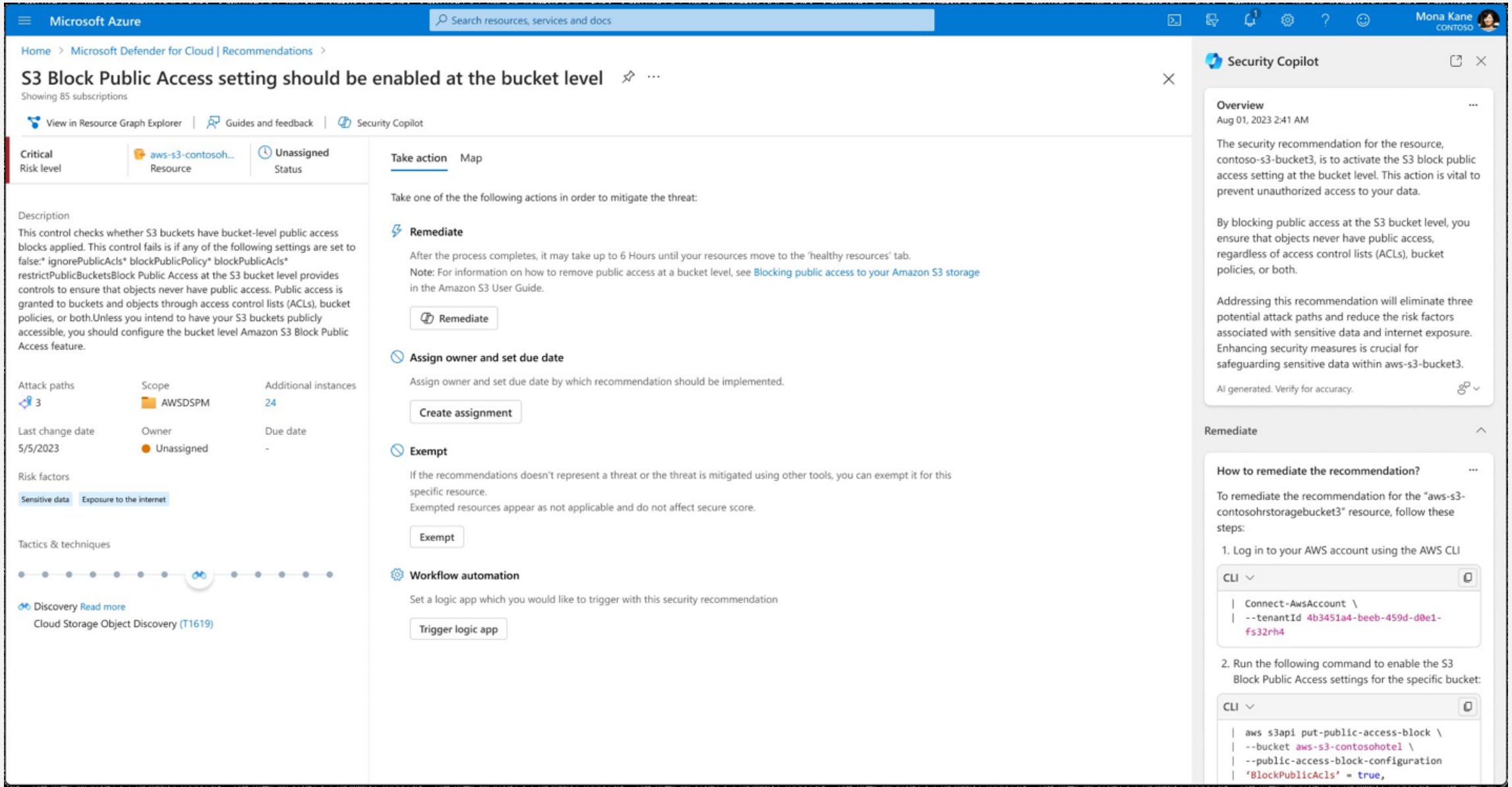
Microsoft Defender External Attack Surface Management

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

Attack Path Analysis in Defender CSPM



Defender for Cloud integration with Security Copilot



Defender CSPM in Action - YouTube

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

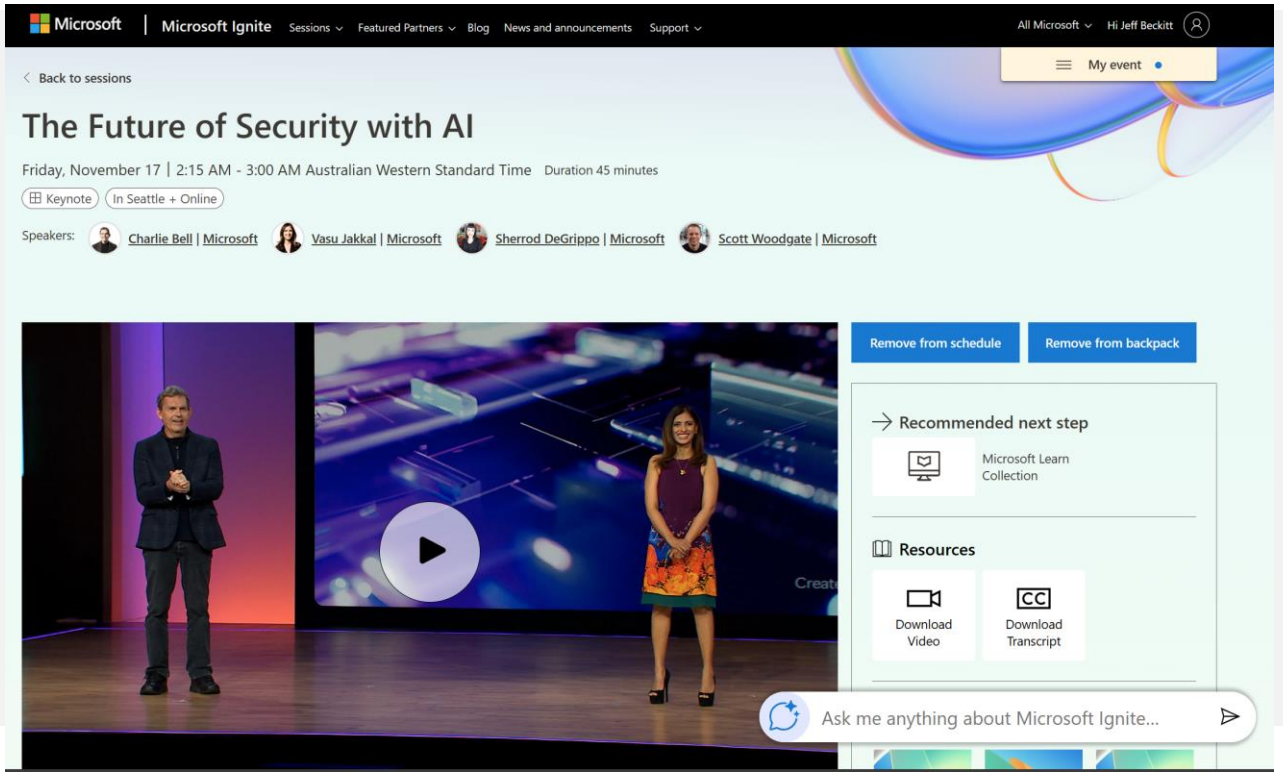
Key announcements

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

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



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

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

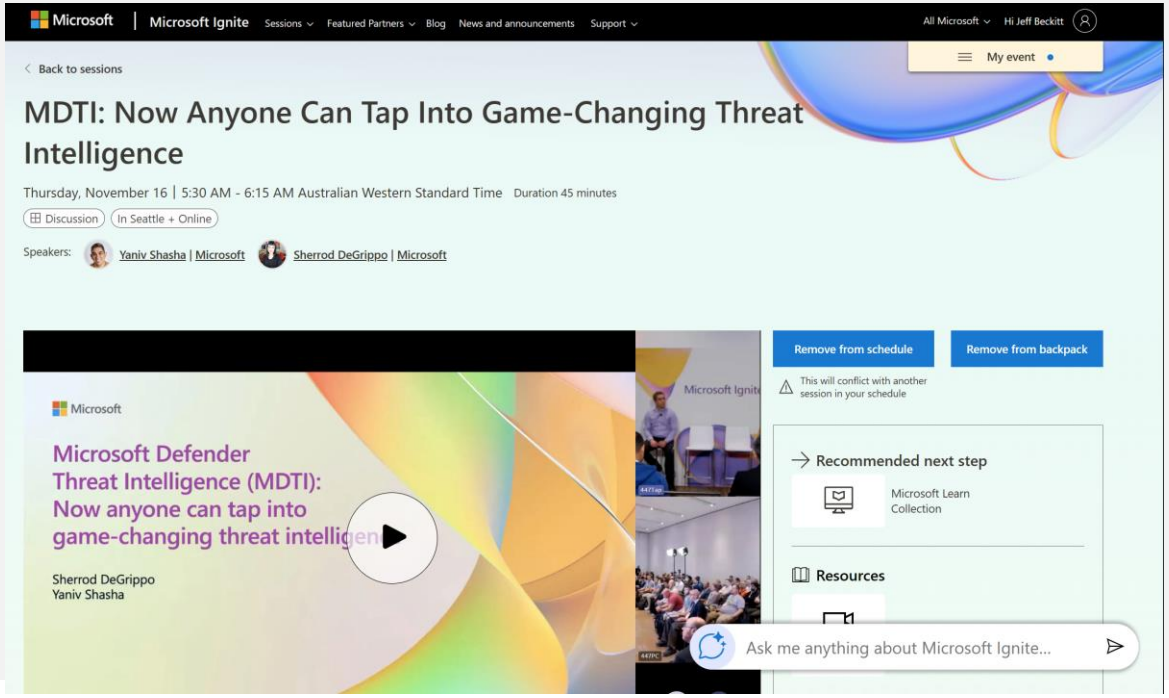
Microsoft Defender Threat Intelligence

- 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

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



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

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

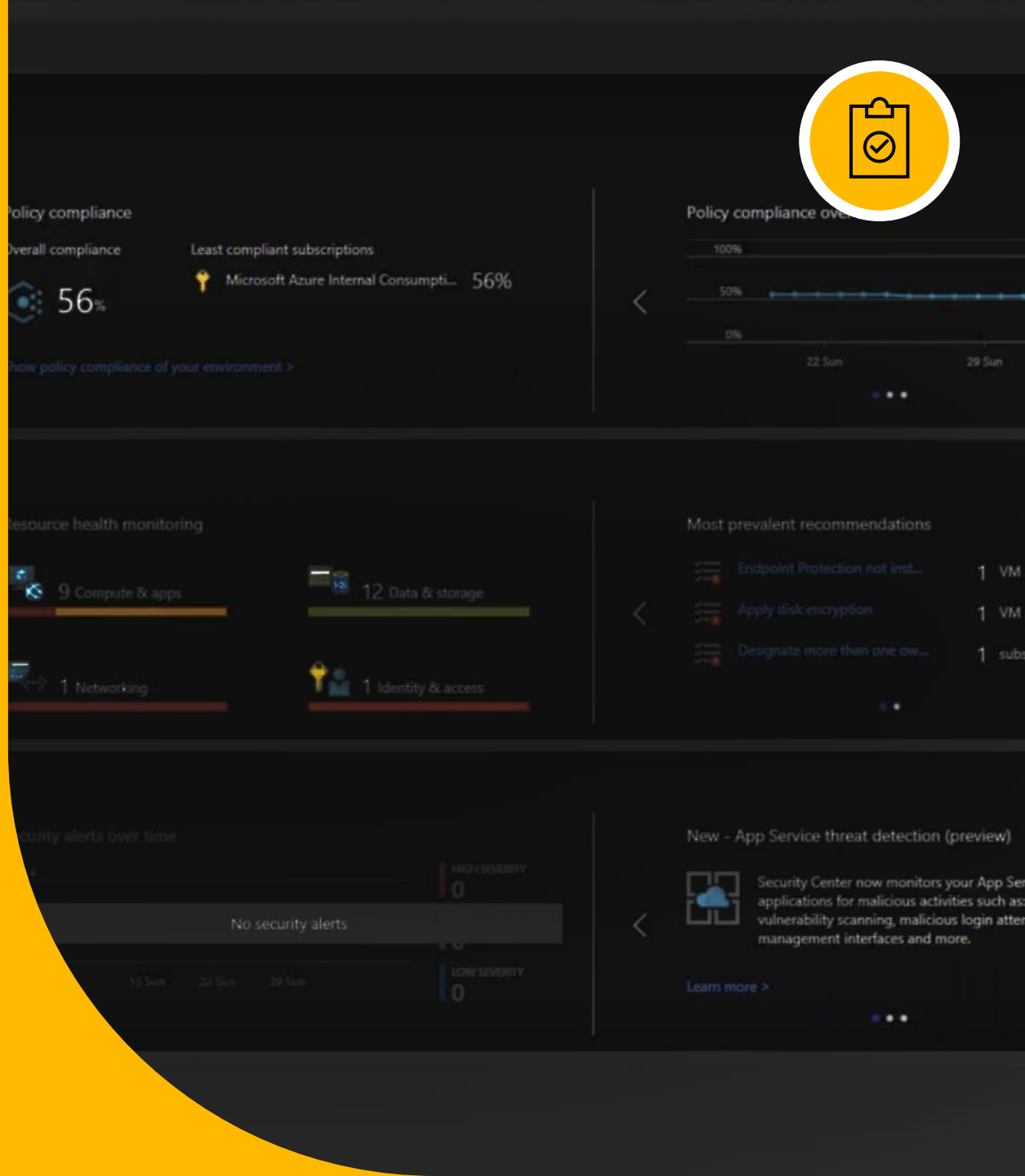
Breakout – New era threat actor: A year battling Octo Tempest

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



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

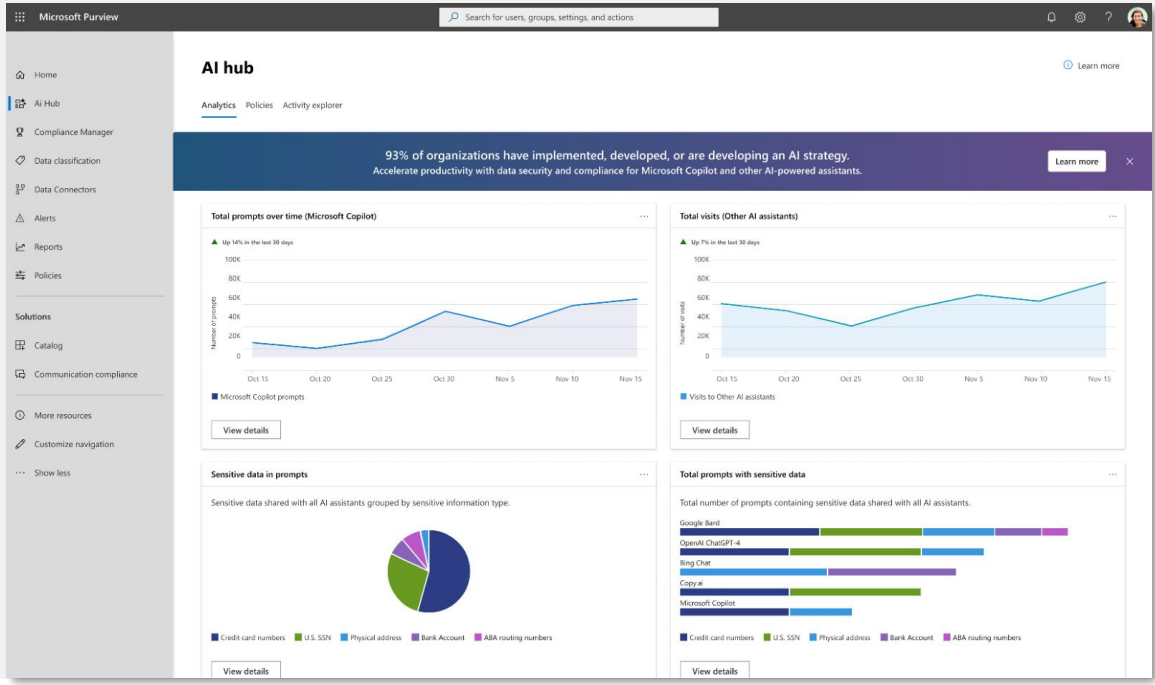
Purview AI hub to provide visibility into AI activity, including total number of users using AI and the sensitive data flowing into AI prompts – for Copilot for M365 and commonly used third-part AI applications.

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

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 that 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

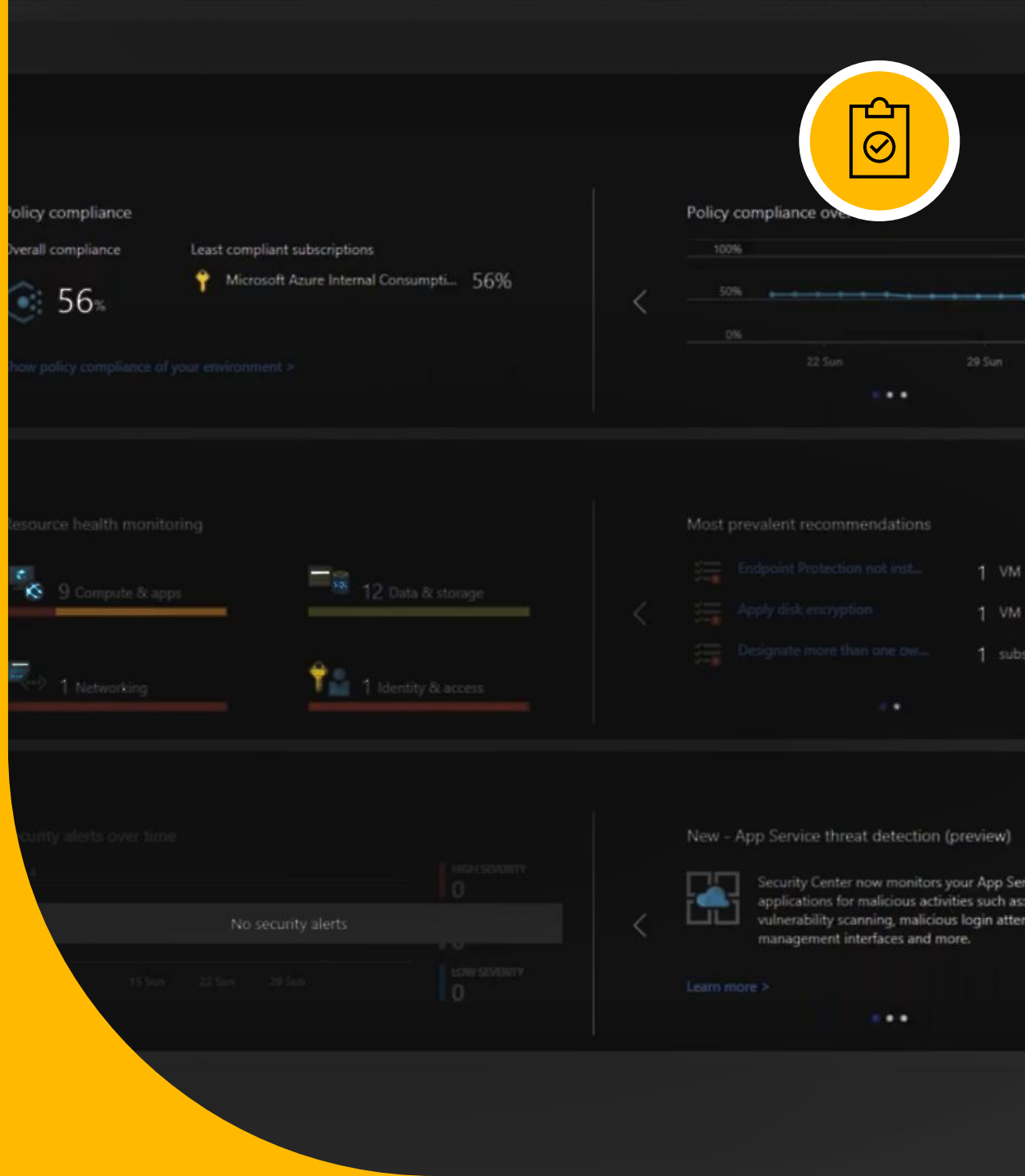
Tier 2 announcements

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



Purview + Security Copilot

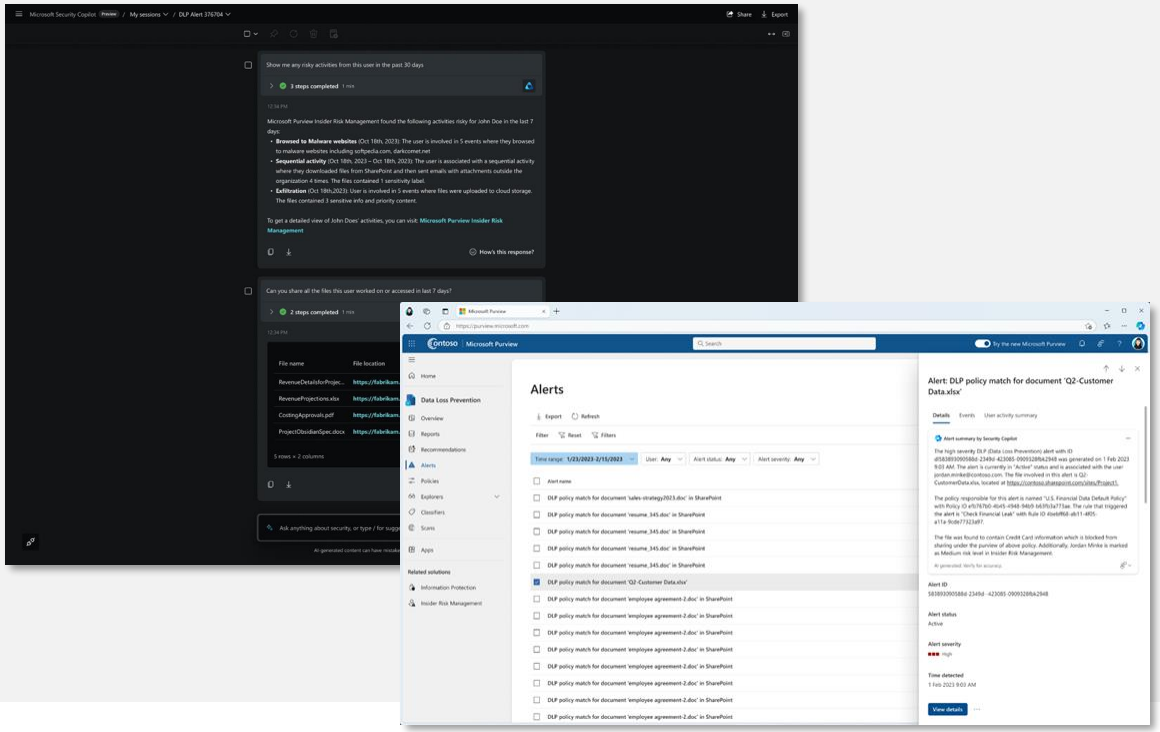
Ignite highlights:

- 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)



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

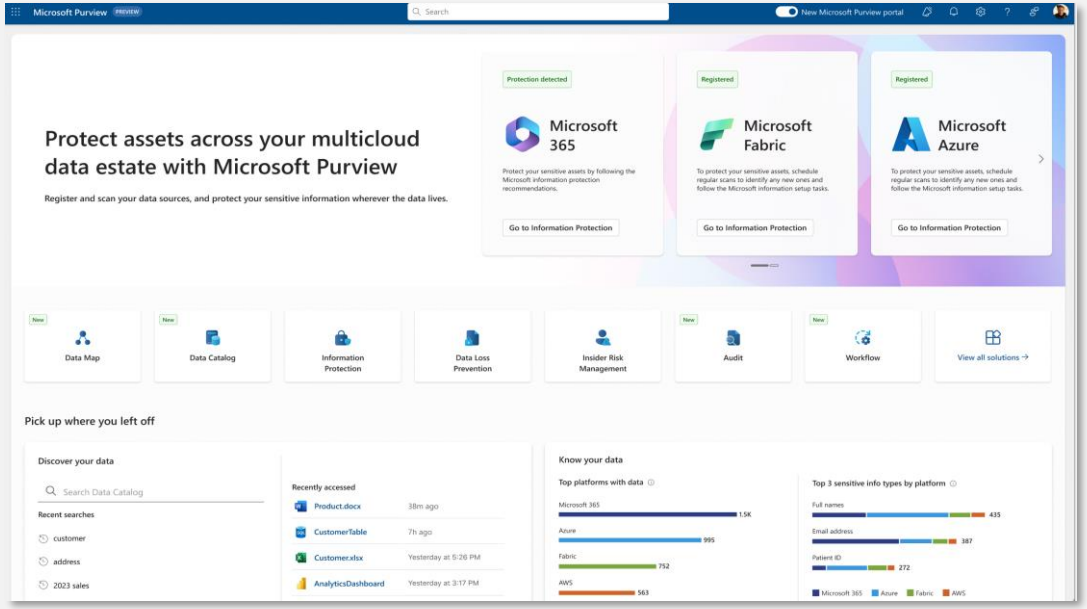
Key announcements

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)



For more information: aka.ms/PurviewExpandingHorizons

Identity

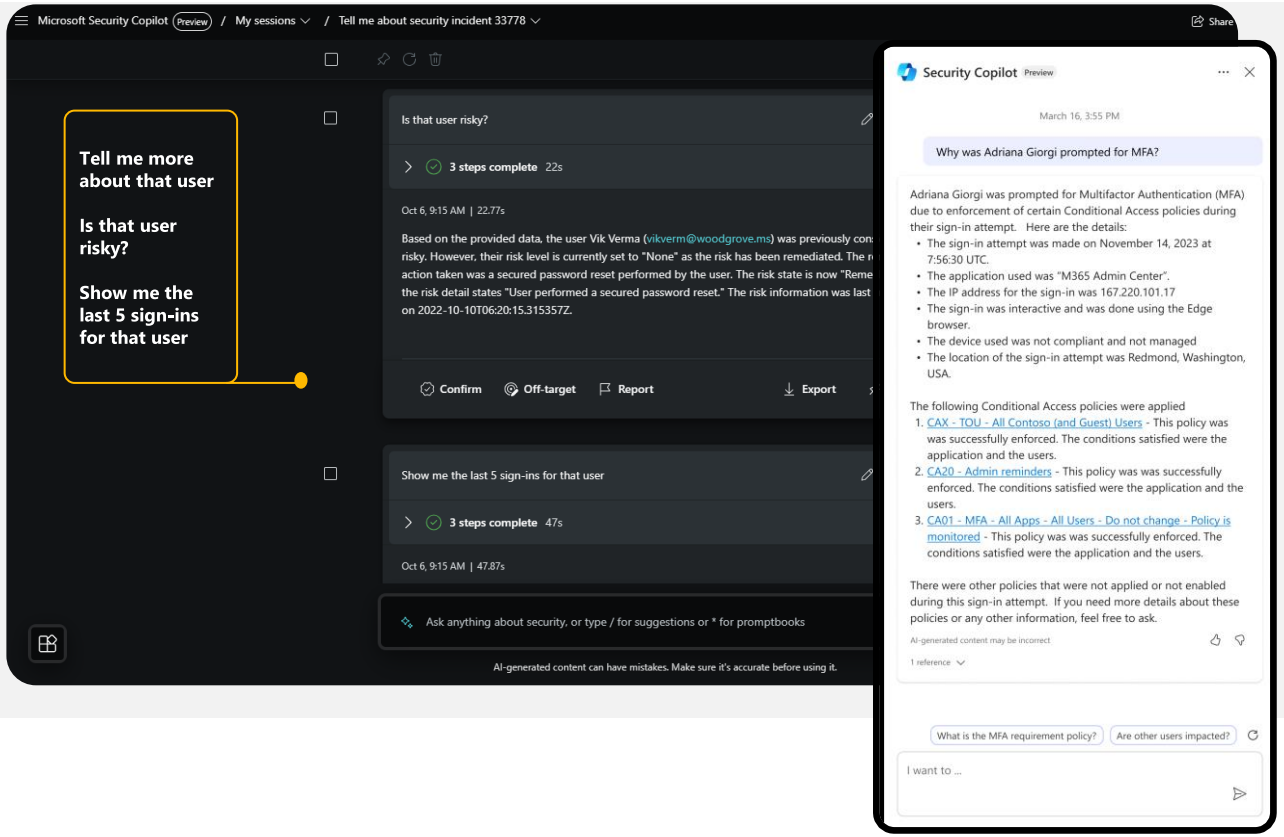
Entra + Security Copilot

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.



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

Security Service Edge (SSE)

Ignite highlights:

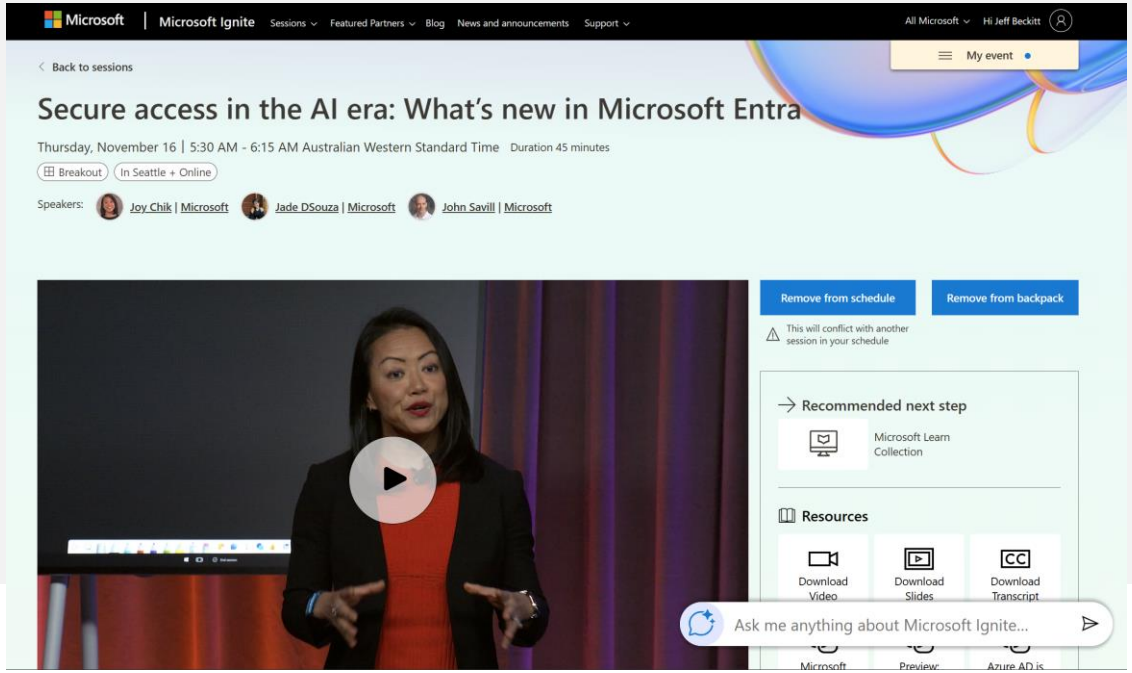
- Microsoft Entra Internet Access for all internet, SaaS, and Microsoft 365 applications and resources – public preview
- Microsoft Entra Private Access additional capabilities – public preview

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.

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



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

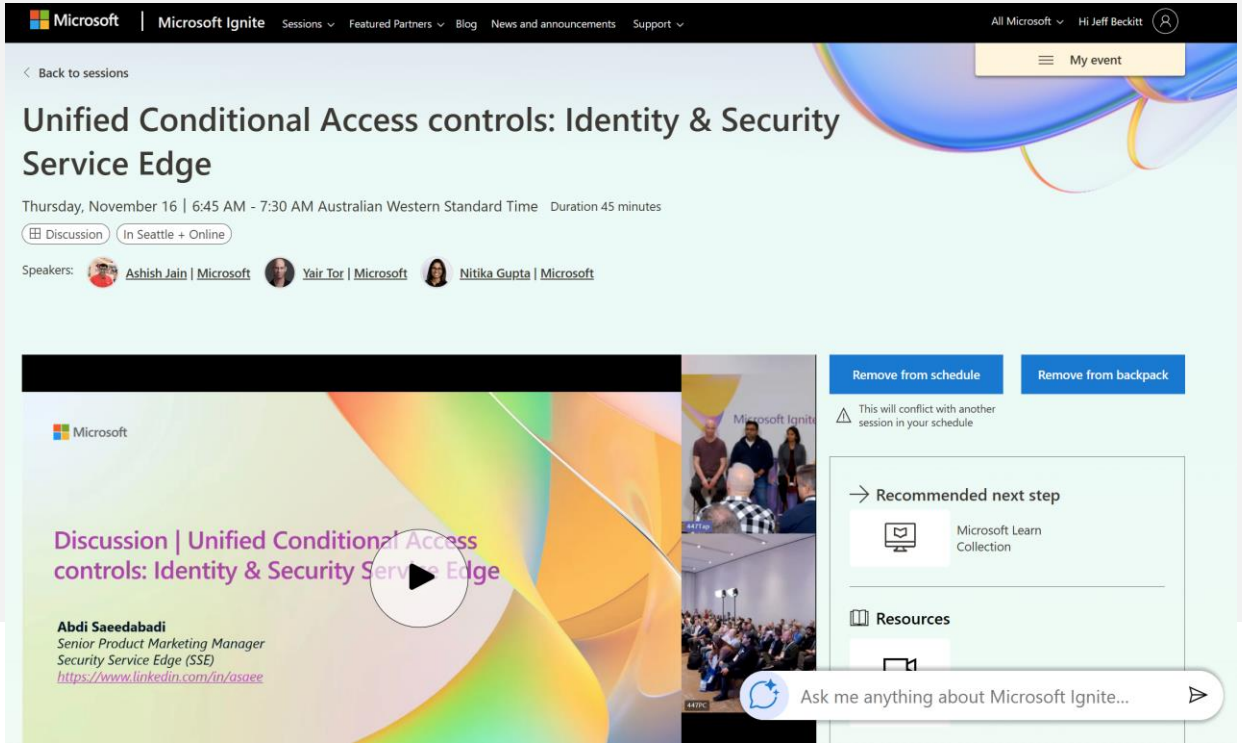
Key announcements

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.

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



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

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:

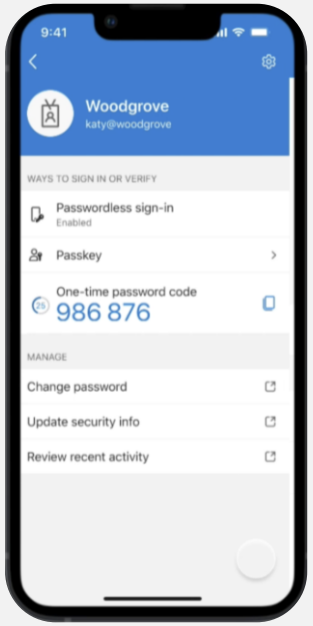
- Microsoft-managed Conditional Access policies - public preview
- Certificate Based Authentication (CBA) - public preview
- Passkeys managed by the Microsoft Authenticator app - public preview

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

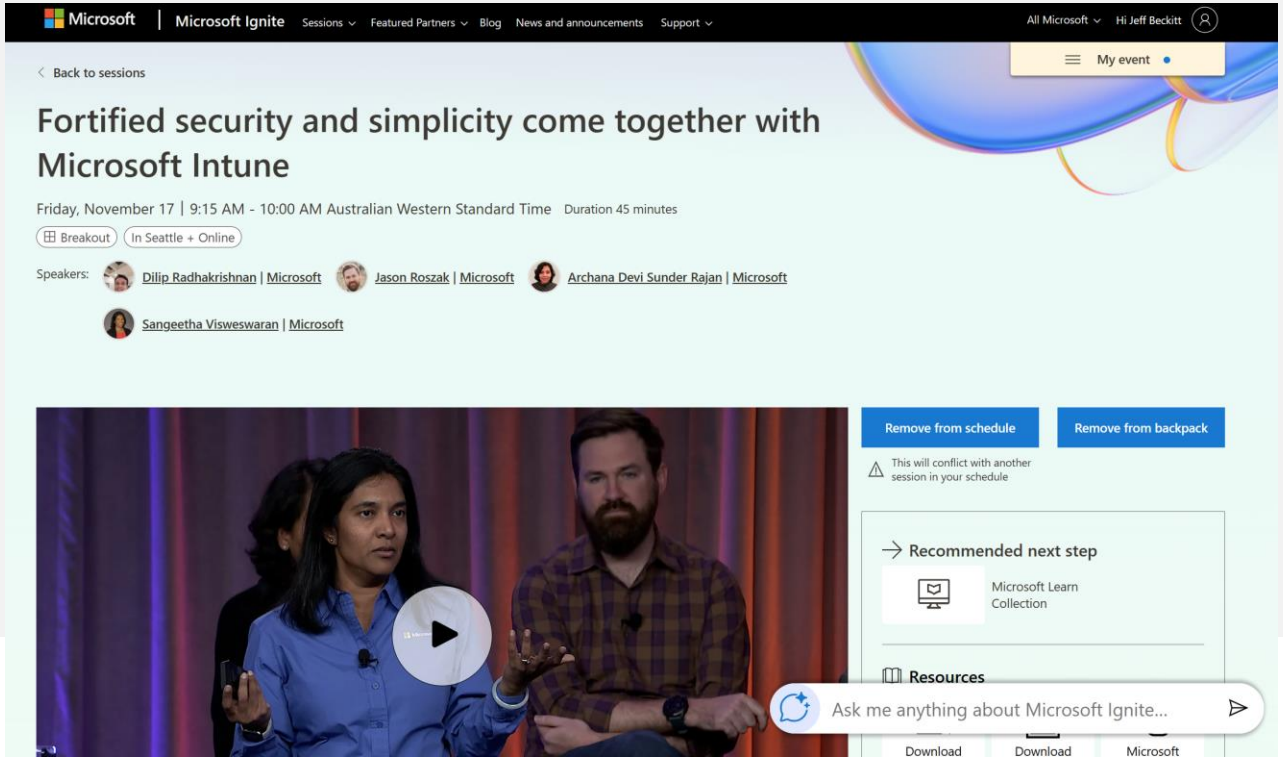
Key announcements

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]



Intune Announcements

Ignite highlights:

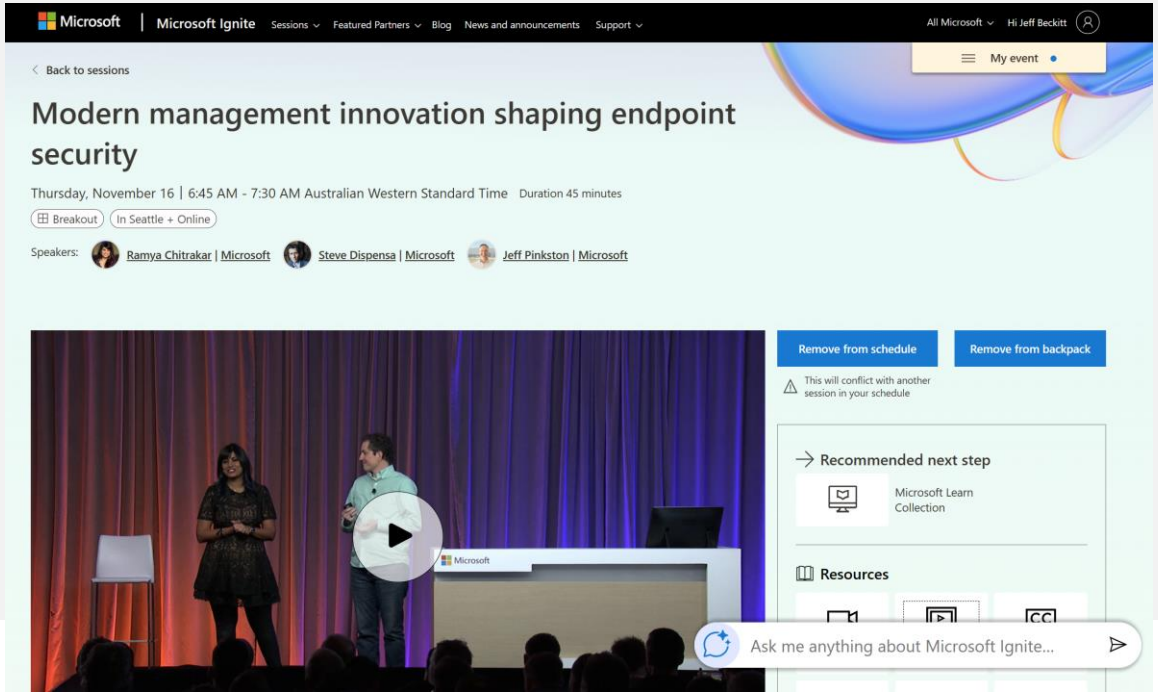
- Security Copilot integration with Microsoft Intune
- New solutions as part of Intune Suite
- Intune and Windows: More secure together

Key announcements

New Intune Suite Solutions - February 2024 GA

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

[Modern Management Innovation Shaping Endpoint Security]



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

Intune Announcements (All)

Additional Announcements

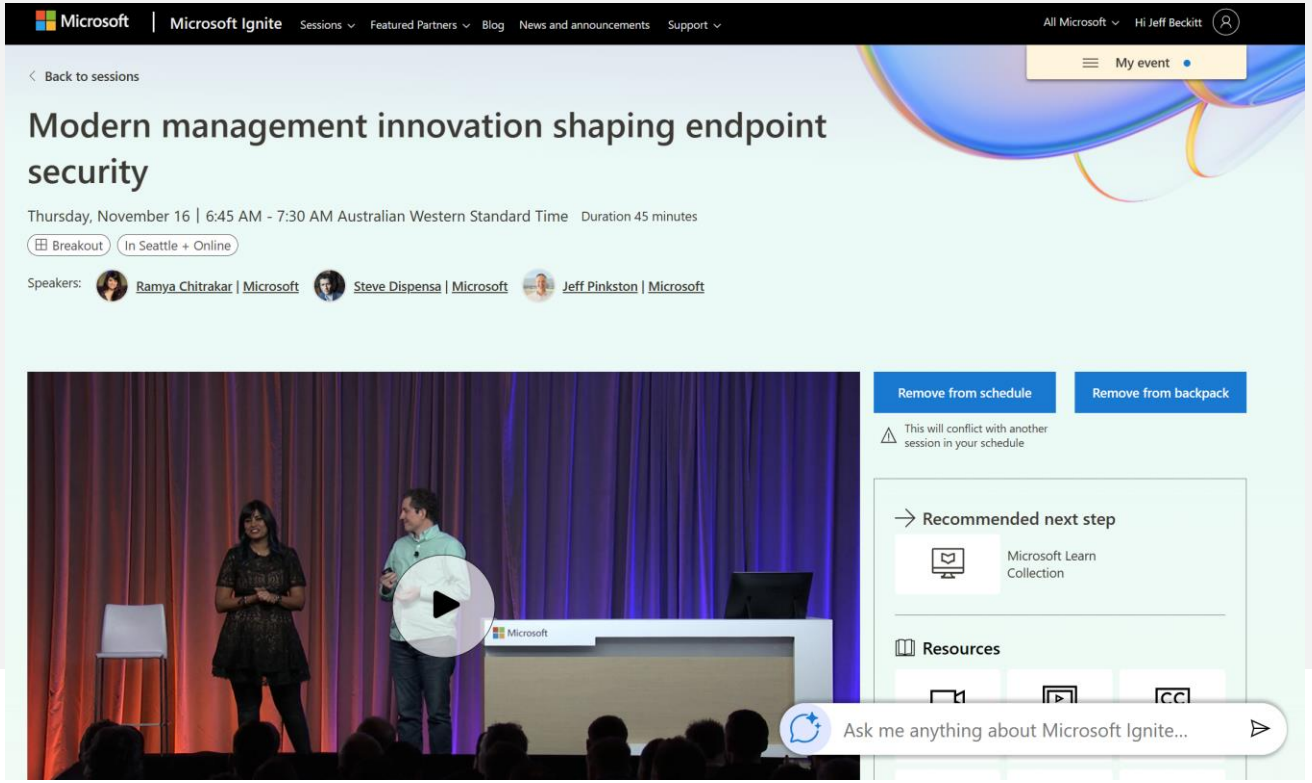
Key announcements

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

Modern management innovation shaping endpoint security https://bit.ly/3SqThkD



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/40qIzN0
- ➞ 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/46YllA8
- ➞ 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

Microsoft

Thank you

Microsoft Ignite