Microsoft Security

What’s New in Security, Compliance and Identity

Technical Presales & Deployment
https://aka.ms/TPD

Ricardo Trigueiro
ritrigue@microsoft.com

Daniela Magalhães
daniela.magalhaes@microsoft.com

Marco Carvalho Cardoso
macardo@microsoft.com

April’25

Agenda

- Intro
- News & Updates:
  - Events, Learning & Training
  - Entra
  - Defender XDR
  - Defender for Cloud
  - Sentinel
  - Security Copilot
  - Purview
- TP&D
- Q&A

Intro

What’s New in Security, Compliance and Identity

- Monthly News and Updates for all things related with Microsoft Security, Compliance and Identity with a partner focus.

- Monthly, every third Thursday at 11am GMT+1

- Technical Presales & Deployment Team:
  - André Barreiros - abarreiros@microsoft.com
  - Daniela Magalhães - daniela.magalhaes@microsoft.com
  - Marco Carvalho Cardoso – macardo@microsoft.com
  - Ricardo Trigueiro – ritrigue@microsoft.com

What’s New series:

What’s New in Security, Compliance and Identity – Cloud Champion
This session :)

What’s New and Highlights in Business Applications – Cloud Champion
Next: April 18th

What’s New in Modern Work – Cloud Champion
Next: April 29th

General News and Highlights

Events, Learning and Training

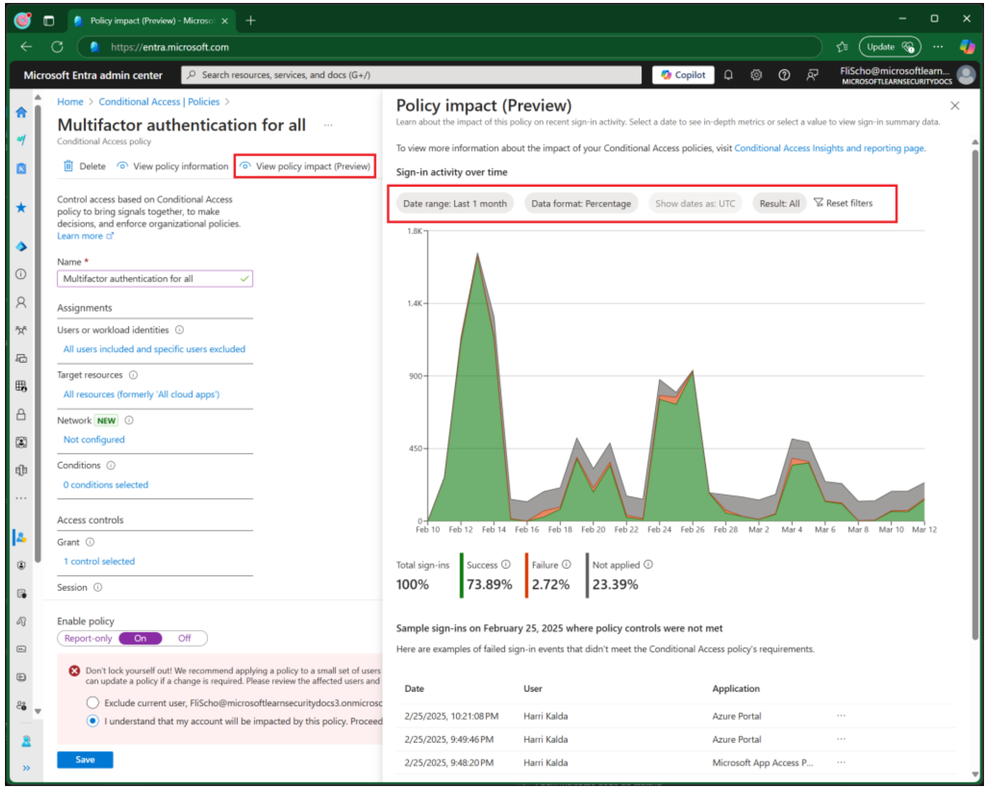
- Learn Live: Security for AI w/ Microsoft Purview & Defender for Cloud
  - April 22nd – Manage Compliance with Microsoft Purview with Microsoft 365 Copilot
  - April 29th – Identify and Mitigate AI Data Security Risks: Microsoft Purview Data Security Posture Management (DSPM)
  - May 13th – Enable Advanced Protection for AI Workloads with Microsoft Defender for Cloud
- Azure Security and AI Adoption
  - April 22nd
- Certification Week for MAICPP Partners: Security
  - April 28th – May 2nd – AZ-500, SC-100, SC-200, SC-300, SC-400
- Level Up your Security Skills with Microsoft Security Virtual Training Days
  - April 22nd -23rd - Modernize your Security Operations with Microsoft Sentinel
  - April 23rd - 24th - Security, Compliance, and Identity Fundamentals
  - April 24th - 25th - Defend Against Threats with Extended Detection and
  - April 28th – 29th - Modernize your Security Operations with Microsoft Sentinel
  - April 29th – 30th - Security, Compliance, and Identity Fundamentals
  - May 1st – 2nd - Implement Data Security with Microsoft Purview
  - May 5th – 6th - Security, Compliance, and Identity Fundamentals
  - May 7th – 8th - Implement Data Security with Microsoft Purview

Entra

Public Preview

Analyze Conditional Access Policy Impact

- Allows admins with at least Security Reader role to see a snapshot of existing and potential impact of policies on interactive sign-ins.
- Check the impact over a period of past 24h, 7 days or 1 month
- Works for both enabled and report-only policies


Policy impact (Preview) - Microsof
https://entra.microsoft.com
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
Update
FliScho@microsoftlearn...
MICROSOFTLEARNSECURITYDOCS
Home > Conditional Access | Policies >

Multifactor authentication for all

Conditional Access policy

Delete
View policy information
View policy impact (Preview)

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *: Multifactor authentication for all

Assignments

Users or workload identities: All users included and specific users excluded

Target resources: All resources (formerly 'All cloud apps')

Network NEW: Not configured

Conditions: 0 conditions selected

Access controls

Grant: 1 control selected

Session

Enable policy: Report-only [✓ On] Off

Don't lock yourself out! We recommend applying a policy to a small set of users can update a policy if a change is required. Please review the affected users and

○ Exclude current user, FliScho@microsoftlearnsecuritydocs3.onmicrosc

● I understand that my account will be impacted by this policy. Proceed

Policy impact (Preview)

Learn about the impact of this policy on recent sign-in activity. Select a date to see in-depth metrics or select a value to view sign-in summary data.

To view more information about the impact of your Conditional Access policies, visit Conditional Access Insights and reporting page.

Sign-in activity over time

Date range: Last 1 month · Data format: Percentage · Show dates as: UTC · Result: All · Reset filters

Total sign-ins	Success	Failure	Not applied
100%	73.89%	2.72%	23.39%

Sample sign-ins on February 25, 2025 where policy controls were not met

Here are examples of failed sign-in events that didn't meet the Conditional Access policy's requirements.

Date	User	Application
2/25/2025, 10:21:08 PM	Harri Kalda	Azure Portal
2/25/2025, 9:49:46 PM	Harri Kalda	Azure Portal
2/25/2025, 9:48:20 PM	Harri Kalda	Microsoft App Access P...

References:

- Analyze Conditional Access policy impact - Microsoft Entra ID | Microsoft Learn

Entra Updates

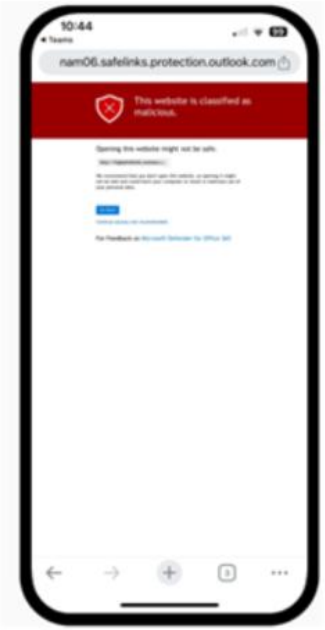
· Analyze Conditional Access policy impact - Microsoft Entra ID | Microsoft Learn	Public Preview
· Entra ID Governance Deployment Guide | Microsoft Entra ID Governance - YouTube	General Availability
- Microsoft Entra Permissions Management End of Sale and Product Retirement	Retiring
- Retirement of Azure AD B2C and Azure AD External Identities	Retiring

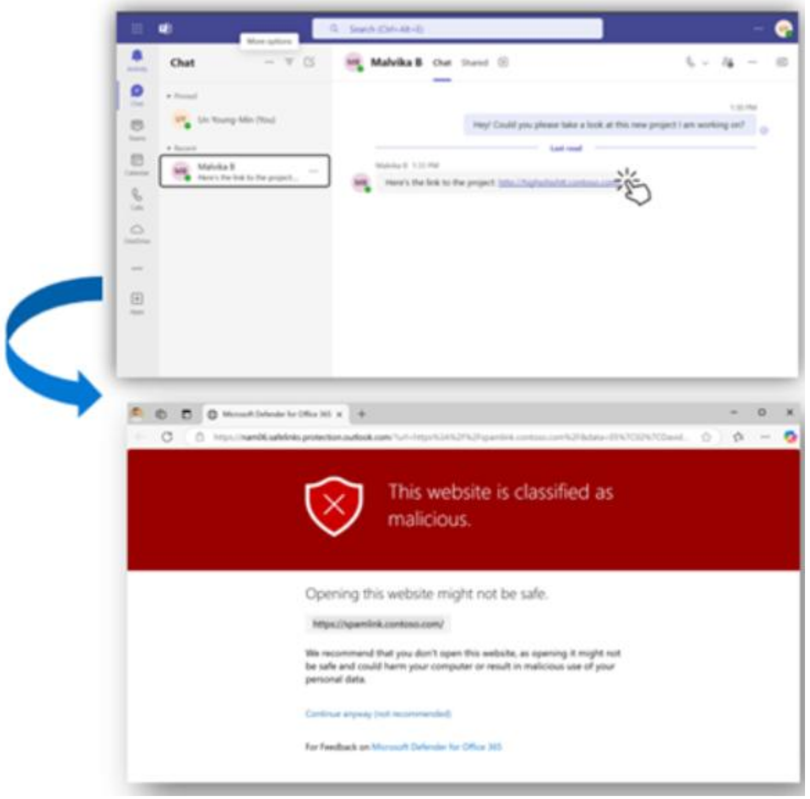
Defender XDR

Public Preview

Defender for Office 365: Collaboration Security for Microsoft Teams

- Improved Teams security posture with increased control over how external organizations communicate with employees
- Better in-line protection for end users from malicious links or attachments
- Easy reporting of suspicious messages to admins and Microsoft
- Threat hunting and response capabilities across Teams messages


10:44
nam06.safelinks.protection.outlook.com
This website is classified as malicious.



Hey! Could you please take a look at this new project I am working on?

Here's the link to the project:

Microsoft Defender for Office 365

This website is classified as malicious.

Opening this website might not be safe.

https://spamlink.contoso.com/

We recommend that you don't open this website, as opening it might not be safe and could harm your computer or result in malicious use of your personal data.

Continue anyway (not recommended)

For Feedback on Microsoft Defender for Office 365

References:

- General Availability for Collaboration Security for Microsoft Teams | Microsoft Community Hub
- Microsoft Defender for Office 365 Plan 2 support for Microsoft Teams - Microsoft Defender for Office 365 | Microsoft Learn

Defender XDR Updates

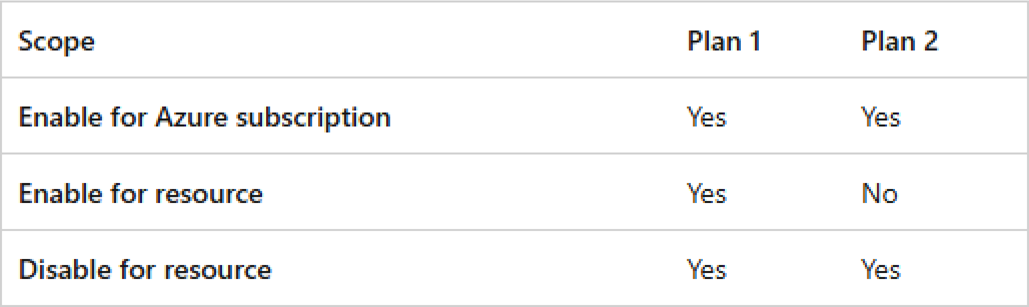
• MDO: General Availability for Collaboration Security for Microsoft Teams	General Availability
• MDO: LLM-based threat classifications in Mail Flow and Threat Protection Status	General Availability
• MDCA: Oauth App insights are now available in Exposure Management	General Availability
• MDTI: Comprehensive Threat Analytics are now available across all Threat Intelligence reports	General Availability

Defender for Cloud

Guidance

Defender for Servers: Can I enable MDS for specific resources in a subscription?

- Yes you can!
- Different experience for MDS P1 and P2
- Plan 1 can be enabled and disabled at resource level.
- Plan 2 can't be enabled at the resource level, but you can disable the plan at the resource level.
- How? Powershell



Scope	Plan 1	Plan 2
Enable for Azure subscription	Yes	Yes
Enable for resource	Yes	No
Disable for resource	Yes	Yes

References:

- Select a Defender for Servers plan - Microsoft Defender for Cloud | Microsoft Learn
- Microsoft-Defender-for-Cloud/Powershell scripts/Defender for Servers on resource level at main · Azure/Microsoft-Defender-for-Cloud · GitHub
- Common questions - Defender for Servers - Microsoft Defender for Cloud | Microsoft Learn
- Overview of Defender for Servers in Defender for Cloud - Microsoft Defender for Cloud | Microsoft Learn

Defender for Cloud Updates

• Updates on AI threat protection - Microsoft Defender for Cloud | Microsoft Learn	Public Preview
• Enhancements for Defender for app service alerts	Public Preview
• Enhanced container protection with vulnerability assessment and malware detection for AKS nodes	General Availability

Sentinel

Sentinel Updates

• Multi workspace and multitenant support for Sentinel in Defender Portal | Virtual Ninja Training: Unified SecOps Experience using Sentinel Latest Features	Public Preview
• Introducing Sentinel Intel Management in Defender Portal	General Availability
• New capabilities coming to Microsoft Sentinel this Spring | Microsoft Community Hub	News

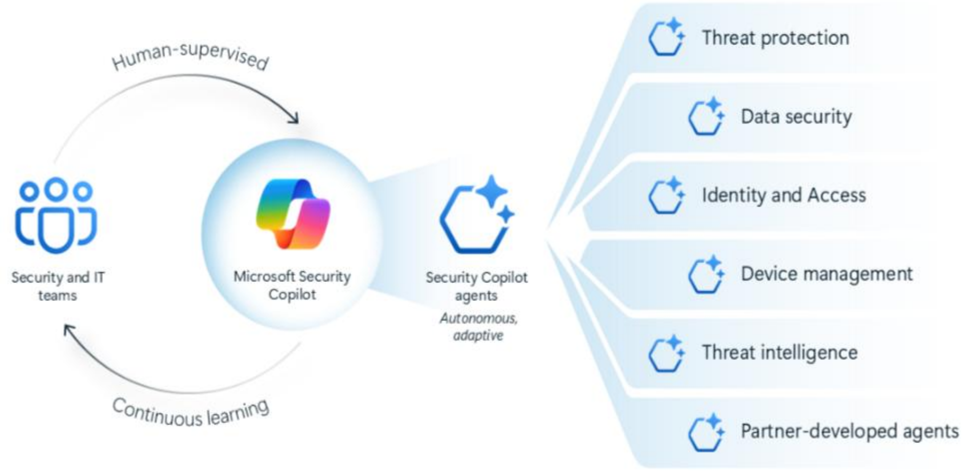
Security Copilot

Microsoft Security Copilot Agents are here!

Public Preview

- Accelerate Response Times: Reduce mean time to resolution by 30% and respond faster to sophisticated threats.
- Automate High-Volume Tasks: Autonomous agents handle intensive security tasks, freeing your team to focus on strategic priorities.
- Enhance Security Posture: Continuous AI-driven optimization ensures your defenses stay ahead of evolving threats.

- Agents:
  - Phishing Triage Agent
  - Alert Triage Agents for Data Loss Prevention and Insider Risk Management
  - Conditional Access Optimization Agent
  - Vulnerability Remediation Agent
  - Threat Intelligence Briefing Agent
  - and Agents from Partner Solutions (OneTrust, Aviatrix, BlueVoyant, Tanium, Fletch)



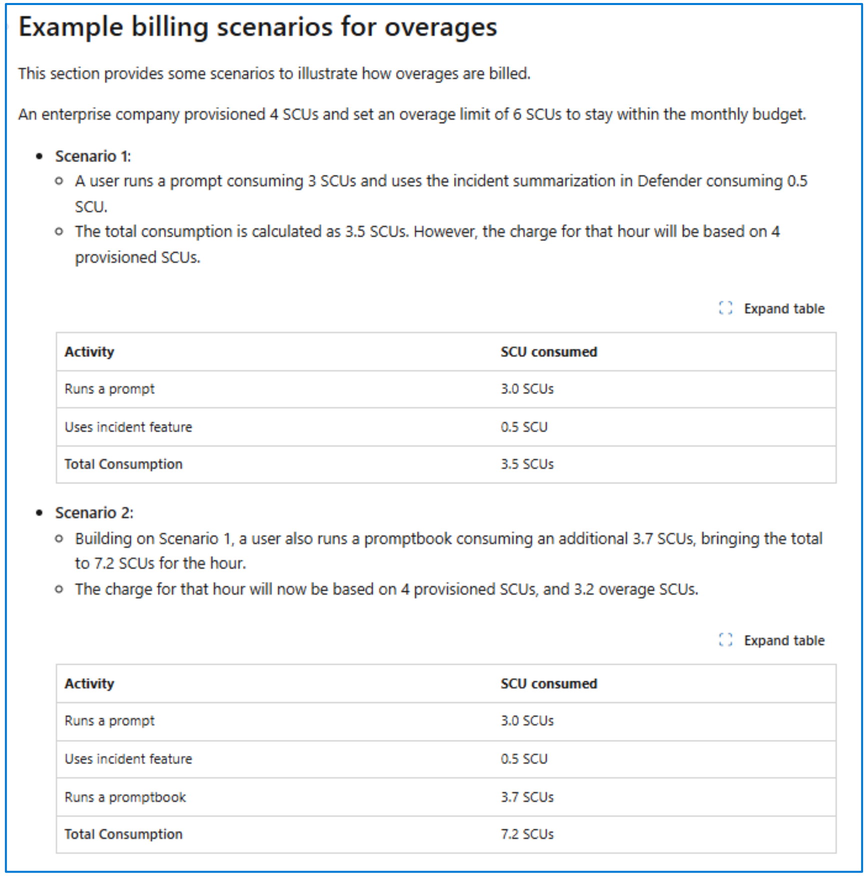
References:

- Automate cybersecurity at scale with Microsoft Security Copilot agents | Microsoft Community Hub
- Microsoft unveils Microsoft Security Copilot agents and new protections for AI | Microsoft Security Blog
- From Alerts to Action: The Impact of AI Agents in Security | LinkedIn

General Availability

Security Copilot overage SCUs

- Security Copilot operates on a provisioned and overage capacity. Provisioned capacity is billed by the hour while the overage capacity is billed on usage.
- You can flexibly provision Security Compute Units (SCUs) to accommodate regular workloads and adjust them anytime without long-term commitments.
- To manage unexpected demand spikes, you can set an overage amount to ensure that additional SCUs are available when initially provisioned units are depleted during unexpected workload spikes. Overage units are billed on-demand and can be set as unlimited or a maximum amount.
- This approach enables predictable billing while providing the flexibility to handle both regular and unexpected usage.



Example billing scenarios for overages

This section provides some scenarios to illustrate how overages are billed.

An enterprise company provisioned 4 SCUs and set an overage limit of 6 SCUs to stay within the monthly budget.

- **Scenario 1:**
  - A user runs a prompt consuming 3 SCUs and uses the incident summarization in Defender consuming 0.5 SCU.
  - The total consumption is calculated as 3.5 SCUs. However, the charge for that hour will be based on 4 provisioned SCUs.

Activity	SCU consumed
Runs a prompt	3.0 SCUs
Uses incident feature	0.5 SCU
Total Consumption	3.5 SCUs

- **Scenario 2:**
  - Building on Scenario 1, a user also runs a promptbook consuming an additional 3.7 SCUs, bringing the total to 7.2 SCUs for the hour.
  - The charge for that hour will now be based on 4 provisioned SCUs, and 3.2 overage SCUs.

Activity	SCU consumed
Runs a prompt	3.0 SCUs
Uses incident feature	0.5 SCU
Runs a promptbook	3.7 SCUs
Total Consumption	7.2 SCUs

References:

- [Manage security compute unit usage in Security Copilot | Microsoft Learn]
- [Microsoft Security Copilot - Pricing | Microsoft Azure]

Purview

Purview Updates

- Protect Teams meeting with Sensitivity label
  Use sensitivity labels to protect calendar items, Teams meetings, and chat

General Availability

- Data Security Posture Management for AI: Updates for Data Assessments and recommendations

Public Preview

- Microsoft Purview Compliance Portal: Policy Sync status on Purview Portal

Public Preview

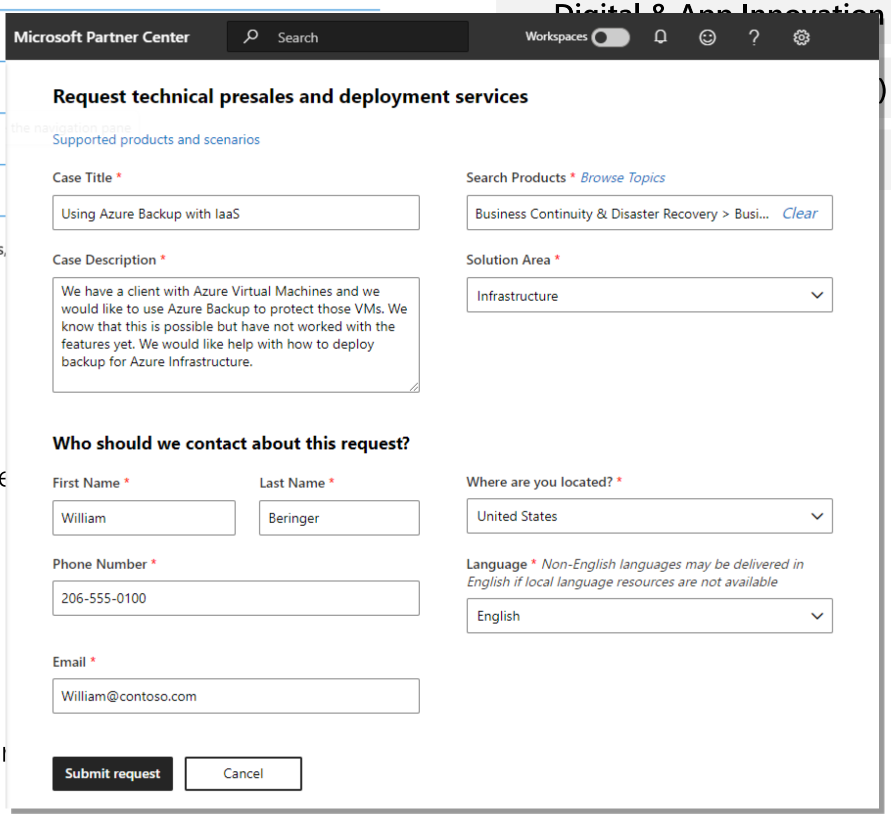
Leverage your MCAIPP benefits and engage TP&D Services

Technical presales and deployment services to help you deliver services and applications faster.

	Advisory hours	Technical sales preparation & deal enablement
Partner Launch Benefits	Not available	Not available
Partner Success Core Benefits	5	
Partner Success Expanded Benefits	10	
Solutions Partner	50	
Specialization / Expert*	50	

*Specialization and Expert MSP designation and TPD benefits shown are the same as, Partner designation benefits.

- Infrastructure (Azure)
- Modern Work
- Digital & App Innovation (Azure)
- Security
-)
- Business Applications
- ISV



Request technical presales and deployment services

Supported products and scenarios

Case Title *	Using Azure Backup with IaaS
Search Products * Browse Topics	Business Continuity & Disaster Recovery > Busi... Clear
Case Description *	We have a client with Azure Virtual Machines and we would like to use Azure Backup to protect those VMs. We know that this is possible but have not worked with the features yet. We would like help with how to deploy backup for Azure Infrastructure.
Solution Area *	Infrastructure

Who should we contact about this request?

First Name *	William
Last Name *	Beringer
Where are you located? *	United States
Phone Number *	206-555-0100
Language * *Non-English languages may be delivered in English if local language resources are not available*	English
Email *	William@contoso.com

Technical consultations scope:

- Delivered remotely
- Consultation service to help plan, build and grow partne technical capabilities
- Provides technical resources, recommendations and deliverables
- Focuses on common partner questions and technical scenarios
- Packaged as a Microsoft Cloud Partner Program advisor benefit

Examples

- Help analyze customer/partner architecture and how to respond with Microsoft capabilities
- Discuss product features, clarify doubts about technical capabilities
- Perform demos/PoCs of Microsoft products
- Provide best practices and recommendations
- Check usage scenarios:

Visit http://aka.ms/TPDMSForm and select 'Create a new TPD request' towards the top of the page, or log into your Partner Center dashboard and select the Benefits tile > Technical benefits.

Q&A

- Ask your questions

- Deep level and complex scenarios? Reach out to our team: https://aka.ms/TPDMSForm
- Or directly to:
  - ritrigue@microsoft.com
  - abarreiros@microsoft.com
  - daniela.magalhaes@microsoft.com
  - macardo@microsoft.com

Microsoft Security

Thank you!