Microsoft Azure

SMB Solution Assessments

SMB Assessment Desk

FY26 portfolio

SMB-Solution Assessment (SA)

Empower your customers and accelerate your business growth by delivering **a SA**—91% of opportunities convert into impactful projects, driving pipeline, elevating lead quality, and enabling you to lead successful security initiatives together.

Eligibility criteria: all customers are eligible

MCEM: Inspire and Design (Stage 2 of the customer sales stage)

Request an Assessment: Partner link, or OneAsk internal link

Why does program exist?

- Help customers to understand their cybersecurity risks
- Evaluate customer Security current state
- Identify gaps and path forward for remediation

How does the program work?

- Partner can nominate customers, or a customer can ask for an assessments thru centralized SMB Assessment Desk Solution Assessment Program (microsoft.com) OR
- Customers/Partners can apply for a Self-Service Assessment if <30 seats Solution Assessment Program (microsoft.com)
- Solution assessment specialist qualifies the opportunity and attach Partner

What are the program outcomes?

- Generate Pipe and increase velocity
- Qualify and rank potential leads
- Drive Security projects thru partners

SMB Assessments: Table of Contents

Click the images to open that section of this PPT

← SMB Program

FY26 SMB Assessment Desk | *Global capability with local touch*

One pages · Sample reports

Security
- Threat Protection
- Data Security
- Protect Cloud, AI Platforms
- Rapid Security
- Secure BVA

UPDATED

Scale assessments focused on Security maturity analysis, risk mitigation and value

Solution Play: Modernize SecOps with Unified Platform

Technology leveraged: CSAT

Cloud & AI Platforms
- Benchmark TCO
- Protect Cloud, AI Platforms

NEW

Drive AI, migration & modernization opportunities, via discovery of customer's environment & recommended mapping to Azure

Azure Security assessment focused on Defender for Cloud & Purview

Solution Play: Migrate and Modernize Your Estate; Protect Cloud AI Platform and Apps

Technology leveraged: Dr Migrate; CSAT

AI Business Solutions
- Secure AI Productivity
- Dark to Cloud
- Copilot Master Class

NEW

Helping customers secure their company data when using generative AI

Moving customers onto M365 Cloud

Moving Copilot customers into Chat adoption

Solution Play: Secure AI Productivity; Copilot and Agents at Work

Technology leveraged: CSAT

How to nominate

Microsoft Internal: OneAsk *, Azure Offer Navigator

Partners: Partner Nomination

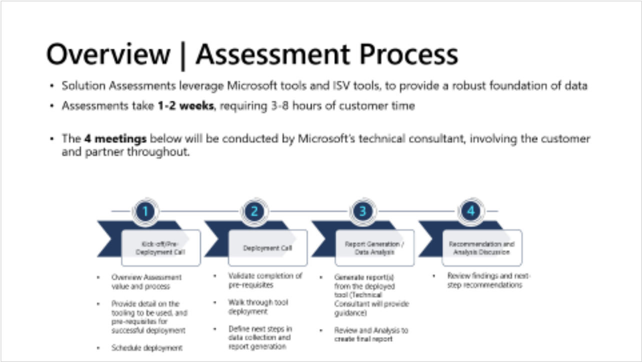
Customers: Customer Nomination, or Self-service Security assessment

*Azure Offer Navigator is the intake for Benchmark TCO only. OneAsk for all others.
Contacts: smbassessmenttriage@microsoft.com

Nomination Criteria	
All	1. MCEM – Stage 2 Inspire & Design 2. Customer pre-agreement on assessment 3. No previous assessment in the same TPID
Benchmark TCO	• > $VM
Azure Security	• Dark to Azure UPDATED
Threat Protection Data Security Rapid Security Secure BVA	• >30 seats
Secure AI Productivity Dark to Cloud	• >30 seats
Copilot Master Class	• >10 Copilot seats + >30 seats UPDATED

4

Assessment portfolio



Overview | Assessment Process

- Solution Assessments leverage Microsoft tools and ISV tools, to provide a robust foundation of data
- Assessments take **1-2 weeks**, requiring 3-8 hours of customer time
- The **4 meetings** below will be conducted by Microsoft's technical consultant, involving the customer and partner throughout.

1 Kick-off/Pre-Deployment Call
- Overview Assessment value and process
- Provide detail on the tooling to be used, and pre-requisites for successful deployment
- Schedule deployment

2 Deployment Call
- Validate completion of pre-requisites
- Walk through tool deployment
- Define next steps in data collection and report generation

3 Report Generation / Data Analysis
- Generate report(s) from the deployed tool (Technical Consultant will provide guidance)
- Review and Analysis to create final report

4 Recommendation and Analysis Discussion
- Review findings and next-step recommendations

Process

Microsoft

Nominate now!

https://www.microsoft.com/en-us/solutionassessments/register

Microsoft

How to nominate

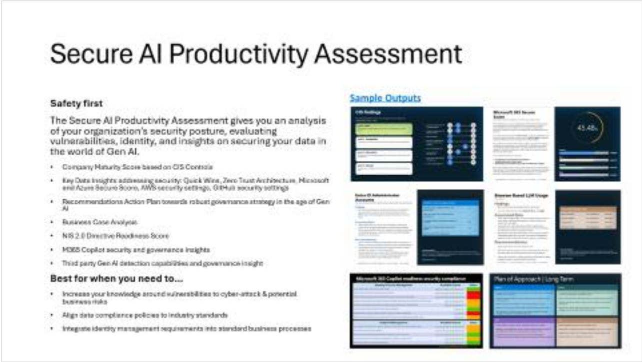
Self-Serve
- Free of charge
- Open to all customers
- Limited endpoints
- Non-curated
- Data-driven insights
- Scope: Email DNS, Microsoft Cloud Scan, AD Scan + Questionnaire

Self-Serve Cybersecurity

Deliverables
- Summary Report & Detailed Report
- Technical Data & Analysis
- Assessment Score, Microsoft & Azure Secure Score
- Urgent Actions
- Conclusion and Recommendations (focus on Business Premium, M365)

Next Steps in Process
- Customer share results with **Partner** for deployment of recommendations
- Partner nominates customer to a curated **Microsoft Solution Assessment**
- Partner and Customer review Final Recommendations from Security **Solution Assessment**

Rapid Security
Threat Protection
Data Security
Security BVA



Secure AI Productivity Assessment

Safety first

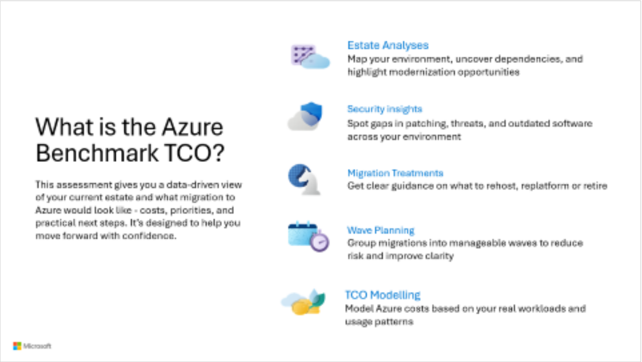
The Secure AI Productivity Assessment gives you an analysis of your organization's security posture, evaluating vulnerabilities, identity, and insights on securing your data in the world of Gen AI.

- Company Maturity Score based on CIS Controls
- Key Data Insights addressing security: Quick Wins, Zero Trust Architecture, Microsoft and Azure Secure Score, AWS security settings, GitHub security settings
- Recommendations Action Plan towards robust governance strategy in the age of Gen AI
- Business Case Analysis
- NIS 2.0 Directive Readiness Score
- M365 Copilot security and governance insights
- Third party Gen AI detection capabilities and governance insight

Best for when you need to…
- Increase your knowledge around vulnerabilities to cyber-attack & potential business risks
- Align data compliance policies to industry standards
- Integrate identity management requirements into standard business processes

Sample Outputs

Secure AI Productivity
Dark to Cloud
Copilot Master Class



What is the Azure Benchmark TCO?

This assessment gives you a data-driven view of your current estate and what migration to Azure would look like - costs, priorities, and practical next steps. It's designed to help you move forward with confidence.

Estate Analyses
Map your environment, uncover dependencies, and highlight modernization opportunities

Security insights
Spot gaps in patching, threats, and outdated software across your environment

Migration Treatments
Get clear guidance on what to rehost, replatform or retire

Wave Planning
Group migrations into manageable waves to reduce risk and improve clarity

TCO Modelling
Model Azure costs based on your real workloads and usage patterns

Microsoft

Azure Benchmark TCO
Azure Security

FY26 SMB Assessment Desk | *Global capability with local touch*

[One pagers] [Sample reports]

Microsoft Security **Security**	• Threat Protection • Data Security • Protect Cloud, AI Platforms • Rapid Security • Secure BVA UPDATED	Scale assessments focused on Security maturity analysis, risk mitigation and value	**Solution Play** Modernize SecOps with Unified Platform	**Technology leveraged:** CSAT
Cloud & AI Platforms	• Benchmark TCO • Protect Cloud, AI Platforms NEW	Drive AI, migration & modernization opportunities, via discovery of customer's environment & recommended mapping to Azure Azure Security assessment focused on Defender for Cloud & Purview	**Solution Play** Migrate and Modernize Your Estate Protect Cloud AI Platform and Apps	**Technology leveraged:** Dr Migrate CSAT
Copilot **AI Business Solutions**	• Secure AI Productivity • Dark to Cloud • Copilot Master Class NEW	Helping customers secure their company data when using generative AI Moving customers onto M365 Cloud Moving Copilot customers into Chat adoption	**Solution Play** Secure AI Productivity Copilot and Agents at Work	**Technology leveraged:** CSAT

How to nominate

Microsoft Internal
- OneAsk *
- Azure Offer Navigator

Partners
- Partner Nomination

Customers
- Customer Nomination, or
- Self-service Security assessment

*Azure Offer Navigator is the intake for Benchmark TCO only. OneAsk for all others.
Contacts: smbassessmenttriage@microsoft.com

Nomination Criteria	
All	1. MCEM – Stage 2 Inspire & Design 2. Customer pre-agreement on assessment 3. No previous assessment in the same TPID
Benchmark TCO	• > 5VM
Azure Security	• Dark to Azure UPDATED
Threat Protection Data Security Rapid Security Secure BVA	• >30 seats
Secure AI Productivity Dark to Cloud	• >30 seats
Copilot Master Class	• >10 Copilot seats + >30 seats UPDATED

What is a Solution Assessment?

Global program funded by Microsoft to help customers by providing in-depth insights and data-backed actionable recommendations for digital transformation projects, cloud migrations and optimizing IT investments

Technical insight

Delivers a deep understanding of the current state of the IT environment.

Security insight

High level Security insight based on real data from customer’s estate

Financial insight

Understand total cost of ownership and/or business value

Enable Pilot/POC

Prepare customer for pilot or POC with partner

Next steps

Clear guidance for customers on next steps based on Assessment results

Migration

Connect the customer to the

right resources who will then help customers in actual migration projects

Increasing partner profitability with SMB Desk

Growing topline business and reducing cost of sales

LEVERAGING DESK FOR PRESALES ASSESSMENTS

MICROSOFT SPONSORED 1ST/3RD PARTY TECHNOLOGY

ACCESS TO MICROSOFT SELLERS

ACCELERATED MIGRATION OPPORTUNITIES THROUGH QUALIFIED LEADS

Request an Assessment: Partner link, or OneAsk internal link

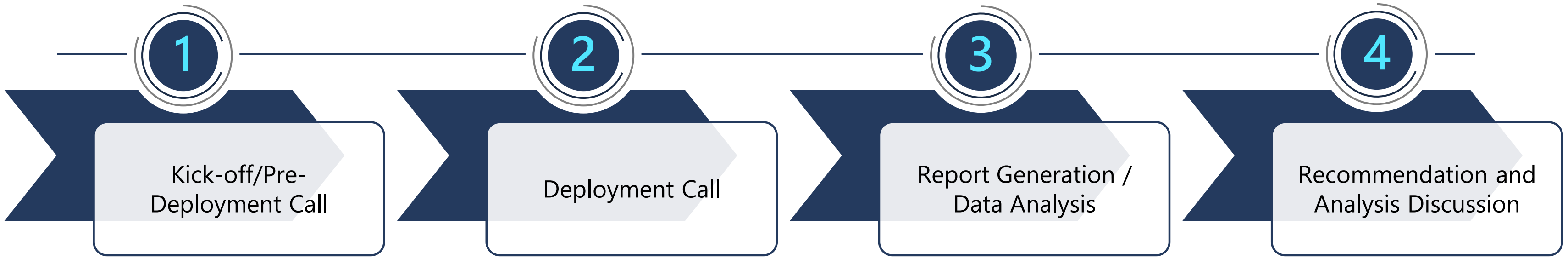
Languages supported

English | Deutsch | Français | Español | Italiano | Português | Polski | العربية (Arabic) | 日本語 (Japanese)

Overview | Assessment Process

- Solution Assessments leverage Microsoft tools and ISV tools, to provide a robust foundation of data
- Assessments take **1-2 weeks**, requiring 3-8 hours of customer time

- The **4 meetings** below will be conducted by Microsoft's technical consultant, involving the customer and partner throughout.



1 Kick-off/Pre-Deployment Call

- Overview Assessment value and process
- Provide detail on the tooling to be used, and pre-requisites for successful deployment
- Schedule deployment

2 Deployment Call

- Validate completion of pre-requisites
- Walk through tool deployment
- Define next steps in data collection and report generation

3 Report Generation / Data Analysis

- Generate report(s) from the deployed tool (Technical Consultant will provide guidance)
- Review and Analysis to create final report

4 Recommendation and Analysis Discussion

- Review findings and next-step recommendations

Microsoft

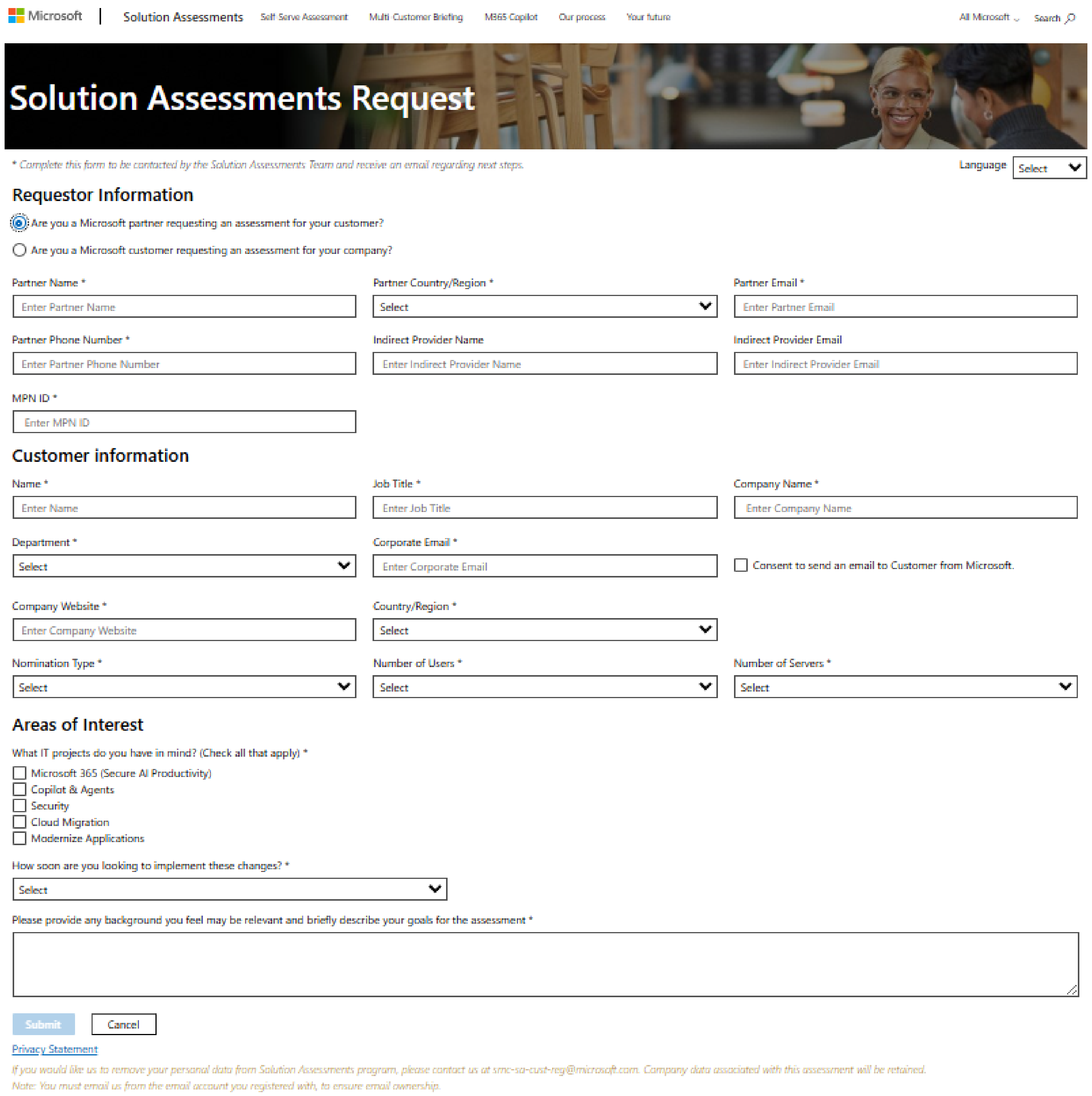
Nominate now!

https://www.microsoft.com/en-us/solutionassessments/register

Microsoft

Nominate now!

https://www.microsoft.com/en-us/solutionassessments/register



Solution Assessments Request

** Complete this form to be contacted by the Solution Assessments Team and receive an email regarding next steps.*

Language: Select

Requestor Information

● Are you a Microsoft partner requesting an assessment for your customer?

○ Are you a Microsoft customer requesting an assessment for your company?

Partner Name * Enter Partner Name	Partner Country/Region * Select	Partner Email * Enter Partner Email
Partner Phone Number * Enter Partner Phone Number	Indirect Provider Name Enter Indirect Provider Name	Indirect Provider Email Enter Indirect Provider Email
MPN ID * Enter MPN ID		

Customer information

Name * Enter Name	Job Title * Enter Job Title	Company Name * Enter Company Name
Department * Select	Corporate Email * Enter Corporate Email	□ Consent to send an email to Customer from Microsoft.
Company Website * Enter Company Website	Country/Region * Select	
Nomination Type * Select	Number of Users * Select	Number of Servers * Select

Areas of Interest

What IT projects do you have in mind? (Check all that apply) *

□ Microsoft 365 (Secure AI Productivity)
□ Copilot & Agents
□ Security
□ Cloud Migration
□ Modernize Applications

How soon are you looking to implement these changes? *

Select

Please provide any background you feel may be relevant and briefly describe your goals for the assessment *

Privacy Statement

If you would like us to remove your personal data from Solution Assessments program, please contact us at smc-sa-cust-reg@microsoft.com. Company data associated with this assessment will be retained.

Note: You must email us from the email account you registered with, to ensure email ownership.

Microsoft

What is the Azure Benchmark TCO?

This assessment gives you a data-driven view of your current estate and what migration to Azure would look like - costs, priorities, and practical next steps. It's designed to help you move forward with confidence.

Estate Analyses

Map your environment, uncover dependencies, and highlight modernization opportunities

Security insights

Spot gaps in patching, threats, and outdated software across your environment

Migration Treatments

Get clear guidance on what to rehost, replatform or retire

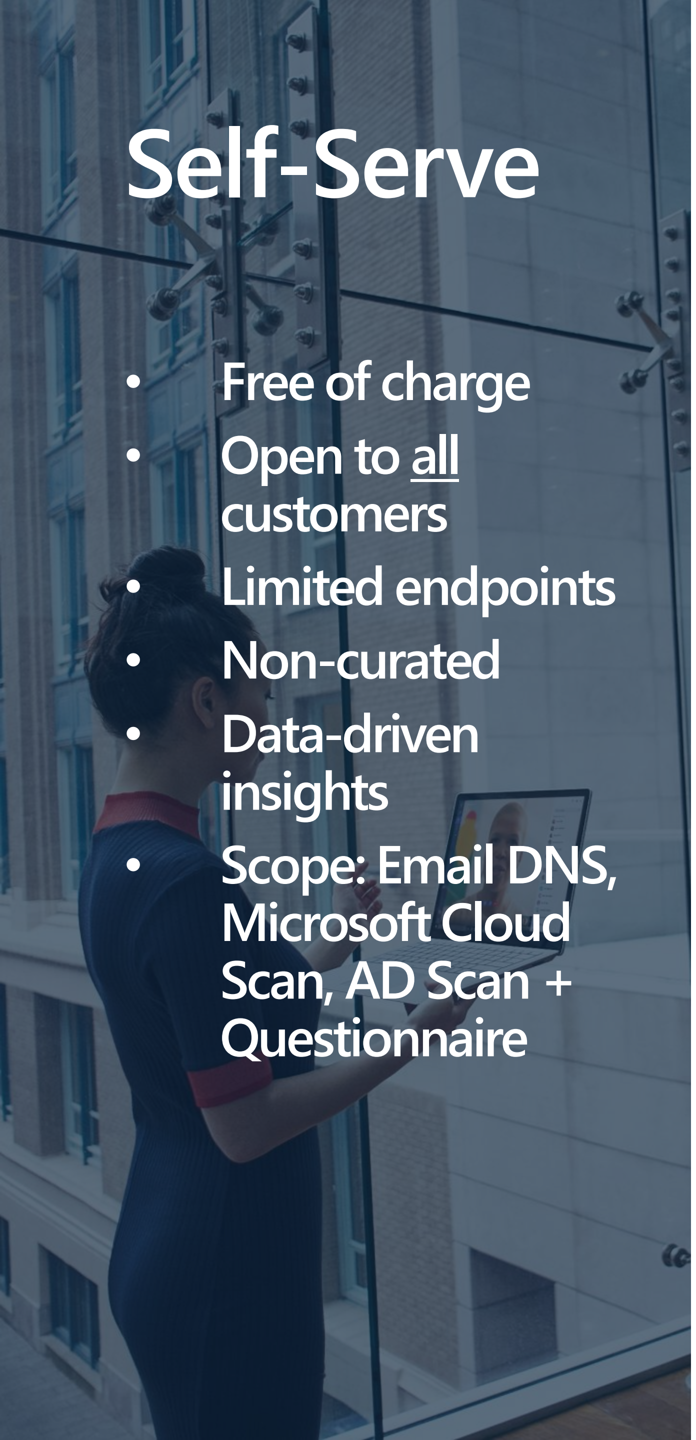
Wave Planning

Group migrations into manageable waves to reduce risk and improve clarity

TCO Modelling

Model Azure costs based on your real workloads and usage patterns

Microsoft



Self-Serve

- Free of charge
- Open to all customers
- Limited endpoints
- Non-curated
- Data-driven insights
- Scope: Email DNS, Microsoft Cloud Scan, AD Scan + Questionnaire

Self-Serve Cybersecurity

Deliverables

- Summary Report & Detailed Report
- Technical Data & Analysis
- Assessment Score, Microsoft & Azure Secure Score
- Urgent Actions
- Conclusion and Recommendations (focus on Business Premium, M365)

Next Steps in Process

- Customer share results with **Partner** for deployment of recommendations
- Partner nominates customer to a curated **Microsoft Solution Assessment**
- Partner and Customer review Final Recommendations from Security **Solution Assessment**

Rapid Security Assessment

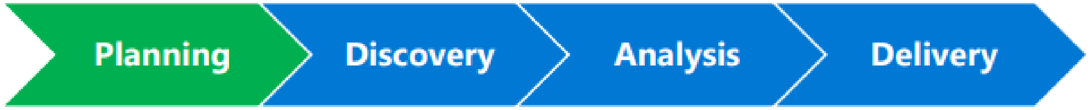
Provides organizations with a review of their security posture by evaluating & addressing immediate vulnerabilities, identifying unmanaged devices, analyzing current software deployment & usage, discussing policies and controls to reduce risk, and delivering remediation recommendations to help establish processes for cyber-risk reduction in the cloud.

Assessment Details

- Tool Used: Questionnaire based
- **Timeline:** 1 to 2 weeks.
- **Customer profile:** Customers looking for more in-depth and customized financial analysis of the economic impact of Microsoft 365.

Data Scope

- Review Modern Work questionnaire via remote session(s)
- Understand current Microsoft/Office 365 licensing portfolio
- Identify current Microsoft solutions and 3rd party products in use



Expectations & prerequisites

Tool Deployment

Deliverables

Close & Handoff

Sample Outputs

CIS findings

Level 1 - Basic

Level 2 - Standardised

Level 3 - Rationalised

Level 4 - Dynamic

Microsoft 365 Secure Score

45.48%

Entra ID Administrator Accounts

Findings

Associated Risks

Recommendations

Browser Based LLM Usage

Findings

Associated Risks

Recommendations

Microsoft 365 Copilot readiness security compliance

Identity & Access Management | Available license | Status

Endpoint Management | Available license | Status

Plan of Approach | Long Term

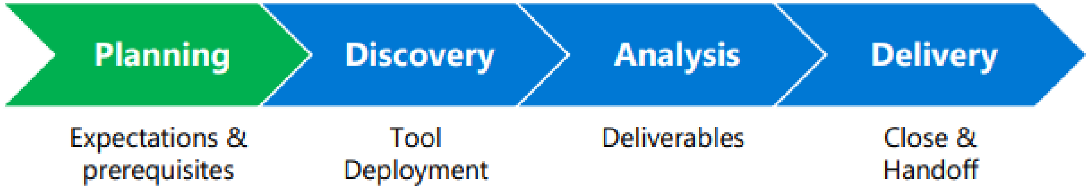
Threat Protection Assessment

Provides organizations with a comprehensive look at their both on-premise and on-cloud security posture and providing recommendations to mitigate risks and implement solutions required. Get insights how to modernize operations, reduce risk, and protect the entire attack surface.

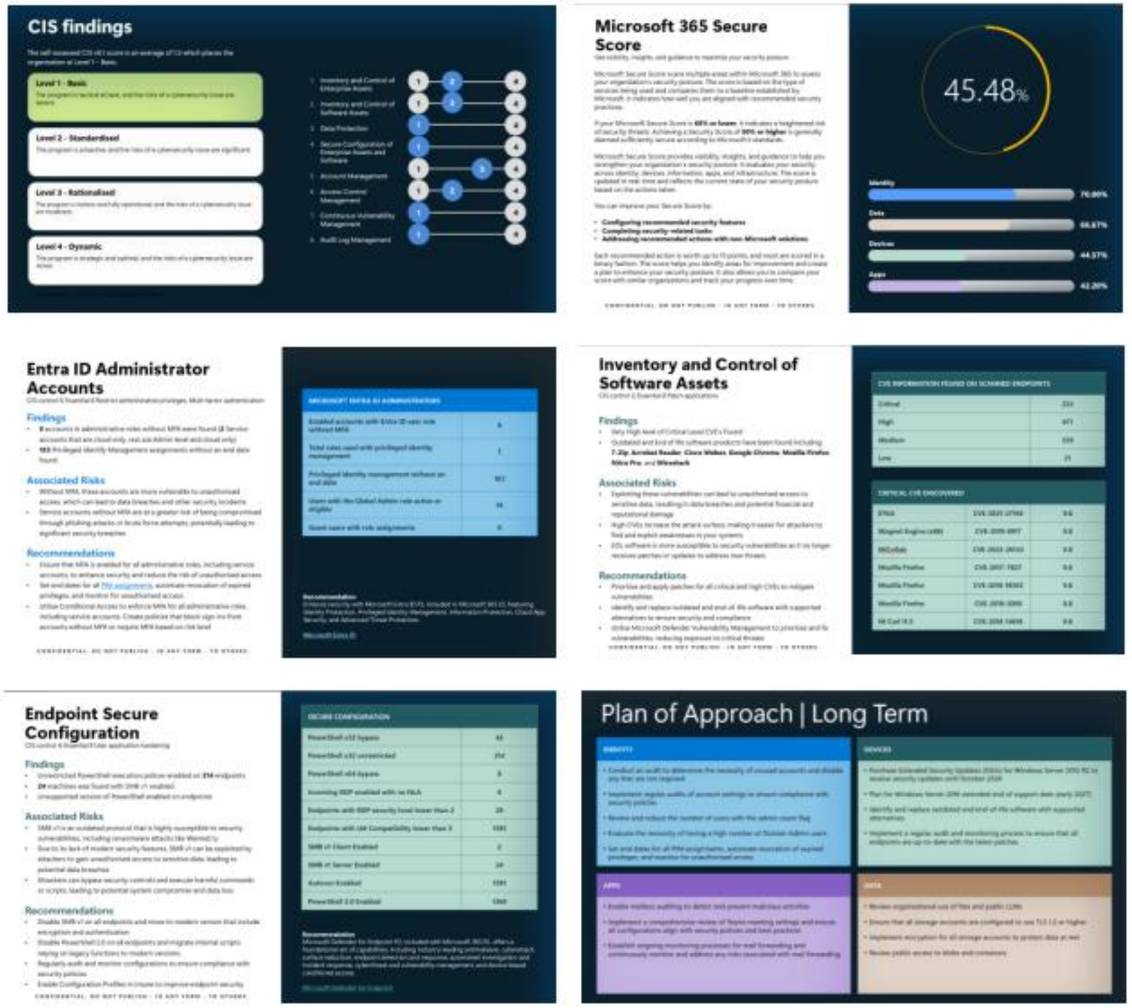
- Company Maturity Score based on CIS Controls
- Key Data Insights addressing security: Quick Wins, Zero Trust Architecture, Microsoft and Azure Secure Score, AWS security settings, GitHub security settings
- Recommended Action Plan for hybrid infrastructures
- Business Case Analysis
- NIS 2.0 Directive Readiness Score
- Detailed insights about on-premise environment security as well as on-cloud security management

Navigate confidently with expert help along the way

Our experts will guide you through our detailed four-phased approach, from identifying your business goals to implementing specific action items.



Sample Outputs



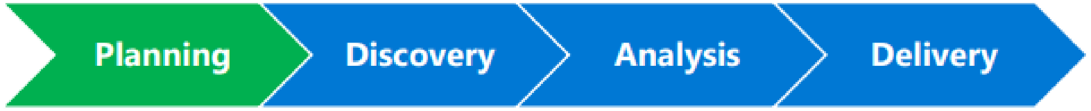
Protect Cloud, AI Platforms & Apps Assessment

Provides organizations with a review focusing on cloud infrastructures, identity, data, and application protection to address emerging threat vectors. Get insights to help you unify security and governance across the full cloud and AI app lifecycle

- Company Maturity Score based on CIS Controls
- Key Data Insights addressing security: Quick Wins, Zero Trust Architecture, Microsoft and Azure Secure Score, AWS security settings, GitHub security settings
- Recommended Action Plan for cloud infrastructures
- Business Case Analysis
- Detailed scanning metrics towards on-cloud security governance observations with recommendations

Navigate confidently with expert help along the way

Our experts will guide you through our detailed four-phased approach, from identifying your business goals to implementing specific action items.



Planning – Expectations & prerequisites

Discovery – Tool Deployment

Analysis – Deliverables

Delivery – Close & Handoff

Sample Outputs

CIS findings

Level 1 - Basic

Level 2 - Standardised

Level 3 - Rationalised

Level 4 - Dynamic

Microsoft 365 Secure Score

45.48%

Identity

Data

Devices

Apps

Azure Policy

Findings

Associated Risks

Recommendations

Multi-Cloud

Findings

Associated Risks

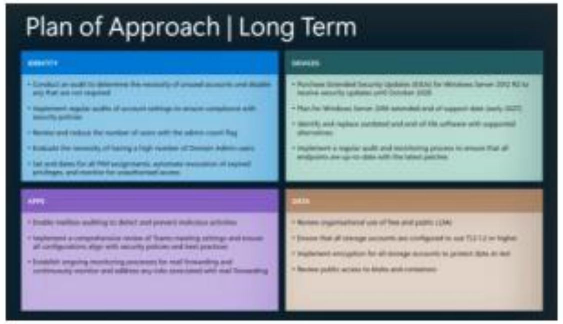
Recommendations

Cloud Storage Accounts

Findings

Associated Risks

Recommendations



Plan of Approach | Long Term

Security Business Value Assessment

- The Security Business Value Assessment offers organizations customized insight into the potential financial savings and benefits of consolidating on the industry leading solutions native to Microsoft 365. Impact areas include estimated costs of licensing, implementation, and training, as well as benefits, such as vendor consolidation, risk mitigation, and sustainability
- **Assessment Details**
- • Tool Used: Questionnaire based
- • **Timeline:** 1 to 2 weeks.
- • **Customer profile:** Customers looking for more in-depth and customized financial analysis of the economic impact of Microsoft 365.
- **Data Scope**
- • Review Modern Work questionnaire via remote session(s)
- • Understand current Microsoft/Office 365 licensing portfolio
- • Identify current Microsoft solutions and 3rd party products in use

Sample Outputs

Cost estimation

3 Yr Breakdown of Estimated Costs

Benefit analysis

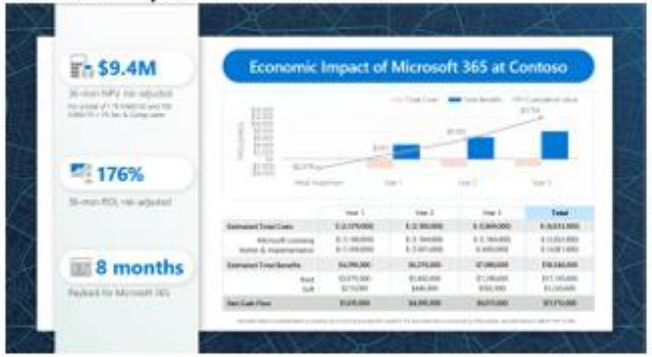
3 Yr Breakdown of Estimated Benefits

Consolidation opportunities

Eliminate Redundant Solutions

$63

Review impact of investment

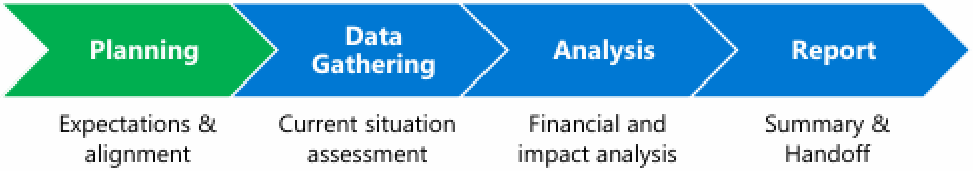


$9.4M

176%

8 months

Economic Impact of Microsoft 365 at Contoso



Secure AI Productivity Assessment

Safety first

The Secure AI Productivity Assessment gives you an analysis of your organization’s security posture, evaluating vulnerabilities, identity, and insights on securing your data in the world of Gen AI.

- Company Maturity Score based on CIS Controls
- Key Data Insights addressing security: Quick Wins, Zero Trust Architecture, Microsoft and Azure Secure Score, AWS security settings, GitHub security settings
- Recommendations Action Plan towards robust governance strategy in the age of Gen AI
- Business Case Analysis
- NIS 2.0 Directive Readiness Score
- M365 Copilot security and governance insights
- Third party Gen AI detection capabilities and governance insight

Best for when you need to...

- Increase your knowledge around vulnerabilities to cyber-attack & potential business risks
- Align data compliance policies to industry standards
- Integrate identity management requirements into standard business processes

Sample Outputs

CIS findings

Level 1 - Basic

Level 2 - Standardised

Level 3 - Rationalised

Level 4 - Dynamic

Microsoft 365 Secure Score

45.48%

Entra ID Administrator Accounts

Findings

Associated Risks

Recommendations

Browser Based LLM Usage

Findings

Associated Risks

Recommendations

Microsoft 365 Copilot readiness security compliance

Identity & Access Management | Available license | Status

Endpoint Management | Available license | Status

Plan of Approach | Long Term

Copilot Master Class

- Smarter ways to be more productive, creative, and connected with Copilot
- Enhanced creativity and productivity with your own AI companion
- Work smarter, be more productive, boost creativity, and stay connected to the people and things in your life with Copilot—an AI companion that works everywhere you do and intelligently adapts to your needs
- -
- Copilot seamlessly integrates AI-powered assistance into your work, enhancing productivity with real-time suggestions and streamlining complex tasks while keeping your data safe.

With the Copilot Master Class, we take a four-phase approach:

1. Discover

Understand Copilot Chat, its UI, its “skills”, and other capabilities.

2. Enable

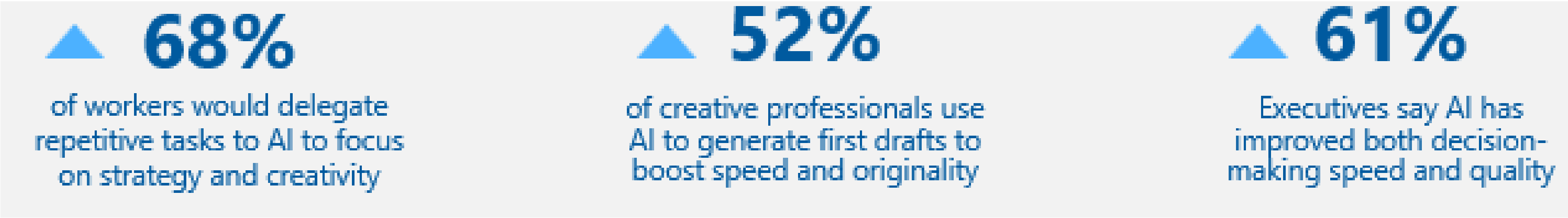
Learn the prompting best practices and Copilot’s Prompt Gallery.

3. Accelerate

Explore Copilot use cases throughout your organization.

4. Extend

Learn how Agents can extend Copilot capabilities.



▲ 68%

of workers would delegate repetitive tasks to AI to focus on strategy and creativity

▲ 52%

of creative professionals use AI to generate first drafts to boost speed and originality

▲ 61%

Executives say AI has improved both decision-making speed and quality

** Extracted from Forrester report “Prediction 2025: Atay at the Forefront of an AI-Driven World”*

Dark to Cloud solution play security assessment

The Security Assessment gives you an analysis of the organization’s security posture, evaluating vulnerabilities, identity, and insights on securing your hybrid IT environment.

- Company Maturity Score based on CIS Controls
- Key Data Insights addressing security: Quick Wins, Zero Trust Architecture, On premise insights in applications , AD, Microsoft on premise usage, Google usage and security insights .
- Recommendations Action Plan towards Improving and modernizing on prem architecture and security
- Business Case Analysis
- Copilot options
- Third party possible vendor consolidation

Hero Offering:
M365 Business Premium/E3/E5, Azure Security

Navigate confidently with expert help along the way

Our experts will guide you through our detailed four-phased approach, from identifying your business goals to implementing specific action items.

Planning

Identify business goals and objectives

Data collection

Provide a clear picture of the current data estate

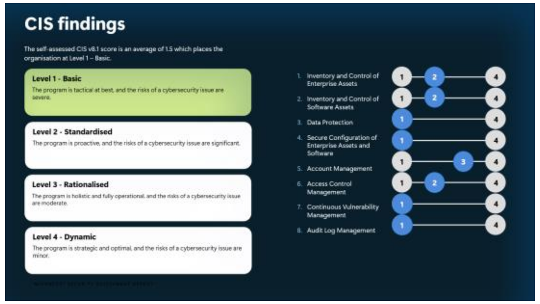
Analysis

Optimize investments with Security infrastructure analysis

Action

Implement a security mitigation action plan specific to your environment

Sample Outputs



CIS findings

The self-assessed CIS v8.1 score is an average of 1.5 which places the organisation at Level 1 – Basic.

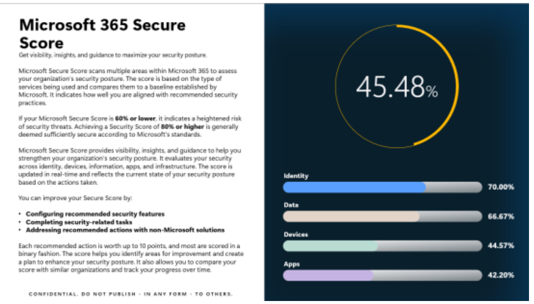
Level 1 - Basic
The program is tactical at best, and the risks of a cybersecurity issue are severe.

Level 2 - Standardised
The program is proactive, and the risks of a cybersecurity issue are significant.

Level 3 - Rationalised
The program is holistic and fully operational, and the risks of a cybersecurity issue are moderate.

Level 4 - Dynamic
The program is strategic and optimal, and the risks of a cybersecurity issue are minor.

1. Inventory and Control of Enterprise Assets
2. Inventory and Control of Software Assets
3. Data Protection
4. Secure Configuration of Enterprise Assets and Software
5. Account Management
6. Access Control Management
7. Continuous Vulnerability Management
8. Audit Log Management



Microsoft 365 Secure Score

Get visibility, insights, and guidance to maximize your security posture.

Microsoft Secure Score scans multiple areas within Microsoft 365 to assess your organization's security posture. The score is based on the type of services being used and compares them to a baseline established by Microsoft. It indicates how well you are aligned with recommended security practices.

If your Microsoft Secure Score is **60% or lower**, it indicates a heightened risk of security threats. Achieving a Security Score of **80% or higher** is generally deemed sufficiently secure according to Microsoft's standards.

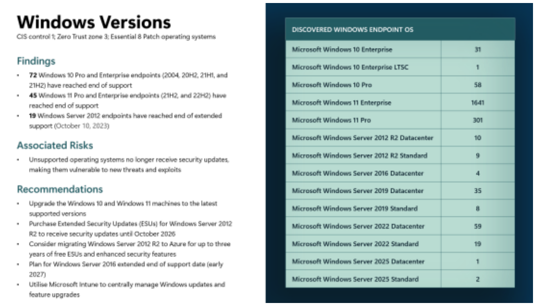
Microsoft Secure Score provides visibility, insights, and guidance to help you strengthen your organization's security posture. It evaluates your security across identity, devices, information, apps, and infrastructure. The score is updated in real-time and reflects the current state of your security posture based on the actions taken.

You can improve your Secure Score by:

- **Configuring recommended security features**
- **Completing security-related tasks**
- **Addressing recommended actions with non-Microsoft solutions**

Each recommended action is worth up to 10 points, and most are scored in a binary fashion. The score helps you identify areas for improvement and create a plan to enhance your security posture. It also allows you to compare your score with similar organizations and track your progress over time.

CONFIDENTIAL. DO NOT PUBLISH - IN ANY FORM - TO OTHERS.



Windows Versions

CIS control 1; Zero Trust zone 3; Essential 8 Patch operating systems

Findings

- **72** Windows 10 Pro and Enterprise endpoints (2004, 20H2, 21H1, and 21H2) have reached end of support
- **45** Windows 11 Pro and Enterprise endpoints (21H2, and 22H2) have reached end of support
- **19** Windows Server 2012 endpoints have reached end of extended support (October 10, 2023)

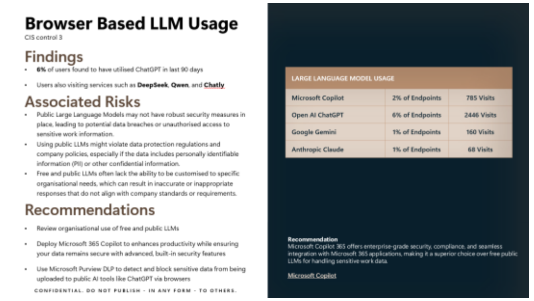
Associated Risks

- Unsupported operating systems no longer receive security updates, making them vulnerable to new threats and exploits

Recommendations

- Upgrade the Windows 10 and Windows 11 machines to the latest supported versions
- Purchase Extended Security Updates (ESUs) for Windows Server 2012 R2 to receive security updates until October 2026
- Consider migrating Windows Server 2012 R2 to Azure for up to three years of free ESUs and enhanced security features
- Plan for Windows Server 2016 extended end of support date (early 2027)
- Utilise Microsoft Intune to centrally manage Windows updates and feature upgrades

DISCOVERED WINDOWS ENDPOINT OS	
Microsoft Windows 10 Enterprise	31
Microsoft Windows 10 Enterprise LTSC	1
Microsoft Windows 10 Pro	58
Microsoft Windows 11 Enterprise	1641
Microsoft Windows 11 Pro	301
Microsoft Windows Server 2012 R2 Datacenter	10
Microsoft Windows Server 2012 R2 Standard	9
Microsoft Windows Server 2016 Datacenter	4
Microsoft Windows Server 2019 Datacenter	35
Microsoft Windows Server 2019 Standard	8
Microsoft Windows Server 2022 Datacenter	59
Microsoft Windows Server 2022 Standard	19
Microsoft Windows Server 2025 Datacenter	1
Microsoft Windows Server 2025 Standard	2



Browser Based LLM Usage

CIS control 3

Findings

- **6%** of users found to have utilised ChatGPT in last 90 days
- Users also visiting services such as **DeepSeek**, **Qwen**, and **Chatly**

Associated Risks

- Public Large Language Models may not have robust security measures in place, leading to potential data breaches or unauthorised access to sensitive work information.
- Using public LLMs might violate data protection regulations and company policies, especially if the data includes personally identifiable information (PII) or other confidential information.
- Free and public LLMs often lack the ability to be customised to specific organisational needs, which can result in inaccurate or inappropriate responses that do not align with company standards or requirements.

Recommendations

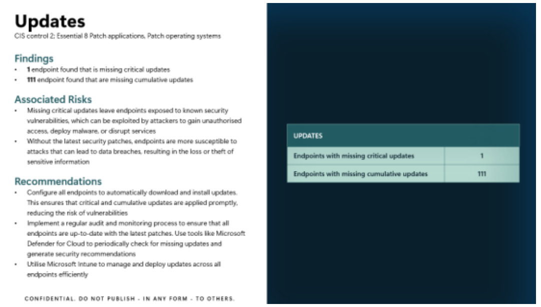
- Review organisational use of free and public LLMs
- Deploy Microsoft 365 Copilot to enhances productivity while ensuring your data remains secure with advanced, built-in security features
- Use Microsoft Purview DLP to detect and block sensitive data from being uploaded to public AI tools like ChatGPT via browsers

CONFIDENTIAL. DO NOT PUBLISH - IN ANY FORM - TO OTHERS.

LARGE LANGUAGE MODEL USAGE		
Microsoft Copilot	2% of Endpoints	785 Visits
Open AI ChatGPT	6% of Endpoints	2446 Visits
Google Gemini	1% of Endpoints	160 Visits
Anthropic Claude	1% of Endpoints	68 Visits

Recommendation
Microsoft Copilot 365 offers enterprise-grade security, compliance, and seamless integration with Microsoft 365 applications, making it a superior choice over free public LLMs for handling sensitive work data.

Microsoft Copilot



Updates

CIS control 2; Essential 8 Patch applications, Patch operating systems

Findings

- **1** endpoint found that is missing critical updates
- **111** endpoint found that are missing cumulative updates

Associated Risks

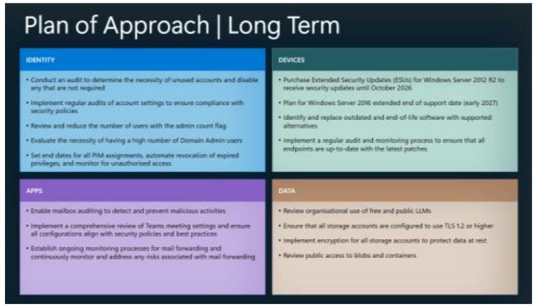
- Missing critical updates leave endpoints exposed to known security vulnerabilities, which can be exploited by attackers to gain unauthorised access, deploy malware, or disrupt services
- Without the latest security patches, endpoints are more susceptible to attacks that can lead to data breaches, resulting in the loss or theft of sensitive information

Recommendations

- Configure all endpoints to automatically download and install updates. This ensures that critical and cumulative updates are applied promptly, reducing the risk of vulnerabilities
- Implement a regular audit and monitoring process to ensure that all endpoints are up-to-date with the latest patches. Use tools like Microsoft Defender for Cloud to periodically check for missing updates and generate security recommendations
- Utilise Microsoft Intune to manage and deploy updates across all endpoints efficiently

CONFIDENTIAL. DO NOT PUBLISH - IN ANY FORM - TO OTHERS.

UPDATES	
Endpoints with missing critical updates	1
Endpoints with missing cumulative updates	111



Plan of Approach | Long Term

IDENTITY

- Conduct an audit to determine the necessity of unused accounts and disable any that are not required
- Implement regular audits of account settings to ensure compliance with security policies
- Review and reduce the number of users with the admin count flag
- Evaluate the necessity of having a high number of Domain Admin users
- Set end dates for all PIM assignments, automate revocation of expired privileges, and monitor for unauthorised access

DEVICES

- Purchase Extended Security Updates (ESUs) for Windows Server 2012 R2 to receive security updates until October 2026
- Plan for Windows Server 2016 extended end of support date (early 2027)
- Identify and replace outdated and end-of-life software with supported alternatives
- Implement a regular audit and monitoring process to ensure that all endpoints are up-to-date with the latest patches

APPS

- Enable mailbox auditing to detect and prevent malicious activities
- Implement a comprehensive review of Teams meeting settings and ensure all configurations align with security policies and best practices
- Establish ongoing monitoring processes for mail forwarding and continuously monitor and address any risks associated with mail forwarding

DATA

- Review organisational use of free and public LLMs
- Ensure that all storage accounts are configured to use TLS 1.2 or higher
- Implement encryption for all storage accounts to protect data at rest
- Review public access to blobs and containers

Microsoft

Nominate now!

https://www.microsoft.com/en-us/solutionassessments/register

Microsoft