global micro

Microsoft 365 Security & Compliance

Secure Productivity
Copilot Readiness with
ISO 27001 and NIS2 Compliance

Copilot for M365 can open exciting new capabilities but it can also expose new vulnerabilities

Copilot for M365 can help your business to harness the power of AI in day-to-day work.

But the breadth of this technology can expose hidden vulnerabilities in your existing security and compliance set up.

70%

of workers would delegate as much as possible to AI to lessen their workloads.

77%

of businesses reported a breach to their AI in the last year.

For example...

If an employee asked Copilot for a piece of information that was restricted to them on a permissions level (such as salary information), it might refuse.

However, Copilot may inadvertently return this information by searching for and returning other unsecured files that contain this information.
See example ↲

To use Copilot securely means making sure all your security settings are in order across users, devices, networks, files, applications, and infrastructure.

Organizations need a way to use the sophisticated security features of Microsoft 365

Microsoft 365 has sophisticated security features to help organizations use Copilot securely.

.

But with **over 2,500 different security settings, how do you verify that your settings** meet the required standard for safe integration of Copilot?

And **how do you maintain these settings** over time as regulation changes, without retaining a large expert security team?

Global Micro provides a way for organizations to solve this problem quickly and simply

Global Micro offer a way to simplify your journey to secure productivity and Copilot readiness.

We do this by using a **proven security framework**—aligned with CIS benchmarks and ISO Compliance Standards—to help you **quickly establish an ultra-secure, Copilot - ready, Microsoft 365 foundation**.

And by **harnessing automated deployment**, we can **make sure your security settings meet the required standards**, right off the bat, and with minimal hassle.

Secure Productivity and Copilot Readiness with Global Micro

Simplify security implementation

Automate security deployment and maintenance across your entire security stack.

Ensure compliance with CIS, NIS2 and ISO standards

Quickly analyze endpoints and automate compliance across your entire environment.

Simplify monitoring and maintenance

Automatically deploy over 2,500 security settings and benefit from automatic patches and updates.

Adopt AI responsibly

Get release management and DevOps to help you deploy responsibly and maintain control.

From a secure environment to Copilot readiness in less than 3 months

PLAN 1

Deploy a Secure M365 Foundation

We help you to assess your security needs and deploy a robust security foundation within your M365 environment.

2–4 weeks

PLAN 2

Ensure Compliant Endpoints

We use automation to help you quickly achieve and maintain compliance across your connected Microsoft 365 endpoints.

4–6 weeks

PLAN 3

Get the business Copilot Ready

We prepare your organization for AI by aligning the organization with advanced security and data governance measures.

6–8 weeks

Next steps

ISO 27001

Achieve ISO 27001:2022 Certification and NIS 2 Compliance within 12 months

ISO 27001: 2022 Controls

Implement ISO 27001 Controls

We help you document and implement your Organizational (37), People (8), Physical (14), and Technical (34) Controls.

6-8 months

Stage 1 Audit

Complete the Stage 1 Audit

We will prepare the evidence and manage your Stage 1 audit.

1 month

Stage 2 Audit and Certification

Complete the Stage 2 Audit

We will prepare the evidence and manage your Stage 2 audit to ensure you achieve ISO 27001:2022 Certification.

3 months

Next steps

Annual Audits

PLAN 1

Deploy a secure Microsoft 365 Foundation

Deploy Microsoft Office, Apps for Business, AvePoint, and Microsoft Defender with pre-set security and compliance settings to run with a strong security posture **right out of the gate**.

INCLUDES

- Initial Assessment
- Security Configuration
- User Education and Training

Assessment and discovery of weaknesses that pose the most urgent and highest risk to your business.

A complete set of prevention, protection, and response capabilities to thwart sophisticated cyberattacks through **Microsoft Defender for Office 365 and Microsoft Entra ID**.

Deploy Backup as a Service, Document and Test Restore procedures.

Microsoft Exchange Online, Teams, Onedrive and SharePoint of data migration (where required).

Hybrid identity deployment (where required): **Entra ID Connect and Entra ID**.

Connect Health sync between on-premises Active Directory and Entra ID.

Deployment of the CIS Microsoft 365 Foundation Security Benchmark: Deployment of **Code Two** Email Signatures

Automate and streamline the process of investigating and responding to threats and sophisticated cyberattacks.

Train end-users and IT personnel about the impact of security measures and on proper usage of all configurations and settings.

Example screenshots

PLAN 2

Ensure compliant endpoints

Automate more than 2,500 settings across endpoints and endpoint management systems (such as Intune) as well as remediation and compliance documentation. Ensure compliance in line with Centre for Internet Security (CIS) benchmarks.

INCLUDES

Endpoint Analysis (using CIS framework)

Remediation Strategies

Compliance Documentation Automation

Automate access-control decisions for accessing cloud apps, based on conditions with **Microsoft Entra ID Conditional Access**.

Provide time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on critical resources with **Microsoft Privileged Identity Access Management**.

Implement policies to configure and manage file elevation requests using **Microsoft Endpoint Privilege Management**.

Discover weaknesses that pose the most urgent and highest risk to your business and prioritize and remediate software vulnerabilities and misconfigurations with **Microsoft Defender for Business**.

Simplify app management by distributing and updating apps from your private app store through **Microsoft Intune**.
Remotely manage users and devices including devices owned by your organization and personally owned devices.

Deployment of the following Security Benchmarks:
CIS Microsoft 365 Foundation + CIS Microsoft Intune for Windows + CIS Microsoft Intune for Office + CIS Apple iOS and iPadOS for Intune + CIS Google Chrome + CIS Microsoft Edge + Android Enterprise.

Example screenshots

PLAN 3

Get your business Copilot-ready

Regularly review and manage user access rights, ensuring that only necessary permissions are granted.

Streamline access rights management, ensuring that users have appropriate entitlements for their roles.

INCLUDES

- Zero Trust Architecture Deployment
- Microsoft 365 Data Loss Prevention Implementation
- Data Classification and Management
- Purview Implementation (Compliance Manager)

Implement Data Loss Prevention for Exchange Online, Sharepoint and Onedrive Endpoint DLP with **Microsoft E5 Information Protection and Governance**.

Gain the capability to do regular **Microsoft Entra ID P2 Access Reviews** of access rights to ensure only the necessary permissions are granted.

Deploy **Microsoft Entra's Entitlement Management** feature across our organization. The objective is to streamline the process of managing access rights, ensuring that users have appropriate entitlements for their roles. This will improve operational efficiency and security by reducing unnecessary access and potential risks.

Implement **Microsoft Purview** sensitivity labels and Cognni auto-labelling to map and classify critical unregulated information assets.

Example screenshots

We are experts in small and medium clients with strict regulatory needs

We deliver state-of-the-art security solutions specifically designed for SMCs. Our solutions have been **tested and trusted by 1,200+ customers across EMEA.**

Our local teams provide specialized planning, implementation, and managed service support to help you extend and augment your resources — **without time and costs going out of control.**

Why Global Micro for Secure Productivity and Copilot Readiness

On average, customers who adopted Global Micro's complete 365 Security & Compliance solution **reached a Secure Score of 75+** and are **proven to be ready for optimum usage of Copilot**.

29+
Years' expertise

1200+
customers across EMEA

4x
Faster deployment than industry average

50K+
seamless migrations

Appendix:

Visualization of our solution

APPENDIX

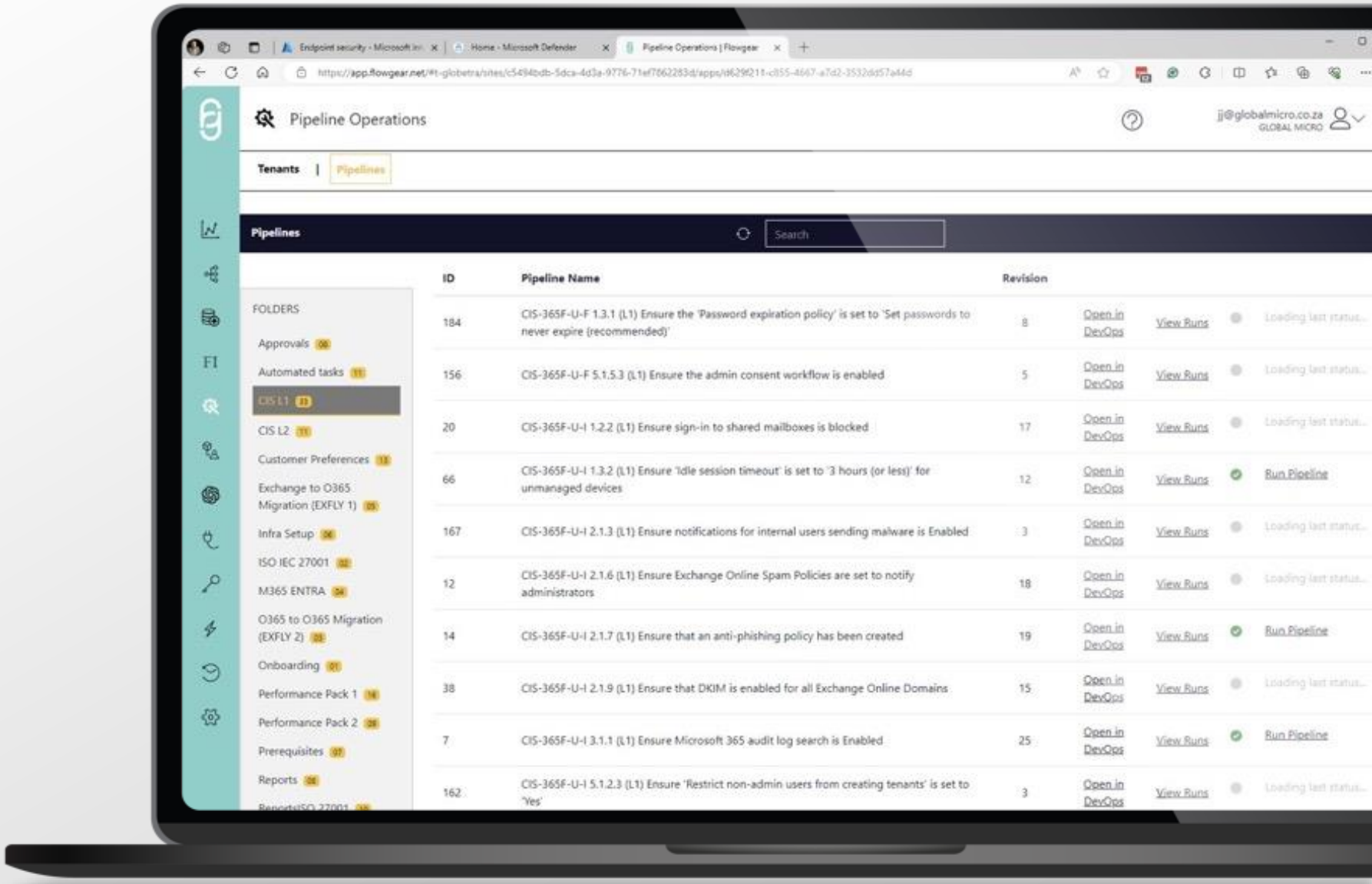
Phase 1:

Deploy a secure Microsoft 365 Foundation

global micro

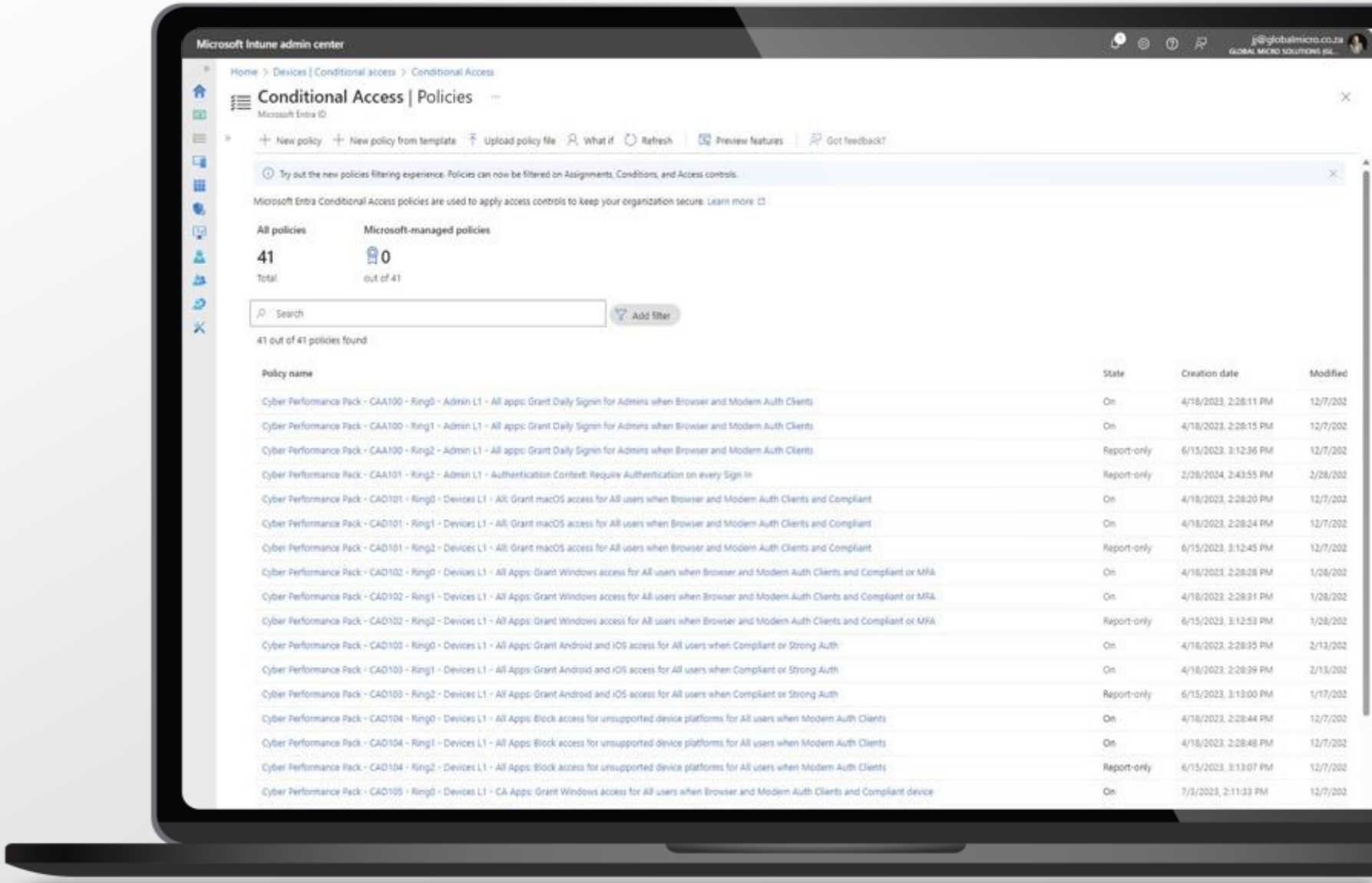
DevOps Frontend

We have built our own front end to Azure DevOps to support ISO20000 Service Management Compliance.



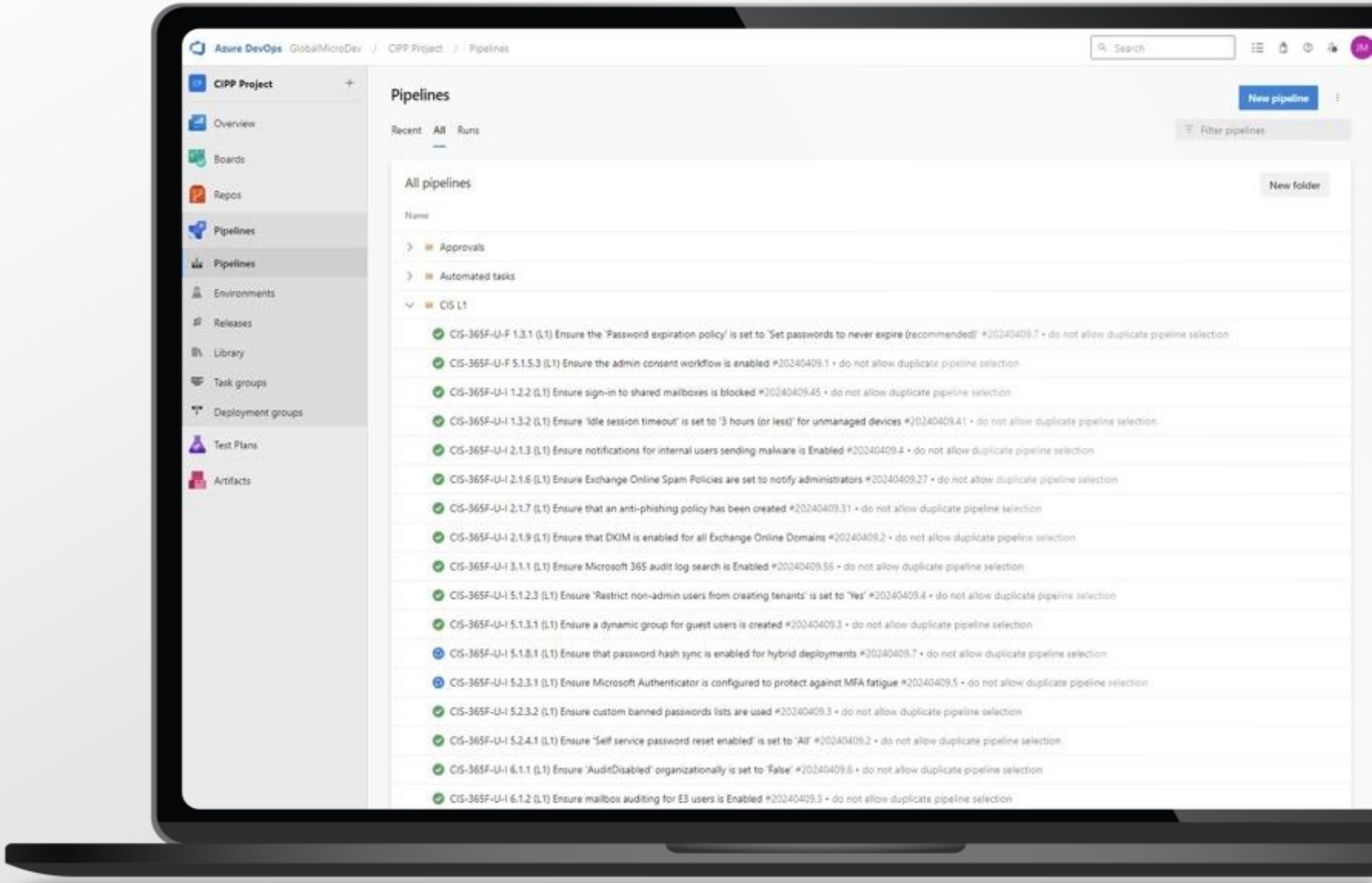
Conditional Access

41 Conditional Access Policies support multiple ring deployments and Zero Trust



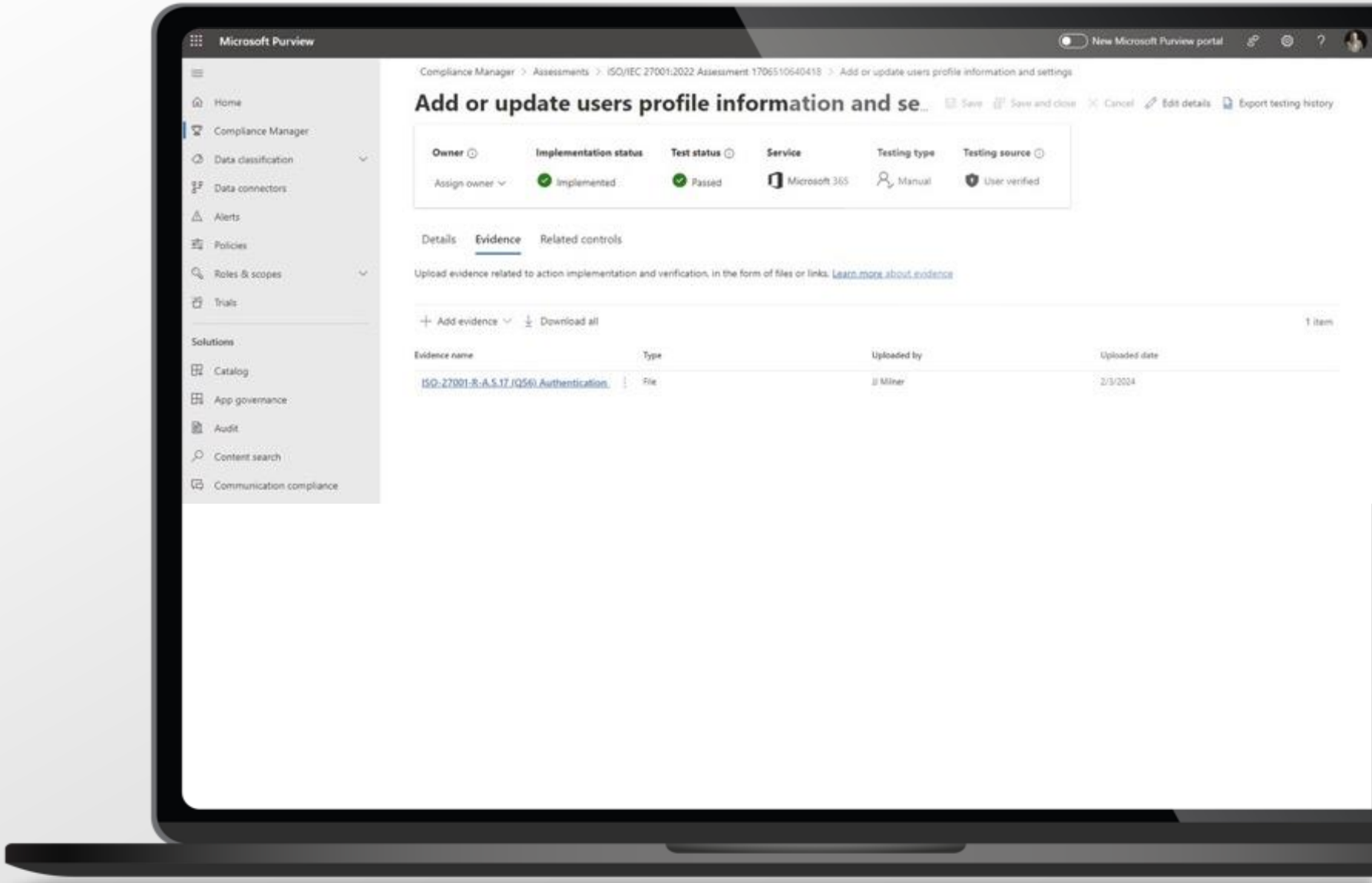
CIS Policies

CIS Policies and Standards are maintained using Azure DevOps.



Compliance Manager

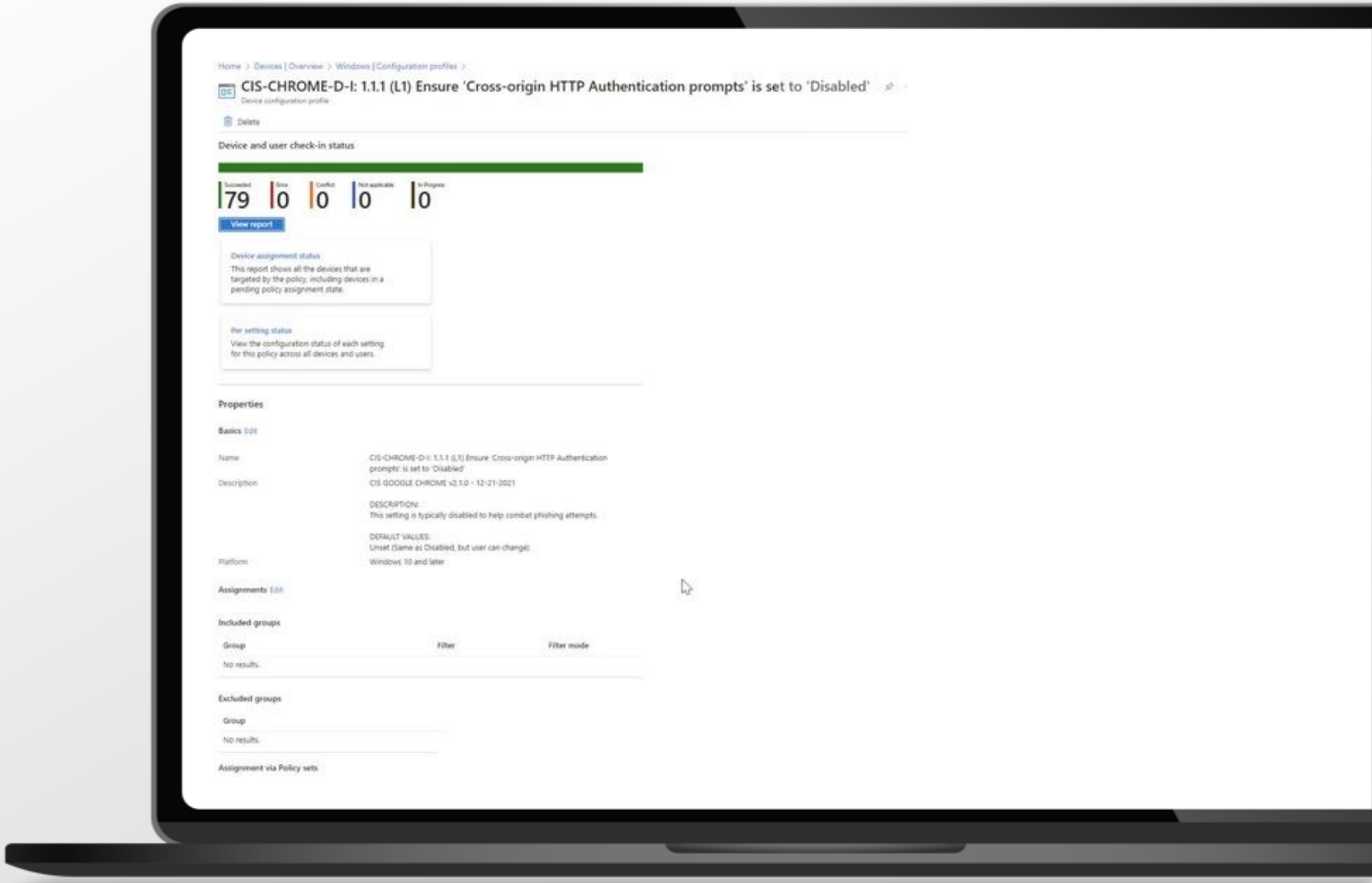
All evidence is also uploaded to Microsoft Purview Compliance Manager.



global micro

Granular Policy Management

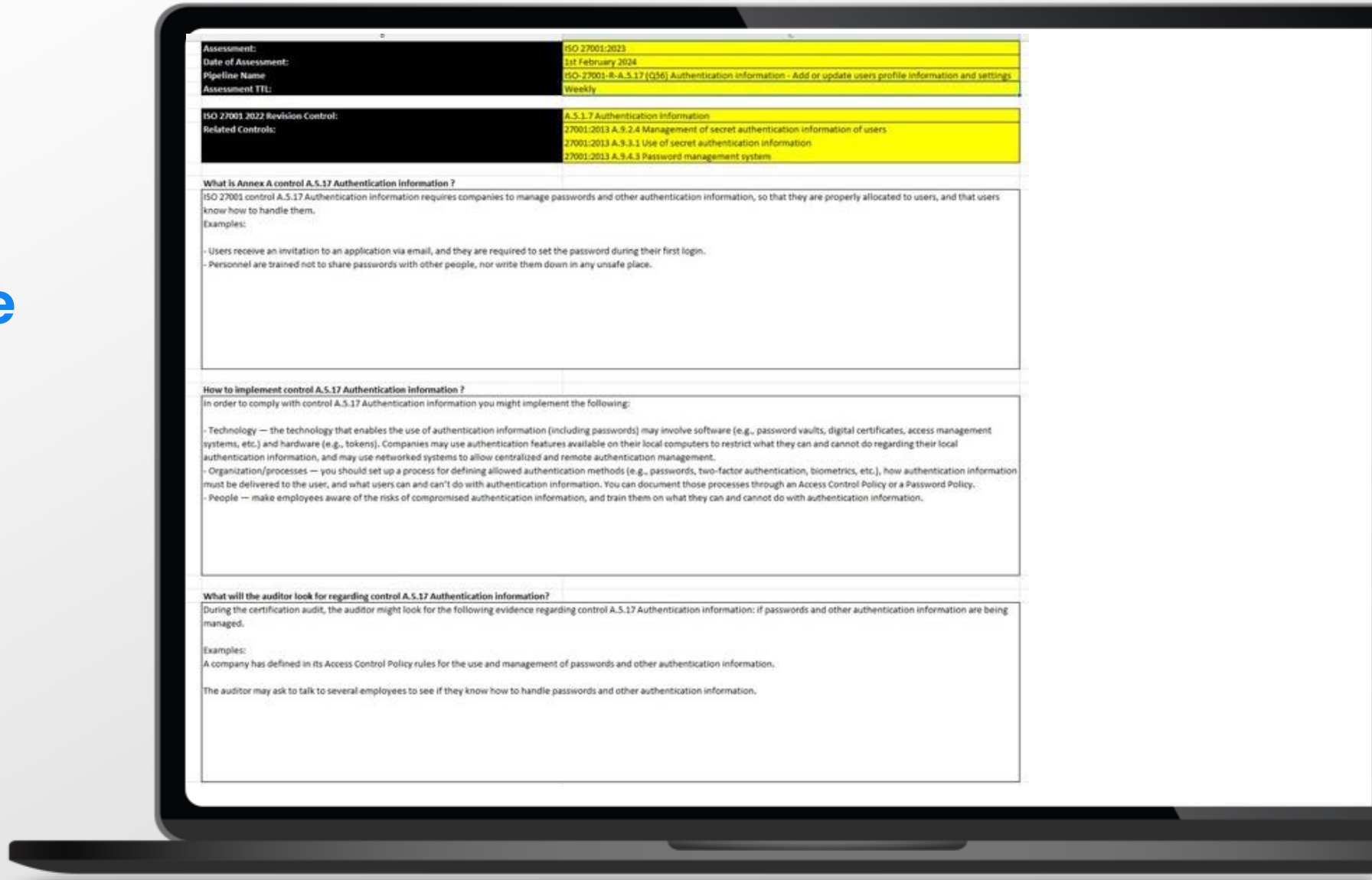
Policies include a description that mirrors the source CIS documentation, including default values.



Example of ISO27001 Evidence

SO report coverage is dependent on which components of Plan 1, 2 and 3 have been deployed.

115 Reports are generated when Plan 3 and all professional services engagements are complete.



Assessment:	ISO 27001:2023
Date of Assessment:	1st February 2024
Pipeline Name	ISO-27001-R-A.5.17 (Q56) Authentication information - Add or update users profile information and settings
Assessment TTL:	Weekly
ISO 27001 2022 Revision Control:	A.5.1.7 Authentication information
Related Controls:	27001:2013 A.9.2.4 Management of secret authentication information of users 27001:2013 A.9.3.1 Use of secret authentication information 27001:2013 A.9.4.3 Password management system

What is Annex A control A.5.17 Authentication information ?

ISO 27001 control A.5.17 Authentication information requires companies to manage passwords and other authentication information, so that they are properly allocated to users, and that users know how to handle them.
Examples:

- Users receive an invitation to an application via email, and they are required to set the password during their first login.
- Personnel are trained not to share passwords with other people, nor write them down in any unsafe place.

How to implement control A.5.17 Authentication information ?

In order to comply with control A.5.17 Authentication information you might implement the following:

- Technology — the technology that enables the use of authentication information (including passwords) may involve software (e.g., password vaults, digital certificates, access management systems, etc.) and hardware (e.g., tokens). Companies may use authentication features available on their local computers to restrict what they can and cannot do regarding their local authentication information, and may use networked systems to allow centralized and remote authentication management.
- Organization/processes — you should set up a process for defining allowed authentication methods (e.g., passwords, two-factor authentication, biometrics, etc.), how authentication information must be delivered to the user, and what users can and can't do with authentication information. You can document those processes through an Access Control Policy or a Password Policy.
- People — make employees aware of the risks of compromised authentication information, and train them on what they can and cannot do with authentication information.

What will the auditor look for regarding control A.5.17 Authentication information?

During the certification audit, the auditor might look for the following evidence regarding control A.5.17 Authentication information: if passwords and other authentication information are being managed.

Examples:
A company has defined in its Access Control Policy rules for the use and management of passwords and other authentication information.

The auditor may ask to talk to several employees to see if they know how to handle passwords and other authentication information.

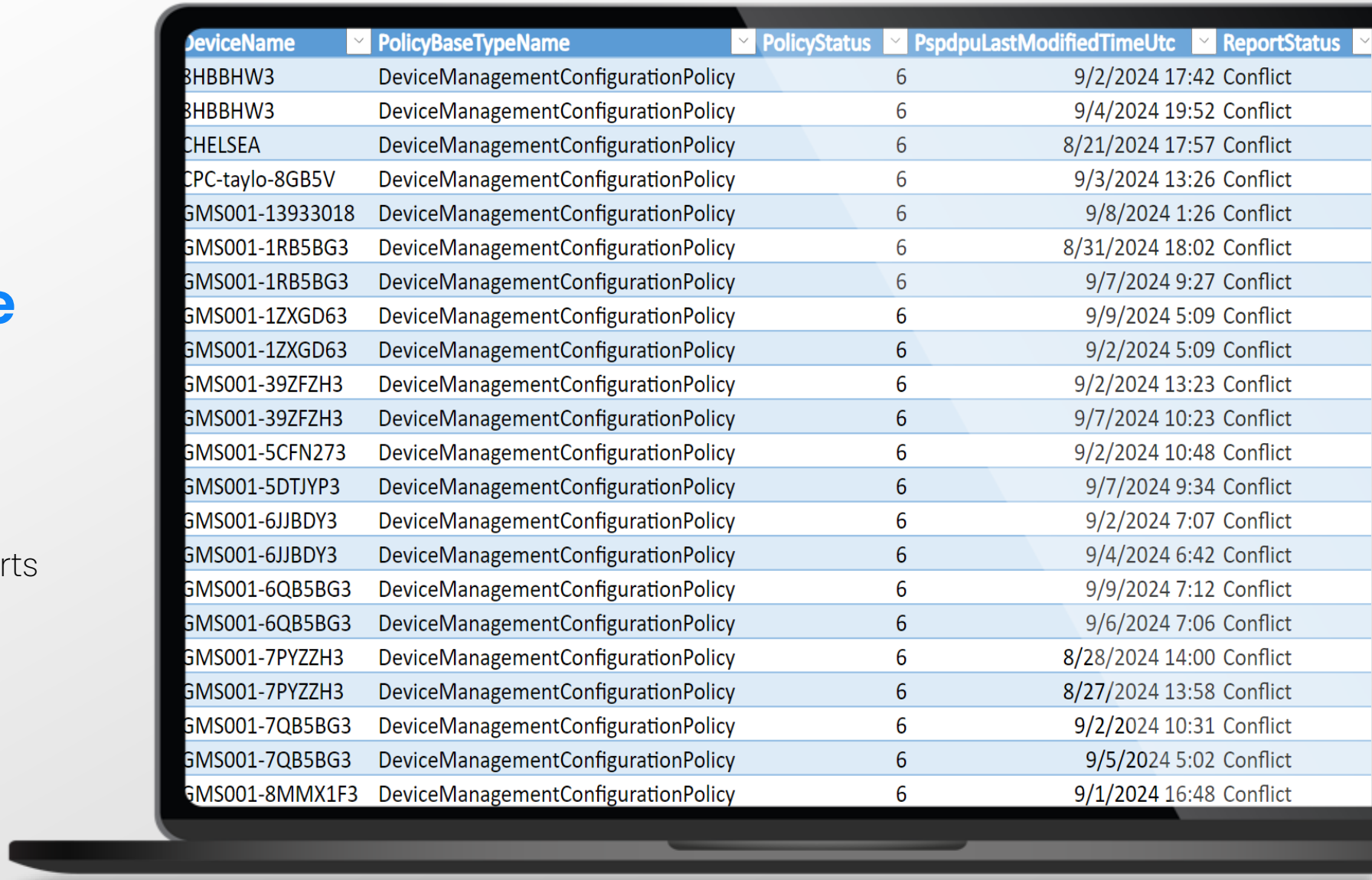
APPENDIX

global micro

Example of ISO27001 Evidence

All ISO Reports include evidence in Microsoft Excel Format

Scheduled DevOps pipelines open alerts for items in the reports which need to be resolved

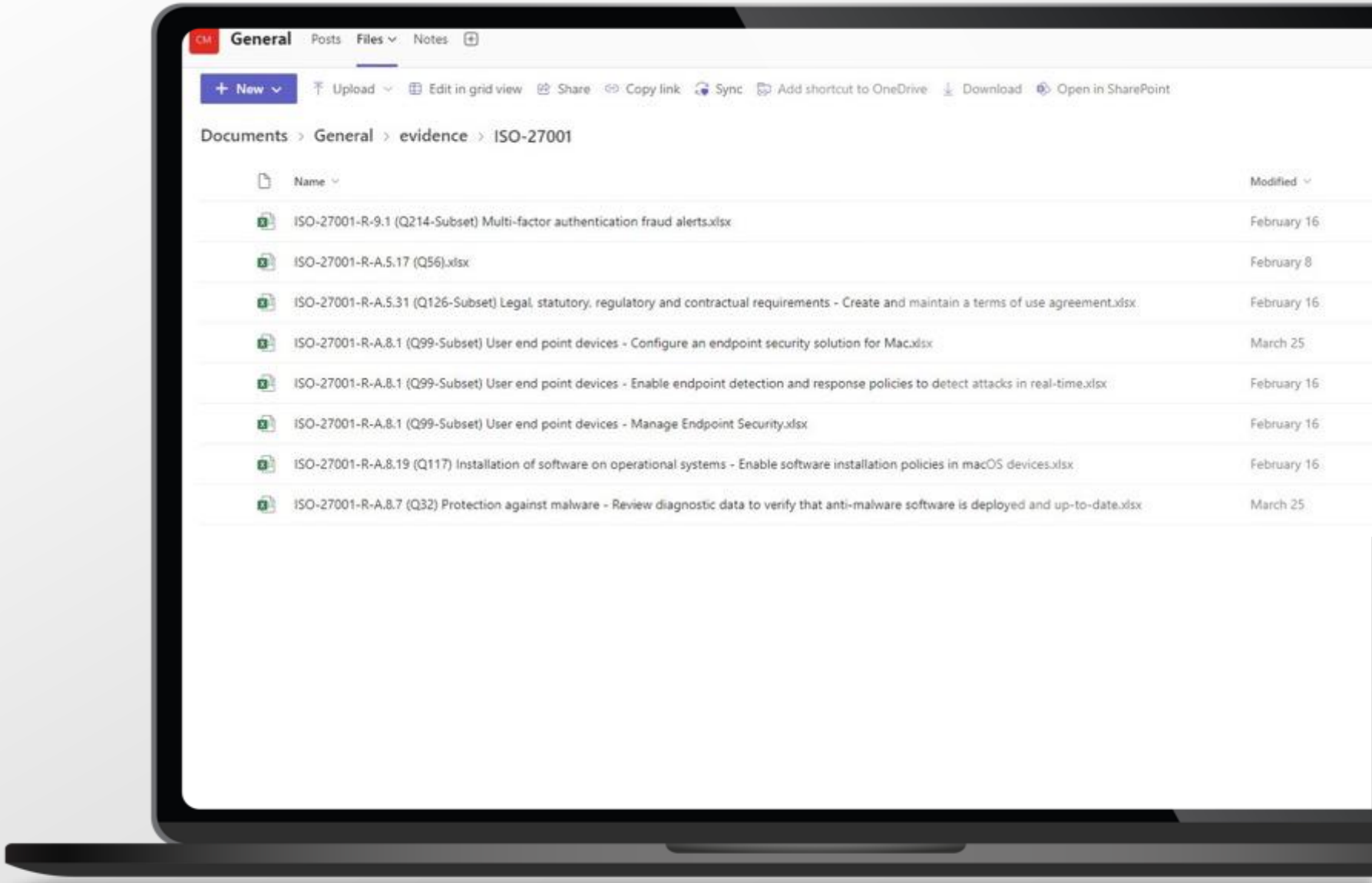


DeviceName	PolicyBaseTypeName	PolicyStatus	PspdpuLastModifiedTimeUtc	ReportStatus
3HBBHW3	DeviceManagementConfigurationPolicy	6	9/2/2024 17:42	Conflict
3HBBHW3	DeviceManagementConfigurationPolicy	6	9/4/2024 19:52	Conflict
CHELSEA	DeviceManagementConfigurationPolicy	6	8/21/2024 17:57	Conflict
CPC-taylo-8GB5V	DeviceManagementConfigurationPolicy	6	9/3/2024 13:26	Conflict
GMS001-13933018	DeviceManagementConfigurationPolicy	6	9/8/2024 1:26	Conflict
GMS001-1RB5BG3	DeviceManagementConfigurationPolicy	6	8/31/2024 18:02	Conflict
GMS001-1RB5BG3	DeviceManagementConfigurationPolicy	6	9/7/2024 9:27	Conflict
GMS001-1ZXGD63	DeviceManagementConfigurationPolicy	6	9/9/2024 5:09	Conflict
GMS001-1ZXGD63	DeviceManagementConfigurationPolicy	6	9/2/2024 5:09	Conflict
GMS001-39ZFZH3	DeviceManagementConfigurationPolicy	6	9/2/2024 13:23	Conflict
GMS001-39ZFZH3	DeviceManagementConfigurationPolicy	6	9/7/2024 10:23	Conflict
GMS001-5CFN273	DeviceManagementConfigurationPolicy	6	9/2/2024 10:48	Conflict
GMS001-5DTJYP3	DeviceManagementConfigurationPolicy	6	9/7/2024 9:34	Conflict
GMS001-6JJBDY3	DeviceManagementConfigurationPolicy	6	9/2/2024 7:07	Conflict
GMS001-6JJBDY3	DeviceManagementConfigurationPolicy	6	9/4/2024 6:42	Conflict
GMS001-6QB5BG3	DeviceManagementConfigurationPolicy	6	9/9/2024 7:12	Conflict
GMS001-6QB5BG3	DeviceManagementConfigurationPolicy	6	9/6/2024 7:06	Conflict
GMS001-7PYZZH3	DeviceManagementConfigurationPolicy	6	8/28/2024 14:00	Conflict
GMS001-7PYZZH3	DeviceManagementConfigurationPolicy	6	8/27/2024 13:58	Conflict
GMS001-7QB5BG3	DeviceManagementConfigurationPolicy	6	9/2/2024 10:31	Conflict
GMS001-7QB5BG3	DeviceManagementConfigurationPolicy	6	9/5/2024 5:02	Conflict
GMS001-8MMX1F3	DeviceManagementConfigurationPolicy	6	9/1/2024 16:48	Conflict

global micro

Compliance Manager Teams Site for all ISO 27001 Evidence

115 Reports are generated when Plan 3 and all professional services engagements are complete.



APPENDIX

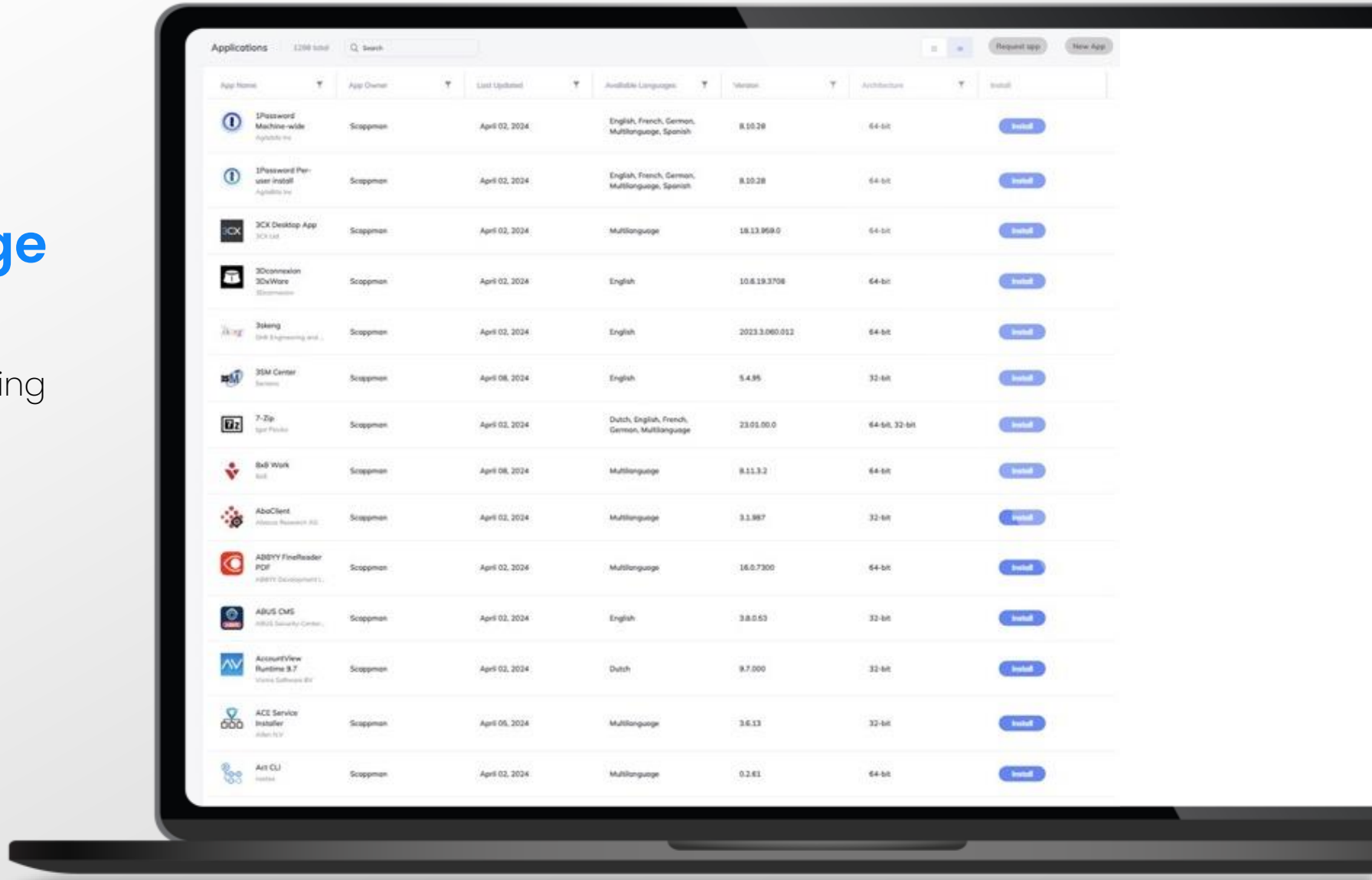
Phase 2:

Ensure compliant endpoints

global micro

Application Package Management

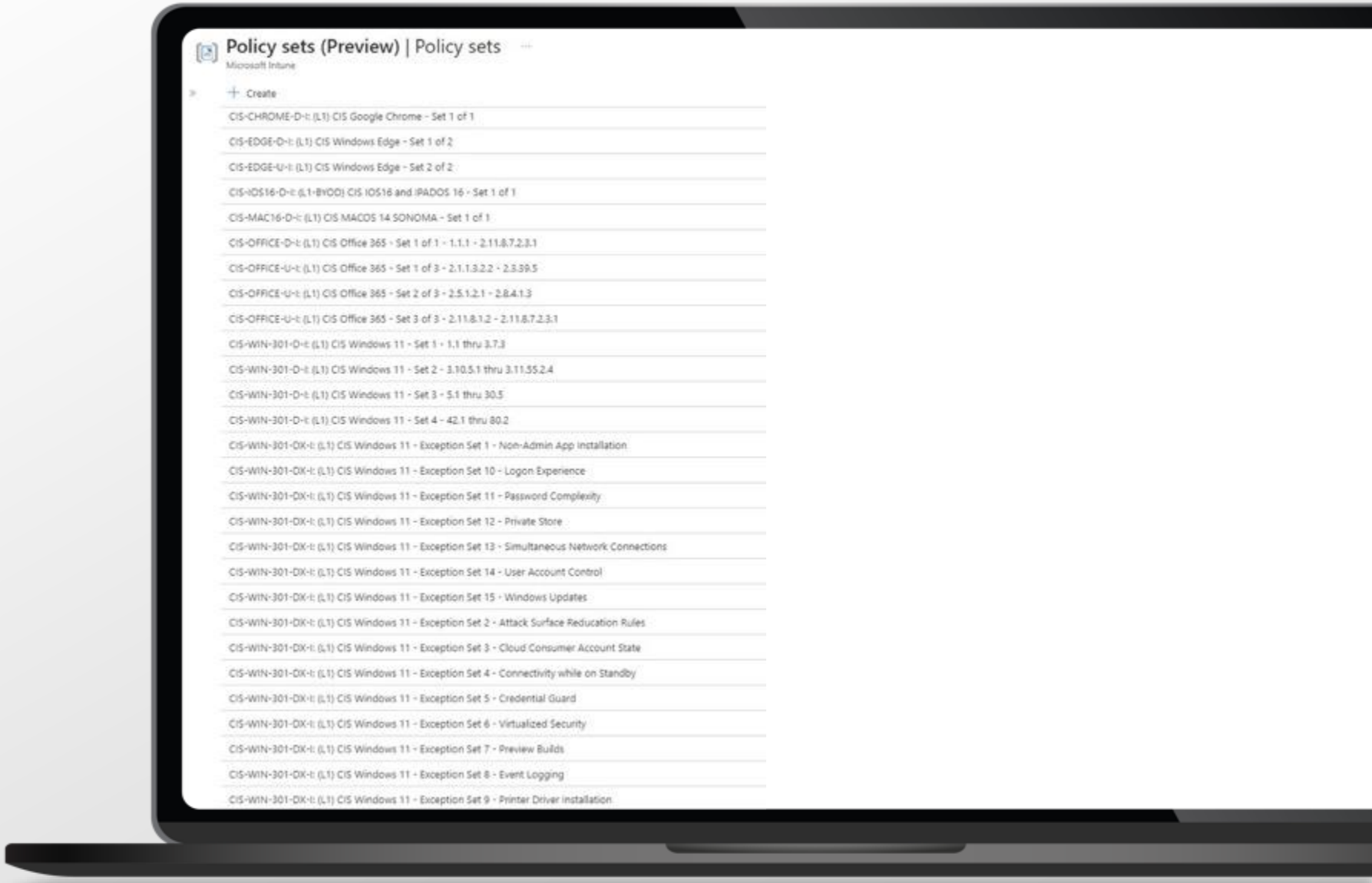
Packaging, patching, and updating 1298 applications.



global micro

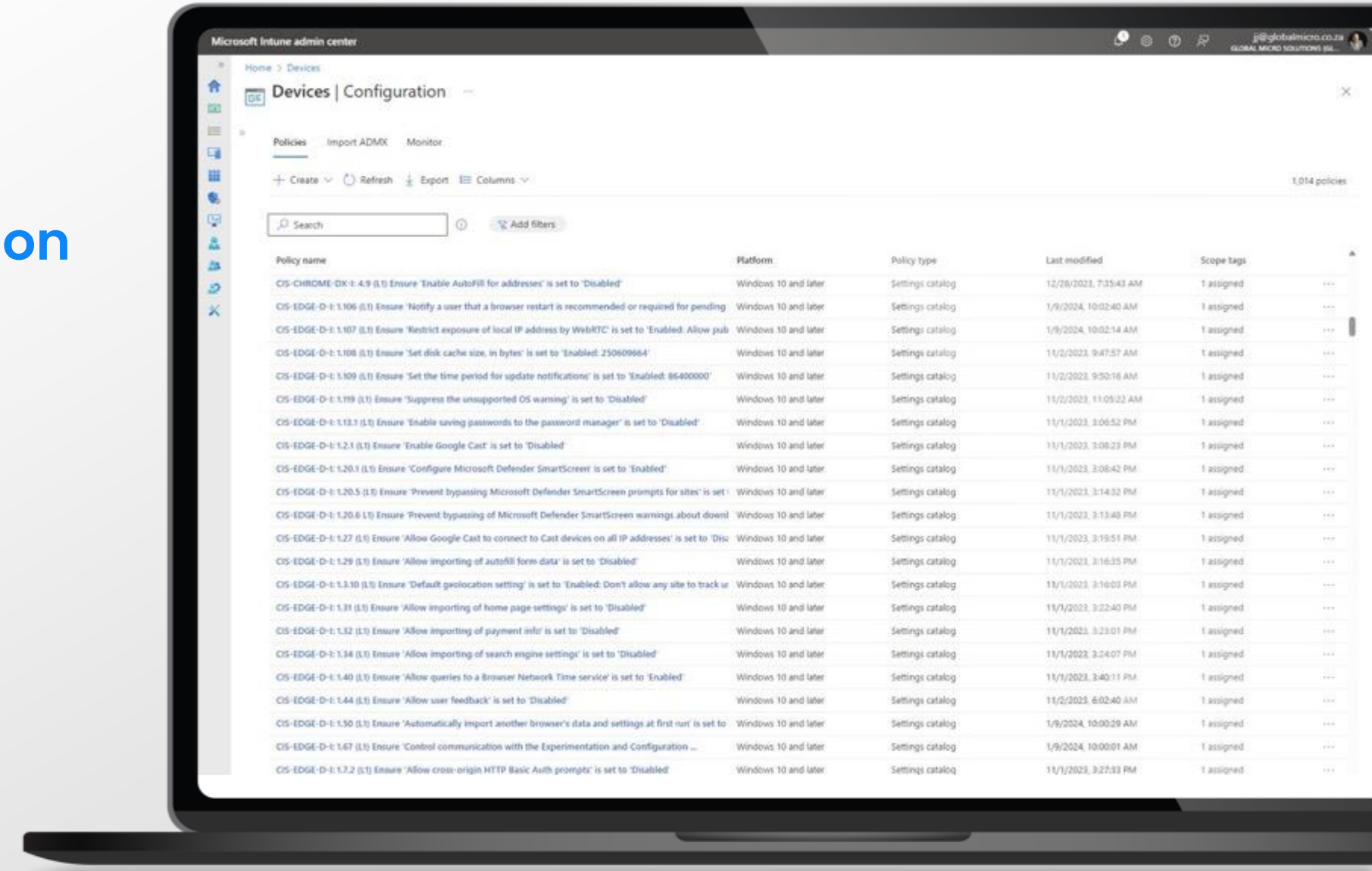
Intune Policy Sets

We maintain policy sets to easily manage thousands of CIS policies, including exception groups.



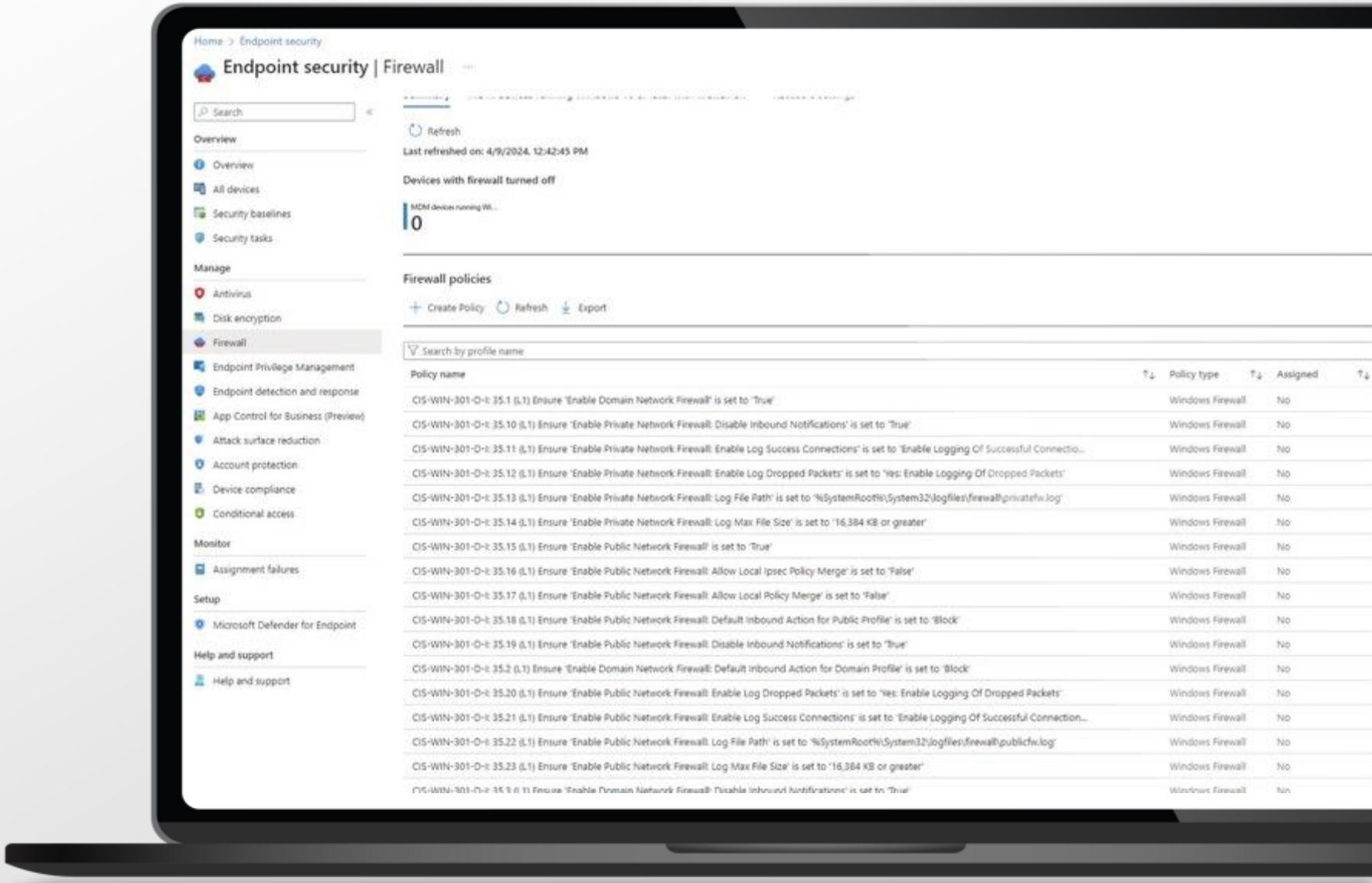
Device Configuration

Over 1,000 device configuration policies are maintained and labelled according to CIS benchmark directives.



Firewall Policies

Firewall Policies are easily identifiable against the CIS Benchmarks.

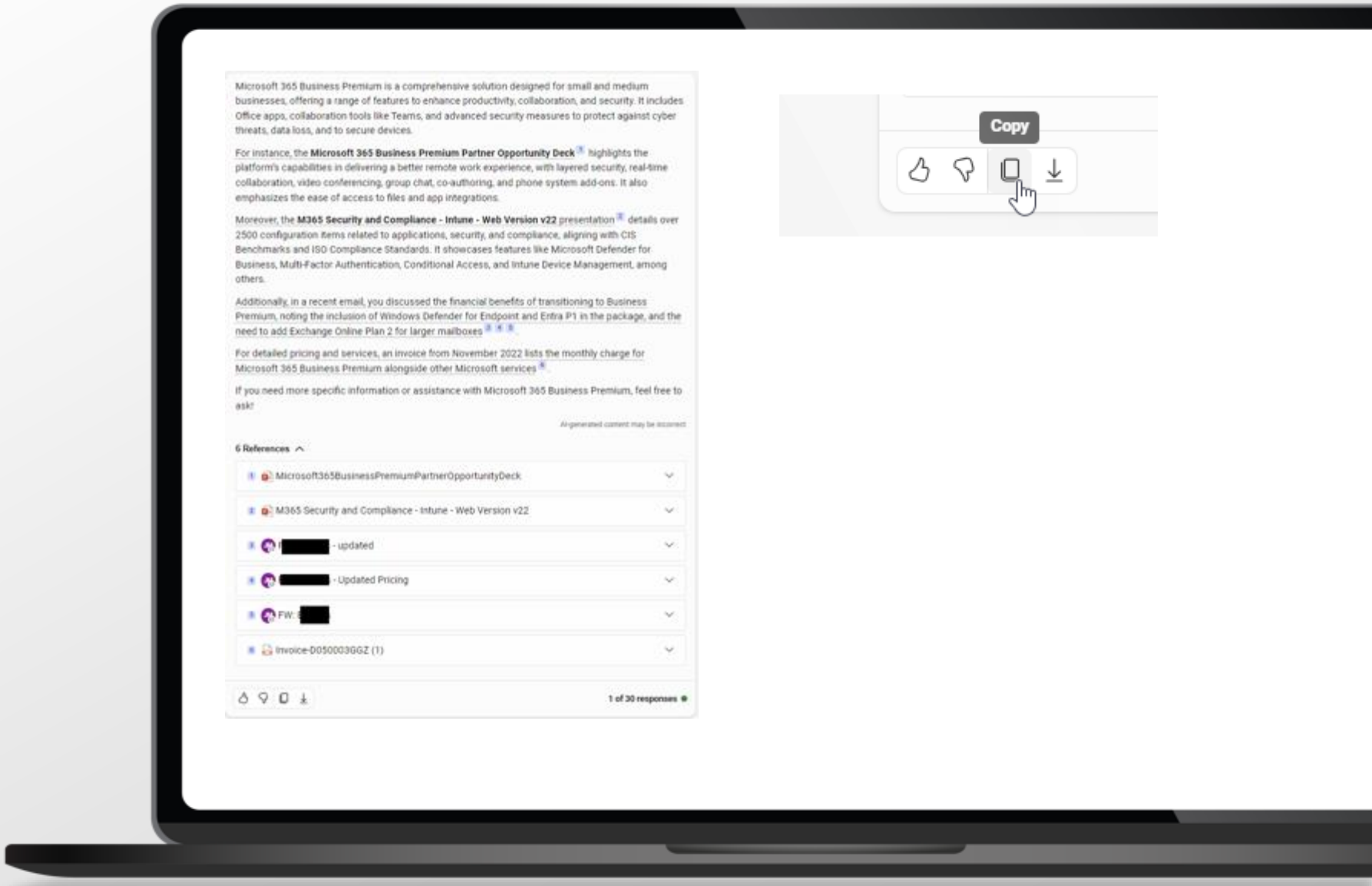


Phase 3:

Get your business Copilot-ready

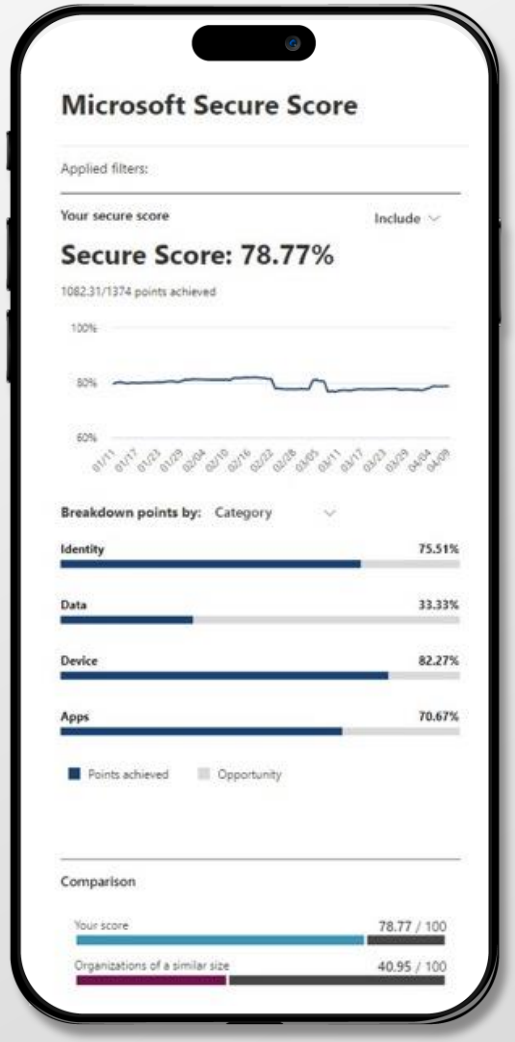
Copilot Risks

Example of Copilot will surface relevant documents that may be sensitive.
These need to be labelled for sensitivity and managed with Data Leakage Prevention.



Typical Microsoft Secure Score after Phase 3

The Microsoft Defender Secure Score is applicable for Microsoft SaaS workloads, such as Microsoft 365, Identity, Devices and Apps. It evaluates your configuration settings and behaviours and gives you a score based on the alignment with security standards.



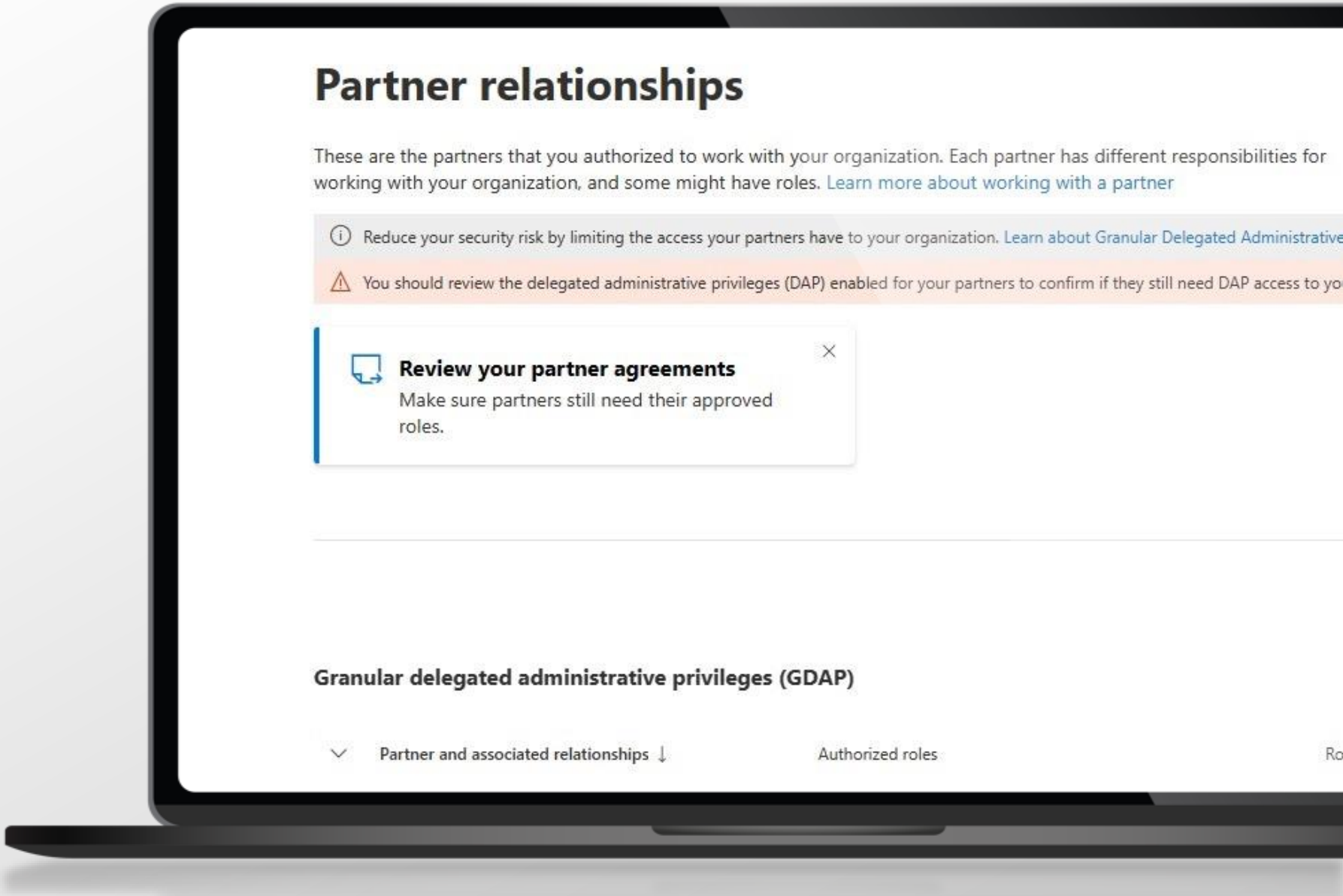
NIS 2 Compliance and Zero Trust Journey

Examples of how M365 Security and Compliance aligns to NIS 2

global micro

Supply chain security

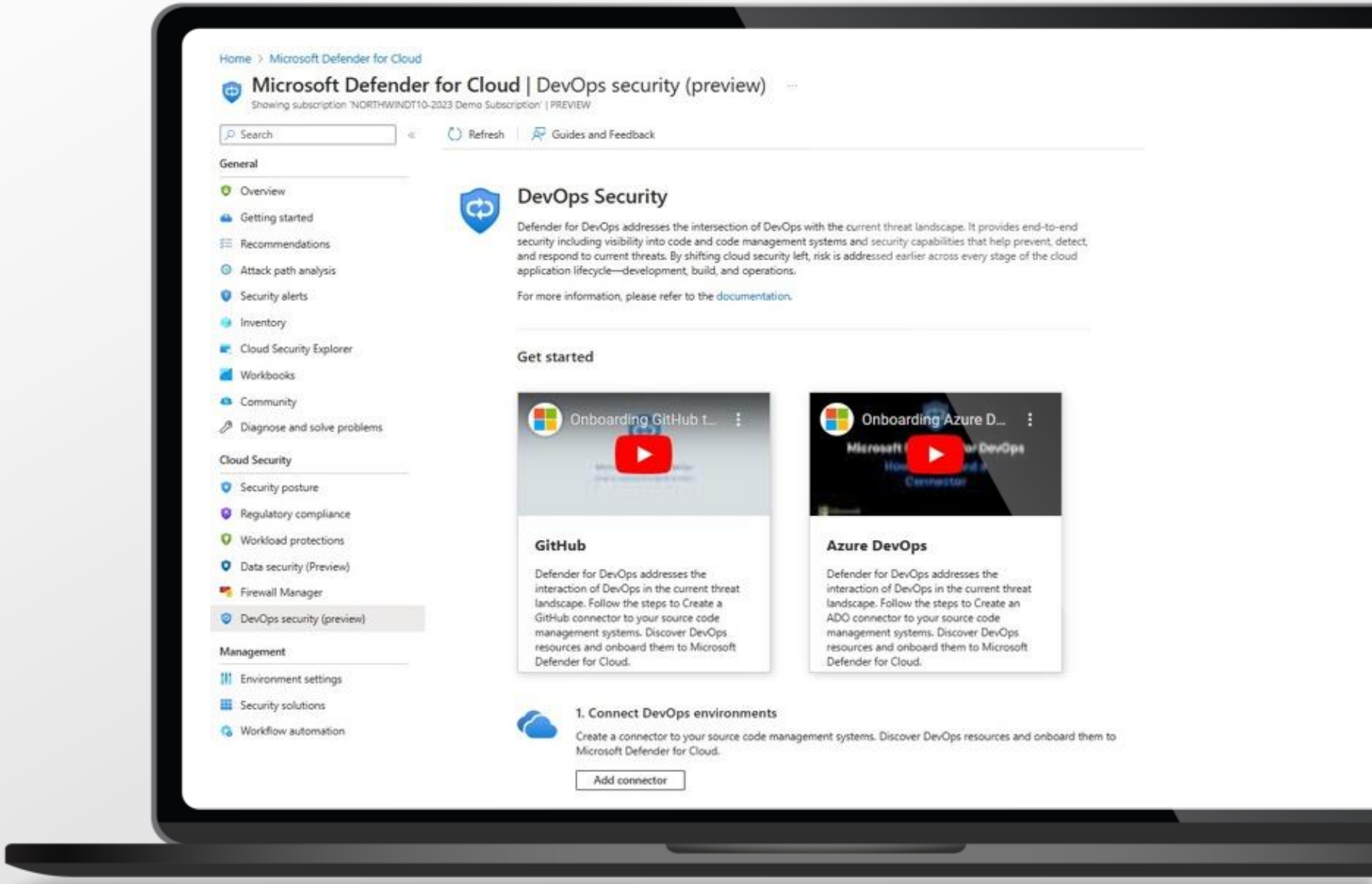
The new GDAP (Granular Delegated Admin Privileges) grants partners access to customers' tenants but only to the necessary roles and use permissions for a limited time.



global micro

Security in development and maintenance

Defender for DevOps uses a central console to empower security teams with the ability to protect applications and resources from code to cloud across multi-pipeline environments, such as GitHub and Azure DevOps.



APPENDIX

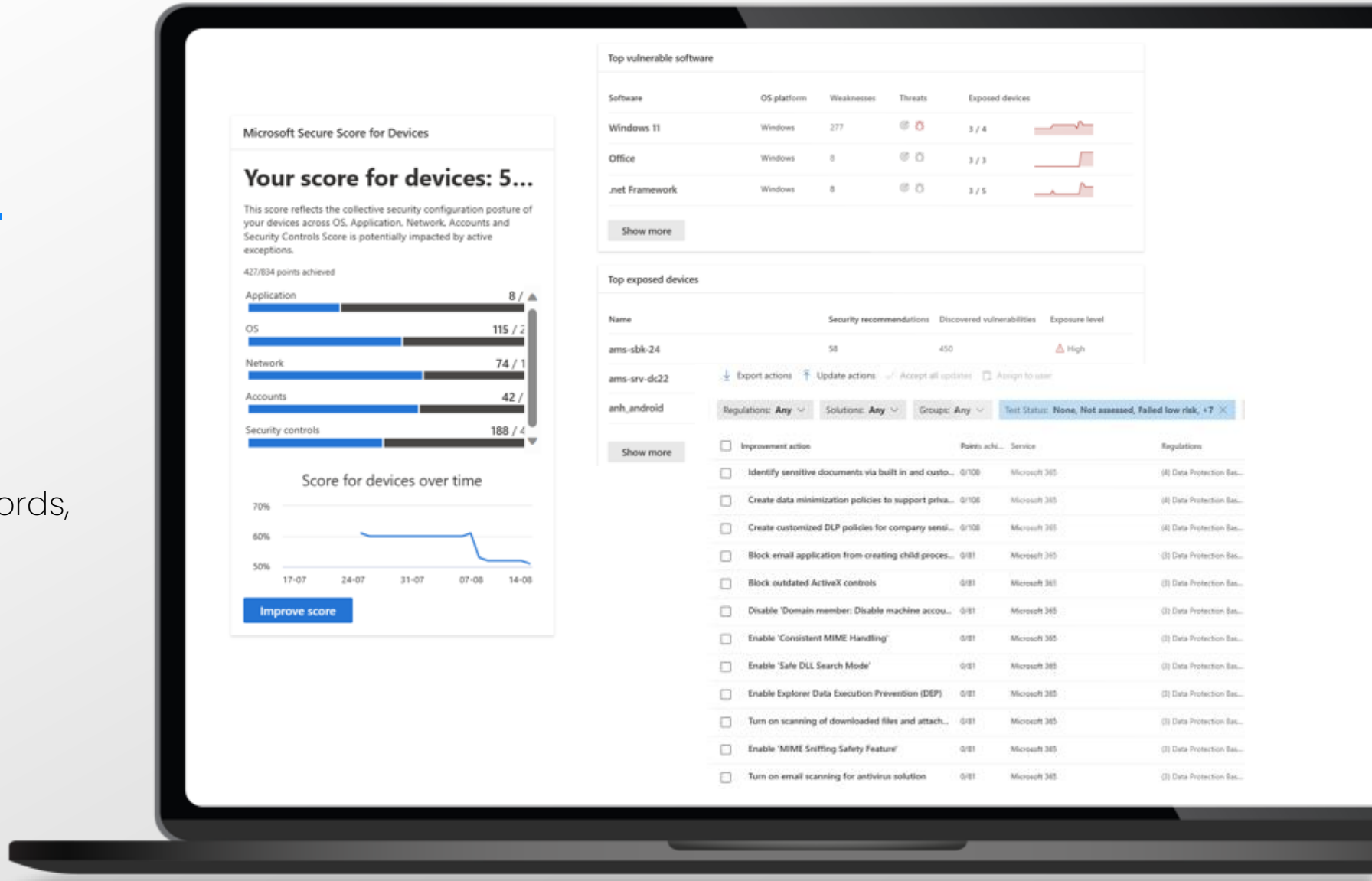
Cybersecurity risk-management measures

Identify gaps in your current cybersecurity controls, such as outdated software, weak passwords, or phishing vulnerabilities with:

- Microsoft Defender
- Exposure Score

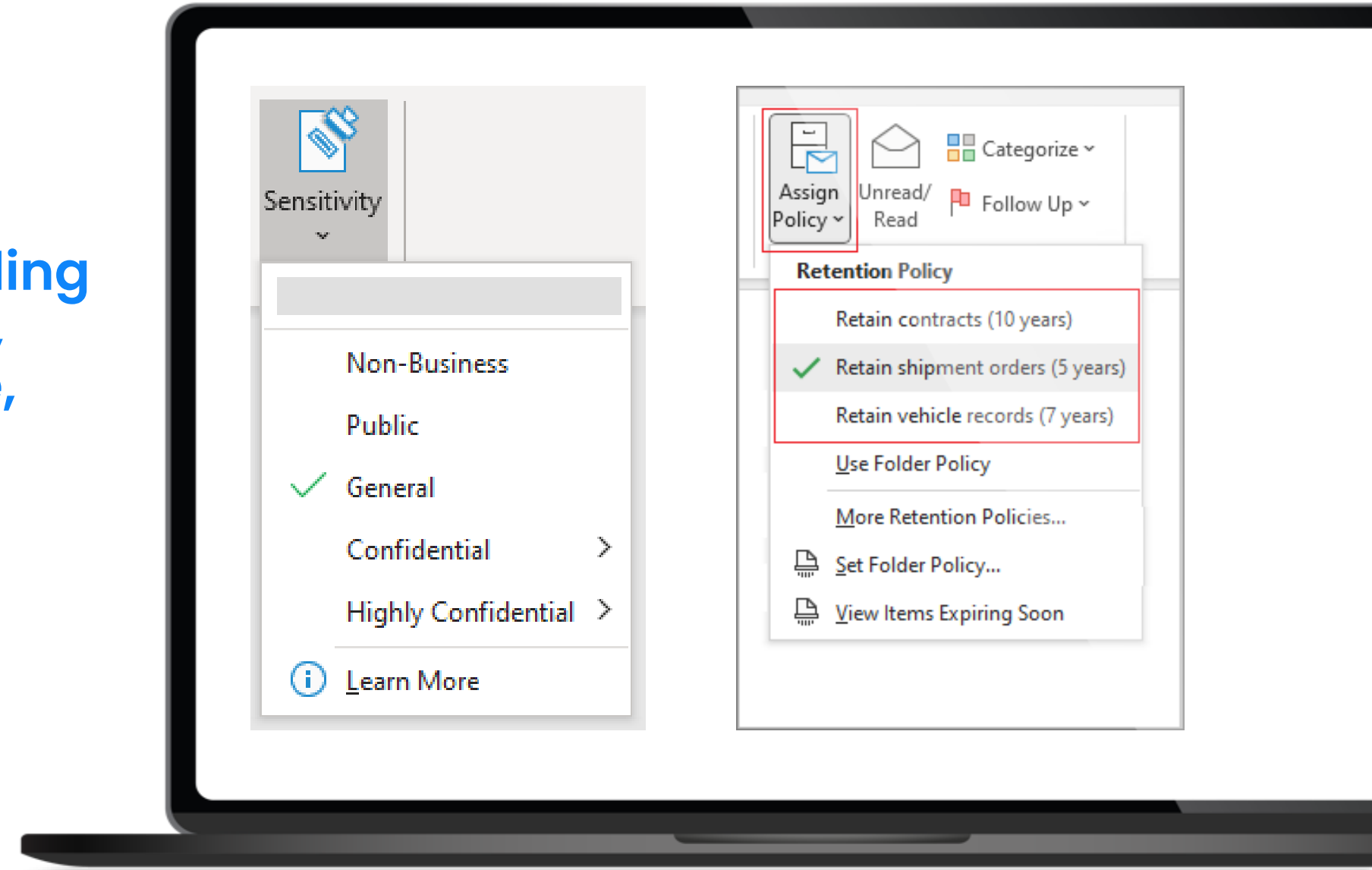
Microsoft Defender for Identity

- Compliance Manager



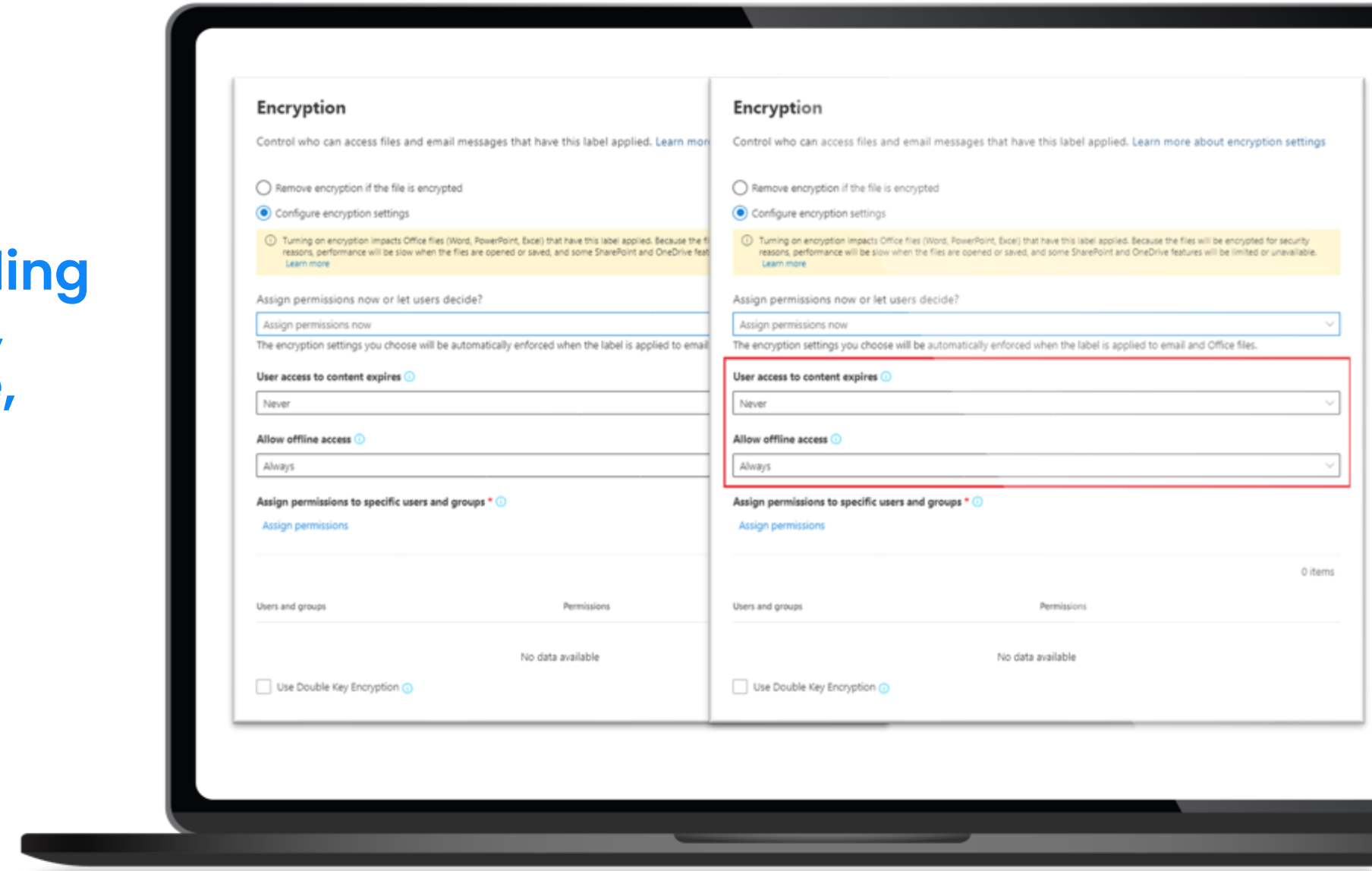
Policies and procedures regarding cryptography and, where appropriate, encryption

Purview Information Protection Sensitivity Labels & Data Lifecycle Management



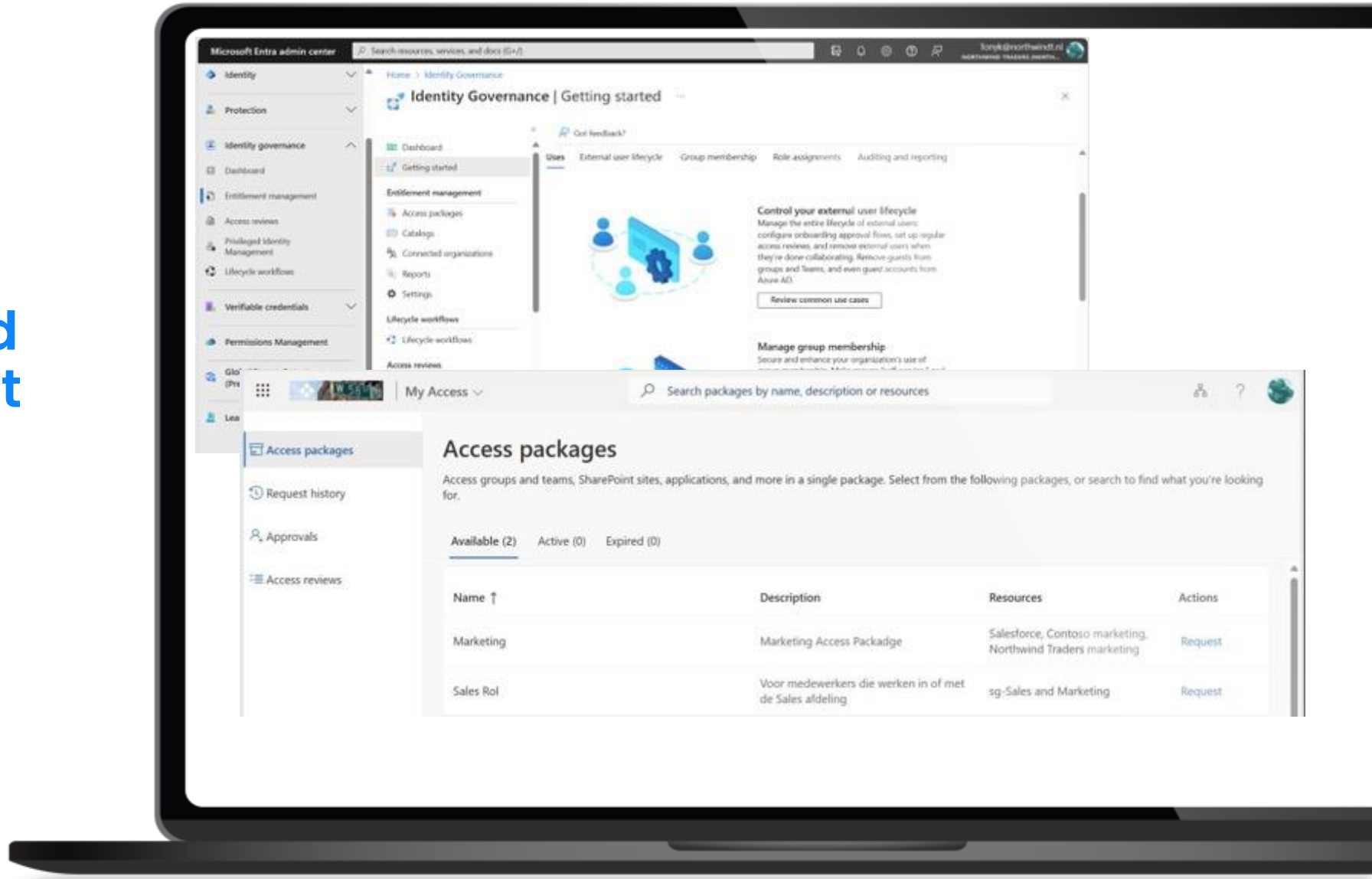
Policies and procedures regarding cryptography and, where appropriate, encryption

Purview Information Protection Sensitivity Labels & Data Lifecycle Management



Human resources security, access control policies and asset management

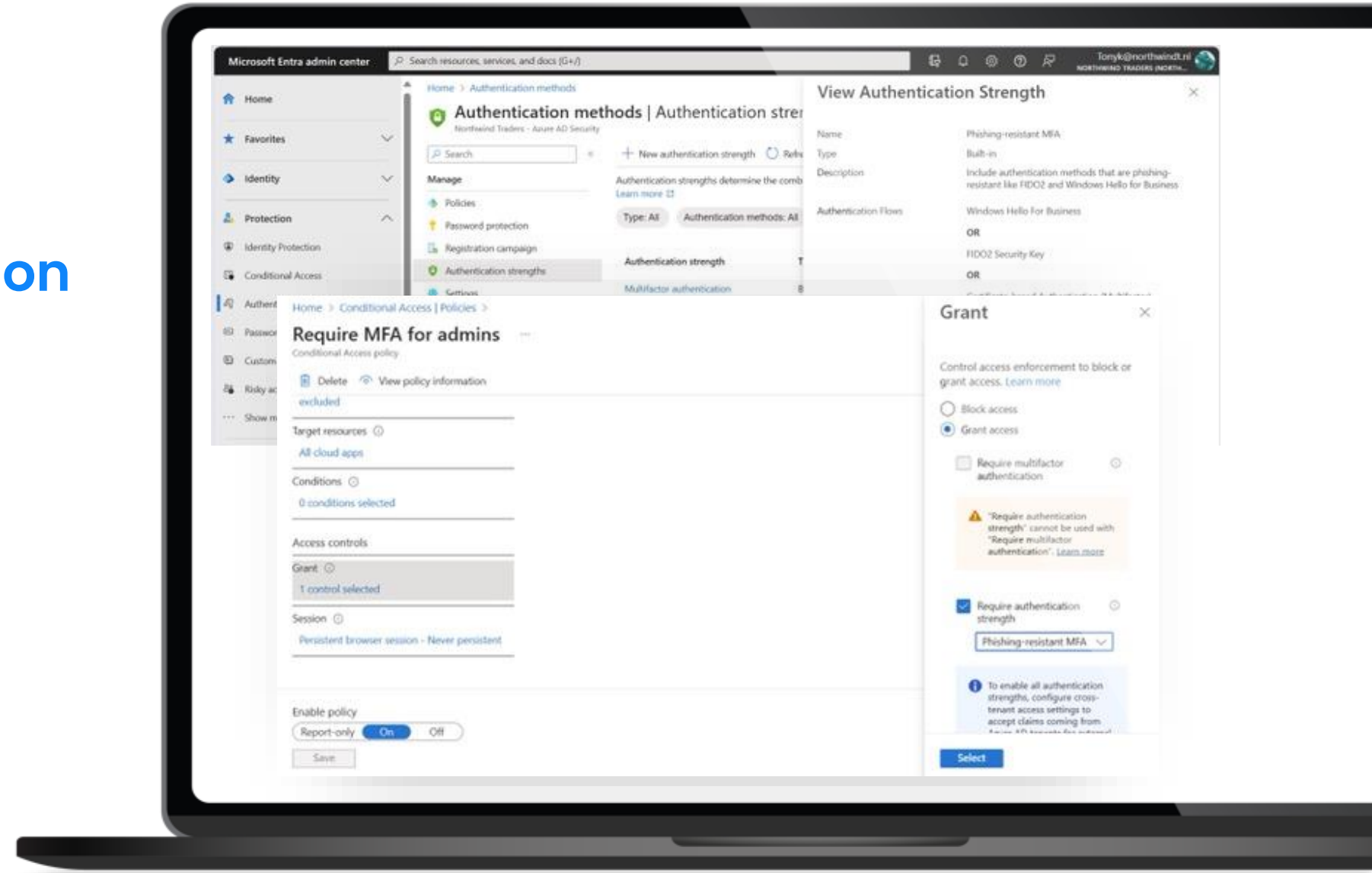
More control over standard procedures as well as timed access reviews.



APPENDIX

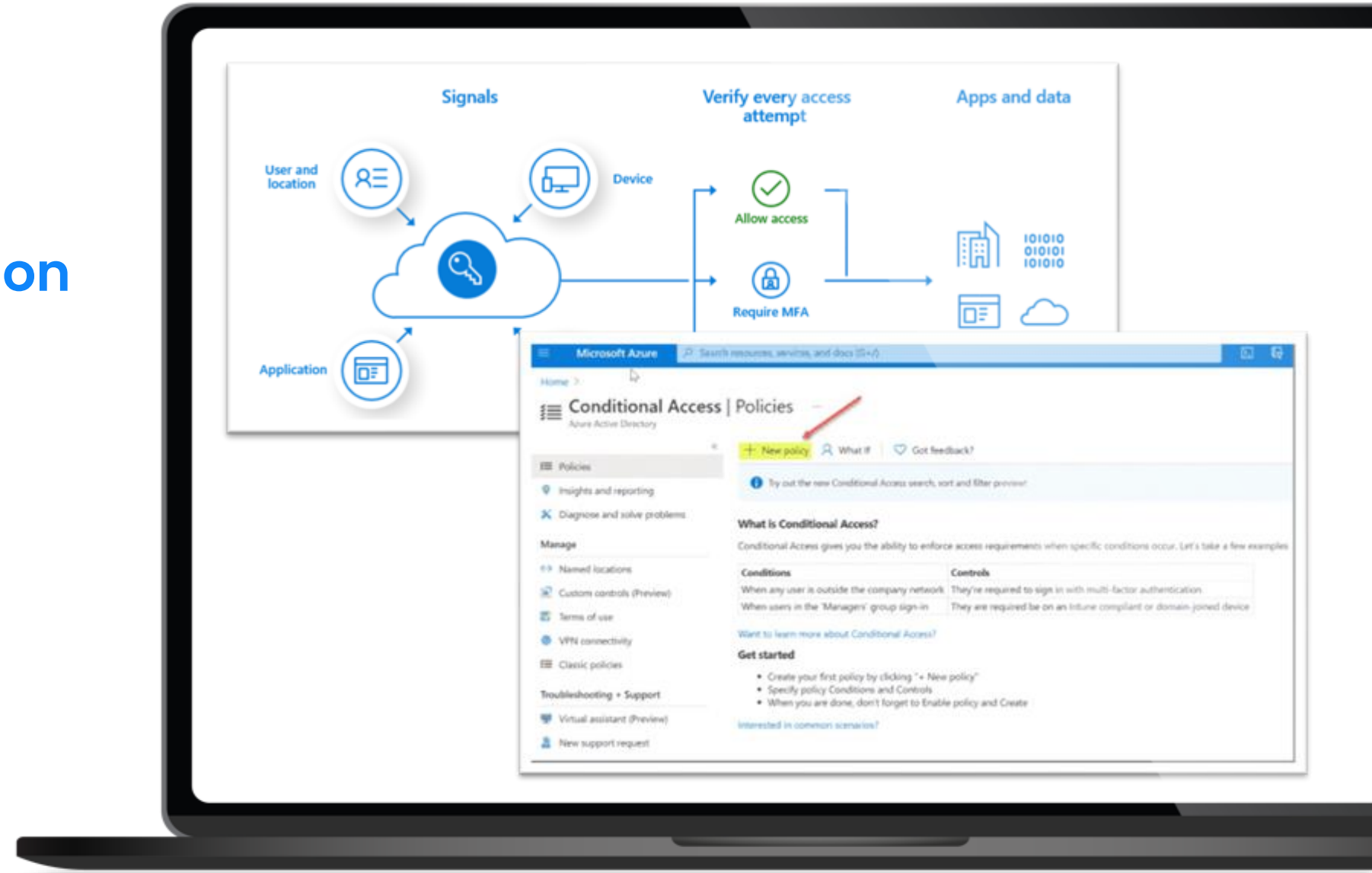
The use of multi-factor authentication or continuous authentication solutions

Mitigate Adversary-in-the-middle attacks with Microsoft Entra Authentication Strengths and Enforce Authentication Strengths through CA



The use of multi-factor authentication or continuous authentication solutions

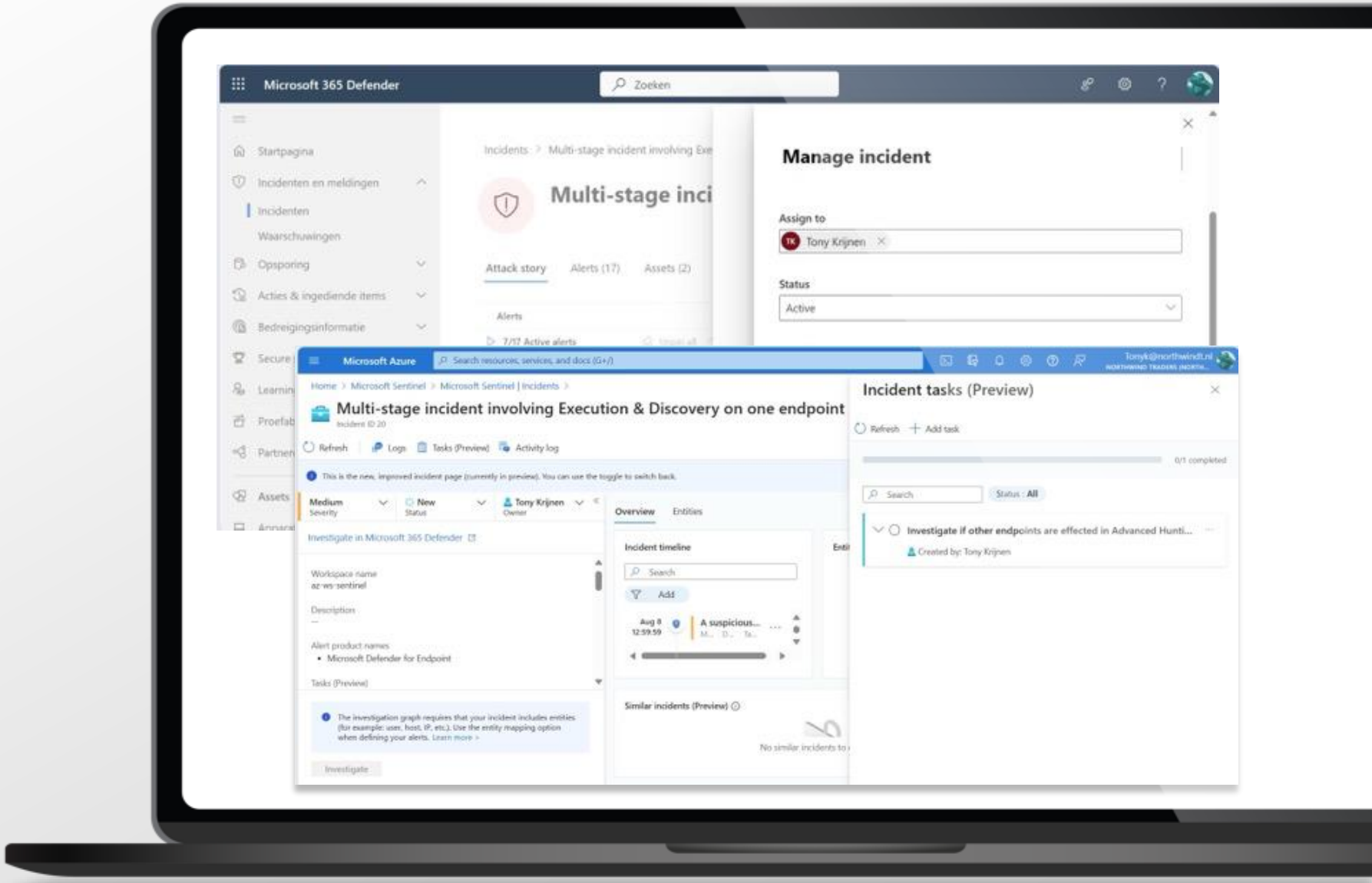
Secured voice, video and text communications and secured emergency communication systems within the entity



Incident handling

Utilising Microsoft Defender and Sentinel to give a robust and comprehensive view and management of any security issues within an IT infrastructure.

All Incidents are synchronised with Global Micro's Security Operations Centre with bi-directional updates.



Marketplace Offers
2025

Commercial Customers

M365 Security & Compliance: Commercial Customers - Marketplace Pricing

	Small 1	Small 2	Small 3
# Users	**1 to 5**	**6 to 10**	**11 to 25**
Deployment of AD-Connection	Extra $1 000	Extra $1 000	Extra $1 000
Deployment of Conditional Access	Extra $1 000	Extra $1 000	Extra $1 000
M365 Security and Compliance	**12 Months** Includes support	**12 Months** Includes support	**12 Months** Includes support
Deployment			
Consulting / working hours @ 8 hours/day			
Plan 1: Implementation	Not Available	Not Available	Not Available
Plan 2: Implementation	Not Available	Not Available	Not Available
Plan 3: Implementation	$9 000 – 9 Days	$9 000 – 9 Days	$9 000 – 9 Days
Management and Support			
	12 Months	**12 Months**	**12 Months**
Plan 1: Managed Service	Not Available	Not Available	Not Available
Plan 2: Managed Service	Not Available	Not Available	Not Available
Plan 3: Managed Service	$1 440	$2 880	$7 200

M365 Security & Compliance: Commercial Customers - Marketplace Pricing

	Medium 1	Medium 2	Medium 3
# Users	**26 to 50**	**51 to 100**	**100 to 200**
Deployment of AD-Connection	Extra $2 000	Extra $2 000	Extra $2 000
Deployment of Conditional Access	Extra $3 000	Extra $6 000	Extra $9 000
M365 Security and Compliance	**12 Months** Includes support	**12 Months** Includes support	**12 Months** Includes support
Deployment			
Consulting / working hours @ 8 hours/day			
Plan 1: Implementation	$3 000 – 3 Days	$3 000 – 3 Days	$3 000 – 3 Days
Plan 2: Implementation	$6 000 – 6 Days	$9 000 – 9 Days	$12 000 – 12 Days
Plan 3: Implementation	$12 000 – 12 Days	$15 000 – 15 Days	$18 000 – 18 Days
Management and Support			
	12 Months	**12 Months**	**12 Months**
Plan 1: Managed Service	$3 600	$7 200	$14 400
Plan 2: Managed Service	$10 800	$21 600	$43 200
Plan 3: Managed Service	$14 400	$28 800	$57 600

M365 Security & Compliance: Commercial Customers - Marketplace Pricing

	Large 1	Large 2	Large 3
# Users	**201 to 300**	**301 to 400**	**401 to 500**
Deployment of AD-Connection	Extra $3 000	Extra $3 000	Extra $3 000
Deployment of Conditional Access	Extra $12 000	Extra $12 000	Extra $12 000
M365 Security and Compliance	**12 Months** Includes support	**12 Months** Includes support	**12 Months** Includes support
Deployment			
Consulting / working hours @ 8 hours/day			
Plan 1: Implementation	$4 000 – 4 Days	$4 000 – 4 Days	$4 000 – 4 Days
Plan 2: Implementation	$16 000 – 16 Days	$16 000 – 16 Days	$16 000 – 16 Days
Plan 3: Implementation	$22 000 – 22 Days	$22 000 – 22 Days	$22 000 – 22 Days
Management and Support			
	12 Months	**12 Months**	**12 Months**
Plan 1: Managed Service	$21 600	$28 800	$36 000
Plan 2: Managed Service	$64 800	$86 400	$108 000
Plan 3: Managed Service	$86 400	$115 200	$144 000

M365 Security & Compliance: Commercial Customers - Marketplace Pricing

	Large 4	Large 5	Large 6
# Users	**501 to 750**	**751 to 1000**	**1001 to 2000**
Deployment of AD-Connection	Extra $4 000	Extra $4 000	Extra $4 000
Deployment of Conditional Access	Extra $16 000	Extra $16 000	Extra $16 000
M365 Security and Compliance	**12 Months** Includes support	**12 Months** Includes support	**12 Months** Includes support
Deployment			
Consulting / working hours @ 8 hours/day			
Plan 1: Implementation	$8 000 – 8 Days	$8 000 – 8 Days	$8 000 – 8 Days
Plan 2: Implementation	$22 000 – 22 Days	$22 000 – 22 Days	$22 000 – 22 Days
Plan 3: Implementation	$28 000 – 28 Days	$28 000 – 28 Days	$28 000 – 28 Days
Management and Support			
	12 Months	**12 Months**	**12 Months**
Plan 1: Managed Service	$54 000	$72 000	$144 000
Plan 2: Managed Service	$162 000	$216 000	$432 000
Plan 3: Managed Service	$216 000	$288 000	$576 000

Marketplace Offers
2025

Non-Profit Customers

M365 Security & Compliance: Non-Profit Customers - Marketplace Pricing

	Small 1	Small 2	Small 3
# Users	**1 to 5**	**6 to 10**	**11 to 25**
Deployment of AD-Connection	Extra $1 000	Extra $1 000	Extra $1 000
Deployment of Conditional Access	Extra $1 000	Extra $1 000	Extra $1 000
M365 Security and Compliance	**12 Months** Includes support	**12 Months** Includes support	**12 Months** Includes support
Deployment			
Consulting / working hours @ 8 hours/day			
Plan 1: Implementation	Not Available	Not Available	Not Available
Plan 2: Implementation	Not Available	Not Available	Not Available
Plan 3: Implementation	$1 800 – 9 Days	$1 800 – 9 Days	$1 800 – 9 Days
Management and Support			
	12 Months	**12 Months**	**12 Months**
Plan 1: Managed Service	Not Available	Not Available	Not Available
Plan 2: Managed Service	Not Available	Not Available	Not Available
Plan 3: Managed Service	$1 440	$2 880	$7 200

M365 Security & Compliance: Non-Profit Customers - Marketplace Pricing

	Medium 1	Medium 2	Medium 3
# Users	**26 to 50**	**51 to 100**	**100 to 200**
Deployment of AD-Connection	Extra $2 000	Extra $2 000	Extra $2 000
Deployment of Conditional Access	Extra $3 000	Extra $6 000	Extra $9 000
M365 Security and Compliance	**12 Months** Includes support	**12 Months** Includes support	**12 Months** Includes support
Deployment			
Consulting / working hours @ 8 hours/day			
Plan 1: Implementation	$600 – 3 Days	$600 – 3 Days	$600 – 3 Days
Plan 2: Implementation	$1 200 – 6 Days	$1 800 – 9 Days	$2 400 – 12 Days
Plan 3: Implementation	$2 400 – 12 Days	$3 000 – 15 Days	$3 600 – 18 Days
Management and Support			
	12 Months	**12 Months**	**12 Months**
Plan 1: Managed Service	$3 600	$7 200	$14 400
Plan 2: Managed Service	$10 800	$21 600	$43 200
Plan 3: Managed Service	$14 400	$28 800	$57 600

M365 Security & Compliance: Not-Profit Customers - Marketplace Pricing

	Large 1	Large 2	Large 3
# Users	**201 to 300**	**301 to 400**	**401 to 500**
Deployment of AD-Connection	Extra $3 000	Extra $3 000	Extra $3 000
Deployment of Conditional Access	Extra $12 000	Extra $12 000	Extra $12 000
M365 Security and Compliance	**12 Months** Includes support	**12 Months** Includes support	**12 Months** Includes support
Deployment			
Consulting / working hours @ 8 hours/day			
Plan 1: Implementation	$800 – 4 Days	$800 – 4 Days	$800 – 4 Days
Plan 2: Implementation	$3 200 – 16 Days	$3 200 – 16 Days	$3 200 – 16 Days
Plan 3: Implementation	$4 400 – 22 Days	$4 400 – 22 Days	$4 400 – 22 Days
Management and Support			
	12 Months	**12 Months**	**12 Months**
Plan 1: Managed Service	$21 600	$28 800	$36 000
Plan 2: Managed Service	$64 800	$86 400	$108 000
Plan 3: Managed Service	$86 400	$115 200	$144 000

M365 Security & Compliance: Non-Profit Customers – Marketplace Pricing

	Large 4	Large 5	Large 6
# Users	**501 to 750**	**751 to 1000**	**1001 to 2000**
Deployment of AD-Connection	Extra $4 000	Extra $4 000	Extra $4 000
Deployment of Conditional Access	Extra $16 000	Extra $16 000	Extra $16 000
M365 Security and Compliance	**12 Months** Includes support	**12 Months** Includes support	**12 Months** Includes support
Deployment			
Consulting / working hours @ 8 hours/day			
Plan 1: Implementation	$1 600– 8 Days	$1 600– 8 Days	$1 600– 8 Days
Plan 2: Implementation	$4 400 – 22 Days	$4 400 – 22 Days	$4 400 – 22 Days
Plan 3: Implementation	$5 600 – 28 Days	$5 600 – 28 Days	$5 600 – 28 Days
Management and Support			
	12 Months	**12 Months**	**12 Months**
Plan 1: Managed Service	$54 000	$72 000	$144 000
Plan 2: Managed Service	$162 000	$216 000	$432 000
Plan 3: Managed Service	$216 000	$288 000	$576 000

APPENDIX

Project Management

Understanding your SLA and Escalation Management

Microsoft Incident and Alert Coverage

RACI Matrix

Roles and responsibilities for each task within the M365 Security & Compliance Project

Responsible:
The person or people who do the work to complete the task.

Accountable:
The person who ensures the task is completed and has the final decision-making authority.

Consulted:
Those whose opinions are sought and with whom there is two-way communication.

Informed:
Those who are kept up-to-date on progress and decisions but do not need to be consulted

Task/Activity	Responsible (R)	Accountable (A)	Consulted (C)	Informed (I)
Project Planning	Project Manager	Project Sponsor	IT Team	All Stakeholders
Requirements Gathering	T3 Business Analyst	Project Manager	IT Team, T3 Security Team	All Stakeholders
Solution Design	T3 Architect	Project Manager	IT Team, T3 Security Team	All Stakeholders
License Procurement	Procurement Team	Procurement Manager	IT Team, Finance Team	All Stakeholders
Infrastructure Setup	T3 Architect	IT Manager	T3 Solution Architect	All Stakeholders
CodeTwo Configuration	T2 Engineer	IT Manager	T3 Architect	All Stakeholders
Autopilot Configuration	T3 Architect	IT Manager	T3 Architect	All Stakeholders
Device Enrollment	IT Team	IT Manager	T3 Architect	All Stakeholders
PIM Configuration	T3 Architect	IT Manager	T3 Architect	All Stakeholders
Conditional Access Configuration	T3 Architect	IT Manager	T3 Security Team	All Stakeholders
Intune Configuration	T3 Architect	IT Manager	T3 Architect	All Stakeholders
Policy Creation	T3 Architect	IT Manager	IT Manager, T3 Security Team	All Stakeholders
Signature Template Design	Marketing Team	Marketing Manager	IT Team, Legal, T2 Support	All Stakeholders
Application Deployment	T3 Solution Architect	IT Manager	T3 Architect	All Stakeholders
User Training	Training Team	HR Manager	IT Team	All Stakeholders
Pilot Testing	T3 Architect, IT Team	IT Manager	Selected Users	All Stakeholders
Full Deployment	IT Team	IT Manager	T3 Architect	All Stakeholders
Monitoring & Reporting	IT Team, T3 Security Team	IT Manager	T3 Security Team	All Stakeholders
Post-Deployment Support	T2 Support, IT Team	IT Manager	T3 Architect	All Stakeholders
Project Closure	Project Manager	Project Sponsor	IT Team	All Stakeholders

Global Micro Customer

SLA & Escalation

Help Desk Coverage
See Master Services Schedule Clause 13

Classification of Support
See Master Services Schedule Clause 14

Resolution of Support Requests
See Master Services Schedule Clause 15

Response Time Commitment
See Master Services Schedule Clause 16

Escalation
Automatic Escalation from Tier 1 to Tier 2 to Tier 3 managed by our Help Desk

Customer Initiated Escalation to Named Tier 3 Engineer (Platinum SLA) or Named Account Manager

Customer Initiated Escalation to Executive Sponsor at any time

Help Desk Hours

SLA	Bronze	Silver	Gold	Platinum
Respond Within	Best Effort	9x5 Working Hours	15x5 Extended Hours	P1 & P2: 24x7 P3 & P4: 15x5 Extended Hours
Plan Within	Best Effort	9x5 Working Hours	15x5 Extended Hours	
Target Temporary Resolution	Best Effort	9x5 Working Hours	15x5 Extended Hours	

Resolution of Support Requests

Priority	Respond 90% Within	Plan 90 % Within	Target Temporary Resolution or Workaround	Target Permanent Fix
1	2 Hours	3 hours	4 hours	15 Business Days
2	4 hours	6 hours	8 hours	15 Business Days
3	6 hours	8 hours	12 hours	30 Business Days
4	8 hours	12 hours	N/A	30 Business Days
5	12 hours	N/A	N/A	Next Release

Penalty for Response Time Commitment for Priority 1 and Priority 2 Requests

Customer Success Plan or SLA Average Response Time Compliance	Bronze Service Credit	Silver Service Credit	Gold Service Credit	Platinum Service Credit
More than 4 hours	No Credit	No Credit	No Credit	15%
More than 8 hours	No Credit	No Credit	25%	
More than 15 hours	No Credit	100%		

APPENDIX

Microsoft 365 Incident & Alert Management

Incidents from Microsoft 365 are synchronised to our service desk every 15 minutes.

In addition, DevOps pipelines periodically monitor platform wide configuration and management telemetry and open alerts directly on our service desk.

Incident Management Coverage

Source System	Plan 1	Plan 2	Plan 3
Microsoft Defender for Office 365 Incidents	**Included**		
Incidents are created when malicious or suspicious activity is detected in emails, users, or mailboxes. These incidents are automatically correlated with related alerts and investigations to provide a comprehensive view of the attack.			
Microsoft Defender for Endpoint Incidents	Excluded	**Included**	
Incidents are generated when threats are detected on endpoints. These incidents include correlated alerts and associated data to help security teams understand and respond to the attack.			
Microsoft Intune Configuration Alerts	Excluded	**Included**	
DevOps pipelines generate alerts when configuration drift is detected, or devices are out of compliance.			
Microsoft Sentinel Incidents	Excluded		**Included**
Automated playbooks can enrich incidents with additional data, such as reputation information from Microsoft Defender Threat Intelligence. This helps in triaging and prioritizing incidents based on the severity.			
Microsoft Information Protection and Governance	Excluded		**Included**
Incidents are created when sensitive data is accessed or shared inappropriately, helping to prevent data leaks and ensure compliance with data protection regulations			
Microsoft Cloud App Security	Excluded		**Included**
Incidents are generated when risky behaviors or threats are detected in cloud applications. This includes unusual user activity, data exfiltration attempts, and compromised accounts.			
Microsoft Defender for Identity	Excluded		**Included**
Incidents are created when suspicious activities related to user identities are detected. This includes potential identity theft, lateral movement, and other advanced identity-based threats			

global micro

Adopt Copilot.
Keep compliant.
Stay in Control.

Give your workforce the gift of Copilot, safely and simply.

Speak to your sales representative to book your initial assessment.

global micro

Secure. Comply. Succeed.

global micro

Microsoft 365 Security & Compliance

Secure Productivity

Copilot Readiness with ISO 27001 and NIS2 Compliance

global micro

Microsoft 365 Security and Compliance

Secure Productivity
Copilot Readiness
with ISO 27001 and
NIS2 Compliance

Organizations need a way to use the sophisticated security features of Microsoft 365

Microsoft 365 has sophisticated security features to **help organizations use Copilot securely**.

But with **over 2,500 different security settings, how do you verify that your settings** meet the required standard for safe integration of Copilot?

And **how do you maintain these settings** over time as regulation changes, without retaining a large expert security team?

Why Global Micro for Secure Productivity and Copilot Readiness

On average, customers who adopted Global Micro's complete 365 Security & Compliance **solution reached a Secure Score of 75+** and are **proven to be ready for optimum usage of Copilot**.

29+
Years' expertise

1200+
customers across EMEA

4x
Faster deployment than industry average

50K+
seamless migrations