

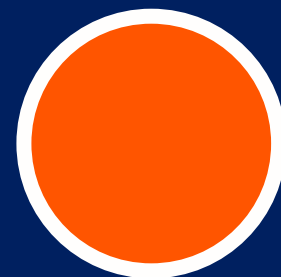
# softwerx

The Microsoft Security Specialists

Microsoft

Cybersecurity Assessment Report

Contoso



Example report

## Contents

Executive summary.....	3
CIS interview   Findings and Recommendations.....	6
Technical Data and Analysis.....	16
Appendix A - Overview of advised security software products.....	41
Appendix B – Secure Score top recommendations.....	44
Appendix C – Vendor Consolidation.....	45
Appendix D – Assessment Scope.....	47
Appendix E – The CSAT Methodology.....	49

Example report

**EXAMPLE VERSION – DO NOT DISTRIBUTE TO OTHERS – SUBJECT TO NDA**

Softwerx Ltd and Contoso confidential.

Do not copy, distribute, or reproduce - in any form - to a third party.

## Executive summary

This document is part of the deliverables of the cybersecurity assessment conducted in February 2021 for Contoso by Softwerx Ltd. It provides an overall review of your cybersecurity status and practices, as assessed through a questionnaire and an automated scan of security-related data from your IT infrastructure.

The size, industry, regulatory requirements, and risk factors of the organization influence the recommendations in this report. The report is not intended to serve as a detailed control review or security audit but can be used in preparation for one. Additionally, the outcomes of the assessment can be utilized as input for an action plan to address the identified risks, improving the organization's security posture and cybersecurity resilience.

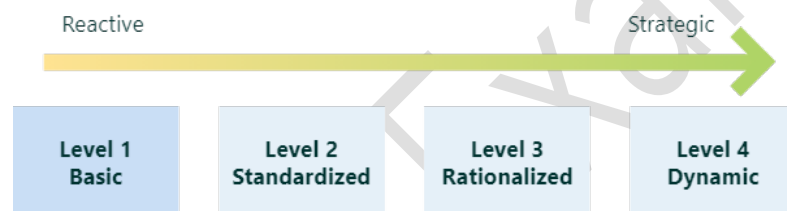
## Organization's Maturity Level

This assessment uses the CIS Controls™ (v8.1) framework, which has been reworked into a maturity level-based score from one to four. The levels are as follows:

- Level one: Basic – High risk of cybersecurity issues.
- Level two: Standardized – Significant risk of cybersecurity issues.
- Level three: Rationalized – Moderate risk of cybersecurity issues.
- Level four: Dynamic – Low risk of cybersecurity issues.

More information about the CSAT methodology and scoring can be found in Appendix E.

The current overall maturity level of Contoso's cybersecurity program and practices matches level 1 - basic. The maturity level of your organization is determined based on the lowest scored CIS control, as identified during the interview with your security team.



**EXAMPLE VERSION – DO NOT DISTRIBUTE TO OTHERS – SUBJECT TO NDA**

Softwerx Ltd and Contoso confidential.

Do not copy, distribute, or reproduce - in any form - to a third party.

The maturity score is calculated based on the average of all answers in the questionnaire. This score can be used as a benchmark for future assessments based on CIS controls. Your current maturity score is shown below.



Security is a risk that requires careful management, rather than a problem with a definitive solution. It involves not only safeguarding your assets but also protecting your reputation, customers, and employees. Organizations should strive to achieve at least level three to ensure adequate defence capabilities. The subsequent chapters will provide a detailed examination of the technical aspects.

## NIS 2

The NIS 2 Directive is an update to the original Network and Information Systems (NIS) Directive. The goal of NIS 2 is to enhance the cybersecurity resilience of critical infrastructure within the European Union and address the evolving threat landscape. This is achieved by implementing measures such as establishing more stringent security requirements, improving incident response capabilities, and promoting greater cooperation among member states. By implementing these measures, NIS 2 seeks to ensure a higher level of protection for essential services and digital infrastructure, thereby safeguarding the stability and security of the EU's digital ecosystem.

### NIS 2 - Maturity overview

The questions in the CSAT questionnaire can be linked to the NIS 2 Directive. The mapping is based on a reference created by the Centre for Internet Security. An overview of the mapping from the CIS version 8 Controls to NIS 2 Directive measures can be found in Appendix E. Based

**EXAMPLE VERSION – DO NOT DISTRIBUTE TO OTHERS – SUBJECT TO NDA**

Softwerx Ltd and Contoso confidential.

Do not copy, distribute, or reproduce - in any form - to a third party.

on the answers provided in the questionnaire, a suggested NIS 2 compliance level can be determined. It is important to note that this is only a

<b>A</b>	Policies on risk analysis and information security	1.4	1	2	3	4
<b>B</b>	Incident handling	1.4	1	2	3	4
<b>C</b>	Business continuity, such as backup management and disaster recovery, and crisis management	1.5	1	2	3	4
<b>D</b>	Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers	1.5	1	2	3	4
<b>E</b>	Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure	1.3	1	2	3	4
<b>F</b>	Policies and procedures to assess the effectiveness of cybersecurity risk-management measures	1.4	1	2	3	4
<b>G</b>	Basic cyber hygiene practices and cybersecurity training	1.3	1	2	3	4
<b>H</b>	Policies and procedures regarding the use of cryptography and, where appropriate encryption	1.4	1	2	3	4
<b>I</b>	Human resources security, access control policies and asset management	1.4	1	2	3	4
<b>J</b>	The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate	1.8	1	2	3	4

suggested level.

EXA

**EXAMPLE VERSION – DO NOT DISTRIBUTE TO OTHERS – SUBJECT TO NDA**

Softwerx Ltd and Contoso confidential.

Do not copy, distribute, or reproduce - in any form - to a third party.

## CIS interview | Findings and Recommendations

This chapter contains detailed ratings for CIS Controls™ (v8.1) and a selection of the ISO/IEC 27001:2022 controls, providing insight into your organization's current policies, procedures, and management. The ratings reflect the current state and can indicate areas for improvement in your security rating in the next assessment, depending on your strategy, policies, risk tolerance, and regulatory requirements. The tables in this chapter include a 'ZTA' column, which maps the control to the Zero Trust Architecture zone mentioned in Appendix E.

### CIS Controls

The controls of CIS and their objectives are mentioned below.

Control	Objective
<b>1. Inventory and Control of Enterprise Assets</b>	Actively manage (inventory, track, and correct) all Enterprise assets on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.
<b>2. Inventory and Control of Software Assets</b>	Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.
<b>3. Data Protection</b>	The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.
<b>4. Secure Configuration of Enterprise Assets and Software</b>	Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.
<b>5. Account Management</b>	Actively manage the life cycle of system and application accounts - their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them.
<b>6. Access Control Management</b>	The processes and tools used to create, assign, manage and revoke credentials and privileged for users, administrators, and service accounts.
<b>7. Continuous Vulnerability Management</b>	Continuously acquire, assess, and track vulnerabilities, to remediate, and minimize the window of opportunity for attackers.
<b>8. Audit Log Management</b>	Collect, manage, and analyse audit logs of events that could help detect, understand, or recover from an attack.
<b>9. Email and Web Browser Protections</b>	Minimize the attack surface and the opportunities for attackers to manipulate human behaviour through their interaction with web browsers and email systems.
<b>10. Malware Defenses</b>	Prevent the installation, spread, and execution of malicious code in the organization, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.
<b>11. Data Recovery</b>	The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

**EXAMPLE VERSION – DO NOT DISTRIBUTE TO OTHERS – SUBJECT TO NDA**

Softwerx Ltd and Contoso confidential.

Do not copy, distribute, or reproduce - in any form - to a third party.

<b>12. Network Infrastructure Management</b>	Establish, implement, and manage network devices, in order to prevent attackers from exploiting vulnerable network devices or services.
<b>13. Network Monitoring and Defense</b>	The processes and tools used to establish and maintain comprehensive network monitoring and defense against security threats across the network infrastructure.
<b>14. Security Awareness and Skills Training</b>	Establish and maintain a security awareness program, to influence behaviour among the users to be security aware and properly skilled. In order to reduce cybersecurity risks.
<b>15. Service Provider Management</b>	The processes and tools to evaluate service providers who hold sensitive data, or are responsible for critical IT platforms or processes, to ensure the providers are protecting the platforms and data appropriately.
<b>16. Application Software Security</b>	Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.
<b>17. Incident Response Management</b>	Protect the organization's information, as well as its reputation, by establishing a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.
<b>18. Penetration Testing</b>	Test the overall strength of an organization's defense (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.

Example

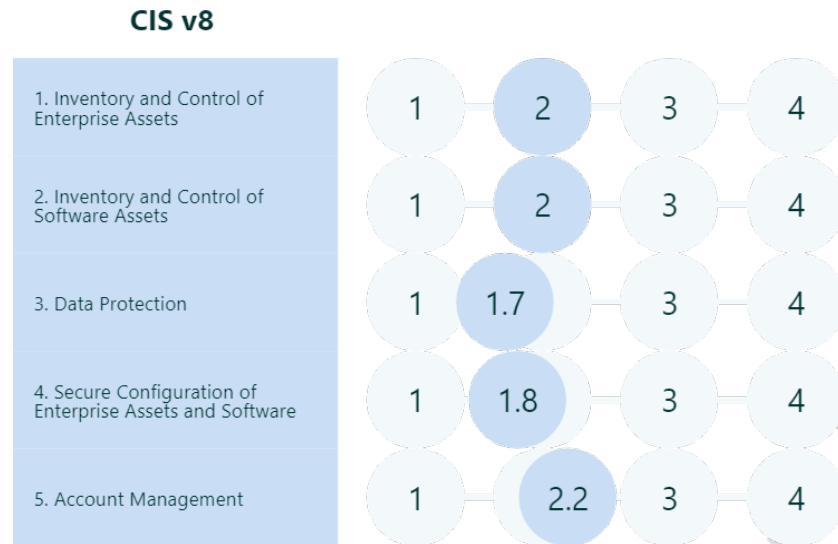
**EXAMPLE VERSION – DO NOT DISTRIBUTE TO OTHERS – SUBJECT TO NDA**

Softwerx Ltd and Contoso confidential.

Do not copy, distribute, or reproduce - in any form - to a third party.

## CIS Controls - Score Overview

Based on the provided answers regarding the CIS controls, your current rating is stated in the below graphic.



**EXAMPLE VERSION – DO NOT DISTRIBUTE TO OTHERS – SUBJECT TO NDA**

Softwerx Ltd and Contoso confidential.

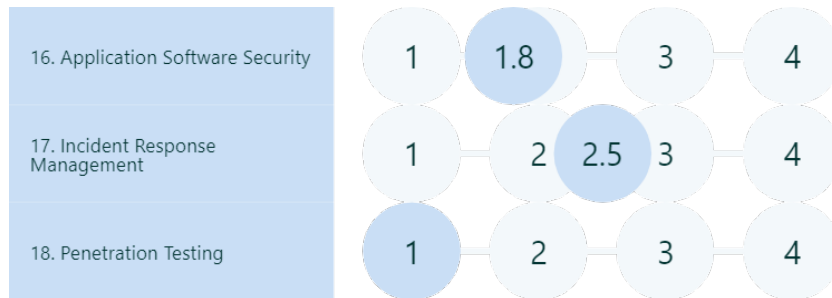
Do not copy, distribute, or reproduce - in any form - to a third party.



**EXAMPLE VERSION – DO NOT DISTRIBUTE TO OTHERS – SUBJECT TO NDA**

Softwerx Ltd and Contoso confidential.

Do not copy, distribute, or reproduce - in any form - to a third party.



### CIS Controls - Findings and Recommendations

The following action items apply to enhance your position with regards to the CIS controls. The number mentioned in the topic column correlates to the respective control.

Urgent					
Topic	Question	Answer	Advice	Advised Products	NIS2 Principle
2. Inventory and Control of Software Assets	How do you ensure and check vendor supportability of used software and operating systems within the organization? How do you control non-approved software?	Basic (1) Unknown/unsupported and/or unwanted (cloud) software or operating systems are being used without documentation	Document the business justification for the continued use of unsupported/unwanted software. Include a plan to migrate to a supported/wanted situation.	Configuration Management Database; Software Asset Management (SAM) tooling; Defender for Cloud Apps	A3: Asset Management; B4: System Security
4. Secure Configuration of Enterprise	How does the organization address device and session locking	Basic (1) Users are not educated to lock their device when they leave it unattended. An automated	Educate the users why they should lock their device when leaving it unattended. Implement a automated lock	Active Directory Services (GPO); Microsoft Intune; Defender for	A2: Risk Management;

**EXAMPLE VERSION – DO NOT DISTRIBUTE TO OTHERS – SUBJECT TO NDA.**

Softwerx Ltd and Contoso confidential.

Do not copy, distribute, or reproduce - in any form - to a third party.

Assets and Software	when the device or session is left unattended or not in use?	lock policy has not been implemented.	policy for Windows servers, laptops and desktops.	Cloud; Windows 10 and 11 Pro/Enterprise	B4: System Security
5. Account Management	Is there an inventory of all used accounts and how are dormant accounts handled?	Basic (1) Unknown or No inventory of the account information and no insight in dormant accounts.	Implement a process to check for dormant administrator, service and user accounts.	Microsoft Entra ID P2 [Access Reviews, Identity Protection]	A1: Governance; B2: Identity and Access control
8. Audit Log Management	Is there a process to analyze the audit logs?	Basic (1) No process in place.	Create a process for analyzing the audit logs.		B4: System Security; C2: Proactive Security Event Discovery
11. Data Recovery	How have you setup the data recovery process?	Basic (1) No data recovery process is available.	Implement automated backups for your most important assets at least on a weekly basis.	Windows Server Backup; Azure Backup; Microsoft 365 OneDrive	D1: Response and recovery planning

High					
Topic	Question	Answer	Advice	Advised Products	NIS2 Principle
2. Inventory and Control	Has your organization implemented software whitelisting , allowing	Standardized (2) An up-to-date list of authorized	Modern malware (ransomware) are often able to install and activate	AppLocker; Microsoft Intune;	A3: Asset Management; B4: System Security; C2:

**EXAMPLE VERSION – DO NOT DISTRIBUTE TO OTHERS – SUBJECT TO NDA.**

Softwerx Ltd and Contoso confidential.

Do not copy, distribute, or reproduce - in any form - to a third party.

of Software Assets	only authorized software to run on all organization's systems?	software and software libraries is available.	without elevated privileges.	Defender for Cloud Apps; Defender for Server Plan 2	Proactive security event discovery
3. Data Protection	How is access to data being controlled, how are checks being carried out on granted permissions?	Standardized (2) Basic security groups have been implemented on shares, folders and collaboration sites/tools. We do not monitor given permissions.	Implement security groups based on the business roles matrix. Implement separate groups for read-only and read-write access to protect shares, folders, sites achieving 'least-privilege' access.	Active Directory Services; Microsoft Entra ID; Azure Storage; PortalTalk	A1: Governance; A2: Risk Management; B2: Identity & Access; B3: Data Security; B4: System Security; D1: Response and Recovery planning
10. Malware Defenses	How are autorun and autoplay configured on the organization systems?	Standardized (2) Users are made aware to disable this functionality, users are able to edit the settings.	Implement tooling to control the autorun and autoplay features.	Microsoft Intune; GPO	B4: System Security
14. Security Awareness and Skills Training	How is the security and privacy awareness training establish and maintained?	Standardized (2) An annual returning security and privacy awareness program is implemented, including training to recognize social engineering attacks and authentication best practices.	Extend your security and privacy training program with data handling best practices and causes of unintentional data exposure	Defender for Office Plan 2 (Attack Simulation Training); Microsoft 365 Premium	B6: Staff Awareness

**EXAMPLE VERSION – DO NOT DISTRIBUTE TO OTHERS – SUBJECT TO NDA**

Softwerx Ltd and Contoso confidential.

Do not copy, distribute, or reproduce - in any form - to a third party.

16. Application Software Security	What is the process on discovered or reported software vulnerabilities?	Basic (1) No process available regarding how to handle the identified or reported software vulnerabilities.	Implement a basic process for handling the identified or reported software vulnerabilities.	A2: Risk Management; A4: Supply Chain; C2: Proactive Security event discovery
--	---	---	---	---

### Additional questions

The CIS Controls are extended with high-level controls from the ISO/IEC 27001:2022 framework, named 'AQ 1' and 'AQ 2'. The added questions relate to IT governance, data governance and cover policies, regulatory compliance, risk management and privacy. These additional questions are included to provide an optimal overview of the security and privacy practices in your IT environment. The additional questions and their objectives are mentioned below.

Control	Objective
19. AQ 1. IT Governance	Create organizational transparency and alignment by establishing a security and privacy policy framework complying with the regulatory and legal requirements applicable to the organization.
20. AQ 2. Data Governance	Adjustment to, and adoption of privacy regulatory requirements with a risk-based approach and focus on the protection of personal identifiable information (PII).

**EXAMPLE VERSION – DO NOT DISTRIBUTE TO OTHERS – SUBJECT TO NDA**

Softwerx Ltd and Contoso confidential.

Do not copy, distribute, or reproduce - in any form - to a third party.

### Additional questions - Score Overview

Based on the provided answers regarding the additional controls, your current rating is stated in the below graphic.

#### Additional questions



### Additional questions - Findings and Recommendations

The following action items apply to enhance your position with regards to the additional controls. The number mentioned in the topic column correlates to the respective control.

Urgent					
Topic	Question	Answer	Advice	Advised Products	NIS2 Principle
19. AQ 1. IT Governance	Do you have a plan/roadmap in place to improve your cybersecurity posture, supported by executive management?	Basic (1) No cyber security plan or road map defined.	Establish an IT security plan or roadmap that covers all relevant business objectives	Annual CSAT assessment; Purview Compliance Manager; Priva Subject Rights Requests; Defender for Cloud	A1: Governance; A2: Risk Management
20. AQ 2. Data Governance	How is data risk management organized within your organization?	Basic (1) No risk management or	Implement a basic risk management process.		A2: Risk Management

**EXAMPLE VERSION – DO NOT DISTRIBUTE TO OTHERS – SUBJECT TO NDA.**

Softwerx Ltd and Contoso confidential.

Do not copy, distribute, or reproduce - in any form - to a third party.

		assessments are performed.			
--	--	----------------------------	--	--	--

High					
Topic	Question	Answer	Advice	Advised Products	NIS2 Principle
19. AQ 1. IT Governance	How are security tasks segregated between positions?	Standardized (2) The division of security tasks are established and documented at the department level. The document contains the responsibilities.	Improve the division of tasks, responsibilities, authorizations and reporting lines are established and documented at the organizational level.	Entra Identity Governance; Defender Cloud Security Posture Management	A1: Governance

Example

**EXAMPLE VERSION – DO NOT DISTRIBUTE TO OTHERS – SUBJECT TO NDA**

Softwerx Ltd and Contoso confidential.

Do not copy, distribute, or reproduce - in any form - to a third party.

## Technical Data and Analysis

Besides the interview with regards to the CIS and additional controls, we conducted an automated scan throughout (a selection of) your IT environment. We have collected information regarding, among others, the current state of configuration of your IT landscape, discovery of personal identifiable information, identity management, software versioning, and many more.

This chapter summarizes the facts we have found along with the respective security risk/threat and recommendations to remediate those vulnerabilities.

### Technical data related to CIS controls

The following tools were used to gather the information:

- Cyber Security Assessment Tool (CSAT).

#### CIS Control 1: Inventory and Control of Enterprise Assets

The Cyber Security Assessment Tool does not provide technical data for this control, though the control is covered in the questionnaire interview. The numbers below were provided by the IT team.

Inventory	Type	Count	Total
Physical Servers	Windows	352	375
	Linux or Other	23	
Virtual Servers	Windows	7.657	13.797
	Linux or other	3.523	
End-User Devices	Desktops	2.625	
	Mobile Devices:		
	- Laptops		
	- Smartphones		
- Tablets			

#### Conclusions and Recommendations

Currently there is no inventory available for the organization's assets. It is recommended to establish and maintain regularly an accurate, detailed, and up-to-date inventory of all assets in the organization. This inventory will help when defending against assets that the organization does not own or manage.

#### CIS Control 2: Inventory and Control of Software Assets

CSAT Output – Operating system version status

DISCOVERED WINDOWS ENDPOINT OS	
Microsoft Windows Server 2022 Datacenter Azure Edition	3
Microsoft Windows 11 Enterprise	2

#### Conclusions and Recommendations

**EXAMPLE VERSION - DO NOT DISTRIBUTE TO OTHERS - SUBJECT TO NDA**

Softwerx Ltd and Contoso confidential.

Do not copy, distribute, or reproduce - in any form - to a third party.

## Windows Operating Systems (OS)

- **five (almost) end-of-life operating systems** were found. It is recommended to phase out these operating systems (OS) as soon as possible. For **Windows Server 2008 (R2) and Server 2012 (R2)** applies that if you move these OS to Azure, you will receive extended Security Support. More information can be found on <https://docs.microsoft.com/en-us/windows-server/get-started/extended-security-updates-overview>.
- One or more Windows 10 endpoints have been found that are not running the latest build of Windows 10. The current build(s) of Windows 10 are supported. However, the support for the Windows 10 build is limited.

### *CSAT Output - AD Computer account overview*

AD COMPUTER ACCOUNT (ENABLED COMPUTER ACCOUNT) - EXPANDEDUNIVERSE	
Enabled Accounts	8
Disabled Accounts	1
Client OS active last 30 days	2
Server OS active last 30 days	3
Client OS inactive more than 30 days	0
Server OS inactive more than 30 days	2

OS LOGGED ON TO AD (LAST 30 DAYS)	
No data	1
Windows 11 Enterprise	1
Windows Server 2022 Datacenter Azure Edition	3

### *CSAT Output - Installed Applications*

CVE INFORMATION FOUND ON THE SCANNED ENDPOINTS	
Critical CVE's found	9
High CVE's found	2
Medium CVE's found	0
Low CVE's found	0

## Conclusions and Recommendations

### Applications

- The (almost) end of life software products **Java and 7-Zip** have been found, start phasing these products out as soon as possible.

- Different (old) versions of applications such as **Winrar** and **CCleaner** have been found. Update these applications to the latest version.
- Based on the endpoint scan, one or more applications have been found that have critical or high severity Common Vulnerability Scoring System (CVSS) score from the Common Vulnerabilities and Exposures (CVE). Usually, the vendor provides an update before the CVE is made public, or a workaround/mitigation is made available. It is recommended to always run the latest version of the software provided by the vendor.

### CSAT Output – Licensing Status

MICROSOFT 365 LICENSES - EXPANDED.ONMICROSOFT.COM				
Product	Consumed	Prepaid	Available	Capability Status
MICROSOFT FLOW FREE	44	10000	9956	Enabled
Microsoft 365 E5	1	1	0	Enabled
Microsoft_Intune_Suite	1	1	0	Enabled
Office 365 Advanced GenThreat Protection (Plan 1)	0	0	0	LockedOut
POWER BI (FREE)	46	500	454	Enabled
RMSBASIC	0	1	1	Enabled
Remote_Help_AddOn	1	1	0	Enabled
WINDOWS STORE FOR BUSINESS	0	50	50	Enabled

### Conclusions and Recommendations

Make sure that the clients are always running on the most stable and supported release from the software. Software tooling like **Defender for Endpoint** or **Microsoft Defender for Cloud** can help you to gain insights in the installed applications on the endpoints. Tooling like **Microsoft Defender for Cloud Apps** can help you to discover the use of Shadow IT Cloud applications.

### CSAT Output – Azure Arc

AZURE ARC - VISUAL STUDIO ENTERPRISE	
Total number of machines connected to Azure Arc	3
Number of machines with Arc agent status expired	0
Number of Arc machines with missing updates	1
Number of machines with out of date OS	0
Number of Machines without the monitoring extension	1

### Conclusions and Recommendations

From the data, it appears that no Azure Arc Machines are present. Azure Arc provides a unified management platform for on-premises, multi-cloud, and edge environments, enhancing security and compliance. It allows you to leverage Azure services anywhere, ensuring consistent operations and innovation. Additionally, it simplifies hybrid and multi-cloud management, reducing complexity and operational overhead.

## CIS Control 3: Data Protection

### CSAT Output – BitLocker Encryption Status

BITLOCKER	
Client Endpoints without BitLocker encryption	164
Server Endpoints without BitLocker encryption	854
Microsoft Intune devices with BitLocker status off - expanded.onmicrosoft.com	463

### CSAT Output – Flagged endpoints

#### Endpoints overview

Flag	Machine/IP	Operating system	AV Name	AV Status	AV Definition	Total active AV	SMBv1 Client	SMBv1 Server	BitLocker	Threat
⚠️	Win2008PC 172.20.100.150	Microsoft Windows Server 2008 R2 Version: 7601	*No AV API*	UNKNOWN		0	Yes	No	No	▲ Bad
⚠️	Win7PC 172.20.100.147	Microsoft Windows 7 Professional Version: 7601	Microsoft Security E	ON	UP_TO_DATE	1	Yes	No	No	▲ Bad
⚠️	WinVistaPC 172.20.100.168	Microsoft Windows Vista™ Ultima Version: 6002	*No AV API*	UNKNOWN	UNKNOWN	0	Yes	No	No	▲ Suspicious
⚠️	VMEU-DCCore1 172.16.5.101	Microsoft Windows Server 2016 Dat Version: 1607	Windows Defender	UNKNOWN		0	Yes	No	Yes	○ Normal
Flag	Machine/IP	Operating system	AV Name	AV Status	AV Definition	Total active AV	SMBv1 Client	SMBv1 Server	BitLocker	Threat
⚠️	VMEU-DC2 172.16.5.102	Microsoft Windows Server 2016 Dat Version: 1607	Windows Defender	UNKNOWN		0	Yes	No	Yes	○ Normal
⚠️	WIN-RF4JEBCAUJ5 172.20.100.151	Microsoft Windows Server 2016 Stai Version: 1607	Windows Defender	UNKNOWN		0	Yes	No	No	○ Normal

## Conclusions and Recommendations.

### BitLocker Encryption

- 198 Client endpoints do not have BitLocker encryption enabled.
- 361 Server endpoints do not have BitLocker encryption enabled.

When unencrypted storage falls into the wrong hands, it poses a high risk of data loss. This specifically applies to mobile devices like laptops, tablets, and smartphones. However, desktop computers that reside in (semi-)public places could fall into the same risk category, as well as server storage when it is being replaced.

### CSAT Output – Azure Storage accounts

AZURE STORAGE ACCOUNTS - EXPANDED.ONMICROSOFT.COM	
Storage Accounts without HTTPS	0
Storage Accounts where TLS 1.1 or lower are allowed	2
Storage Accounts where Blob public access is allowed	3
Storage Accounts where no encryption is used	0
Storage Accounts where partly encryption is used	0

## Conclusions and Recommendations.

**EXAMPLE VERSION - DO NOT DISTRIBUTE TO OTHERS - SUBJECT TO NDA**  
**Softwerx Ltd and Contoso confidential.**

**Do not copy, distribute, or reproduce - in any form - to a third party.**

## Azure storage accounts

- 4 Storage accounts do not have HTTPS enabled.
- 34 Storage accounts have TLS 1.1 or lower enabled.
- 25 Storage accounts do not have encryption enabled.

To ensure the confidentiality and integrity of data in transit to and from the Azure Storage accounts it is recommended to always enforce a secure connection. It is recommended to only allow HTTPS connections and the latest TLS version to and from Azure storage accounts.

To fully protect your Azure storage accounts, enable Microsoft Defender for Storage to detect potential threats. It helps prevent three major impacts on your data and workload: malicious file uploads, sensitive data exfiltration, and data corruption. Additionally, the 'Sensitive Data Discovery' engine, an agentless tool that uses a smart sampling method to find resources with sensitive data, can help identify and protect sensitive data in your accounts.

### CSAT Output – SharePoint Site Permissions

Flag	Site	Title	Sharing Capability	Site Owner	Last Modified Date
	<a href="https://expanded.sharepoint.com/sites/EUDepartments">https://expanded.sharepoint.com/sites/EUDepartments</a>	Expanded Universe Depart	ExternalUserAndGuestSharing		11-10-2020
	<a href="https://expanded.sharepoint.com/sites/EUDeptFinance">https://expanded.sharepoint.com/sites/EUDeptFinance</a>	Finance Department	ExternalUserAndGuestSharing		12-10-2020
	<a href="https://expanded.sharepoint.com/sites/EUDeptHR">https://expanded.sharepoint.com/sites/EUDeptHR</a>	HR Department	ExternalUserAndGuestSharing		12-10-2020
	<a href="https://expanded.sharepoint.com/sites/EUProjects">https://expanded.sharepoint.com/sites/EUProjects</a>	Expanded Universe Project	ExternalUserAndGuestSharing		11-10-2020
	<a href="https://expanded.sharepoint.com/sites/itadmingroup">https://expanded.sharepoint.com/sites/itadmingroup</a>	IT admin group	ExternalUserSharingOnly		12-10-2020

### Conclusions and Recommendations

Data breaches often result from unauthorized or poorly managed access. Organizations should encrypt sensitive data in transit and restrict access to critical resources. **Microsoft Entra Private Access** ensures encrypted, secure access to private applications. Additionally, **Microsoft Entra Identity Governance** enforces access control policies to protect sensitive data by limiting access to authorized users only.

### CSAT Output – SharePoint Externally Shared

Flag	Name	Email	Permission	Path	Role	Anonymous Access	Threat ↑
	Doeke Moerman	Doeke.Moerman@	Beperkte toegang	https://expanded.sharepoint.com/sites/EUComm	(Directly Assigned)	Yes	Suspicious
	Doeke Moerman	Doeke.Moerman@	Beperkte toegang	/sites/EUCommSolarFlares/Gedeelde documente	(Directly Assigned)	Yes	Suspicious
	Peaav van Amelsvo	Peaav.van.Amelsvo	Beperkte toegang	/sites/EUCommSolarFlares/Gedeelde documente	(Directly Assigned)	Yes	Suspicious
	Doeke Moerman	Doeke.Moerman@	Lezen	/sites/EUCommSpaceconference/Gedeelde docu	(Directly Assigned)	Yes	Suspicious
	Doeke Moerman	Doeke.Moerman@	Lezen	/sites/EUProiMissiontoMars/Gedeelde document	(Directly Assigned)	Yes	Suspicious

### CSAT Output – Google Workspace Drive Externally Shared

GOOGLE WORKSPACE - GENTP.CYBERSECURITYASSESSMENTTOOL.NL	
PII documents	7
Number of shared files	18

## Conclusions and Recommendations

### Externally sharing data

Sharing data can have a (significant) risk impact when shared with external users like business partners, customers/consumers, through SharePoint and Teams. While mostly under legitimate reasons, external users are not managed centrally. Internal user accounts are probably disabled when someone leaves the organization, or the user is removed from the access group(s) when moving to another role. Tooling like Microsoft Defender for Cloud Apps contains 'sharing control' policies that can detect and enforce Automate governance and guarantee a compliant collaboration environment

To govern the collaboration environment to get and hold it in a compliant state, automation can help. Give controlled access to sites and teams by only let the owner use defined functional roles. The owner is not the owner of the site or team and cannot modify permissions by himself. Only the preset roles can be used.

### CSAT Output – Potential PII Data

Document Name	Path	#Keywords found	#Total	Threat ↑
Password document	<a href="https://expanded.sharepoint.com/sites/EUDeptIT/Gedeelde documenten/General/Passw...">https://expanded.sharepoint.com/sites/EUDeptIT/Gedeelde documenten/General/Passw...</a>	Password Userna...	3	⚠ Suspicious
Networks Operational Ha...	<a href="https://expanded.sharepoint.com/sites/EUHome/Gedeelde documenten/IT general/Net...">https://expanded.sharepoint.com/sites/EUHome/Gedeelde documenten/IT general/Net...</a>	Password Bank a...	7	⚠ Suspicious
Password document	<a href="https://expanded.sharepoint.com/sites/EUIdeas/Gedeelde documenten/Password docu...">https://expanded.sharepoint.com/sites/EUIdeas/Gedeelde documenten/Password docu...</a>	Password Userna...	3	⚠ Suspicious
Employee quick start for ...	<a href="https://expanded.sharepoint.com/sites/EUDeptIT/Gedeelde documenten/General/Office...">https://expanded.sharepoint.com/sites/EUDeptIT/Gedeelde documenten/General/Office...</a>	Password Accou...	2	⚠ Suspicious

GENTPCYBERSECURITYASSESSMENTTOOL.NL

Flag	Document Name	Path	#Keywords found	Writers Can Share	Last Edited By	Shared	#Total	Threat
🚫	1. Ano natsu ni sake acoustic.mp3	Show Ukiyo Yosakoi			mizuotoproject	Yes	0	🟢 Normal
🚫	2. Wakamono Subete acoustic.mp3	Show Ukiyo Yosakoi			mizuotoproject	Yes	0	🟢 Normal
🚫	[FURIN] MIZUOTO PROJECT				ukiyovlu	Yes	0	🟢 Normal

GENTPCYBERSECURITYASSESSMENTTOOL.NL

Flag	Document Name	Path	#Keywords found	Writers Can Share	Last Edited By	Shared	#Total	Threat
🚫	Show Ukiyo Yosakoi				mizuotoproject	Yes	0	🟢 Normal
🚫	[FURIN] MIZUOTO PROJECT	[FURIN] MIZUOTO PROJECT				Yes	0	🟢 Normal

Example

**EXAMPLE VERSION - DO NOT DISTRIBUTE TO OTHERS - SUBJECT TO NDA**

Softwerx Ltd and Contoso confidential.

Do not copy, distribute, or reproduce - in any form - to a third party.

## CSAT Output – Microsoft 365 overview

MICROSOFT 365 - EXPANDED.ONMICROSOFT.COM	
PII documents	15
Externally shared items	69
Anonymous Link Count	0
Internal Sharing Count	0
Secure Link For Guest Count	0
Secure Link For Member Count	0

Number of enabled Guests users	5
Number of enabled accounts (guests excluded)	42
Number of disabled accounts (guest excluded)	2
Number of enabled accounts after 30 days of inactivity	8
Number of enabled accounts after 90 days of inactivity	8
Number of enabled accounts where no login was found	35
Number of accounts that are flagged as bad	0

## CSAT Output – SharePoint Data and Sensitivity labels

SHAREPOINT ONLINE DATA	
Total number of files not modified for more than 180 days	2603
Total number of site collection where more than 65% of files not modified for more than 180 days	5
Total number of files not modified for more than 365 days	1611
Total number of site collection where more than 65% of files not modified for more than 365 days	4
Total number of files without purview labels	2668

## Conclusions and Recommendations.

### Potential PII Data

- **46** Documents have been flagged that require special attention. These documents contain keywords such as **Password**.

On the scanned site collections there are no documents labelled, leading to potential risks related to data loss, unauthorized access, and non-compliance with regulatory requirements. To mitigate these risks, it is recommended to implement file labelling.

Leveraging **Microsoft Purview Information Protection (MPIP) with a Microsoft 365 E5** license allows for the automatic labelling and protection of data. Automatic labelling reduces the risk of human error and ensures compliance with regulatory requirements. By implementing this feature, organizations can safeguard their data more effectively and maintain a higher level of data security.

**EXAMPLE VERSION - DO NOT DISTRIBUTE TO OTHERS - SUBJECT TO NDA**  
**Softwerx Ltd and Contoso confidential.**

**Do not copy, distribute, or reproduce - in any form - to a third party.**

Stale data, which refers to outdated and unused information that remains stored within an organization, can pose significant security risks. Based on the scanned data, there are SharePoint team sites found where more than 65% of the files are not modified for more than 180 days. Such data is often overlooked during security audits and can become an easy target for cyberattacks. It is recommended to regular audit and implement data lifecycle management to identify and securely dispose of stale data. By systematically removing or archiving outdated information, organizations can reduce their attack surface and mitigate the risk of data leakage.

By implementing a feature called Conditional Access, access to sensitive information can be restricted or granted to users using devices that are either managed or unmanaged, while performing a risk analysis on several parameters to check if user should get access to that specific data, application, or resource.

#### CSAT Output – Endpoint Shares

Server Name	Path	Shared Name	Size	Description
VMEU-DC1	C:\Install	Install\$	1.43 GB	
VMEU-MGMT2	C:\Localdata	EU Local data	42.17 MB	
VMEU-DC1	C:\Shares\IT	IT Share	0	

#### Conclusions and Recommendations

##### Endpoints Shares

Shares might contain confidential data. We recommend creating procedures for the business to do attestation on user permissions and assign an owner to this. With this periodic check you can check if the users have the rights, they need and cannot see data they are not supposed to see.

#### CIS Control 4: Secure Configuration of Enterprise Assets and Software

##### CSAT Output – Active Directory Domain and Forest function levels

DOMAIN FUNCTIONAL LEVEL - EXPANDEDUNIVERSE	
Domain Name	expandeduniverse
Domain Functional Level	WINDOWS SERVER 2016
Forest Functional Level	WINDOWS SERVER 2016

#### Conclusions and Recommendations

##### Active Directory Domain and Forest function levels

It is recommended to Upgrade the Active Directory Domain and Forest Functional levels to the highest available level. Each new version of Active Directory on Windows Server

**EXAMPLE VERSION - DO NOT DISTRIBUTE TO OTHERS - SUBJECT TO NDA**

**Softwerx Ltd and Contoso confidential.**

**Do not copy, distribute, or reproduce - in any form - to a third party.**

incorporates new or improved (security) features. Those features can only be used when all domain controllers (DC), in either the domain or forest, are at a certain minimal level.

In Windows Server 2025 for example, there are various new security features introduced, including:

- LDAP Support for TLS 1.3: This version of TLS enhances security by eliminating obsolete cryptographic algorithms and encrypting more of the handshake process, thereby providing a more secure connection for LDAP communications.
- Kerberos Support for AES SHA-256 and AES SHA-384: These stronger encryption methods improve the cryptographic strength of Kerberos authentication, offering better protection against potential attacks and enhancing overall security for authentication processes.

By ensuring that all domain controllers are updated and that functional levels are raised, your organization can fully leverage these advanced security features, significantly strengthening your security posture against evolving threats.

#### CSAT Output – Endpoints Secure Configuration

SECURE CONFIGURATION	
Incoming RDP enabled with no NLA	2
Endpoints with LM Compatibility lower than 5	1
Autorun Enabled	1
PowerShell 2.0 Enabled	1

### Conclusions and Recommendations

#### Operating system hardening baseline

Hardening of systems is not applied on systems which is why old, unsafe security protocols are still allowed. Advice is to implement the **CIS hardened images** from the **Azure VM store** to deploy new VM's safe and faster. CIS has various free benchmarks available on <https://www.cisecurity.org/cis-benchmarks/>.

#### Secure configuration of vulnerable services

**33258** endpoints found with **SMBv1 not disabled**, make sure SMBv1 is disabled on all systems. It is advised to use newer version of SMBv2 or SMBv3 to enhance security.

**353** endpoints found that have **RDP enabled without NLA**, make sure managed RDP endpoints have NLA enabled on remote machines or disable RDP on machines if unnecessary.

#### CSAT Output – Firewall GPO status

Windows endpoints with any disabled firewalls GPO	2
---	---

#### Endpoints with firewall disabled GPO

**EXAMPLE VERSION - DO NOT DISTRIBUTE TO OTHERS - SUBJECT TO NDA**

Softwerx Ltd and Contoso confidential.

Do not copy, distribute, or reproduce - in any form - to a third party.

Endpoints with disabled Domain firewall	0
Endpoints with disabled Private firewall	1
Endpoints with disabled Public firewall	1

### Conclusions and Recommendations

- **294** Endpoints found with one or more disabled Windows Firewall profiles; it is advised to enable the firewalls on these machines.

Windows Firewall provides protection from network attacks on the endpoints that pass through your perimeter network or originate inside your organization, such as Trojan horse attacks, worms, or any other type of malicious program spread through unsolicited incoming traffic. Any infected machine that gets access to your corporate intranet can potentially make a connection to unprotected endpoints or servers and compromises it by exposing a vulnerability in a Windows service or 3rd-party application.

Recommended is to implement **Defender for Endpoint** and enforce it on all endpoints. It is a total EDR (Endpoint Detection and Response) solution, which provides preventative endpoint protection, post-breach detection, automated investigation, and response.

### CSAT Output – Intune Devices

INTUNE DEVICES - EXPANDED.ONMICROSOFT.COM	
Computer accounts	4
Intune Devices active 30 days	0
Intune Devices inactive 30 days	0
Intune Devices marked as not compliant	4
Number of unsupported OSes found in Microsoft Intune	3

### Conclusions and Recommendations

- 2345 Intune device are inactive more than 30 days. Review these devices and remove the unused devices.
- 10 Intune devices are marked as not compliant. Review and enforce policies on these devices to get them compliant.

There are Intune devices found that are non-compliant. It is recommended to clean up old devices and only allow compliant devices to connect to the organization environment.

## CIS Control 5: Account Management

### CSAT Output – Active Directory Account Status

AD ACCOUNTS - EXPANDEDUNIVERSE	
Enabled Accounts (without expired accounts)	25
Disabled Accounts	4
Enabled Accounts no login more than 30 days	3
Enabled Accounts no login more than 90 days	3
Enabled Accounts never logged in	20
Accounts flagged as bad	0
Expired Accounts	0

### CSAT Output – Active Directory User Account Control Flags (enabled accounts)

AD UAC DETAILS ENABLED ACCOUNTS - EXPANDEDUNIVERSE	
Password is not Required	1
Cannot Change Password	0
Don't Require PreAuth	1
Reversible Text Password	0
Password is not going to expire	6
Smartcard Required	0
Use DES Key Only	1
Trusted To Auth For Delegation	0
Partial Secrets Account	0

## Conclusions and Recommendations

### Active Directory Accounts

- **318** Accounts have **not logged on for 90 days** and 218 accounts have **never logged on**. Review these accounts and disable the unused accounts.
- **521** Accounts are **disabled**, clean these accounts up.
- **13** Accounts **cannot change their passwords**, review these accounts and remove this setting if possible.

## CSAT Output – Active Directory Password policy

PASSWORD POLICY - EXPANDEDUNIVERSE	
Complex password required	true
Lockout Duration in Minutes	30
Lockout Threshold	0
Max Password Age	42
Min Password Age	1
Min Password Length	7
Password History	24

## Conclusions and Recommendations

### Password Policy

It is advised to configure the password policy to recommended practices such as:

1. Maximum password age: **60** or **90** days
2. Password must meet complexity requirements: **Enabled (true)**
3. Account lockout threshold: **4** or **5** invalid sign-in attempts
4. Password history: **10** or **24** passwords
5. Minimum password length: **8** or **12** characters

## CSAT Output – Microsoft Entra ID Account status

Tenant Name	External User	Enabled User	Disabled User	Enabled User without MFA	O365 Audit log search
expanded.onmicrosoft.com	5	42	2	35	Yes

## CSAT Output – Google Workspace

GOOGLE WORKSPACE INFORMATION - GENTP.CYBERSECURITYASSESSMENTTOOL.NL	
Enabled users	21
Disabled users (Deleted, Suspended, and Archived)	0
Enabled Users Without MFA	14

## Conclusions and Recommendations

### Microsoft Entra ID Users

A strong, complex password is the first line of defence in protecting your accounts. Multi Factor Authentication provides a second line of defence. It is advised to implement MFA together with Conditional Access to protect your users, as this is highly effective at stopping attacks. Enforce it with **Azure MFA** and **Microsoft Entra ID Conditional Access**. By setting up a Conditional Access policy you can block access to resources for devices that exceed the threat level you set in your compliance policy.

**EXAMPLE VERSION - DO NOT DISTRIBUTE TO OTHERS - SUBJECT TO NDA**

**Softwerx Ltd and Contoso confidential.**

**Do not copy, distribute, or reproduce - in any form - to a third party.**

Multi-Factor Authentication (MFA) fatigue attacks occur when users receive repeated authentication requests, leading them to approve one out of frustration or by mistake. To mitigate this risk, it is recommended to implement security measures that prevent such attacks.

- Require Additional Context in MFA Approvals – Enable number matching and application details in Microsoft Authenticator to reduce accidental approvals.
- Block MFA Approvals from Risky Locations – Define trusted locations and block MFA requests from high-risk geographies or unauthorized networks.

### Google Workspace

During the analysis several disabled (service) accounts were found. When an account is disabled, it still exists in the system, allowing for potential unauthorized access. Disabled accounts can be targeted by malicious actors who may attempt to exploit the account to gain access to sensitive data or resources. We recommend cleaning up these disabled (service) accounts in your Google Workspace environment.

### *CSAT Output – Microsoft Entra ID – External Users*

Flag	Name	Email	Enabled
	*****@expanded.onmicrosoft.com	*****@M365x162515.onmicrosoft.com	No
	*****@expanded.onmicrosoft.com	*****@outlook.com	Yes
	*****@expanded.onmicrosoft.com	*****@outlook.com	Yes
	*****@expanded.onmicrosoft.com	*****@outlook.com	Yes

## Conclusions and Recommendations

### Microsoft Entra ID External Users

- There were external users found in Microsoft Entra ID that have been invited on their personal email account. Review these accounts and disable them where needed.

It is recommended to review the external users, and their access authorizations regularly. Especially users who have been invited on their personal email account, such as Outlook, Gmail, Hotmail, Yahoo mail etc. When these external users leave their organization, and your organization will not be notified, the users will still have access through their personal email account.

### *CSAT Output - Local accounts*

Inventory	Count
Local Administrator account enabled on scanned endpoints	253
Guest accounts enabled on scanned endpoints	2773

## Conclusions and Recommendations

### Local Accounts

- There are endpoint(s) found where the default local Administrator(s) account(s) is enabled.
- There are endpoint(s) found where the guest(s) account(s) is enabled.

Local accounts should not be used on an organization’s network with a centralized authentication platform. However sometimes a local administrator is necessary, we

recommend implementing Local Administrator Password Solutions (LAPS). LAPS is a tool to automatically manage the local admin passwords on domain joined Windows machines and keep them stored in AD that can be looked up whenever you need them.

## CIS Control 6: Access Control Management

### Windows Active Directory Domain Services

CSAT Output – Active Directory Administrative Groups

AD ADMINISTRATORS - EXPANDEDUNIVERSE	
Built in Administrators domain group	6
Domain Admin	3
Enterprise Admin	2
Schema Admin	1
Users with admin count	4

### Conclusions and Recommendations

- **A high number of Domain Admins was found.** Members of this group have full control of the domain; therefore, membership must be limited as much as possible. Review these accounts and clean up old/unused accounts.
- **A high number of Enterprise admins was found.** Members of this group have full control of all domains in a forest. Ideally this group should only contain 0 or 1 user. Review these accounts and clean up old/unused accounts.
- **There is no clear separation between administrator accounts and normal user accounts.**  
This is a risk, if a malicious program or attackers are able to get control of your user account, they can do a lot more damage with an administrator account than with a standard account

### Microsoft Entra ID

CSAT Output – Microsoft Entra ID roles

Roles are only shown if the role contains one or more members.

#### MICROSOFT ENTRA ID USER ROLES - EXPANDED.ONMICROSOFT.COM

Directory Synchronization Accounts	1
Microsoft Entra ID Joined Device Local Administrator	3
Global Administrator	1

#### CSAT Output – Microsoft Entra ID Administrators status

#### MICROSOFT ENTRA ID ADMINISTRATORS - EXPANDED.ONMICROSOFT.COM

Number of enabled accounts with Microsoft Entra ID user roles without MFA	0
Total roles used with privileged identity management	8
Privileged identity management assignments without an end date	31
Users with the Global admin role active or eligible	4
Total of guest users with role assignments	0

### Conclusions and Recommendations

It is recommended to avoid using on-premises synchronized accounts. for administrative role assignments. If you are using a synced on-premises account, and that account is compromised, it can also compromise your cloud resources as well. We recommend only assigning administrative roles to cloud only accounts.

Administrator accounts bring high risk to an organization's network, since they have access to your network, or systems and sensitive data. Therefore, it is recommended to limit the number of administrators as much as possible, and to enable Advanced Multi Factor Authentication (MFA) included in the Microsoft Entra ID Suite, for all privileged accounts. Our advice is to implement a process to regularly review authorizations for privileged accounts.

### Azure Subscriptions

#### CSAT Output – Azure Subscription roles

Roles are only shown if the role contains one or more members.

**AZURE SUBSCRIPTION ROLE ASSIGNMENT - EXPANDED.ONMICROSOFT.COM  
SUBSCRIPTION - VISUAL STUDIO ENTERPRISE SUBSCRIPTION – MPN - QS**

Owner	5
Reader	5
Security Admin	4
User Access Administrator	4
Azure Arc Enabled Kubernetes Cluster User Role	1
Resource Policy Contributor	1

### Conclusions and Recommendations

Based on the subscription information, it appears that only the Owner role is being used. It is recommended to use the principle of least privilege for all administrative roles. The principle of least privilege is to assign only the administrative permissions that are required to complete the specific task. Therefore, it is recommended to review the administrative tasks the users perform and only assign the administrative role(s) that are necessary to complete their task(s).

### CSAT Output – Azure Key Vault

**AZURE KEY VAULTS - EXPANDED.ONMICROSOFT.COM**

Total number of key vaults	2
Number of key vaults without purge protection	0
Number of certificates older than one year	0
Number of keys older than one year	0
Number of secrets older than one year	0
Number of Disk encryption keys found with encryption algorithms less than SHA-256	0

### Conclusions and Recommendations

There are key vault secrets, certificates, or keys that are older than one year. It is essential to regularly update these items to mitigate security risks, as older secrets may become vulnerable to exposure or compromise. Keeping them current helps ensure that cryptographic practices remain robust against evolving threats. Additionally, regular updates support compliance with industry standards and regulations, which often mandate timely key management to protect sensitive data effectively.

## CIS Control 7: Continuous Vulnerability Management

### CSAT Output – Update Status

Endpoints with missing critical updates	0
Endpoints with missing cumulative updates	7

EndpointName	Critical	Important	Moderate	Low	Cumulative updates	Other
LAPTOP-1I2J23EK	0	0	0	0	1	69
VMEU-MGMT2	0	0	0	0	2	7
VMEU-CSAT2022	0	0	0	0	2	5
VMEU-DC1	0	0	0	0	2	5

### Conclusions and Recommendations

- 465 found with missing cumulative updates, roll out the available updates as soon as possible.

Operating Systems vulnerabilities are a potential security threat for the IT infrastructure. Especially if the security vulnerabilities are publicly known, attacking your organization through rapidly spreading mechanisms. It is recommended to establish a patch management process, adopting the publishing cycle for Microsoft security updates (patch Tuesday) and feature updates, and to enforce updating all your systems safely and effectively. It is also recommended to regularly gain insights on the patch status of all endpoints.

Not all the cloud workload protection plans are enabled in Microsoft Defender for Cloud. Enabling these protection plans is crucial for robust security across your cloud and hybrid environments, offering advanced threat detection and continuous monitoring. This enhances your security posture, streamlines compliance with industry standards, and ensures swift responses to potential threats. With seamless integration across platforms, it provides comprehensive protection, mitigating risks and safeguarding your critical assets.

Microsoft Security Copilot, has the capability to respond to your specific questions and suggest action to mitigate those concerns. For example, questions can be asked which devices are not compliant and a list of devices will be shown.

## CIS Control 8: Audit Log Management

CSAT Output – Active Directory Bad password attempts

### AD BAD PASSWORD ATTEMPTS (ENABLED ACCOUNTS, TOP 5) - EXPANDEDUNIVERSE

S-1-5-21-2697241934-572864812-3163282084-1115	45
S-1-5-21-2697241934-572864812-3163282084-1118	16
S-1-5-21-2697241934-572864812-3163282084-1112	15
S-1-5-21-2697241934-572864812-3163282084-1108	4
S-1-5-21-2697241934-572864812-3163282084-1113	3

\*Usernames have been changed to the user SID; the full details can be found in CSAT.

### Conclusions and Recommendations

- A high number of failed password attempts were retrieved. This is a sign that the account(s) are being attacked. We recommend checking the account(s), reset the password, enable MFA, and inform the user how to proceed.

To mitigate the risk of cyberattacks through stolen identities, organizations should monitor suspicious logons. Implementing **Microsoft Defender for Identity** is recommended, as it provides early warnings about attacks on on-premises domain controllers. Combining it with **Microsoft Entra ID Identity Protection** for cloud users enhances protection across both on-premises and cloud environments.

#### Audit logs

The CSAT tool does not assess inventory of the Audit logs. This control is covered in chapter 4, CIS Controls.

### Conclusions and Recommendations

Auditing on Azure SQL server should be enabled. Enable auditing on your SQL Server to track database activities across all databases on the server and save them in an audit log.

why a SIEM solution is so essential. Therefore, it is advised to consider implementing **Microsoft Sentinel** and enforce collecting logs on all cloud and on-premises systems.

## CIS Control 9: Email and Web Browser Protections

CSAT Output – Email authentication and DNS protection

Inventory	Value	Notes
expandeduniverse.nl		
DNSSEC enabled	Yes	
SPF record	r0Xh73bkxzg	
DKIM record	selector1: v=DKIM1; k=rsa;   selector2: v=DKIM1; k=rsa;	
DMARC record	v=DMARC1;p=reject;pct=100;rua=mailto:	
CAA records	[{"Flags":0,"Tag":"issuewild","Value":"sectigo.com"}]	

### Conclusions and Recommendations

**EXAMPLE VERSION - DO NOT DISTRIBUTE TO OTHERS - SUBJECT TO NDA**  
**Softwerx Ltd and Contoso confidential.**

**Do not copy, distribute, or reproduce - in any form - to a third party.**

## Email authentication and DNS protection

- **The SPF record is setup with a soft fail.** With a soft fail the senders that are not in the SPF record are still allowed to send e-mail from the e-mail domain. If the SPF records is changed to a hard fail the e-mails send from the not allowed addresses will be discarded.
- **The DMARC record is setup without a policy.** The DMARC policy determines what will happen with the messages if the SPF and/or DKIM check fail. It is recommended to set the policy to 'Reject'. With the reject policy the unauthorized mail will be dropped.

It is recommended to implement Microsoft 365 Advanced Threat Protection (Microsoft Defender for Office 365). This solution, with the correct policies places, safeguards your organization against malicious threats posed by email messages, links (URLs) and collaboration tools.

### CSAT Output – Insights from Web Behaviour

AI AND LARGE LANGUAGE MODEL USAGE		
Microsoft Copilot	60% of the endpoints	35 visits
OpenAI ChatGPT	60% of the endpoints	640 visits
Google Gemini	Not found	Not found
Anthropic Claude	Not found	Not found

\*The items shown are calculated from the scanned Windows endpoints where the browser scan feature is enabled.

## Conclusions and Recommendations

Based on the collected data it appears that several different AI solutions are used. It is recommended to standardize on a single AI provider like Microsoft Copilot. Utilizing multiple AI solutions can lead to inconsistencies, integration challenges, and security vulnerabilities. By choosing one AI provider, your organization can ensure a unified approach to AI implementation, streamline management and support, and maintain better control over AI-driven processes. This approach will also enable more efficient use of resources and facilitate compliance with your organization's policies and standards.

Encouraging a culture of continuous learning and adaptation within your IT team will enable them to stay updated on the latest AI and cybersecurity advancements. Support participation in training programs, certifications, and industry conferences to ensure your team is equipped with the necessary knowledge and skills to effectively manage AI-driven security systems.

## CIS Control 10: Malware Defenses

CSAT Output – Antivirus overview

ENDPOINTS	
Server endpoints with no Windows Defender	234
Client endpoints with no Antivirus	64
Endpoints with out of date Antivirus definitions	74

### Conclusions and Recommendations

- **74** Endpoints found with outdated antivirus definitions. These endpoints are vulnerable for attacks; outdated antivirus software cannot recognize and respond to the latest threats.
- **64** Endpoints found with disabled or no antivirus. Mitigate this risk by enabling antivirus software on these machines.

## CIS Control 11: Data Recovery

The Cyber Security Assessment Tool does not provide technical data for this control, though the control is covered in the questionnaire interview.

### Conclusions and Recommendations.

To maintain compliance with many regulations, engage in disaster recovery drills every 6 months. Ensure that the procedures are not only available online, but also in hard copies at designated secure places.

## CIS Control 12: Network Infrastructure Management

CSAT Output – Azure Network Security group status

AZURE NSG RULES - EXPANDED.ONMICROSOFT.COM	
Number of allow rules with Any to Any on all ports	1
Number of allow rules with Any to Any on specific ports	3
Number of allow rules with Any to Any to RDP port	1

### Conclusions and Recommendations.

Subnets should be associated with a Network Security Group. Protect your subnet from potential threats by restricting access to it with a Network Security Group (NSG). NSGs contain a list of Access Control List (ACL) rules that allow or deny network traffic to your subnet.

**EXAMPLE VERSION - DO NOT DISTRIBUTE TO OTHERS - SUBJECT TO NDA**  
**Softwerx Ltd and Contoso confidential.**

**Do not copy, distribute, or reproduce - in any form - to a third party.**

## CIS Control 13: Network Monitoring and Defense

The Cyber Security Assessment Tool does not provide technical data for this control, though the control is covered in the questionnaire interview.

### Conclusions and Recommendations.

For hybrid networks, prevent that cloud services, like databases and virtual machines are addressable directly from the internet. Create site-to-site VPN connections between your on-premises locations and the cloud network, place Web Application Gateways in front of cloud and/or on-premises Line of Business applications, and enable DDoS protection for public available websites, applications, and services.

## CIS Control 14: Security Awareness and Skills Training

The Cyber Security Assessment Tool does not provide technical data for this control, though the control is covered in the questionnaire interview.

### Conclusions and Recommendations

Phishing attacks often lead to credential compromise and unauthorized access, especially with static authentication methods. To mitigate this risk, organizations should implement **Adaptive Multifactor Authentication (MFA)** and **secure access policies**. **Microsoft Entra Suite** supports these measures by dynamically adjusting authentication based on risk factors such as user behaviour and login location, requiring additional verification in high-risk scenarios. Combined with regular phishing awareness training, these measures enhance security by preventing unauthorized access and minimizing exposure to attacks.

## CIS Control 15: Service Provider Management

The Cyber Security Assessment Tool does not provide technical data for this control, though the control is covered in the questionnaire interview.

### Conclusions and Recommendations

To ensure the service providers adhere to your security standards, it is recommended that the service provider contracts include security requirements. Use policies to enforce the set security standards to the service providers accounts. This is to ensure contracts and policies are not missing any security requirements.

## CIS Control 16: Application Software Security

CSAT Output – GitHub Advanced Security overview

GITHUB ADVANCED SECURITY - CONTOSO	
Number of unresolved Secret scanning	26
Number of open Code scanning alerts	28
Number of open Code scanning alerts with severity error	5
Number of open Code scanning alerts with severity warning	3

### Conclusions and Recommendations

Maintaining application software security could be a daunting task. Not only to gain accurate insight of which software is being used, keeping track of possible vulnerabilities of said software can be difficult. Here are some key practices to consider:

- Adopt a Security Development Lifecycle (SDL) to ensure in-house build software is as secure as possible. Support this Security Development Lifecycle with tooling like GitHub Advanced Security
- Establish a solid patch process; implement critical patches immediately, other patches as soon as possible. Keep in mind that when vulnerabilities are known in public cybercriminals will be using them for their benefit.

AI can help the developers to create secure coding. A solution like GitHub CoPilot can help with the development of code by automating the detection of security vulnerabilities, enhancing code review processes, and providing proactive recommendations to mitigate potential threats, thereby reducing the risk of security breaches in software applications. Additionally, AI can assist in identifying and patching vulnerabilities quickly, improving overall software security and reducing the potential for exploitation by malicious actors.

## CIS Control 17: Incident Response Management

The Cyber Security Assessment Tool does not provide technical data for this control, though the control is covered in the questionnaire interview.

### Conclusions and Recommendations

When all measures are made to protect your organization against the risk of disruption by a security event, statistics show that it is just a matter of time that you will become targeted by one – and get hit.

## CIS Control 18: Penetration Testing

The Cyber Security Assessment Tool does not provide technical data for this control, though the control is covered in the questionnaire interview.

### Conclusions and Recommendations

**EXAMPLE VERSION - DO NOT DISTRIBUTE TO OTHERS - SUBJECT TO NDA**

**Softwerx Ltd and Contoso confidential.**

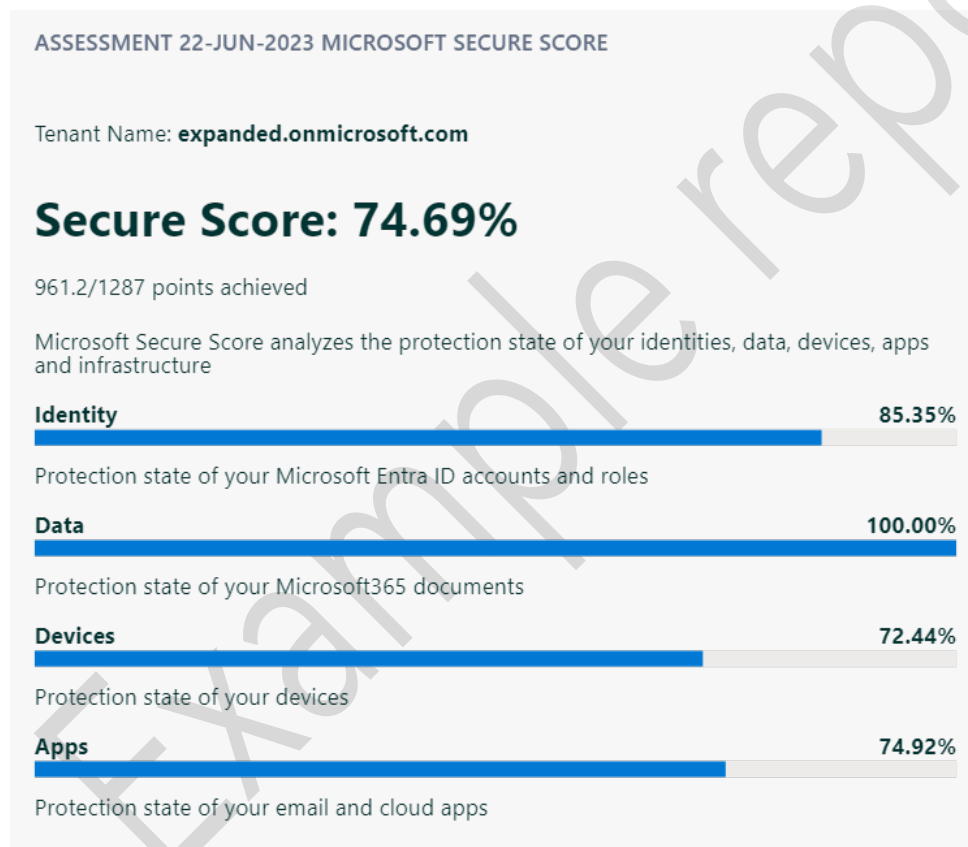
**Do not copy, distribute, or reproduce - in any form - to a third party.**

Microsoft Security Copilot, can help to create various reports or suggestions based on the available information. Microsoft describes it as follows "Identify an ongoing attack, assess its scale, and get instructions to begin remediation based on proven tactics from real-world security incidents." To learn more about Microsoft Security Copilot visit <https://learn.microsoft.com/en-us/security-copilot/?view=o365-worldwide>.

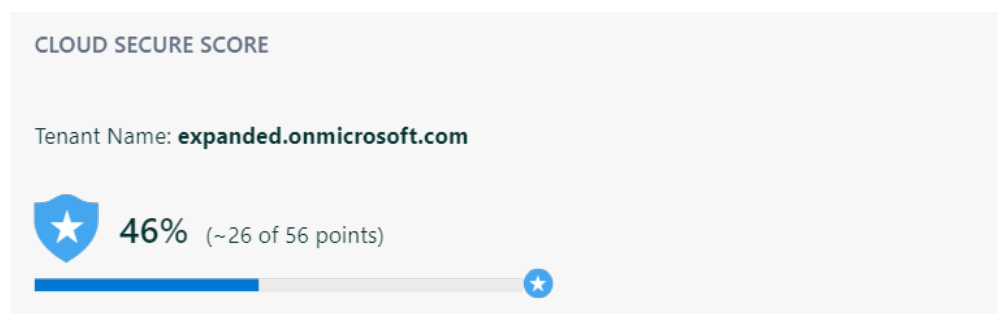
## Microsoft and Defender for Cloud Secure Score

The Microsoft Secure Score looks at multiple items within the Microsoft 365 and Azure environments, these scores are retrieved from [Expandeduniverse.onmicrosoft.com](https://expandeduniverse.onmicrosoft.com). The score is based on the type of services being used on Microsoft 365 and Azure. The scores are compared to a baseline established by Microsoft. The score shows at what level you are aligned with the best security practices.

The Contoso's Microsoft Secure Score:



The Contoso's Cloud Secure Score:



**EXAMPLE VERSION - DO NOT DISTRIBUTE TO OTHERS - SUBJECT TO NDA**

Softwerx Ltd and Contoso confidential.

Do not copy, distribute, or reproduce - in any form - to a third party.

For more information about the Microsoft Secure Score you can visit the following [link](#). Or check the score directly at: <https://security.microsoft.com/securescore>

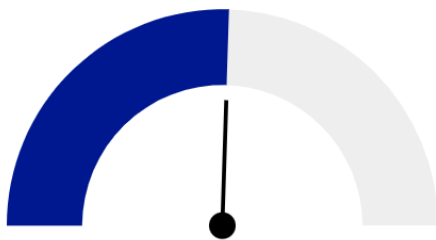
## Microsoft Purview Compliance Manager Score

The Microsoft Purview Compliance Manager looks at the compliance status in the Microsoft 365 environment, this score is retrieved from [expanded.onmicrosoft.com](https://expanded.onmicrosoft.com). The score is based on the type of services being used in Microsoft 365 and compares them to a baseline established by Microsoft.

The Contoso's Microsoft Purview Compliance Manager Score:

Overall compliance score

**Your compliance score: 51%**



23873/46079 points achieved

Your points achieved ⓘ

1918/ 23584

Microsoft managed points achieved ⓘ

21955/ 22495

For more information about the Microsoft Purview Compliance Manager Score you can visit the following [link](#). Or check the score directly at: <https://compliance.microsoft.com/compliancemanager>

Example report

## Microsoft Product Support

Microsoft product support comes in two phases. Starting from the release date support is called Mainstream Support. At some point Microsoft announces that a product goes into Extended Support. During Mainstream Support product support benefits are available to all customers and consist of security fixes and product updates. In the Extended Support phase, security updates are provided to all customers for free, yet to get product break fixes an additional support contract is required. Because of that, we recommend planning life-cycle management to replace products around the end of Mainstream Support. Note that not all Microsoft products are eligible to extended support.

In addition, Microsoft normally requires that all available updates are installed before requesting support for the issue at hand.

The following information about the Microsoft Operating systems has been discovered:

END OF LIFE OVERVIEW	
Amount of Intune devices found with end of life OS	2
Amount of scanned endpoint devices found with end of life OS	0
Amount of Azure Arc machines found with end of life OS	0
Amount of Active Directory machines found with end of life OS	1
Amount of Google Workspace devices found with end of life OS	0

End of life products	
Windows XP	
Windows Server 2000	
Windows Server 2003	
Windows 10 Builds:	10240, 10586, 14393
Windows Vista	

These products will become end of life soon

Soon to become End of life products	
SQL Server 2008	July 2019
Windows Server 2008 R2	January 2020
Windows 7	January 2020
Exchange Server 2010	January 2020
Office 2010	October 2020
SharePoint 2010	October 2020

## Azure Policy

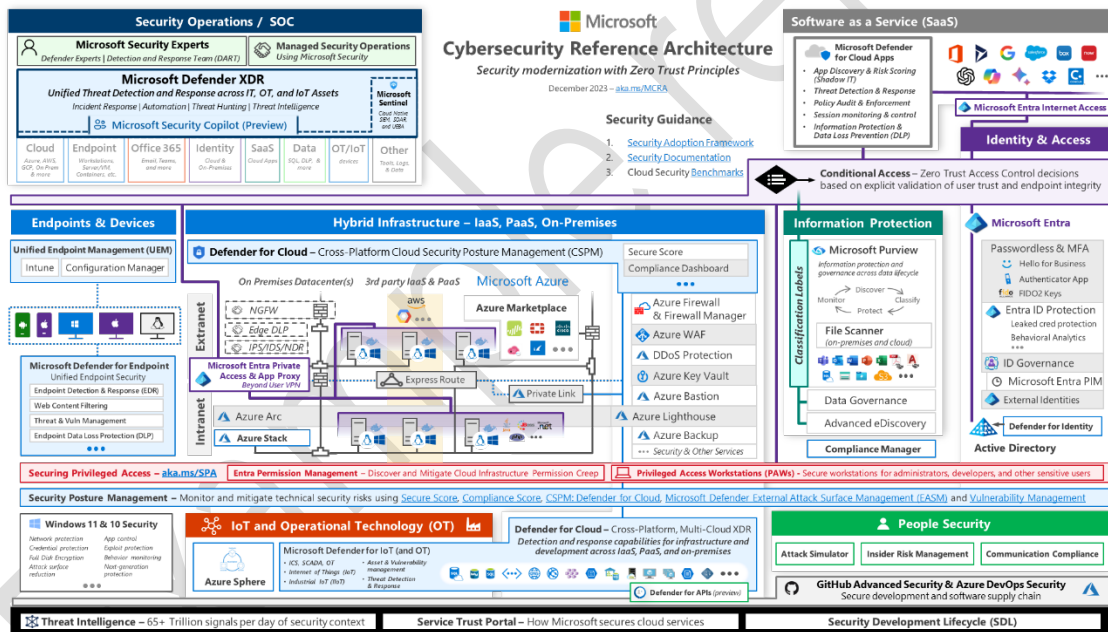
Azure Policy can help to assess and enforce organizational standards based on the specified definitions. Based on the assigned policies an Azure policy compliance score is calculated. This compliance score is calculated on the alignment of the resources and actions with the assigned Azure policies. There are various policy sets available like 'ISO

27001:2013' and 'CIS Microsoft Azure Foundations Benchmark v1.3.0'. The following Azure policy information is retrieved from the scanned subscriptions.

AZURE POLICIES - EXPANDED.ONMICROSOFT.COM	
Overall resource compliance	56% (75 out of 132)
Total policy assignments	43
Non-Compliant resources	57
Exempt resources	18

## Appendix A - Overview of advised security software products

The references made to Microsoft products help mitigating the security vulnerabilities that were discovered. The recommended products integrate in Microsoft's Cybersecurity Reference Architecture, a holistic architecture approach that also adheres to the Open Group's Zero Trust Architecture. The picture below represents the MCRA and can be viewed better by going to <https://aka.ms/mcra>.

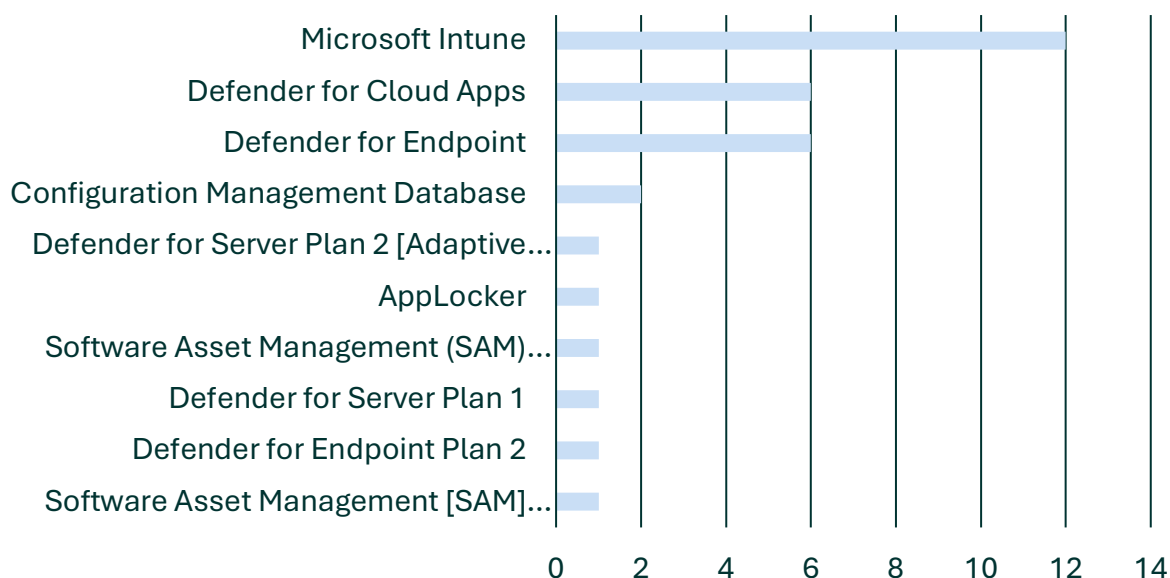


Source: <https://aka.ms/mcra>

## Top 10 recommended software products

This chart presents the top 10 recommended software products.

## Top advised software



### Microsoft 365 Business Standard and Microsoft 365 E3

The following security products are available in Microsoft 365 Business. Note that Microsoft 365 Business has a maximum of three hundred seats. If there is a need for more seats, Microsoft 365 E3 is required. Microsoft 365 E3 includes the basic security suite Enterprise Mobility + Security E3, which is not included in Microsoft 365 Business Standard.

The items marked with (E3) are included only in Microsoft 365 E3.

- Office 365
  - [Exchange Online Protection](#)
  - [Compliance Manager](#)
  - [Data Loss Prevention \(E3\)](#)
  - [Secure Score](#)
- Enterprise Mobility + Security
  - Microsoft Entra ID Plan 1 (E3)
    - [Password Protection](#)
    - [Cloud App Discovery](#)
    - [Conditional Access](#)
    - [Windows Autopilot](#)
  - Microsoft Entra ID free
    - [Multi-Factor Authentication](#)
    - [Passwordless Authentication](#)
  - [Intune Plan 1 \(E3\)](#)
  - [Information Protection \(E3\)](#)
- Windows
  - [BitLocker \(E3\)](#)
  - [Windows Hello for Business \(E3\)](#)
  - [Defender for Endpoint Plan 1 \(E3\)](#)
  - [Credential Guard \(E3\)](#)

**EXAMPLE VERSION - DO NOT DISTRIBUTE TO OTHERS - SUBJECT TO NDA**  
**Softwerx Ltd and Contoso confidential.**

**Do not copy, distribute, or reproduce - in any form - to a third party.**

## Recommended Azure Security Solutions

Azure has many security-related services and technologies to offer in order to help customers enhance the security of their Azure services. A list of recommended Azure Security solutions is shown below:

- Microsoft Defender for Cloud
- Key Vault
- Azure Sentinel
- Azure Role-Based Access Control (Azure RBAC)
- Azure Firewall
- Azure Virtual Desktop – <https://azure.microsoft.com/en-us/services/virtual-desktop/>
- Azure Log Analytics
- Azure VM CIS hardened images

## Appendix B – Secure Score top recommendations

### Microsoft Secure score

The following recommendations were sourced through Microsoft Secure Score and should be double checked. These are the top ten of the total overviews. We recommend checking the secure score regularly. to improve the security posture.

Microsoft 365 Secure Scores   Title	Category	Score	Description
expanded.onmicrosoft.com			
Require MFA for all users	Identity	4/30	Requiring multi-factor authentication (MFA) for all user accounts helps protect devices and data that are accessible to these users. You have 32 of 37 user accounts that do not use MFA.
Turn on audit data recording	Data	0/15	Turning on audit data recording for your Microsoft 365 service ensures that you have a record of every user and administrator's interaction with the service, including Microsoft Entra ID, Exchange Online, and SharePoint Online/OneDrive for Business.
Review permissions & block risky OAuth	Apps	0/15	Cloud App Security permissions lets you see which user-installed applications have access to Microsoft 365 data, what permissions the apps have, and which users granted these apps access.
Consume audit data weekly	Data	0/5	Consume your audit data either through the audit log search or through the Activity API to a third-party security information system at least every week.

### Cloud Secure score

The following items were sourced through Microsoft Defender for Cloud Secure Score and should be double checked. These are the top fifteen recommendations of the total overview. We recommend checking the secure score regularly to improve your security posture.

Recommendation	Description	Affected resource
expanded.onmicrosoft.com		
Only approved VM extensions should be installed		18
Audit diagnostic setting for selected resource types		11
Endpoint protection health issues on machines should be resolved	NA	9
Access to storage accounts with firewall and virtual network configurations should be restricted		8
Secure transfer to storage accounts should be enabled		8
Storage account public access should be disallowed		8
Storage account should use a private link connection		8

**EXAMPLE VERSION - DO NOT DISTRIBUTE TO OTHERS - SUBJECT TO NDA**

Softwerx Ltd and Contoso confidential.

Do not copy, distribute, or reproduce - in any form - to a third party.

## Appendix C – Vendor Consolidation

Expanded Universe is using all manner of security vendors. Having too many cybersecurity vendors will present several risks and disadvantages, including:

- **Complexity:** As the number of cybersecurity vendors increases, so does the complexity of managing them. Each vendor may have its own set of tools and processes, which can make it challenging for organizations to integrate them into a coherent cybersecurity strategy. This complexity can lead to operational inefficiencies, increased costs, and potential security gaps.
- **Overlapping Capabilities:** When using multiple cybersecurity vendors, organizations risk having overlapped or redundant capabilities. This can occur when multiple vendors offer similar products or services, leading to duplication of effort and increased costs. It can also make it difficult to determine which vendor is responsible for addressing a particular security issue, leading to confusion and delays in incident response.
- **Integration Challenges:** As the number of cybersecurity vendors increases, so does the difficulty of integrating their products and services into an organization's overall cybersecurity strategy. Achieving a high cybersecurity maturity is all about having an integrated and proactive security approach. Having too many vendors can lead to interoperability issues, creating security gaps that cybercriminals can exploit.
- **Management Burden:** Managing multiple cybersecurity vendors can be time-consuming and resource intensive. Each vendor may require its own set of processes for implementation, training, and ongoing support. This can lead to increased administrative burdens and reduced efficiency, making it more challenging for organizations to stay on top of the latest cybersecurity threats.

Consolidating the number of cybersecurity vendors can provide several benefits to organizations, including:

- **Simplified Management:** Using multiple cybersecurity vendors can create a complex and disjointed cybersecurity infrastructure, making it challenging for organizations to manage and monitor their security posture effectively. Consolidating vendors can streamline the management process, enabling organizations to more easily and efficiently monitor their security controls.
- **Cost Savings:** Managing multiple vendors can be costly, as it requires more resources and time to manage and maintain each vendor's products and services. Consolidating vendors can lead to cost savings by reducing licensing and maintenance fees, minimizing training and support costs, and optimizing security investments.
- **Improved Integration:** Different cybersecurity solutions from various vendors may not always work well together, which can create interoperability challenges and increase the risk of security gaps. Consolidating vendors can enable organizations to choose solutions that integrate more seamlessly, providing a more comprehensive and effective security posture.
- **Enhanced Cybersecurity:** Consolidating cybersecurity vendors can improve an organization's cybersecurity posture by providing better visibility and control over security threats. With a more integrated and comprehensive approach to cybersecurity, organizations can more effectively detect and respond to threats,

**EXAMPLE VERSION - DO NOT DISTRIBUTE TO OTHERS - SUBJECT TO NDA**  
**Softwerx Ltd and Contoso confidential.**

**Do not copy, distribute, or reproduce - in any form - to a third party.**

reducing the likelihood of a successful cyberattack.

Overall, Microsoft has a unique opportunity to help organizations consolidate their security vendors by offering integrated solutions, partnering with other vendors, providing consultancy services, and promoting best practices. By doing so, Microsoft can help organizations improve their cybersecurity posture, reduce costs, and simplify their security infrastructure. You will find an overview of the Security Vendors and Solutions used by Expanded universe including the suggested Microsoft Solution to help make use of Microsoft's best of breed cloud and security platform below.

Found Application	Number Of Endpoints	Suggested Solution	Application Category	Application Subcategory
ESET Endpoint Security	15	Windows Antivirus	Security	Antivirus
Akamai Enterprise Application Access	0	Azure Virtual WAN with Azure Firewall	Security	Secure Access Service Edge
Google Cloud Platform (GCP) Security	0	Azure Security Center	Security	Infrastructure-as-a-Service (IaaS) Security
Teramind Insider Threat Detection	0	Microsoft Insider Risk Management	Security	Insider Risk Management

## Appendix D – Assessment Scope

The Cybersecurity Assessment was fulfilled considering the following scoping information:

Organization	
<i>Customer name</i>	Contoso
<i>Customer address</i>	1234 Somewhere street Netherlands, Amersfoort 9876 AB
<i>Number of employees</i>	300

Assessment Key dates and deadlines	
Activity	Date
<i>Customer Kick-off call</i>	16-10-2018
<i>Complete interview series and on-site inventory collection</i>	19-10-2018
<i>Inventory data analysis/review</i>	22-10-2018

Partner Assessment participants		
Name	Organization	Project role
Henri Johnson	Contoso	IT project manager
Renee Towell	Contoso	Security officer
Leo Richards	Softwerx Ltd	Reviewer

Interviews were conducted by <csat\_text\_qn\_cat2.21.77.answer> with key stakeholders to gather information in addition to the automated inventory of the IT infrastructure. The results are based on the answers to the questions outlined in the Cybersecurity Questionnaire. Interviews were conducted with the following stakeholders:

Interviewee	Title
Henri Johnson	IT Project manager
Renee Towell	Security officer
John Henson	IT Manager

### Cybersecurity Assessment Goals

Like many organizations, Contoso is dealing with the major trend's IT is facing today, including the proliferation of mobile devices, the impact of social networks on organizational operation, the rapid growth of unstructured data, the accelerated adoption of the Cloud and privacy regulations. All these areas are impacted by a shifting threat landscape, meaning security programs and practices are heavily impacted across the board.

The Cybersecurity Solution Assessment provides a high-level review regarding the maturity of Contoso's security program based on security controls in the CIS Controls™ Version 8.1 framework as published by the Center for Internet Security®.

The goals of the Cybersecurity Assessment are to:

- Initiate a foundation for protecting IT assets, and for promoting modern cybersecurity practices in a holistic, integrated way.

- Align with the security "recommended practices" of a well-known and highly regarded security-framework as the foundation for a cybersecurity program.

**EXAMPLE VERSION - DO NOT DISTRIBUTE TO OTHERS - SUBJECT TO NDA**  
**Softwerx Ltd and Contoso confidential.**

**Do not copy, distribute, or reproduce - in any form - to a third party.**

Project a security pathway to move to the cloud where internal controls around areas such as authentication, authorization, and data protection will be even more critical.

Provide recommendations based on the interviews and facts found during the scan of the IT environment.

Uncover critical issues related to cybersecurity.

Establish a prioritized action list, based on the criticality of the findings which can serve as a short-term roadmap in the cybersecurity program of the organization.

## Inventory Tools

To assess Contoso's IT infrastructure (Technical Topics), the Cyber Security Assessment Tool was used to gather the required information of their current configuration state.

## Cyber Security Assessment Tool

CSAT is developed by experienced security experts to quickly assess the status of your organization's security maturity, and to recommend improvements based on facts.

The tool collects relevant data from the IT environment by scanning for example endpoints, Active Directory and SharePoint Online. Additionally, CSAT uses a questionnaire to collect data about policies and other key indicators.



Organizations are looking for a way to check their security status simple and quickly. They want insight into their vulnerabilities, based on data from the organization's IT infrastructure and Microsoft 365. The Cyber Security Assessment Tool (CSAT) from Softwerx Ltd provides this through automated scans and analyses. This is the basis on which the CSAT scan provides recommendations and a short-term action plan in this report to improve your security. It is the perfect way to maximize security and demonstrate that your organization takes security seriously. This is also important given the EU GDPR and other privacy regulations.

## Appendix E – The CSAT Methodology

This report aims to bring you a better understanding of your organization's current cybersecurity posture, and actionable items to mitigate the discovered risks. The Cyber Security Assessment Tool (CSAT) consists of a technical scan of your environment and an interview based on renowned CIS controls. The report that you are reading now is packed with recommendations to enhance your IT environment, based on industry recommended practices. In this appendix the CSAT methodology will be explained.

### Introduction

Security is relative to the threats and risks an organization faces; there is no absolute security. That which is good for one organization can be overkill for another, a one-size fits all security program does not exist. A maturity-based approach can help to address these variations in security threats and IT risk management.

To establish a measurable security framework a solid foundation of security "recommended practices" is needed. For this reason, the Cybersecurity Assessment is using the **CIS Controls™ (v8.1)** security framework published by the **Center for Internet Security® (CIS)** (<http://www.cisecurity.org>).

During the Cybersecurity Assessment, Contoso's cybersecurity practices level has been measured by answering a Questionnaire. The measurement was scoped on the practices of the CIS Control™ (v8.1) security framework.

Besides the measurement through the Questionnaire, relevant security related data was collected from Contoso's IT environment. With this measurement through the Questionnaire, and with the analysis of the collected data, a list of findings, recommendations, action items and a compiled short-term roadmap is provided to improve the cybersecurity program and practices of Contoso.

### Network and Information Security Directive (NIS2)

The NIS 2 Directive is the EU-wide legislation on cybersecurity, aimed at establishing a baseline of security measures for digital service providers and operators of essential services. Its goal is to mitigate the risk of cyber-attacks and improve the overall level of cybersecurity in the EU. NIS 2 is an expansion of the original Network and Information Systems (NIS) Directive, driven by the increasing frequency and sophistication of cyber-attacks, the pressures of addressing multi-cloud IT environments, and the increasingly complex regulatory landscape.

NIS 2 introduces stronger requirements and affects more sectors, focusing on securing business continuity, including supply chain security, and improving and streamlining reporting obligations. The repercussions for non-compliance are more severe, with potential legal ramifications for management in addition to fines. Enforcement is localized in all European member states.

CIS has made a mapping available from CIS Controls v8.1 to NIS 2. The mapping below provides an overview of the alignment between CIS v8 Controls, and the measures outlined in the NIS 2 Directive. This mapping demonstrates which CIS v8 control in the CSAT questionnaire corresponds to the specific requirements of the NIS 2 Directive. This mapping is derived from the CIS\_Controls\_v8.1\_Mapping\_to\_NIS2\_Directive\_2\_2025.xlsx.

NIS 2 Article 21.2 Measure	CIS Control safeguard
A	6.8
	15.4
B	3.14
	8.1 – 8.2
	8.4 – 8.5
	8.9 – 8.11
	13.11
	14.6
	15.4
	17.2 – 17.9
C	11.1
	11.3 – 11.5
D	15.1 – 15.2
	15.4 -15.7
E	2.2
	4.1 – 4.2
	7.1 – 7.2
	7.5 – 7.7
	9.2
	9.5
	10.1
	12.1 – 12.2
	12.4
	12.6
	12.8
	13.3
	15.2
	16.1
	16.10
	18.1
F	No links to CIS control made
G	14.1
	14.9
H	3.1
	3.6
I	1.1
	3.1
	3.3
	3.5
	3.7
	3.9
	3.12
	4.3
	4.10
	5.1

**EXAMPLE VERSION - DO NOT DISTRIBUTE TO OTHERS - SUBJECT TO NDA**

Softwerx Ltd and Contoso confidential.

Do not copy, distribute, or reproduce - in any form - to a third party.

	5.4
	6.1 - 6.8
	10.3 – 10.4
J	CIS did not link this, however CIS control 6.3, 6.4, and 6.5 cover Multi-Factor Authentication

## Control Framework background (CIS)

The Center for Internet Security® (CIS) is a nonprofit organization responsible for the globally recognized CIS Controls® and CIS Benchmarks™, offering best practices for securing IT systems and data. The CIS community continually updates these standards to address emerging threats.

The CSAT questionnaire is based on the CIS Controls and includes questions related to ISO27001:2022 controls. It aims to gather relevant information about your IT processes. To learn more about the Center for Internet Security, visit <https://cisecurity.org>.

CIS Controls™ (v8.1) take a community-based approach, derived from consensus risk assessments involving experts from government, industry, and academia. These controls focus on common threats and vulnerabilities in large enterprises, serving as a strong foundation for high-impact actions. They complement, rather than replace, comprehensive IT and security risk management frameworks.

For the Cybersecurity Assessment, the technical CIS Controls™ (v8.1) are expanded with high-level controls from ISO/IEC 27001:2022 in the Organizational control domain. These questions are related to IT- and data governance, and cover the areas of policies, compliancy, risk management and privacy.

## Zero Trust Model

The Zero Trust Security Model, established by The Open Group, collaborates with over 790 organizations globally to define technology standards that support business objectives. They work through various groups to capture, integrate, and share requirements, ensuring openness, interoperability, and consensus. Companies such as IBM and Microsoft have already integrated these principles into their reference architectures, aiding organizations in aligning their solutions with the Zero Trust model's core principles.

The architecture principles are product-neutral, allowing your organization to choose which products and solutions align with your strategy. Given our focus on assessing IT environments predominantly using Microsoft-based on-premises and cloud solutions, our recommendations draw from Microsoft's recommended practices and their Zero Trust Reference Architecture.

More information on can be found at <https://theopengroup.org> and <https://www.microsoft.com/en/security/business/zero-trust>.

The Zero Trust Principles are:

1. Verify explicitly  
Always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies.
2. Use least privileged access

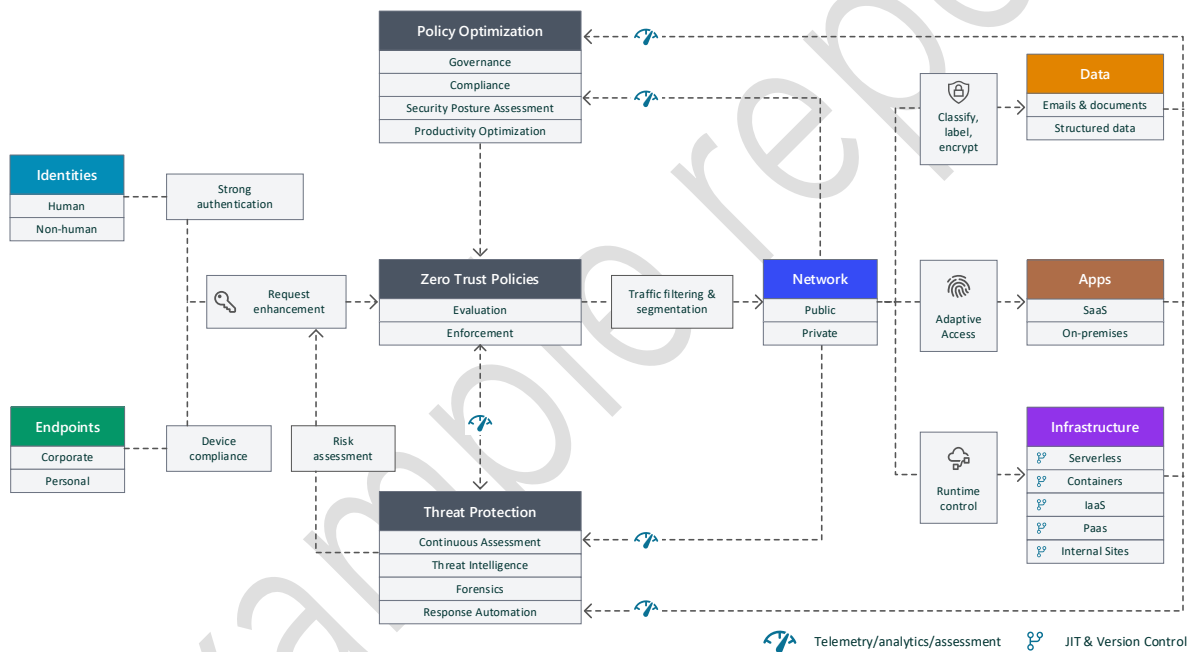
Limit user access with just-in-time and just-enough-access (JIT/JEA), risk-based adaptive policies, and data protection to help secure both data and productivity.

3. Assume breach

Minimize blast radius for breaches and prevent lateral movement by segmenting access by network, user, and devices. Verify all sessions are encrypted end to end. Use analytics to get visibility, drive threat detection, and improve defenses.

Rather than assuming safety behind the corporate firewall, the Zero Trust Model assumes a breach and verifies every request as if it is from an open network. It adheres to the principle of "never trust, always verify.". Every access request is fully authenticated, authorized, and encrypted before granting access, regardless of their origin or target resource. To minimize lateral movement, it employs micro-segmentation and enforces least privileged access. Real-time anomaly detection and response leverage rich intelligence and analytics. This translates into the following schematic overview:

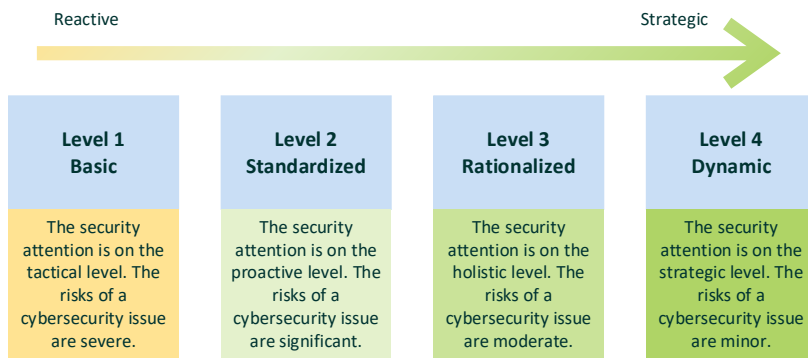
### Zero Trust Architecture Diagram



The zones above correlate to the respective CSAT recommendations, mapping the respective CIS control to the Zero Trust Security Architecture zone.

### SOM Model

To achieve this goal, the Cybersecurity Assessment utilizes a Maturity Model to communicate the findings and recommendations. The maturity model construct for the Cybersecurity Assessment is based on a similar model developed by Microsoft (Security Maturity Model v1) and is consistent with the Software Optimization Model (SOM). The below reflects the levels:



The complete score of the organization is determined by the lowest score in the organization, for example if most processes are at Level 3, but one process is at Level 1, the whole organization is rated at Level 1.