Solution Assessment
Secure Infrastructure Assessment

Contoso

QS Solutions
David Lane

Issued in November | 2020

Contents

1. Introductions
2. Management summary
3. Plan of Approach
4. Interview Results
5. Summary of Scan Findings
6. Security Landscape Evolutions
7. Suggested roadmap
8. Next steps

Management Summary

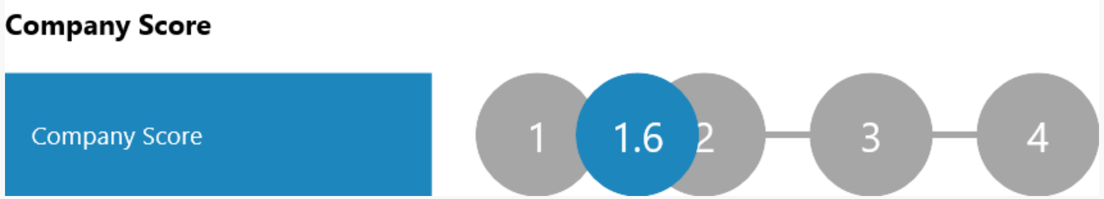
Management Summary | Current State and Major Risks

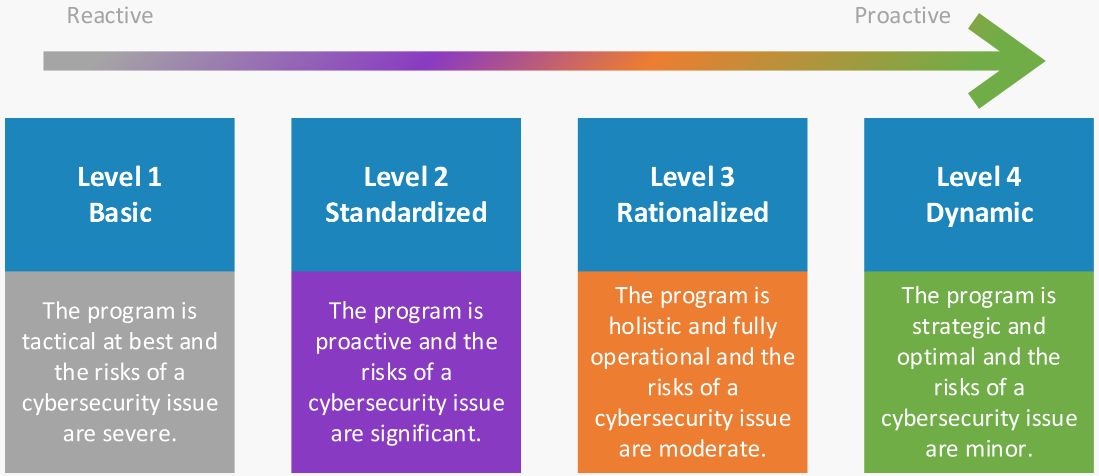
CIS Maturity Level

Your current security maturity level is between Basic and Standardized.

Major Risks

- Identity theft
- Unsupported systems
- Unsupported legacy software





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

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

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

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

QS Solutions and Contoso Confidential. Do not publish - in any form - to others.

Management Summary | Security Strategy Recommendations

The security risks facing the organization are generally understood although not in a managed way.

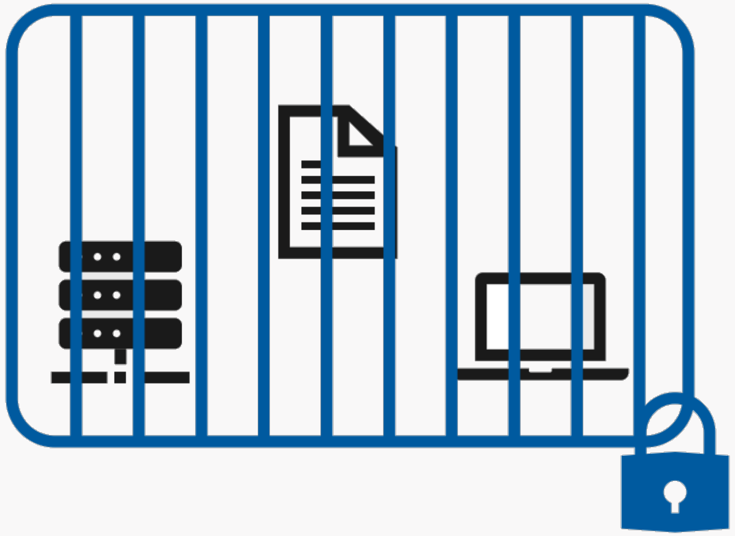
The governance of the cybersecurity program is structured but not fully integrated with other governance areas.

The organization’s employees are unaware of today’s (cyber)security threats and related training around security and privacy awareness is missing.

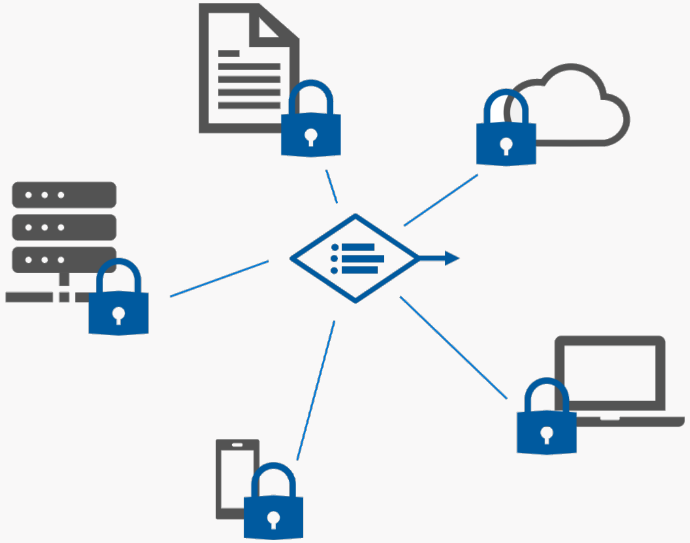
Management summary | Zero Trust Security

Modern security architecture principles, defined by The Open Group

Microsoft and many other vendors have embraced these principles in their reference architectures



Classic Approach – Secure all assets in your own castle



Zero Trust – Protect assets from central location

Plan of Approach

Suggested Roadmap

Plan of Approach | Quick Wins 0-30 days

Cybersecurity Strategy Workshop
Oneday workshow in which the cyber security priciples are explained. Based opon the current security developments.

Identities

- Cleanup and separate admin accounts
- Cleanup unused user accounts; fix accounts without passwords
- Implement MFA (AAD P1) ✓
- Implement Conditional Access (AAD P1)

Devices

- Implement Intune Security Baseline (incl disk encryption enforcement) (M365 F3)✓
- Implement & Patch Management (M365 F3)
- Conditional access (AAD P1) ✓
- Implement Top 8 Azure Secure Score recommendations ✓

Data

- Implement Top 8 Azure Secure Score recommendations ✓
- Cloud Application Security – trial – monitoring
- Defender for Office (O365/M365 E5)

Plan of Approach | 30 – 90 days

Cybersecurity Strategy

Define policies and procedures based on workshop outcomes

- Identity & Access Management
- Device Management
- Data Protection, Management

Identities

- Implement PIM (AAD P2)
- Defender for Identities (M365 E5)
- Implement MFA for remote login access on Remote Desktop Services (RDS)

Devices

- Implement Risk-based Conditional Access (AAD P2)
- Implement Defender for Endpoints – policy enforcement

Plan of Approach | Beyond 90 days

Define lifecycle management procedures for

- Applications
- Operating Systems
- Security Architecture

Enhance data protection by implementing automated labeling, classification and encryption of sensitive data (AIP P2, M365 E5)

Implement remaining recommendations mentioned in the CSAT report, aligned with the Cybersecurity Strategy and compliance regulations

Interview Results

Interview results| Basic CIS controls

Lowest ranked controls:

2. Inventory and Control of Software Assets

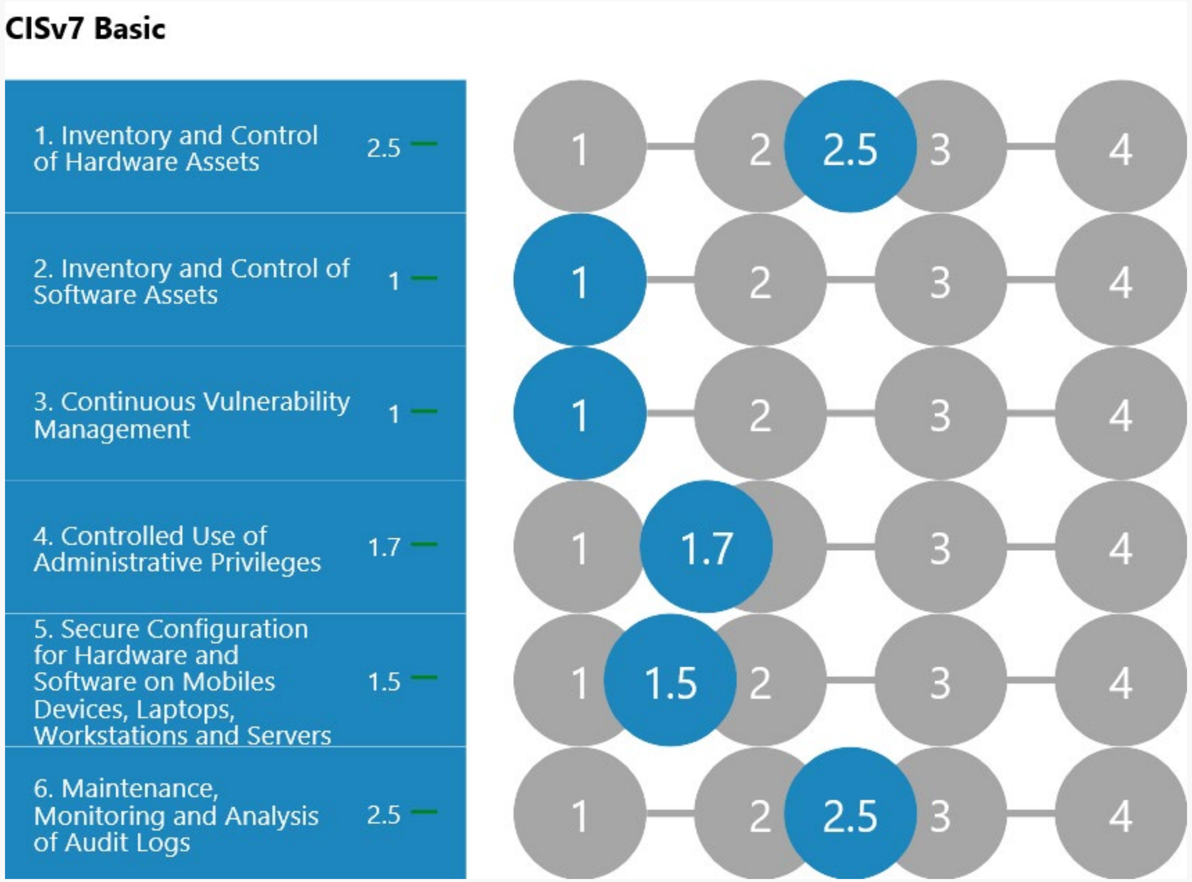
Embed a discovery tool for software asset management.

3. Continuous Vulnerability Management

Implement vulnerability scan software. Scan for vulnerabilities regularly, especially on systems contain sensitive information.

3. Continuous Vulnerability Management

Implement a patch management process and tooling. Gain insights on the patch status of all systems



CISv7 Basic

1. Inventory and Control of Hardware Assets	2.5	1	2	2.5	3	4
2. Inventory and Control of Software Assets	1	1	2		3	4
3. Continuous Vulnerability Management	1	1	2		3	4
4. Controlled Use of Administrative Privileges	1.7	1	1.7		3	4
5. Secure Configuration for Hardware and Software on Mobiles Devices, Laptops, Workstations and Servers	1.5	1	1.5	2	3	4
6. Maintenance, Monitoring and Analysis of Audit Logs	2.5	1	2	2.5	3	4

Interview results| Foundational CIS controls

Lowest ranked controls:

8. Malware Defenses

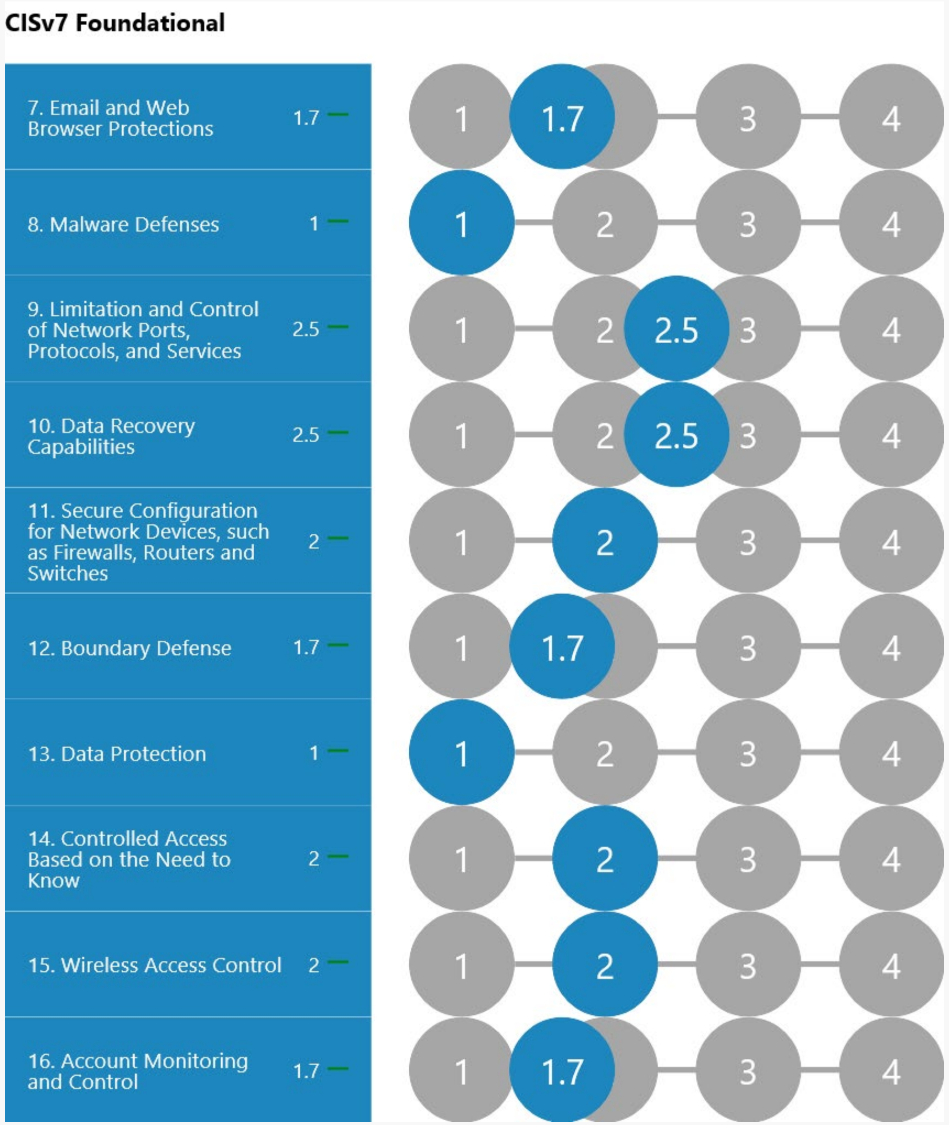
Enable the default tools for antivirus, anti-malware and DEP on the organization's systems.

8. Malware Defenses

Store the AV logs centrally and apply alerting to gain insights.

13. Data Protection

Identify sensitive information on the organization's main data sources. Apply labeling and classification.



CISv7 Foundational

7. Email and Web Browser Protections	1.7
8. Malware Defenses	1
9. Limitation and Control of Network Ports, Protocols, and Services	2.5
10. Data Recovery Capabilities	2.5
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches	2
12. Boundary Defense	1.7
13. Data Protection	1
14. Controlled Access Based on the Need to Know	2
15. Wireless Access Control	2
16. Account Monitoring and Control	1.7

QS Solutions and Contoso Confidential. Do not publish - in any form - to others.

Interview results| Organizational CIS controls

Lowest ranked controls:

17. Implement a Security Awareness and Training Program

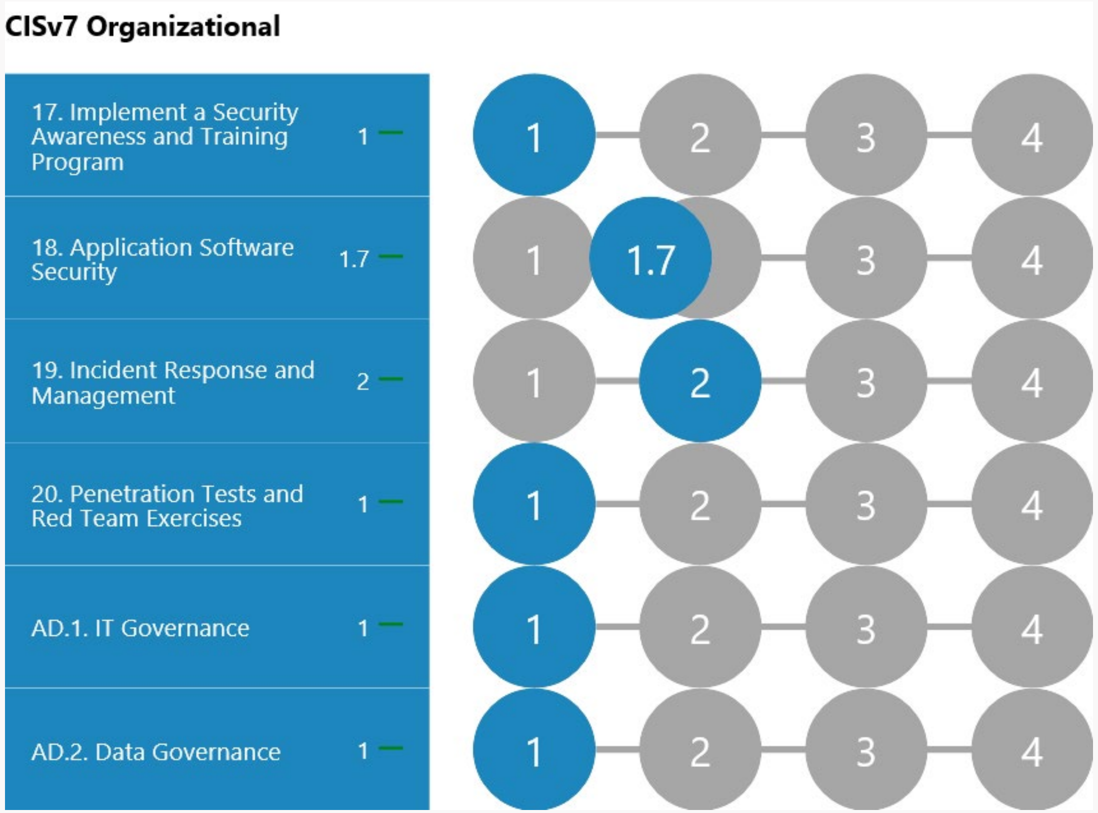
Establish a security and privacy awareness program.

AD.1. IT Governance

Create a security and privacy policy and define the processes related operational processes.

AD.1. IT Governance

Formalize the segregation of tasks, responsibilities and authorizations by implementing a role matrix.



CISv7 Organizational

17. Implement a Security Awareness and Training Program	1
18. Application Software Security	1.7
19. Incident Response and Management	2
20. Penetration Tests and Red Team Exercises	1
AD.1. IT Governance	1
AD.2. Data Governance	1

Summary of Scan Findings

Scan Findings | Windows versions

CIS control 2; Zero Trust zone 3

Findings:

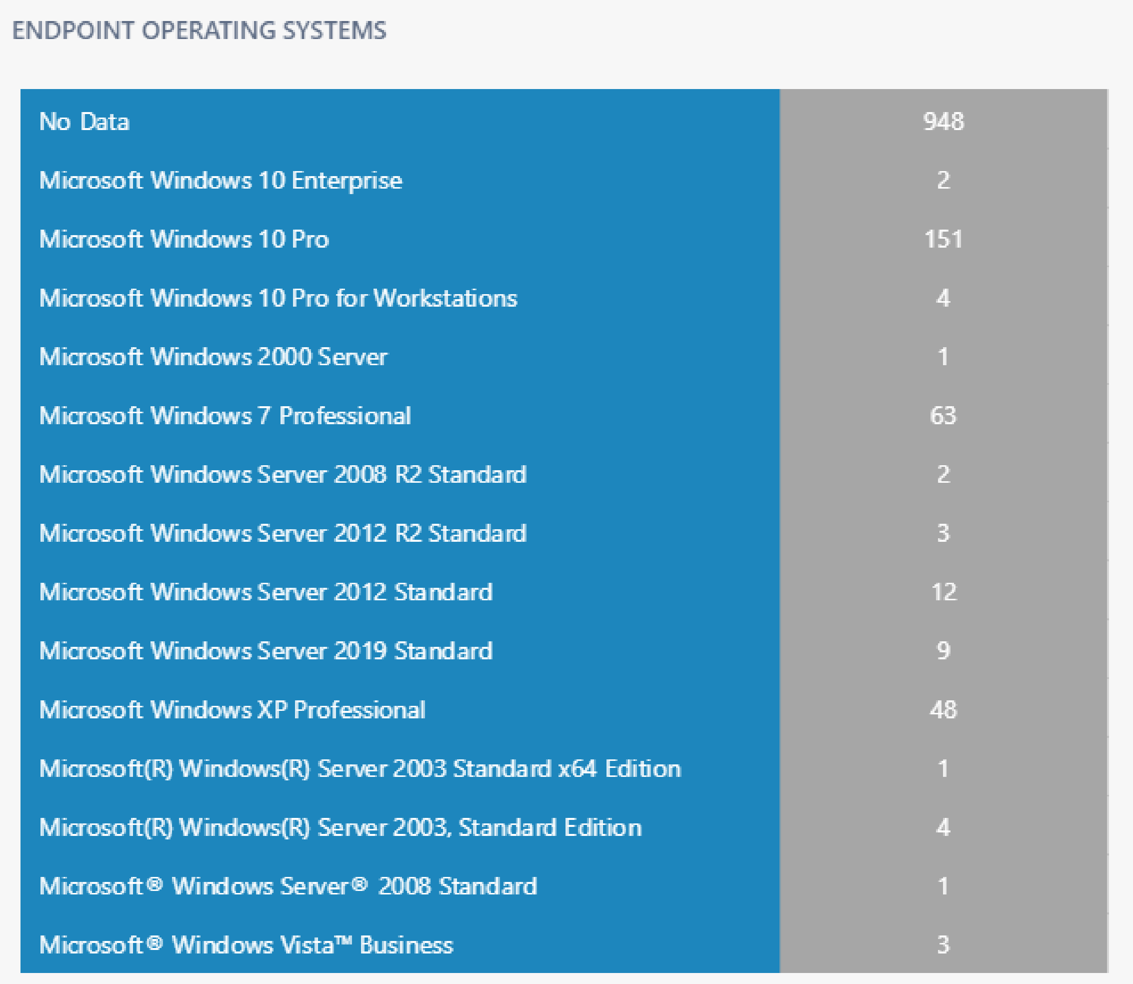
- End of Life and almost end of life operating systems have been found
- There are various versions of Windows 10 found. The various found versions are not up to date

Associated Risks

- Software incompatibility: New applications are optimized for the most recent OS's
- Compliance issues: Regulated industries like healthcare and e-commerce deal with lots of sensitive customer data

Recommendations:

- Create a plan to phase these operating systems (OS) out
- Update all endpoints to the latest version



ENDPOINT OPERATING SYSTEMS

No Data	948
Microsoft Windows 10 Enterprise	2
Microsoft Windows 10 Pro	151
Microsoft Windows 10 Pro for Workstations	4
Microsoft Windows 2000 Server	1
Microsoft Windows 7 Professional	63
Microsoft Windows Server 2008 R2 Standard	2
Microsoft Windows Server 2012 R2 Standard	3
Microsoft Windows Server 2012 Standard	12
Microsoft Windows Server 2019 Standard	9
Microsoft Windows XP Professional	48
Microsoft(R) Windows(R) Server 2003 Standard x64 Edition	1
Microsoft(R) Windows(R) Server 2003, Standard Edition	4
Microsoft® Windows Server® 2008 Standard	1
Microsoft® Windows Vista™ Business	3

Scan Findings | Administrator accounts

CIS control 4

Findings:

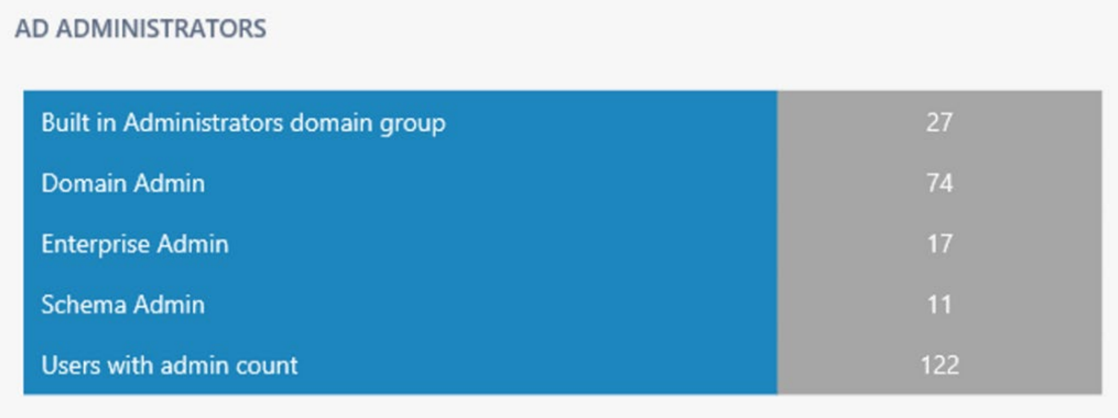
- A high number or domain, enterprise and schema admins are found

Associated Risks

- Well known targets: Administrators are a well-known target for unwanted people
- Unlimited access: Administrators have no limit to what they can access

Recommendations:

- Review if all the users in the admin groups need that level of permissions, perhaps other groups like “helpdesk admin” can be used to limit access
- Use Multi Factor Authentication the for the Admin users



AD ADMINISTRATORS

Built in Administrators domain group	27
Domain Admin	74
Enterprise Admin	17
Schema Admin	11
Users with admin count	122

Scan Findings | Administrator accounts (2)

CIS control 4

Findings:

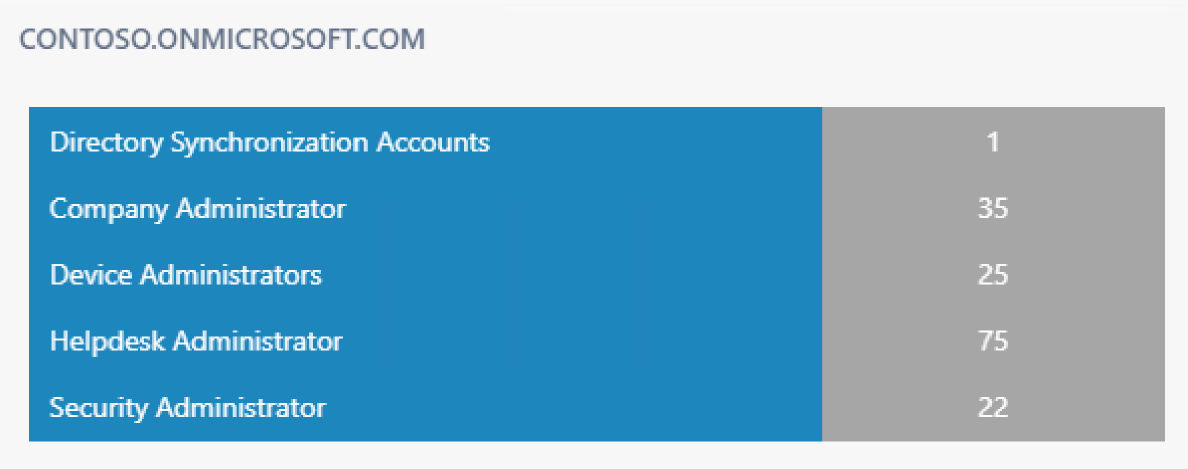
- A high number or domain, enterprise and schema admins are found
- Multi Factor Authentication is not used on multiple admin accounts

Associated Risks

- Well known targets: Administrators are a well-known target for unwanted people
- Unlimited access: Administrators have no limit to what they can access

Recommendations:

- Review if all the users in the admin groups need that level of permissions, perhaps other groups like “helpdesk admin” can be used to limit access
- Use Multi Factor Authentication the for the Admin users



CONTOSO.ONMICROSOFT.COM

Directory Synchronization Accounts	1
Company Administrator	35
Device Administrators	25
Helpdesk Administrator	75
Security Administrator	22

Scan Findings | Secure configuration endpoints

CIS control 5

Findings:

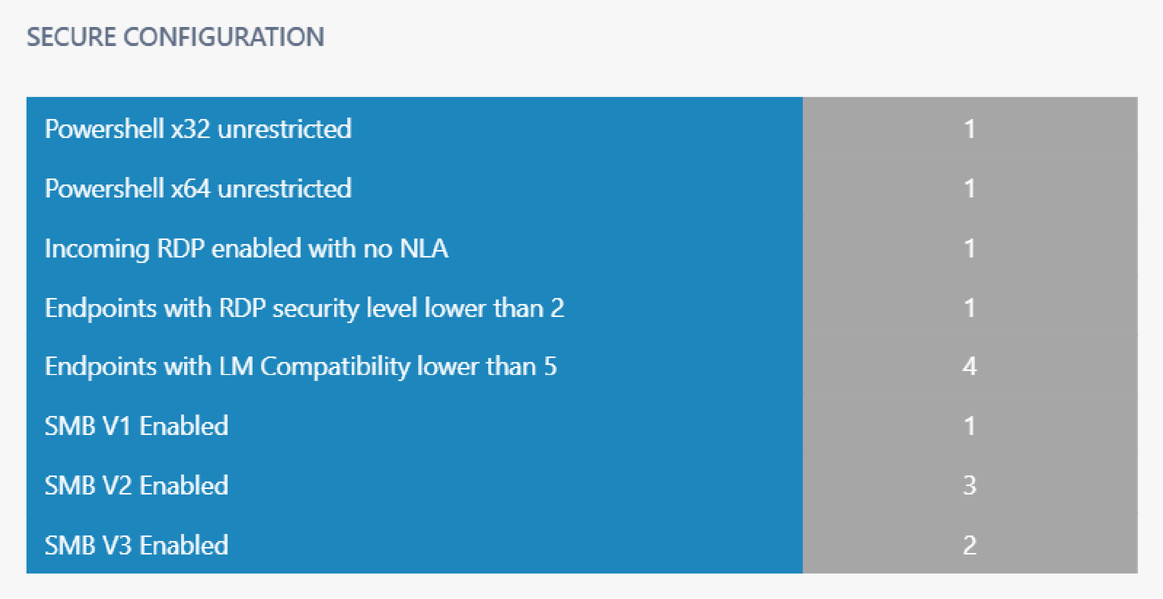
- Endpoint have been found that have SMB v1 enabled
- Several endpoints have been found that are not using the secure remote connection protocol
- There is no secure baseline applied to the endpoints

Associated Risks

- Security vulnerabilities: (older) protocols have well known security hazards that are often misused
- To many services enabled: by default, there are service that are not used however they are enabled, creating a possible entry way for unwanted people

Recommendations:

- Find a security baseline that fits your company and apply that to the endpoints
- Ensure SMB v1 is disabled on all the endpoints



SECURE CONFIGURATION

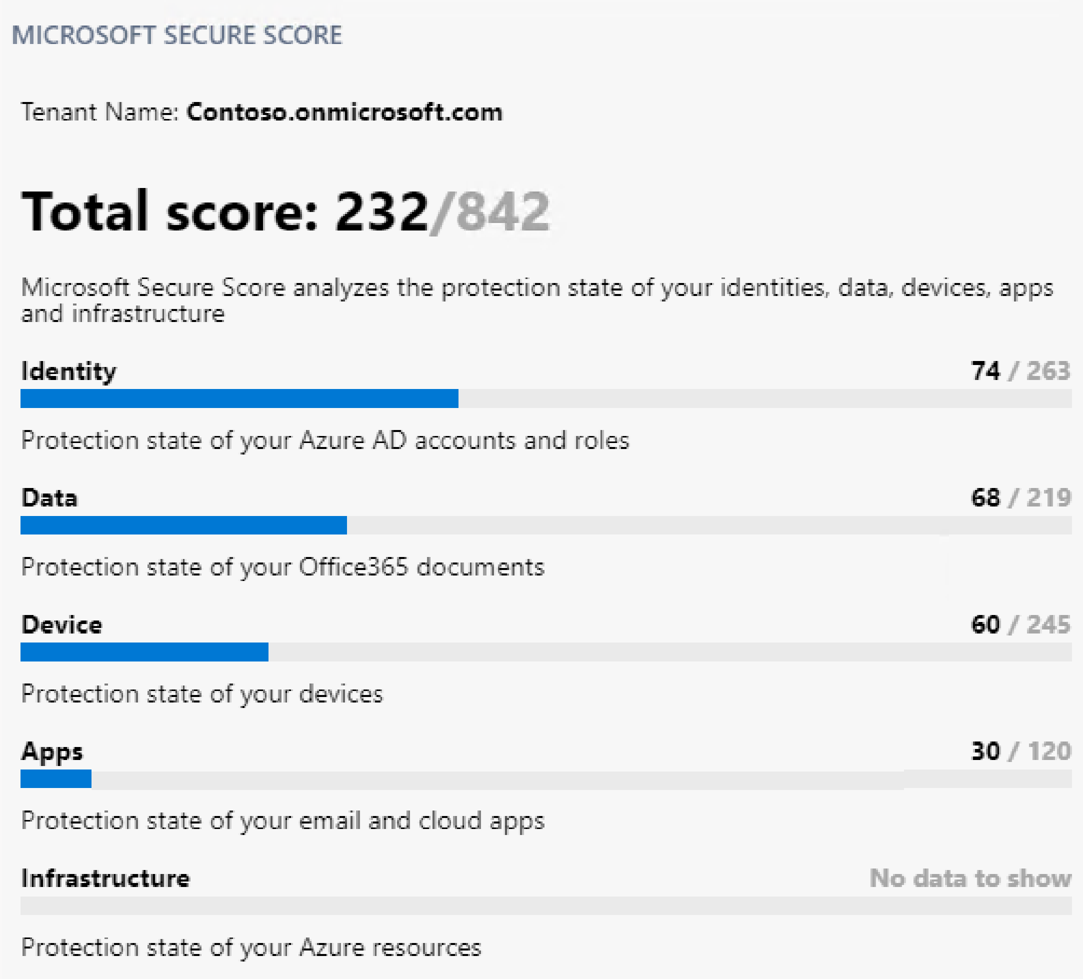
Powershell x32 unrestricted	1
Powershell x64 unrestricted	1
Incoming RDP enabled with no NLA	1
Endpoints with RDP security level lower than 2	1
Endpoints with LM Compatibility lower than 5	4
SMB V1 Enabled	1
SMB V2 Enabled	3
SMB V3 Enabled	2

Scan Findings | Microsoft 365 Secure Score

The Microsoft Secure Score looks at multiple areas within the Office 365 and Azure AD environment. The score is based on the type of services being used in Office 365 and compares them to a baseline established by Microsoft. The score shows in what level you are aligned with the best security practices.

We recommend starting with the following items

- Require MFA for administrative roles
- Designate fewer than 5 global admins
- Turn on sign-in risk policy
- Enable policy to block legacy authentication



MICROSOFT SECURE SCORE

Tenant Name: **Contoso.onmicrosoft.com**

Total score: 232/842

Microsoft Secure Score analyzes the protection state of your identities, data, devices, apps and infrastructure

Identity 74 / 263

Protection state of your Azure AD accounts and roles

Data 68 / 219

Protection state of your Office365 documents

Device 60 / 245

Protection state of your devices

Apps 30 / 120

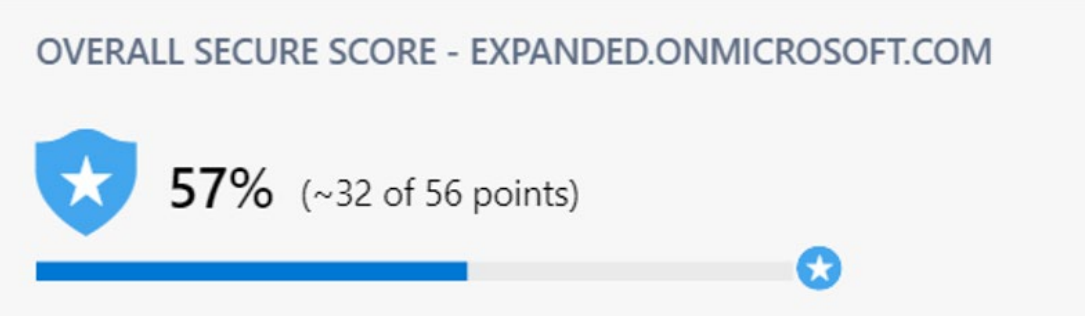
Protection state of your email and cloud apps

Infrastructure No data to show

Protection state of your Azure resources

Scan Findings | Azure Secure Score

The Azure Secure Score looks at all resources created within the Azure environment. The Secure Score is based on the type of services being used and compares them to Microsoft security baselines and recommended practices.



OVERALL SECURE SCORE - EXPANDED.ONMICROSOFT.COM

57% (~32 of 56 points)

We recommend starting with the following items

- MFA should be enabled on accounts with write permissions on your subscription
- Internet-facing virtual machines should be protected with network security groups
- Web Application should only be accessible over HTTPS

Security Landscape Evolutions

Zero Trust Security Architecture principles
Rapid Cyberattack mitigations

Security Landscape | Zero Trust Security Architecture

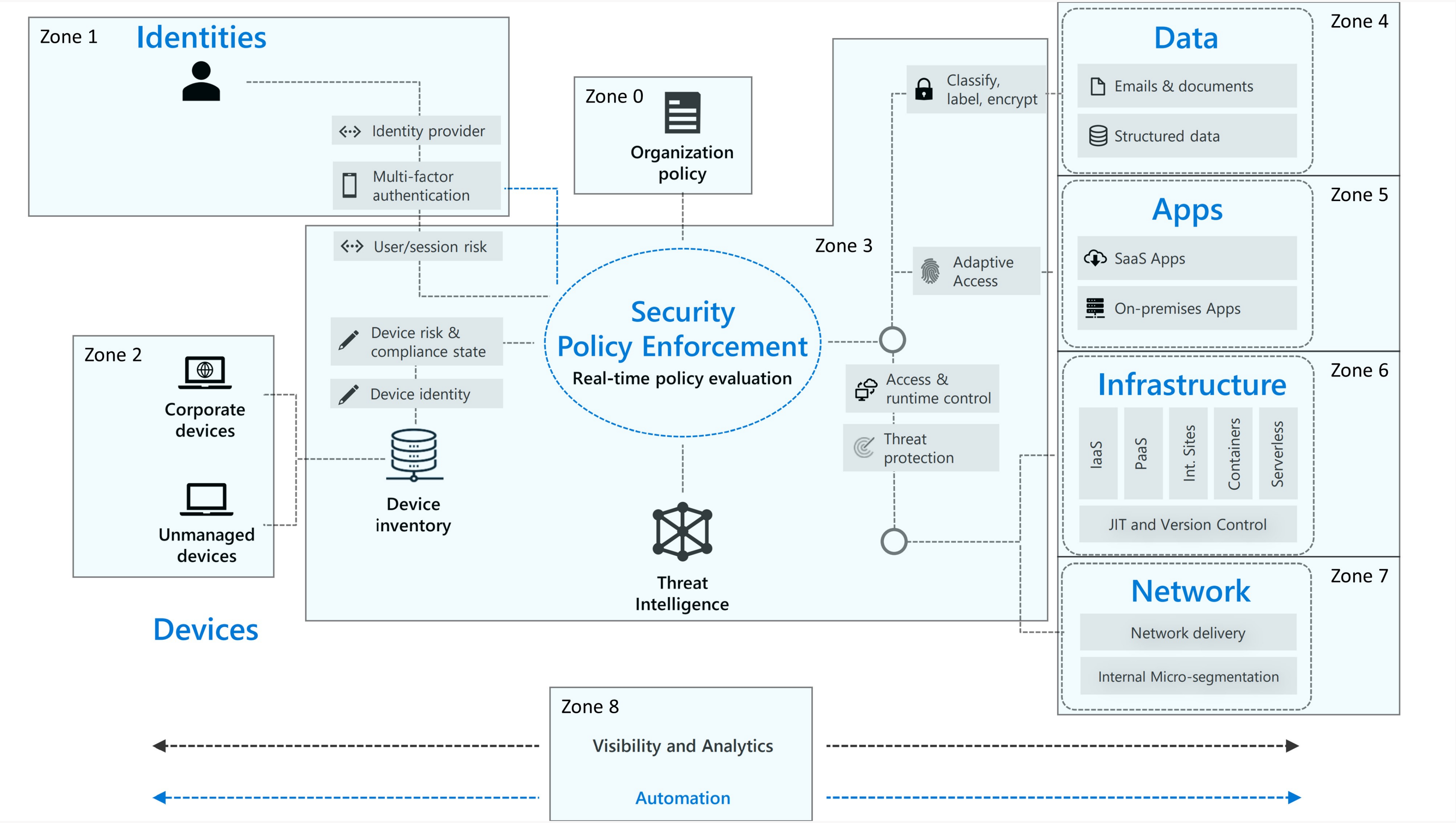
Modernized security architecture principles, defined by The Open Group

Microsoft and many other vendors have embraced these principles in their reference architectures

The Zero Trust Security Architecture 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 polices, 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, devices, and app awareness. Verify all sessions are encrypted end to end. Use analytics to get visibility, drive threat detection, and improve defenses

Security Landscape | Zero Trust Architecture Overview



QS Solutions and Contoso Confidential. Do not publish - in any form - to others.

Security Landscape | RCA Recommendations

DEFAULT RECOMMENDATIONS

Measures that directly impact the known attack playbook

Quick wins: 0-30 Days

DIRECT ATTACK MITIGATION
RAPID ENABLEMENT

1. Create **destruction-resistant backups** of your critical systems and data
2. Immediately deploy **critical security updates** for OS, browser, & email
3. **Isolate (or retire) computers** that cannot be updated and patched
4. Implement **advanced e-mail and browser protections**
5. Enable host anti-malware and network defenses get near-**realtime blocking responses from cloud** (if available in your solution)
6. Implement **unique local administrator passwords** on all systems
7. Separate and protect **privileged accounts**

Less than 90 Days

DIRECT ATTACK MITIGATION
LONGER ENABLEMENT

1. **Validate** your backups using standard restore procedures and tools
2. **Discover and reduce** broad permissions on file repositories

Next Quarter + Beyond

3. Rapidly deploy all **critical security updates**
4. **Disable unneeded** legacy protocols
5. **Stay current –** Run only current versions of operating systems and apps

QS Solutions and Contoso Confidential. Do not publish - in any form - to others.

Security Landscape | How CSAT Relates To Said Topics

Many CSAT recommendations are linked to Zero Trust Security Architecture zones and to the Rapid CyberAttack migitation recommendations.

This helps prioritizing the CSAT recommendations in order to better protect your organization against rapid cybeattacks.

It also shows that the recommendations fit into the long-term strategy to rejuvenate your IT environment into a secure infrastructure, based on the Zero Trust Security architecture principles.

Suggested roadmap

Suggested roadmap | Quick wins

From the assessment there are quick wins that can be accomplished in less than 30 days and with as minimal cost as possible. All the Quick wins can be found in the report.

Topic	Action	Associated Software Products
Quick Wins		
(Azure) Active Directory Accounts	• Review accounts with risky UAC details (see chapter 4.1.16) and remove these AD settings • Disable old/unused accounts • Implement Multi Factor Authentication (MFA) for all user accounts • Review External AAD users	• Azure MFA • Conditional Access • Azure AD reporting
Administrators	• Implement a process to regularly review administrator accounts and clean up old/unused accounts • Ensure admin roles are only placed on admin accounts and not on normal user accounts	• Azure Privileged Identity Management (PIM)
Password Policy	• Enhance the password policy (see chapter 4.1.16) and enable Multi Factor Authentication for all users.	• Azure MFA

Suggested roadmap | Urgent action items

From the assessment there are several actions found that should get attention of the business. All the urgent action can be found in the report.

Topic	Action	Associated Software Products
Urgent		
5. Secure Configuration for Hardware and Software on Mobiles Devices, Laptops, Workstations and Servers	• Define a secure hardening baseline for all key systems, to lock down these systems by default.	• Azure VM's • Azure CIS hardened images • Microsoft Endpoint Manager
7. Email and Web Browser Protections	• Create the appropriate SPF and DKIM record for all email domains.	• Defender for Office
16. Account Monitoring and Control	• Define a standard password policy definition for all the applications and infrastructure services. Start implementing MFA on all systems, increase password length if MFA is not yet available	• Azure Multi-Factor Authentication (MFA) • Conditional Access
AD.3. Risk Management	• Implement a basic risk assessment process.	• Microsoft Compliance Manager • Cyber Security Assessment Tool (CSAT)

Suggested roadmap | Advised software products

The following software is advised based on the found recommendations in this assessment.

Software product	Helps to improve:
AIP scanner	Runs as a service on Windows Server to discover, classify and protect, data that is stored on on-premises systems.
Azure AD Identity Protection	Enables organization to configure automated responses to detect suspicious actions related to user identities.
Azure Information Protection (AIP)	Label, Classify and Protect documents, by applying automatic detection.
Azure Multi-Factor Authentication (MFA)	Add a layer of security to the user login with Azure MFA.
Conditional Access	It provides granular access control to keep your corporate data secure, while giving users an experience that allows them to do their best work from any device, and from any location.
Microsoft Defender ATP	Deploy the Azure anti-malware solution to the endpoints to ensure the latest patches, and check for software vulnerabilities.
Office 365 Data Loss Prevention	Office 365 data loss prevention (DLP) tools help protect content such as HIPAA-related and General Data Protection Regulation-related (GDPR) data.
PortalTalk 365	Gain insight and control on Microsoft Teams, Outlook groups and SharePoint Sites.

Next steps

Next steps | 0-30 days

0-30 days

- Security Strategy workshop: 1 day
- Implement MFA: 5 days
- Separate Administrative accounts: 3 days
- Implement Azure Privileged Identity Manager: 5 days
- Implement Intune Security Baseline for all machines: 10 days

Next steps | How can we assist?

Engage in a Cybersecurity Strategy Workshop

Implement 0-30 days actions

Assess Security Maturity on regular basis

Define project plans based on Cybersecurity Strategy workshop outcomes