An introduction to Security Posture Assessments

Tom Waller | Architect

Secure Digital Transformation

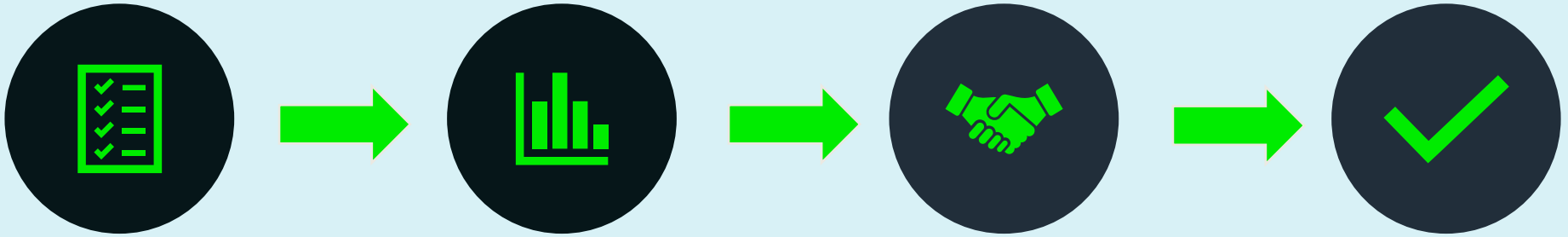
Kocho

BECOME GREATER

Security Posture Assessment – What is it?

Strategic engagement model to help you understand and visualise your security posture

Delivers a roadmap of improvement areas and recommendations
to uplift your security posture



CONDUCT ASSESSMENT

CREATE DASHBOARD

STRATEGIC ENGAGEMENT

REMEDIATION

People and challenges

- People
  - Chief Information Security Officer (CISO)
  - IT Security Managers
  - Security Architects
  - Any senior level person with responsibility for security

- Challenges
  - Communicating risk to board level roles
  - Don’t know where my security gaps are
  - Justifying E3 to E5 license uplifts
  - Am I using all the technology I have access to?
  - Difficult to understand where I need to invest my money and time to drive security improvements
  - Resource constraints

Security Posture Assessment – Key areas

Assessment focus area	Key deliverables	Value
• Current cyber strategy, challenges and priorities • M365/AAD tenant configuration discovery • Credential assessment of local AD • Shadow IT assessment • Alignment with CIS benchmarks	• Detailed, interactive dashboard focussing on risk, business/end user impact and prioritisation • Highlights the benefits of E5 components and promotes the use of existing entitlements • Third-party mitigation support	• Promotes a more strategic engagement • Maximises existing investment in Microsoft technology • Enables visibility of improvement areas • Supports business cases • Visual representation

Key Benefits of the SPA

Improved visibility

Business Support

Reduced Risk

Measurable Returns

Confident Decision Making

Lower Costs

Key Pillars

Identity & access management

Threat protection

Information protection

Security management

Awareness

Governance

Organisational Security

VISUALISE BY FRAMEWORK

Use the buttons on the right to navigate between dashboard views and visualise recommendations by various frameworks.

MITRE ATT&CK | CIS | Zero Trust Security

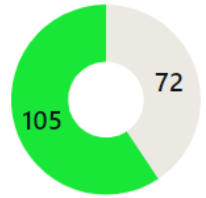
RECOMMENDATIONS

Search

RECOMMENDATION	LICENCED	PRIORITY
Ensure multifactor authentication is enabled for all users in all roles.	✓	High
Ensure DLP policies are enabled for Microsoft Teams.	✓	High
Ensure multifactor authentication is enabled for all users in administrative roles.	✓	High
Ensure SQL server's TDE protector is encrypted with Customer-managed key.	✓	Medium
Ensure that 'OS and Data' disks are encrypted with CMK.	✓	Medium
Ensure that the latest OS Patches for all Virtual Machines are applied.	✓	Medium
Ensure that 'Unattached disks' are encrypted with CMK.	✓	Medium
Ensure that VHD's are encrypted.	✓	Medium
Use Just In Time privileged access to Office 365 roles.	✓	Medium
Delete/block accounts not used in last 30 days.	✓	Medium
Ensure expiration time for external sharing links is set.	✓	Medium
Ensure mobile device management polices are set to require advanced security configurations to protect from basic internet attacks.	✓	Medium
Ensure mobile device management policies are required for email profiles.	✓	Medium
Ensure that DKIM is enabled for all Exchange Online Domains.	✓	Medium
Ensure that RDP access is restricted from the internet.	✓	Medium
Ensure that Resource Locks are set for mission critical Azure resources.	✓	Medium
Ensure that the endpoint protection for all Virtual Machines is installed.	✓	Medium

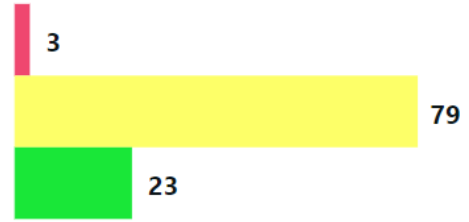
SEE DETAILS

APPLICABLE RECOMMENDATIONS



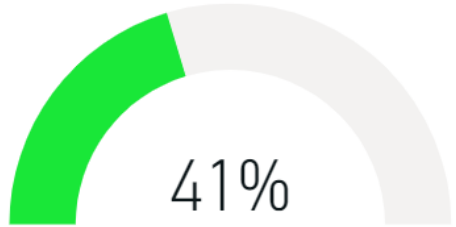
Compliant | Non-compliant

PRIORITY ANALYSIS

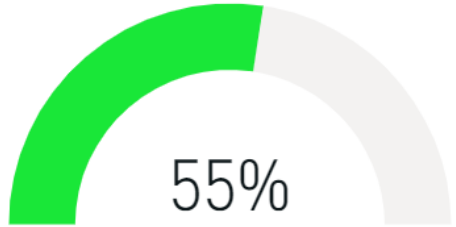


High | Medium | Low

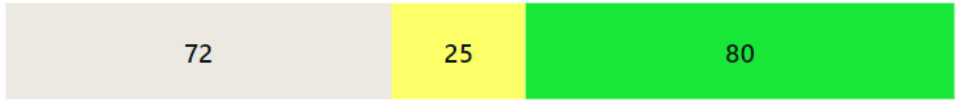
YOUR SCORE



YOUR SCORE WITH MITIGATIONS



COMPLIANCE OVERVIEW



Compliant | Non-compliant but mitigated | Non-compliant

SEE DETAILS

COMPLIANCE WITHIN YOUR CURRENT LICENSE SUITE

Compliant | Non-compliant

CLEAR PAGE FILTERS | SPA DATE: 15 November 2021 | BASELINE: All | SHOW HELP TEXT | RECOMMENDATION EXPLORER

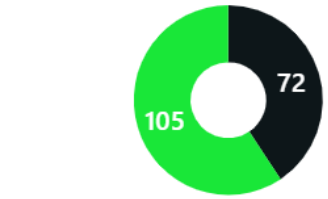
MITRE ATT&CK MAPPING

Search

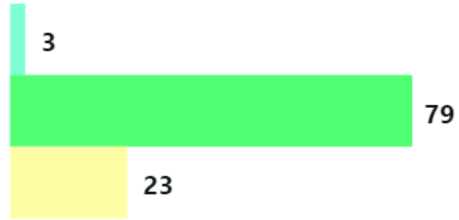
RECOMMENDATION	LICENCED	PRIORITY
Ensure multifactor authentication is enabled for all users in all roles.	✓	
Ensure DLP policies are enabled for Microsoft Teams.	✓	
Ensure multifactor authentication is enabled for all users in administrative roles.	✓	
Ensure SQL server's TDE protector is encrypted with Customer-managed key.	✓	
Ensure that 'OS and Data' disks are encrypted with CMK.	✓	
Ensure that the latest OS Patches for all Virtual Machines are applied.	✓	
Ensure that 'Unattached disks' are encrypted with CMK.	✓	
Ensure that VHD's are encrypted.	✓	
Use Just In Time privileged access to Office 365 roles.	✓	
Delete/block accounts not used in last 30 days.	✓	
Ensure expiration time for external sharing links is set.	✓	
Ensure mobile device management polices are set to require advanced security configurations to protect from basic internet attacks.	✓	
Ensure mobile device management policies are required for email profiles.	✓	
Ensure that DKIM is enabled for all Exchange Online Domains.	✓	
Ensure that RDP access is restricted from the internet.	✓	
Ensure that Resource Locks are set for mission critical Azure resources.	✓	
Ensure that the endpoint protection for all Virtual Machines is installed.	✓	
Using Microsoft Defender for Cloud Apps, create a custom activity policy to discover suspicious usage patterns.	✓	
Ensure any of the ASC Default policy setting is not set to "Disabled".	✗	
Ensure that 'All users with the following roles' is set to 'Owner'.	✗	
Configure automatic device quarantine rules.	✓	

SEE DETAILS

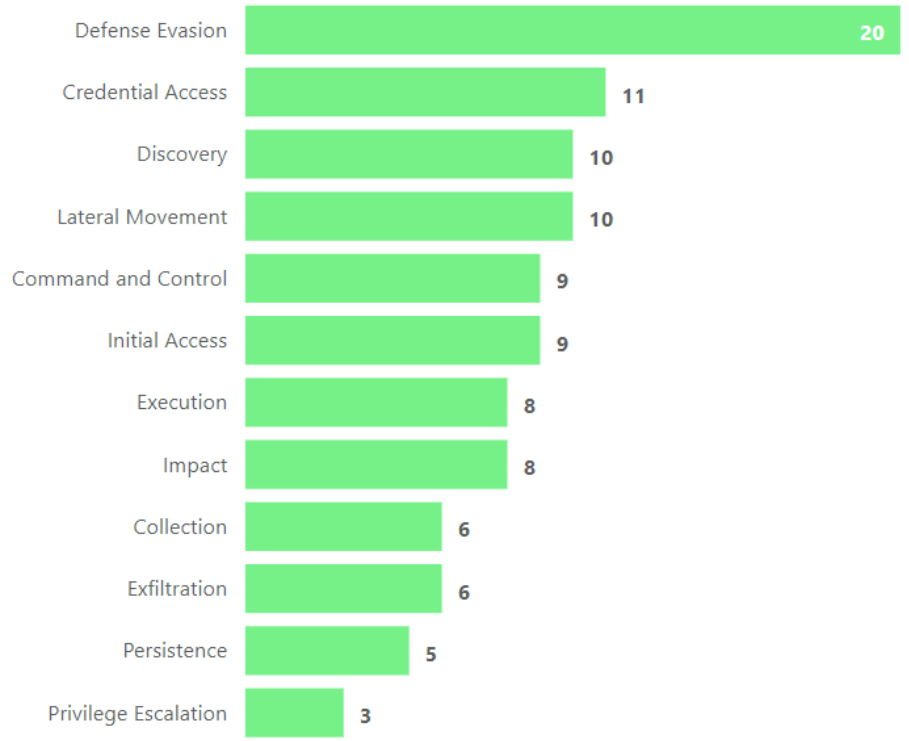
APPLICABLE RECOMMENDATIONS



PRIORITY ANALYSIS



RECOMMENDATION DISTRIBUTION BY MITRE ATT&CK TACTIC



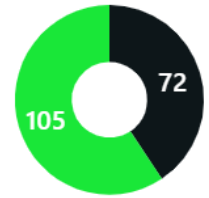
CIS AREA MAPPING

Search

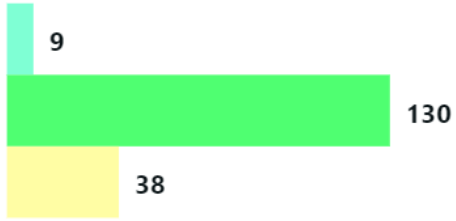
RECOMMENDATION	LICENCED	PRIORITY
Ensure multifactor authentication is enabled for all users in all roles.	✓	
Ensure DLP policies are enabled for Microsoft Teams.	✓	
Ensure multifactor authentication is enabled for all users in administrative roles.	✓	
Ensure SQL server's TDE protector is encrypted with Customer-managed key.	✓	
Ensure that 'OS and Data' disks are encrypted with CMK.	✓	
Ensure that the latest OS Patches for all Virtual Machines are applied.	✓	
Ensure that 'Unattached disks' are encrypted with CMK.	✓	
Ensure that VHD's are encrypted.	✓	
Use Just In Time privileged access to Office 365 roles.	✓	
Delete/block accounts not used in last 30 days.	✓	
Ensure expiration time for external sharing links is set.	✓	
Ensure mobile device management polices are set to require advanced security configurations to protect from basic internet attacks.	✓	
Ensure mobile device management policies are required for email profiles.	✓	
Ensure that DKIM is enabled for all Exchange Online Domains.	✓	
Ensure that RDP access is restricted from the internet.	✓	
Ensure that Resource Locks are set for mission critical Azure resources.	✓	
Ensure that the endpoint protection for all Virtual Machines is installed.	✓	
Using Microsoft Defender for Cloud Apps, create a custom activity policy to discover suspicious usage patterns.	✓	
Ensure any of the ASC Default policy setting is not set to "Disabled".	✗	
Ensure that 'All users with the following roles' is set to 'Owner'.	✗	
Configure automatic device quarantine rules.	✓	

SEE DETAILS

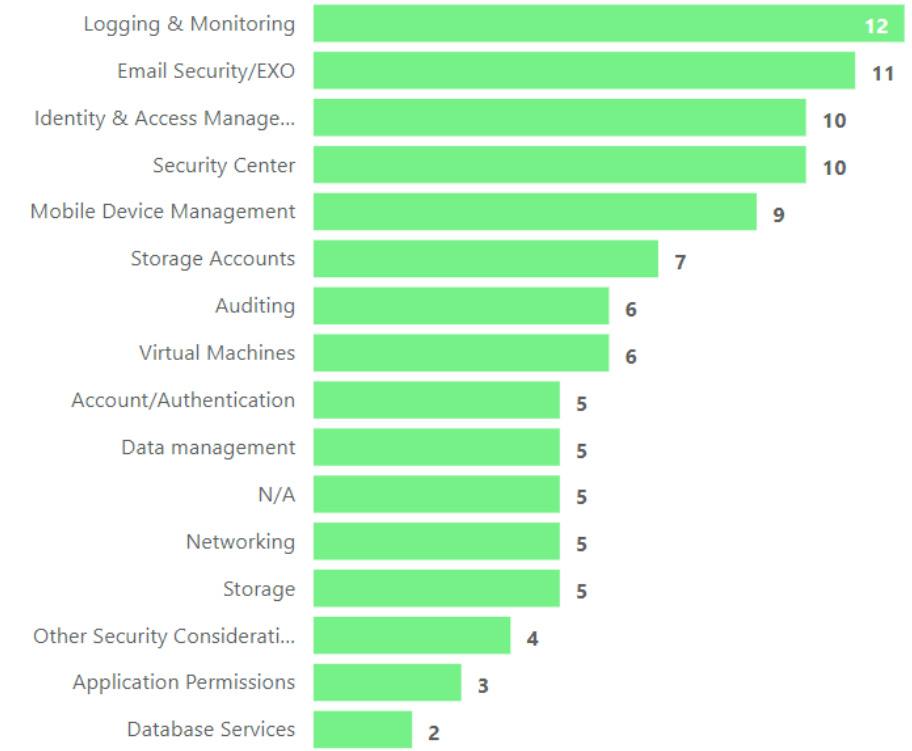
APPLICABLE RECOMMENDATIONS



PRIORITY ANALYSIS



RECOMMENDATION DISTRIBUTION BY CIS AREA



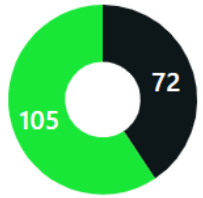
ZERO TRUST PILLAR MAPPING

Search

RECOMMENDATION	LICENCED	PRIORITY
Ensure multifactor authentication is enabled for all users in all roles.	✓	
Ensure DLP policies are enabled for Microsoft Teams.	✓	
Ensure multifactor authentication is enabled for all users in administrative roles.	✓	
Ensure SQL server's TDE protector is encrypted with Customer-managed key.	✓	
Ensure that 'OS and Data' disks are encrypted with CMK.	✓	
Ensure that the latest OS Patches for all Virtual Machines are applied.	✓	
Ensure that 'Unattached disks' are encrypted with CMK.	✓	
Ensure that VHD's are encrypted.	✓	
Use Just In Time privileged access to Office 365 roles.	✓	
Delete/block accounts not used in last 30 days.	✓	
Ensure expiration time for external sharing links is set.	✓	
Ensure mobile device management polices are set to require advanced security configurations to protect from basic internet attacks.	✓	
Ensure mobile device management policies are required for email profiles.	✓	
Ensure that DKIM is enabled for all Exchange Online Domains.	✓	
Ensure that RDP access is restricted from the internet.	✓	
Ensure that Resource Locks are set for mission critical Azure resources.	✓	
Ensure that the endpoint protection for all Virtual Machines is installed.	✓	
Using Microsoft Defender for Cloud Apps, create a custom activity policy to discover suspicious usage patterns.	✓	
Ensure any of the ASC Default policy setting is not set to "Disabled".	✗	
Ensure that 'All users with the following roles' is set to 'Owner'.	✗	
Configure automatic device quarantine rules.	✓	

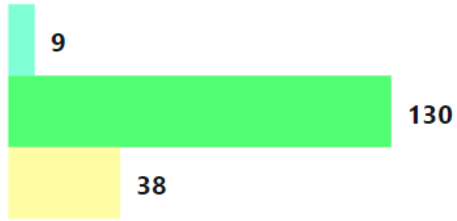
SEE DETAILS

APPLICABLE RECOMMENDATIONS



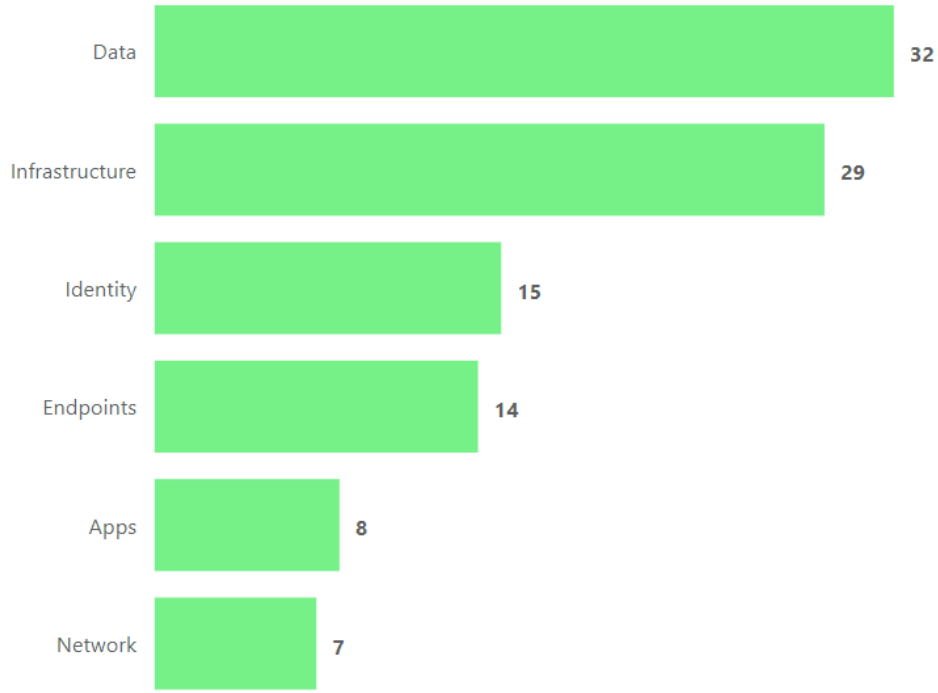
Compliant Non-compliant

PRIORITY ANALYSIS



High Medium Low

RECOMMENDATION DISTRIBUTION BY ZERO TRUST PILLAR



FILTERS

Use the filters below to apply selection criteria to the recommendations table.

PEOPLE, POLICY, PROCESS AND TECHNOLO...
Technology

SPA PILLAR
All

CIS AREA
Multiple selections

MITRE ATT&CK
All

ZERO TRUST PILLAR
All

ZERO TRUST GUIDING PRINCIPLE
All

TECHNICAL EFFORT
All

OPERATIONAL IMPACT
All

USER IMPACT
All

RESET

RECOMMENDATIONS

The table below lists all the applicable, non-compliant recommendations that require action. To investigate a recommendation further, select the item in the table and click the 'see details' button.

RECOMMENDATION	LICENSED	PRIORITY	OPERATIONAL IMPACT	USER IMPACT	TECHNICAL EFFORT
Enable Conditional Access policies to block legacy authentication.	✓	🔴	🟠	🟢	🟢
Ensure multifactor authentication is enabled for all users in all roles.	✓	🔴	🔴	🔴	🔴
Ensure self-service password reset is enabled.	✓	🔴	🟠	🔴	🟠
Ensure multifactor authentication is enabled for all users in administrative roles.	✓	🔴	🟠	🟠	🟠
Use Just In Time privileged access to Office 365 roles.	✓	🟠	🟠	🟠	🟠
Ensure that Resource Locks are set for mission critical Azure resources.	✓	🟠	🟠	🟢	🟠
Enable Azure AD Identity Protection sign-in risk policies.	✓	🟠	🟢	🟢	🟢
Enable Azure AD Identity Protection user risk policies.	✓	🟠	🟢	🟢	🟢
Ensure modern authentication for Exchange Online is enabled.	✓	🟠	🟢	🟢	🟢
Ensure modern authentication for SharePoint applications is required.	✓	🟠	🟢	🟢	🟢
Ensure modern authentication for Skype for Business Online is enabled.	✓	🟠	🟢	🟢	🟢
Ensure that Azure Defender is set to On for Servers.	✗	🟠	🟠	🟢	🟢
Ensure user consent to apps accessing company data on their behalf is not allowed.	✓	🟠	🟢	🟢	🟢
Enabled Identity Protection to identify anomalous logon behaviour.	✓	🟠	🟠	🟢	🟢
Ensure that Azure Defender is set to On for Azure SQL database servers.	✗	🟠	🟢	🟢	🟢
Ensure that Azure Defender is set to On for Container Registries.	✗	🟠	🟢	🟢	🟢
Ensure that Azure Defender is set to On for Key Vault.	✗	🟠	🟢	🟢	🟢
Ensure that Azure Defender is set to On for Kubernetes.	✗	🟠	🟢	🟢	🟢
Ensure that Azure Defender is set to On for SQL servers on machines.	✗	🟠	🟢	🟢	🟢
Ensure that Azure Defender is set to On for Storage.	✗	🟠	🟢	🟢	🟢
Ensure that password hash sync is enabled for resiliency and leaked credential detection.	✓	🟠	🟢	🟢	🟢
Ensure that Azure Defender is set to On for App Service.	✗	🟢	🟢	🟢	🟢

SEE DETAILS

MITIGATED RECOMMENDATIONS

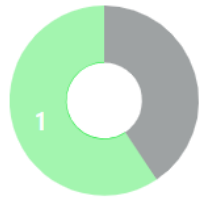
The table below lists all the applicable, non-compliant and potentially mitigated recommendations that may require action. To investigate a recommendation further, select the item in the table and click the 'see details' button. Mitigated recommendations are identified where they are applicable and non-compliant but may have alternative measure in place that counter the recommendation. Mitigated recommendations still impact the overall compliance score as Kocho are unable to validate third-party solutions as part of the SPA.

Search

MITIGATED RECOMMENDATION	LICENCED	PRIORITY
Ensure basic authentication for Exchange Online is disabled.	✓	
Ensure that settings are enabled to lock multiple devices after a period of inactivity to prevent unauthorised access.	✓	
Ensure the Microsoft Defender for Office 365 Safe Attachments policy is enabled.	✓	
Ensure the Microsoft Defender for Office 365 Safe Links policy is enabled.	✓	
Configure automatic device quarantine rules.	✓	
Ensure soft delete is enabled for Azure Storage.	✓	
Ensure that logging for Azure Key Vault is 'Enabled'.	✓	
Ensure that only approved extensions are installed.	✓	
Ensure that SSH access is restricted from the internet.	✓	
Ensure that the expiration date is set on all keys.	✓	
Ensure that the expiration date is set on all Secrets.	✓	
Ensure that UDP Services are restricted from the Internet.	✓	
Use the OneDrive for Business Admin Centre to block OneDrive for Business sync from unmanaged devices.	✓	
Delete/block accounts not used in last 30 days.	✓	
Ensure mobile device management policies are required for email profiles.	✓	
Ensure that RDP access is restricted from the internet.	✓	
Ensure multifactor authentication is enabled for all users in administrative roles.	✓	
Ensure multifactor authentication is enabled for all users in all roles.	✓	

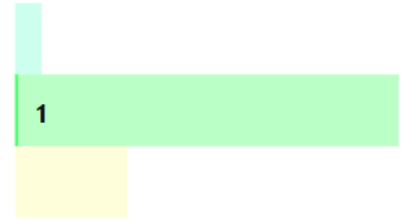
SEE DETAILS

APPLICABLE RECOMMENDATIONS



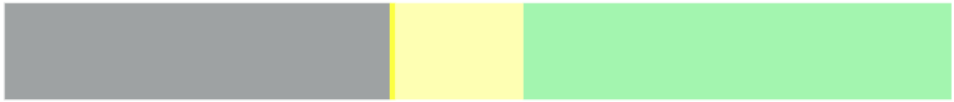
Compliant Non-compliant

PRIORITY ANALYSIS



High Medium Low

COMPLIANCE OVERVIEW



Compliant Non-compliant but mitigated Non-compliant

MITIGATION COMMENT

Logging configured to Log Analytics workspace rather than a storage account.

RECOMMENDATION MAPPINGS

Security SPA PILLAR	Technology PPPT	Logging & Monitoring CIS AREA
Lateral Movement MITRE ATT&CK	Infrastructure ZERO TRUST PILLAR	

Ensure basic authentication for Exchange Online is disabled.

DESCRIPTION

Basic authentication allows users to access Exchange Online using legacy or unapproved email clients. These clients do not support modern authentication mechanisms, such as multifactor authentication.

REASONING

Basic authentication for Exchange Online has not been disabled within Exchange Online within the tenant.

BENEFITS

Disabling basic authentication prevents use of legacy and unapproved email clients with weaker authentication mechanisms.

CONSEQUENCES

Increased the risk of email account credential compromise.

IMPACT ASSESSMENT

This recommendation has been assessed for impact across various metrics as displayed in this section. This allows you to plan remediation in many ways by targeting specific exposure levels.

USER IMPACT	TECHNICAL EFFORT	OPERATIONAL EFFORT	INITIATIVE IMPACT	PRIORITY
Low	Low	Moderate	Low	Moderate

AT A GLANCE

This recommendation requires **Microsoft 365 E3, Microsoft 365 E5, Microsoft EM**

This recommendation falls under the **Security** SPA pillar.

Aligned to the **Application Security** initiative.

TRAINING REQUIREMENTS

Whilst specific technical training isn't required to support this recommendation, an understanding of any potential user and, or organisational impact is required ahead of implementation. This should be gained as part of a formal change request process.

REPORTING MECHANISM

Exchange Admin Center.

RECOMMENDATION MAPPINGS

Credential Access MITRE ATT&CK	Email Security/EXO CIS AREA
Identity ZERO TRUST PILLAR	Exchange PRIMARY TECHNOLOGY

RECOMMENDATION ID

34

Compromised accounts by user name

The table below lists the user accounts which were discovered to have a compromised credential associated to it. Kocho recommend taking immediate steps to ensure that these accounts are remediated as they could represent a significant risk to your organisation.

User principal name	sAMAccountName	Display name	Description
test1@contoso.com	Test1	Test 1	Description: 1
test10@contoso.com	Test10	Test 10	Description: 10
test11@contoso.com	Test11	Test 11	Description: 11
test12@contoso.com	Test12	Test 12	Description: 12
test13@contoso.com	Test13	Test 13	Description: 13
test14@contoso.com	Test14	Test 14	Description: 14
test15@contoso.com	Test15	Test 15	Description: 15
test16@contoso.com	Test16	Test 16	Description: 16
test17@contoso.com	Test17	Test 17	Description: 17
test18@contoso.com	Test18	Test 18	Description: 18
test19@contoso.com	Test19	Test 19	Description: 19
test2@contoso.com	Test2	Test 2	Description: 2
test20@contoso.com	Test20	Test 20	Description: 20
test21@contoso.com	Test21	Test 21	Description: 21
test22@contoso.com	Test22	Test 22	Description: 22
test23@contoso.com	Test23	Test 23	Description: 23
test24@contoso.com	Test24	Test 24	Description: 24
test25@contoso.com	Test25	Test 25	Description: 25
test26@contoso.com	Test26	Test 26	Description: 26
test27@contoso.com	Test27	Test 27	Description: 27
test28@contoso.com	Test28	Test 28	Description: 28

Key figures

30.5% Accounts compromised

of which

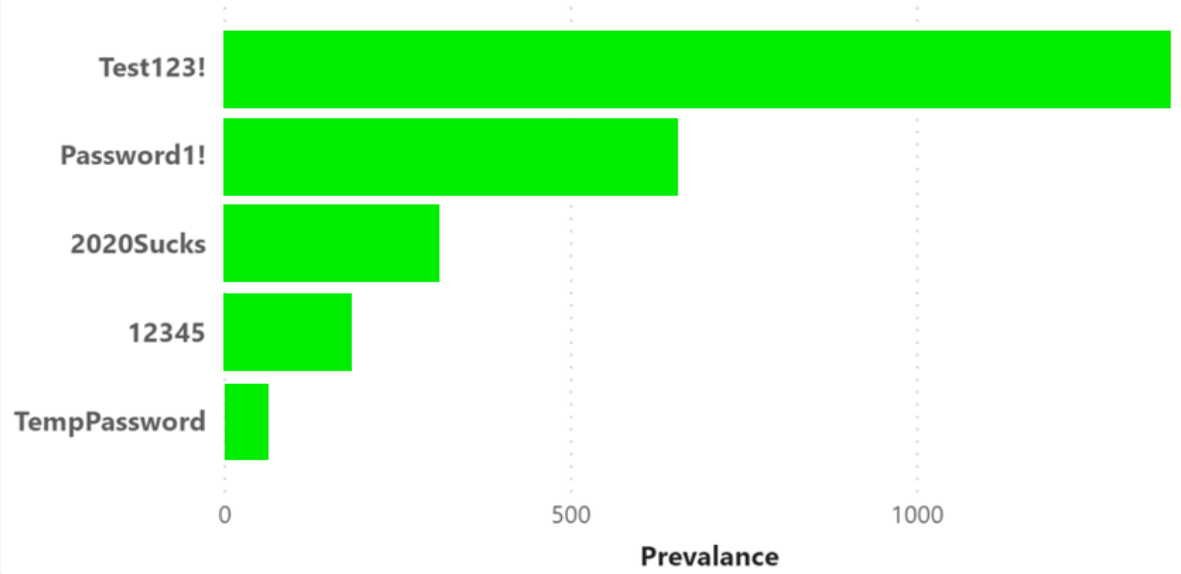
54.7% Active in last 90 days

4852 out of 11965 Total compromised accounts

2654 Total active in last 90 days

Prevalance by password

The graph below shows the usage distribution of compromised password within your environment. Look for trends that may indicate issues with your new user processes or password complexity failures.



Kocho

BECOME GREATER

Thank you

→ Any questions?

About Kocho

Kocho
BECOME GREATER

At Kocho, we believe greatness lies in everyone. That's why we exist, to help ambitious companies realise their potential.

By combining the power of Microsoft cloud technology with world-class identity, cyber security and our team of talented people, we take our clients on a journey of secure cloud transformation.

And we're with you every step of the way. Because the path to greatness isn't walked alone. We help you adopt and embrace the right technology solutions at the right time.

The result? Sustainable and secure growth that amplifies your business success.

Kocho. Become Greater.

Award-winning solutions

Eight-time winner of the Microsoft Partner of the Year Award for Identity Management, Enterprise Mobility, and Security and Compliance.

Microsoft Partner

Microsoft

- Gold Security
- Gold Datacenter
- Gold Cloud Platform
- Gold Cloud Productivity
- Gold Application Developer
- Gold Windows and Devices
- Gold Enterprise Mobility Management
- Gold Small and Midmarket Cloud Solutions

hello@kocho.co.uk

0800 044 5009