

Microsoft 365 Review Report

Project	SAMPLE - Microsoft 365 Review	Reference	
Publication Date		Version	1.0 Release

Limitations

As with all security reviews, this work has been performed using information and tools currently available from national and international security organisations.

The results represent a snapshot of the environment as it was at the time of the review. It is incumbent upon the organisation to ensure that the site is kept up to date with intrusion control methods.

Kaon Security Limited, its Directors and staff cannot be held liable for any losses, direct or consequential which may result from actioning, or not actioning, recommendations provided in the report.

Confidentiality

The data gathered during this process will be used for the purposes of this review only.

All information gathered on site is stored on an encrypted hard drive.

All information gathered during the review and reports generated, with the exception of the executive and technical summaries, will be wiped from Kaon Security's information systems upon acceptance of the report by you.

Any output produced by Kaon Security (and all the information within) is strictly for the eyes of SAMPLE staff members and senior management only. In the event where any part of the information is required to be shared with any 3rd party, sister organisation, or vendor, Kaon Security's written approval is required.



Table of Contents

4
4
5
6
6
7
8
8
9
0
2
2
2
2

Executive Summary

SAMPLE appointed Kaon Security (KS) to perform a security review of the current Microsoft 365 setup.

A detailed scope is defined within the section titled Scope.

Kaon Security performed a remote interview of a nominated SAMPLE staff member...

Microsoft 365 Review

Kaon Security found that the Microsoft 365 environment at SAMPLE is well configured in many areas. We did however find many critical and high risk security issues, and numerous opportunities for improvement.

The following table illustrates the high level findings across the Microsoft 365 environment.

Please note: Numbers in this table are not representative - example purposes only

M365 Review Outcome								
Configuration Section	Critical	High	Medium	Low	Total			
M365	1	1	1	1	4			
Azure Active Directory (AAD)	2	2	2	2	8			
Endpoint Manager	3	3	3	3	12			
Exchange Admin	4	4	4	4	16			
OneDrive	5	5	5	5	20			
Security	6	6	6	6	24			
Compliance	7	7	7	7	28			
SharePoint	8	8	8	8	32			
Power Apps	9	9	9	9	36			
Dynamics 365	10	10	10	10	40			
Cloud App Security	11	11	11	11	44			
Power Automate	12	12	12	12	48			
Teams	13	13	13	13	52			
Other	14	14	14	14	56			



Recommendations for Security Posture

Kaon Security provides these recommendations based on the limited information collected during a passive interview. We therefore advise taking these as guidelines only.

Kaon Security believes that the following additional security considerations would benefit SAMPLE by integrating security, monitoring, intelligence, and incident response components. Furthermore, end to end security integration would help to train and prepare SAMPLE for future security activities.

- 1. Document a well-defined ICT Data Governance security policy.
- 2. Data discovery, identification, classification, and sensitive data registry.

Please note: Recommendations for Security Posture can vary from site to site, can be up to 15 recommendations.



Key Observations and Recommendations

This section provides key observations and relevant recommendations.

Microsoft 365 Review

Kaon Security performed a detailed review of the current configurations of Microsoft 365 and Microsoft 365 specific items within Azure Active Directory for SAMPLE and found the following issues:

- 1. SAMPLE infrastructure allows users to join any new device to their Microsoft 365 account without a defined approval process. In the case of a compromised account, an attacker would have easy access to register rogue devices.
- 2. The Microsoft 365 online configuration allows third-party storage systems to be used for sharing and viewing content. It is unusual to allow this inter-cloud functionality because Microsoft 365 provides 1TB of OneDrive secure storage at no additional cost.

Please note: Microsoft 365 Review content varies from site to site, can be up to 25 findings



Additional Recommendations

Kaon Security identified the following key summarised recommendations:

- 1. A detailed fine tuning of the Microsoft 365 configurations as per the Key Findings section.
- 2. Perform a Cloud exposure mapping activity to identify all other SaaS solutions used across the SAMPLE IT infrastructure.

Please note: Additional Recommendations varies from site to site, can be between 10 to 20 recommendations.



Key Findings

Urgent Attention Required

This section looks through some of the items in urgent need of review or analysis. We consider these items to potentially be active risks and recommend attending to them ASAP. Refer finding number 49 in <u>All Issues Found</u> table.

 * randition * active factor before applications * excent to be each of the factor of the sector of the	Dashboard	Construction Construction Construction Construction					×
 Aura Advo Diversion 		₽ Search (Ctrl+/) «	🕕 Learn more 🗸 Download 🚝 Select all 🗴	Confirm user(s) compromised 🗸 Dism	iss user(s) risk 🖒 Refresh 🛛 🎫 Columns 🖉 Go	t feedback?	
Image: Section of the control of th	Azure Active Directory		•				
Protect Protect Risk notion R	Users		Auto refresh : Off Show dates as : Local	Risk state : 2 selected Status	: Active + Add filters		
* Sign-in risk policy Low 11/d/2020, 80330 PM * MAr egistration policy Low 9/30/2020, 43607 PM Report Low 9/30/2020, 43607 PM * Risky sign-ins Low 9/30/2020, 43607 PM * Risky sign-ins Low 9/30/2020, 43607 PM * Risky sign-ins Low 0/6/2020, 33807 PM * Risky sign-ins Low 0/6/2020, 10/4853 AM * Risky sign-ins Low 7/20200, 11/3254 FM * Risky sign-ins Low 10/6/2020, 11/3545 AM * Uses at risk detected alerts Atrisk Low 6/26/202, 05/0541 PM * Uses at risk detected alerts Atrisk Low 6/26/202, 05/0541 PM * Toubleshooting + Support reguest Atrisk Medium 6/26/202, 05/0541 PM * Toubleshooting + Support reguest Atrisk Medium 6/26/202, 02/02, 02/04/233 PM * Toubleshooting + Support reguest Atri			User ↑↓	Risk state ↑↓	Risk level ↑↓	Risk last updated 🛧	
MA registration policy Arrisk Low 9/9/0200, 43807 PM Report Cow 9/9/0200, 43807 PM Report Cow 0 9/9/0200, 03807 PM Report Arrisk Medium 0/9/0200, 05709 PM Report Arrisk Medium 0/16/0200, 0114281 NA Report Arrisk Medium 0/9/0200, 0113545 AM Report Arrisk Medium 0/2/0200, 0505041 PM Report Arrisk Medium 0/2/0200, 050, 0541 PM Report Arrisk Medium 0/2/0200, 05200 PM Report Arr			の名類の言語になった。	At risk	Low	11/6/2020, 8:03:30 PM	
MAR registration policy Artisk Low 9/J2020,83:08 AM Report Artisk Low 06/2020,33:007 PM Naky sign-ins: Artisk Medium 7/27/2020,1048:53 AM Naky sign-ins: Artisk Low 7/27/2020,1048:53 AM Notify Low 7/15/2020,114/23 PM Artisk Notify Artisk Low 7/15/2020,114/23 PM Wedky digest Artisk Low 7/16/2020,33:33 FM Youbleshooting + Support Artisk Low 7/6/2020,50:541 PM Youbleshooting + Support Artisk Low 6/2020,50:541 PM Youbleshooting + Support request Artisk Medium 6/2020,50:541 PM Artisk Medium Medium 6/2020,21:13:54 SM Youbleshooting + Support request Artisk Low 6/2020,21:13:54 SM Artisk Medium Medium 6/2020,21:13:54 SM Artisk Low Medium 6/2020,21:13:54 SM Artisk Medium 6/2020,21:13:54 SM Medium Motopool Artisk Medium 6/2020,21:13:54 SM Artisk		📍 Sign-in risk policy	State State State State	At risk	Low	9/30/2020. 4:36:07 PM	
Pept Dev		Ø MFA registration policy		At risk	low		
Image: Nisky users At risk Medium 7/27/2020, 10:48:53 AM Image: Nisky sign: nis At risk Low 7/20/2020, 657:09 PM Image: Nisky sign: nis At risk Low 7/15/2020, 10:48:53 AM Image: Nisky sign: nis At risk Low 7/15/2020, 10:48:53 AM Image: Nisky sign: nis At risk Low 7/15/2020, 10:48:53 AM Image: Nisky sign: nis At risk Low 7/15/2020, 10:48:53 AM Image: Nisky sign: nis At risk Low 7/15/2020, 11:42:3 PM Image: Nisky sign: nis At risk Low 7/6/2020, 11:35:45 AM Image: Nisky sign: nisky		Report					
Risky sign-insAt riskLow7/20/200, 657.09 PMRisk detectionsLow7/15/202, 1:1423 PMNoticyAt riskLow7/15/202, 1:1423 PMI Users at risk detected alertsAt riskLow7/6/200, 3:3735 PMI Weekly digestAt riskLow7/6/200, 1:3545 AMTotubleshooting + SupportAt riskLow6/6/2020, 1:3545 AMX TotubleshootAt riskLow6/6/2020, 1:3545 AMR we support requestAt riskMedium6/6/2020, 1:3545 AMAt riskLowMedium6/6/2020, 1:3545 AMAt riskLowMedium6/6/2020, 1:3545 AMAt riskLowMedium6/6/2020, 1:3545 AMAt riskMediumMedium6/6/2020, 1:3545 AMAt riskMediumMedium6/2/2020, 1:145 AM		📩 Risky users	11 Mar 10 10 1				
A Risk detections At risk Low 7/5/2020, 1:423 PM Notify At risk Medium 7/13/2020, 1:45:11 AM I Users at risk detected alerts At risk Low 7/6/2020, 1:35:35 PM I Veekly digest At risk Low 7/6/2020, 1:35:45 AM Totubleshooting + Support At risk Low 6/2/2020, 0:37:35 PM X Totubleshoot At risk Medium 6/2/2020, 0:30:32:32 PM X Totubleshoot At risk Medium 6/2/2020, 0:20, 0:21:35 AM X Totubleshoot At risk Low 6/2/2020, 0:20, 0:21:45 AM X Totubleshoot At risk Low 6/2/2020, 0:21:45 AM X Totubleshoot At risk Low			and the second				
NotifyMedium7/13/2020, 11:45:11.AMIL Users at risk detected alertsAt riskLow7/6/2020, 3:37:35 PMIC Weekly digestAt riskLow7/6/2020, 11:35:45 AMTotubleshooting + SupportAt riskLow6/26/2020, 50:54:11 PMX TotubleshootAt riskMedium6/26/2020, 50:54:11 PMX TotubleshootAt riskMedium6/26/2020, 4:12:33 PMX TotubleshootAt riskMedium6/26/2020, 4:12:33 PMX New support requestAt riskLow6/26/2020, 4:12:33 PMAt riskLowMedium6/26/2020, 9:11:45 AMAt riskLowCow6/26/2020, 9:11:45 AMAt riskLowMedium6/26/2020, 9:11:45 AM		A Risk detections					
I Users at risk detected alerts At risk Low 7/6/2020, 3:3735 PM I Users at risk detected alerts At risk Low 7/6/2020, 1:35.45 AM I Weekly digest At risk Low 6/26/2020, 5:05.41 PM Totubleshooting + Support At risk Low 6/26/2020, 5:05.41 PM X Troubleshoot At risk Medium 6/26/2020, 4:12:33 PM At risk Medium 6/26/2020, 4:12:33 PM At risk Low 6/26/2020, 4:12:33 PM At risk Medium 6/26/2020, 4:12:33 PM At risk Low 6/26/2020, 9:11:45 AM At risk Low 6/26/2020, 9:11:45 AM		Markie.	1.5100-150 ABC				
Weekly digest At risk Low 7/6/2020, 11:35:45 AM Troubleshooting + Support At risk Low 6/26/2020, 5:05:41 PM X Troubleshoot At risk Medium 6/26/2020, 4:12:33 PM At risk Medium 6/26/2020, 4:12:33 PM At risk Medium 6/26/2020, 3:28:21 PM At risk Low 6/26/2020, 9:11:45 AM At risk Low 6/26/2020, 3:28:21 PM At risk Low 6/26/2020, 9:11:45 AM At risk Low 6/26/2020, 9:11:45 AM At risk Medium 6/24/2020, 3:25:09 PM							
Troubleshooting + Support At risk Low 6/26/2020, 5/05/41 PM X Troubleshoot At risk Medium 6/26/2020, 4/12/33 PM X Troubleshoot At risk Medium 6/25/2020, 3/28/21 PM X Troubleshoot At risk Medium 6/25/2020, 3/28/21 PM At risk Low 6/26/2020, 3/28/21 PM			新生活的				
Troubleshooting + Support At risk Medium 6/26/2020, 4:12:33 PM Troubleshoot At risk Medium 6/25/2020, 3:28:21 PM New support request At risk Low 6/25/2020, 9:11:45 AM At risk Medium 6/26/2020, 9:11:45 AM At risk Medium 6/26/2020, 9:11:45 AM		Weekly digest					•••
K Troubleshoot At risk Medium 6/25/2020, 3:28:21 PM R New support request At risk Low 6/25/2020, 9:11:45 AM At risk Medium 6/25/2020, 9:11:45 AM At risk Medium 6/24/2020, 3:25:09 PM		Troubleshooting + Support	「「「「				
At risk Low 6/25/2020, 9:11:45 AM At risk Medium 6/24/2020, 9:21:45 AM		× Troubleshoot	and the second second	At risk	Medium	6/26/2020, 4:12:33 PM	
At risk Medium 6/24/2020, 3:25:09 PM		New support request	1. 2. 2. 21 2	At risk	Medium	6/25/2020, 3:28:21 PM	
			and the second sec	At risk	Low	6/25/2020, 9:11:45 AM	••••
			the states	At risk	Medium	6/24/2020, 3:25:09 PM	•••
Load Mole					Load more		
			Details				^



All Issues Found

	Microsoft 365 Configuration Review										
Sr. No	Configuration Panel	Configuration Item	Description	Current Value	Recommended Value	Severity	Complexity	Time to Achieve	Security Impact	Issue Type	
1	M365	Users				Critical	Easy	5 Min	High	Security Exposure	
2	M365	Domains				High	Easy	1 Hour	High	Misconfigur ation	
23	AAD	Password Reset				Low	Easy	TBC	Medium	None	
46	AAD	Password Reset				High	Easy	5 Min	High	Data Security	
65	Compliance	Improvement Actions		Classified		Medium	High	TBC	High	Data Security	
73	Compliance	Data Classification				Medium	Medium	TBC	High	Data Security	
84	Endpoint Manager	Noncompliant Devices				Critical	Easy	1 hour	High	Data Security	

Kaon Security categorised multiple issues based on their risk type; the following table lists all the issues found during this activity.

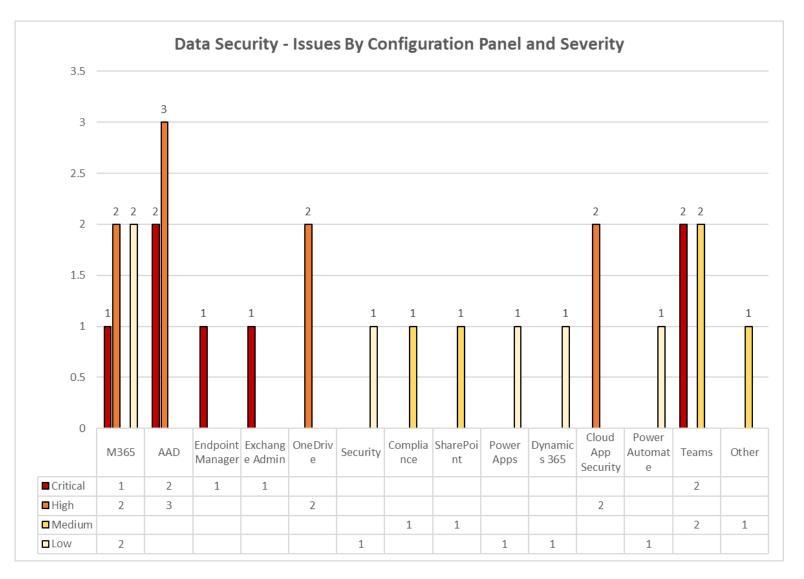
Please note: content of table varies from site to site, can be between 60 to 100 entries!



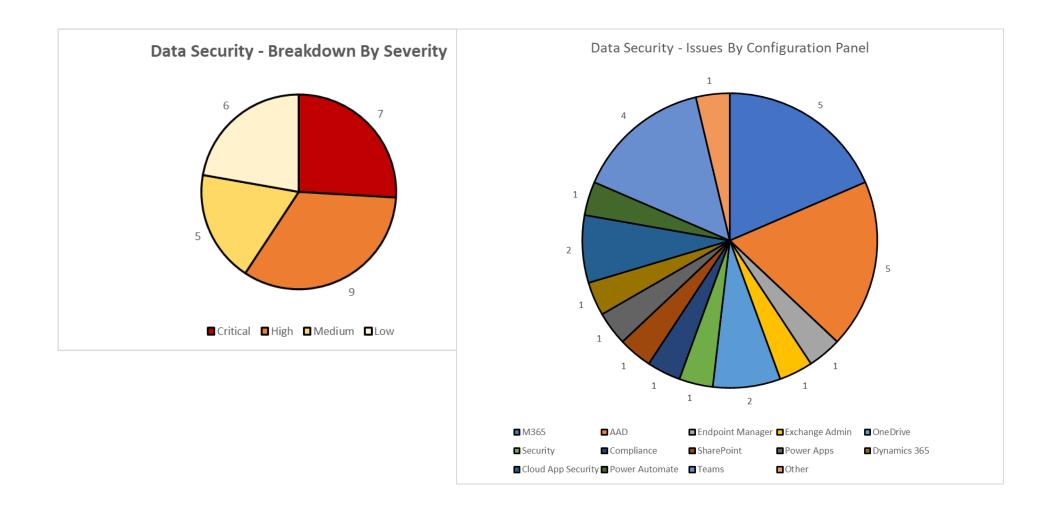
SAMPLE - Microsoft 365 Review

Data Security Issues

Kaon Security categorised multiple issues based on their risk type; the following issues are identified as Data Security.









Security Exposure Issues

Kaon Security categorised multiple issues based on their risk type; the following issues are identified as Security Exposure.

Please note: Additional graphs will be provided for Security Exposure Issues

Privacy Issues

Kaon Security categorised multiple issues based on their risk type; the following issues are identified as Privacy.

Please note: Additional graphs will be provided for Privacy Issues

Misconfiguration Issues

Kaon Security categorised multiple issues based on their risk type; the following issues are identified as Misconfiguration.

Please note: Additional graphs will be provided for Misconfiguration Issues

Other Issues

Kaon Security categorised multiple issues based on their risk type; the following issues are identified as Other.

Please note: Additional graphs will be provided for Other Issues

