



Microsoft Defender for Cloud

Microsoft cloud security benchmark

Compliance Report

8/6/2023 4:55:43 AM UTC

Table of contents

- i. Executive summary
- ii. Microsoft cloud security benchmark sections summary
- iii. Microsoft cloud security benchmark controls status

Executive summary

Introduction

Microsoft Defender for Cloud executes a set of automated assessments on your Cloud environment which can help provide evidence relevant to specific controls in a compliance framework or standard. This report summarizes the current status of those assessments on your environment, as they map to the associated controls. This report does not represent a complete compliance report for the standard, nor does it ensure compliance.

Compliance with Microsoft cloud security benchmark controls

Your environment is compliant with 63 of 63 supported Microsoft cloud security benchmark controls.

Coverage

subscriptions: 1









resources: 110



Subscription Name	Subscription ID
OnEyko	

Microsoft cloud security benchmark sections summary

The following is a summary status for each of the sections of the Microsoft cloud security benchmark. For each section, you will find the overall number of passing and failing controls, based on automated assessments run by Defender for Cloud.

A failing control indicates that at least one Defender for Cloud assessment associated with this control failed. A passing control indicates that all the Defender for Cloud assessments associated with this control passed. Note that status is shown only for supported controls, i.e. controls that have relevant Defender for Cloud assessments associated with them.

Area	Failed controls	Passed controls	
AM. Asset Management	0	5	
BR. Backup and recovery	0	2	
DP. Data Protection	0	8	
DS. DevOps Security	0	2	
ES. Endpoint security	0	3	
IM. Identity Management	0	9	
IR. Incident Response	0	5	
LT. Logging and threat detection	0	6	
NS. Network Security	0	9	

PA. Privileged Access	0	8	
PV. Posture and Vulnerability Management	0	6	






Microsoft cloud security benchmark controls status

The following is a summary status for each supported control of the Microsoft cloud security benchmark. For each control, you will find the overall number of passing, failing and skipped assessment associated with that control.



A failing assessment indicates a Defender for Cloud assessment that failed on at least one resource in your environment. A passing Defender for Cloud assessment indicates an assessment that passed on all resources. A skipped assessment indicates an assessment that was not run, whether because this assessment type is disabled or because there are no relevant resources in your environment.

Note that status is shown only for supported controls, i.e. controls that have relevant Defender for Cloud assessments associated with them.









AM. Asset Management

Control	Failed assessments	Passed assessments	Skipped assessments	
AM.1. Track asset inventory and their risks	0	1	0	
AM.2. Use only approved services	0	3	0	
AM.3. Ensure security of asset lifecycle management	0	5	0	
AM.4. Limit access to asset management	0	4	0	
AM.5. Use only approved applications in virtual machine	0	3	0	


BR. Backup and recovery

Control	Failed assessments	Passed assessments	Skipped assessments	
BR.1. Ensure regular automated backups	0	10	0	
BR.2. Protect backup and recovery data	0	13	0	



DP. Data Protection

Control	Failed assessments	Passed assessments	Skipped assessments	
DP.1. Discover, classify, and label sensitive data	0	1	1	
DP.2. Monitor anomalies and threats targeting sensitive data	0	5	1	
DP.3. Encrypt sensitive data in transit	0	21	0	
DP.4. Enable data at rest encryption by default	0	23	2	
DP.5. Use customer-managed key option in data at rest encryption when required	0	16	0	
DP.6. Use a secure key management process	0	11	0	
DP.7. Use a secure certificate management process	0	5	0	
DP.8. Ensure security of key and certificate repository	0	8	0	



DS. DevOps Security

Control	Failed assessments	Passed assessments	Skipped assessments	
DS.3. Secure DevOps infrastructure	0	2	0	
DS.6. Enforce security of workload throughout DevOps lifecycle	0	6	1	

ES. Endpoint security

Control	Failed assessments	Passed assessments	Skipped assessments	
ES.1. Use Endpoint Detection and Response (EDR)	0	2	0	
ES.2. Use modern anti-malware software	0	4	1	
ES.3. Ensure anti-malware software and signatures are updated	0	1	0	

IM. Identity Management

Control	Failed assessments	Passed assessments	Skipped assessments	
IM.1. Use centralized identity and authentication system	0	10	0	
IM.2. Protect identity and authentication systems	0	6	0	

IM.3. Manage application identities securely and automatically	0	6	0	
IM.4. Authenticate server and services	0	3	0	
IM.5. Use single sign-on (SSO) for application access	0	2	0	
IM.6. Use strong authentication controls	0	23	0	
IM.7. Restrict resource access based on conditions	0	4	0	
IM.8. Restrict the exposure of credential and secrets	0	13	0	
IM.9. Secure user access to existing applications	0	2	0	

IR. Incident Response

Control	Failed assessments	Passed assessments	Skipped assessments	
IR.2. Preparation - setup incident notification	0	3	0	
IR.3. Detection and analysis - create incidents based on high-quality alerts	0	14	1	
IR.4. Detection and analysis - investigate an incident	0	17	0	
IR.5. Detection and analysis - prioritize incidents	0	13	1	








IR.6. Containment, eradication and recovery - automate the incident handling	0	1	0	
--	---	---	---	--

LT. Logging and threat detection





Control	Failed assessments	Passed assessments	Skipped assessments	
LT.1. Enable threat detection capabilities	0	20	2	
LT.2. Enable threat detection for identity and access management	0	22	1	
LT.3. Enable logging for security investigation	0	41	0	
LT.4. Enable network logging for security investigation	0	6	0	
LT.5. Centralize security log management and analysis	0	27	0	
LT.6. Configure log storage retention	0	2	0	





NS. Network Security

Control	Failed assessments	Passed assessments	Skipped assessments	
NS.1. Establish network segmentation boundaries	0	40	3	
NS.2. Secure cloud services with network controls	0	54	6	




NS.3. Deploy firewall at the edge of enterprise network	0	31	1	
NS.5. Deploy DDOS protection	0	1	1	
NS.6. Deploy web application firewall	0	7	0	
NS.7. Simplify network security configuration	0	0	1	
NS.8. Detect and disable insecure services and protocols	0	8	0	
NS.9. Connect on-premises or cloud network privately	0	2	0	
NS.10. Ensure Domain Name System (DNS) security	0	6	0	

PA. Privileged Access

Control	Failed assessments	Passed assessments	Skipped assessments	
PA.1. Separate and limit highly privileged/administrative users	0	12	0	
PA.2. Avoid standing access for user accounts and permissions	0	4	0	
PA.3. Manage lifecycle of identities and entitlements	0	3	0	
PA.4. Review and reconcile user access regularly	0	7	0	

PA.5. Set up emergency access	0	1	0	
PA.6. Use privileged access workstations	0	6	0	
PA.7. Follow just enough administration (least privilege) principle	0	11	0	
PA.8. Determine access process for cloud provider support	0	1	0	

PV. Posture and Vulnerability Management

Control	Failed assessments	Passed assessments	Skipped assessments	
PV.1. Define and establish secure configurations	0	1	0	
PV.2. Audit and enforce secure configurations	0	39	2	
PV.3. Define and establish secure configurations for compute resources	0	2	0	
PV.4. Audit and enforce secure configurations for compute resources	0	24	0	
PV.5. Perform vulnerability assessments	0	2	1	
PV.6. Rapidly and automatically remediate vulnerabilities	0	13	1	