Azure Security Center

Azure Security Benchmark

Compliance Report

5/6/2021 9:44:09 PM UTC

Table of contents

Executive summary

Introduction

Azure Security Center executes a set of automated assessments on your Azure 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 Azure Security Benchmark controls

Your environment is compliant with 39 of 39 supported Azure Security Benchmark controls.

Azure Security Benchmark sections summary

The following is a summary status for each of the sections of the Azure Security Benchmark. For each section, you will find the overall number of passing and failing controls, based on automated assessments run by Security Center.

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

Area	Failed controls	Passed controls	
AM. Asset Management	0	2	
BR. Backup and Recovery	0	3	
DP. Data Protection	0	5	
ES. Endpoint Security	0	3	
IM. Identity Management	0	4	
IR. Incident Response	0	3	
LT. Logging and Threat Detection	0	6	
NS. Network Security	0	5	
PA. Privileged Access	0	4	
PV. Posture and Vulnerability Management	0	4	

Azure Security Benchmark controls status

The following is a summary status for each supported control of the Azure 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 Security Center assessment that failed on at least one resource in your environment. A passing Security Center 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 Security Center assessments associated with them.

AM. Asset Management

Control	Failed assessments	Passed assessments	Skipped assessments	
AM.3. Use only approved Azure services	0	2	0	
AM.6. Use only approved applications in compute resources	0	2	0	

BR. Backup and Recovery

Control	Failed assessments	Passed assessments	Skipped assessments	
BR.1. Ensure regular automated backups	0	4	0	
BR.2. Encrypt backup data	0	4	0	

BR.4. Mitigate risk of lost keys	0	2	0	

DP. Data Protection

Control	Failed assessments	Passed assessments	Skipped assessments	
DP.1. Discovery, classify and label sensitive data	0	1	0	
DP.2. Protect sensitive data	0	8	0	
DP.3. Monitor for unauthorized transfer of sensitive data	0	4	0	
DP.4. Encrypt sensitive information in transit	0	15	0	
DP.5. Encrypt sensitive data at rest	0	14	0	

ES. Endpoint Security

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

IM. Identity Management

Control	Failed assessments	Passed assessments	Skipped assessments	
IM.1. Standardize Azure Active Directory as the central identity and authentication system	0	5	0	
IM.2. Manage application identities securely and automatically	0	4	0	
IM.4. Use strong authentication controls for all Azure Active Directory based access	0	3	0	
IM.7. Eliminate unintended credential exposure	0	3	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	9	0	
IR.5. Detection and analysis - prioritize incidents	0	9	0	

LT. Logging and Threat Detection

Control	Failed assessments	Passed assessments	Skipped assessments	
LT.1. Enable threat detection for Azure resources	0	9	0	
LT.2. Enable threat detection for Azure identity and access management	0	9	0	
LT.3. Enable logging for Azure network activities	0	3	0	
LT.4. Enable logging for Azure resources	0	13	0	
LT.5. Centralize security log management and analysis	0	8	0	
LT.6. Configure log storage retention	0	1	0	

NS. Network Security

Control	Failed assessments	Passed assessments	Skipped assessments	
NS.1. Implement security for internal traffic	0	20	2	
NS.2. Connect private networks together	0	11	4	
NS.3. Establish private network access to Azure services	0	9	4	
NS.4. Protect applications and services from external network attacks	0	13	1	

NS.5. Deploy intrusion detection/intrusion prevention systems (IDS/IPS)	0	1	0	

PA. Privileged Access

Control	Failed assessments	Passed assessments	Skipped assessments	
PA.1. Protect and limit highly privileged users	0	4	0	
PA.3. Review and reconcile user access regularly	0	5	0	
PA.5. Automate entitlement management	0	3	0	
PA.7. Follow just enough administration (least privilege principle)	0	1	0	

PV. Posture and Vulnerability Management

Control	Failed assessments	Passed assessments	Skipped assessments	
PV.2. Sustain secure configurations for Azure services	0	22	2	
PV.4. Sustain secure configurations for compute resources	0	3	0	
PV.6. Perform software vulnerability assessments	0	6	0	

PV.7. Rapidly and automatically remediate software vulnerabilities	0	11	0	