



Autozama

Security Posture Assessment

Comprehensive Security Analysis and
Remediation Roadmap

REPORT DATE

SECURITY SCORE

TOTAL FINDINGS

October 26, 2025

75/100

95

Security Posture Assessment

Client: Autozama

Generated: October 26, 2025 at 3:23 AM

Report Type: Security Assessment

Industry: other



Needs Improvement

Based on 95 findings

IMMEDIATE

33

Within 24 hours



SHORT-TERM

33

Within 1 week



MEDIUM-TERM

56

Within 1 month





Threat Landscape Overview

Security Posture Summary

Azure Advisor has identified **95 security findings** across your Azure environment. **33 critical vulnerabilities** pose significant risk and require immediate remediation within 24 hours to prevent potential security breaches. An additional **33 high-priority issues** should be addressed within one week to maintain a strong security posture.

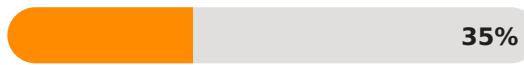
Security Findings by Severity

Risk distribution analysis

Critical (33)



High Priority (33)



Medium Priority (56)



Findings by Resource Type

Most vulnerable components

95



Critical Security Issues - Immediate Action Required

HIGH RISK: These 33 critical security issues pose significant risk to your environment and require immediate remediation to prevent potential security breaches, data loss, or compliance violations. Executive escalation recommended.

#	SECURITY ISSUE	AFFECTED RESOURCE	RISK LEVEL	TIMELINE
1	Guest accounts with owner permissions on Azure resources should be removed	3a658a26-399e-409d-96...	CRITICAL	24 Hours
2	Microsoft Defender for servers should be enabled	3a658a26-399e-409d-96...	CRITICAL	24 Hours
3	Microsoft Defender for Azure SQL Database servers should be enabled	3a658a26-399e-409d-96...	CRITICAL	24 Hours
4	Microsoft Defender for Resource Manager should be enabled	3a658a26-399e-409d-96...	CRITICAL	24 Hours
5	A maximum of 3 owners should be designated for subscriptions	3a658a26-399e-409d-96...	CRITICAL	24 Hours
6	Secure transfer to storage accounts should be enabled	cs23a658a26399ex409dx...	CRITICAL	24 Hours
7	Microsoft Defender for Storage plan should be enabled with Malware Scanning and Sensitive Data Threat Detection	3a658a26-399e-409d-96...	CRITICAL	24 Hours
8	Disabled accounts with read and write permissions on Azure resources should be removed	3a658a26-399e-409d-96...	CRITICAL	24 Hours
9	SQL servers should have vulnerability assessment configured	autzsqlazure	CRITICAL	24 Hours
10	Microsoft Defender CSPM should be enabled	3a658a26-399e-409d-96...	CRITICAL	24 Hours
11	Windows virtual machines should enable Azure Disk Encryption or EncryptionAtHost.	svrsapint	CRITICAL	24 Hours
12	Machines should be configured to periodically check for missing system updates	svrit	CRITICAL	24 Hours
13	Machines should be configured to periodically check for missing system updates	svrteam	CRITICAL	24 Hours

#	SECURITY ISSUE	AFFECTED RESOURCE	RISK LEVEL	TIMELINE
14	Windows virtual machines should enable Azure Disk Encryption or EncryptionAtHost.	svrsapcomp	CRITICAL	24 Hours
15	Machines should be configured to periodically check for missing system updates	svrsaprds	CRITICAL	24 Hours
16	Machines should be configured to periodically check for missing system updates	svrweb	CRITICAL	24 Hours
17	Windows virtual machines should enable Azure Disk Encryption or EncryptionAtHost.	svrsap	CRITICAL	24 Hours
18	Secure transfer to storage accounts should be enabled	autozamahdd	CRITICAL	24 Hours
19	Machines should be configured to periodically check for missing system updates	svrdcazure	CRITICAL	24 Hours
20	Machines should be configured to periodically check for missing system updates	svrsapint	CRITICAL	24 Hours
21	Linux virtual machines should enable Azure Disk Encryption or EncryptionAtHost.	srvconfig	CRITICAL	24 Hours
22	Microsoft Defender for SQL should be enabled for unprotected Azure SQL servers	autzsqlazure	CRITICAL	24 Hours
23	Windows virtual machines should enable Azure Disk Encryption or EncryptionAtHost.	svrit	CRITICAL	24 Hours
24	Secure transfer to storage accounts should be enabled	autozamadiag	CRITICAL	24 Hours
25	Secure transfer to storage accounts should be enabled	autozamassd	CRITICAL	24 Hours

#	SECURITY ISSUE	AFFECTED RESOURCE	RISK LEVEL	TIMELINE
26	Machines should be configured to periodically check for missing system updates	svrsap	CRITICAL	24 Hours
27	Windows virtual machines should enable Azure Disk Encryption or EncryptionAtHost.	svrteam	CRITICAL	24 Hours
28	Machines should be configured to periodically check for missing system updates	srvconfig	CRITICAL	24 Hours
29	Machines should be configured to periodically check for missing system updates	svrsapcomp	CRITICAL	24 Hours
30	Windows virtual machines should enable Azure Disk Encryption or EncryptionAtHost.	svrweb	CRITICAL	24 Hours
31	Windows virtual machines should enable Azure Disk Encryption or EncryptionAtHost.	svrsaprds	CRITICAL	24 Hours
32	Linux virtual machines should enable Azure Disk Encryption or EncryptionAtHost.	srvconfig-2	CRITICAL	24 Hours
33	Windows virtual machines should enable Azure Disk Encryption or EncryptionAtHost.	svrdcazure	CRITICAL	24 Hours



High Priority Security Issues

These 33 security issues should be addressed within one week to maintain a strong security posture and prevent potential exploitation.

SECURITY ISSUE	AFFECTED RESOURCE	RISK LEVEL	TIMELINE
Guest accounts with owner permissions on Azure resources should be removed	3a658a26-399e-409d-96...	HIGH	1 Week
Microsoft Defender for servers should be enabled	3a658a26-399e-409d-96...	HIGH	1 Week
Microsoft Defender for Azure SQL Database servers should be enabled	3a658a26-399e-409d-96...	HIGH	1 Week
Microsoft Defender for Resource Manager should be enabled	3a658a26-399e-409d-96...	HIGH	1 Week
A maximum of 3 owners should be designated for subscriptions	3a658a26-399e-409d-96...	HIGH	1 Week
Secure transfer to storage accounts should be enabled	cs23a658a26399ex409dx...	HIGH	1 Week
Microsoft Defender for Storage plan should be enabled with Malware Scanning and Sensitive Data Threat Detection	3a658a26-399e-409d-96...	HIGH	1 Week
Disabled accounts with read and write permissions on Azure resources should be removed	3a658a26-399e-409d-96...	HIGH	1 Week
SQL servers should have vulnerability assessment configured	autzsqlazure	HIGH	1 Week
Microsoft Defender CSPM should be enabled	3a658a26-399e-409d-96...	HIGH	1 Week
Windows virtual machines should enable Azure Disk Encryption or EncryptionAtHost.	svrsapint	HIGH	1 Week
Machines should be configured to periodically check for missing system updates	svrit	HIGH	1 Week
Machines should be configured to periodically check for missing system updates	svrteam	HIGH	1 Week
Windows virtual machines should enable Azure Disk Encryption or EncryptionAtHost.	svrsapcomp	HIGH	1 Week
Machines should be configured to periodically check for missing system updates	svrsaprds	HIGH	1 Week

SECURITY ISSUE	AFFECTED RESOURCE	RISK LEVEL	TIMELINE
Machines should be configured to periodically check for missing system updates	svrweb	HIGH	1 Week
Windows virtual machines should enable Azure Disk Encryption or EncryptionAtHost.	svrsap	HIGH	1 Week
Secure transfer to storage accounts should be enabled	autozamahdd	HIGH	1 Week
Machines should be configured to periodically check for missing system updates	svrdcazure	HIGH	1 Week
Machines should be configured to periodically check for missing system updates	svrsapint	HIGH	1 Week
Linux virtual machines should enable Azure Disk Encryption or EncryptionAtHost.	srvconfig	HIGH	1 Week
Microsoft Defender for SQL should be enabled for unprotected Azure SQL servers	autzsqlazure	HIGH	1 Week
Windows virtual machines should enable Azure Disk Encryption or EncryptionAtHost.	svrit	HIGH	1 Week
Secure transfer to storage accounts should be enabled	autozamadiag	HIGH	1 Week
Secure transfer to storage accounts should be enabled	autozamassd	HIGH	1 Week
Machines should be configured to periodically check for missing system updates	svrsap	HIGH	1 Week
Windows virtual machines should enable Azure Disk Encryption or EncryptionAtHost.	svrteam	HIGH	1 Week
Machines should be configured to periodically check for missing system updates	srvconfig	HIGH	1 Week
Machines should be configured to periodically check for missing system updates	svrsapcomp	HIGH	1 Week
Windows virtual machines should enable Azure Disk Encryption or EncryptionAtHost.	svrweb	HIGH	1 Week

SECURITY ISSUE	AFFECTED RESOURCE	RISK LEVEL	TIMELINE
Windows virtual machines should enable Azure Disk Encryption or EncryptionAtHost.	svrsaprds	HIGH	1 Week
Linux virtual machines should enable Azure Disk Encryption or EncryptionAtHost.	srvconfig-2	HIGH	1 Week
Windows virtual machines should enable Azure Disk Encryption or EncryptionAtHost.	svrdcazure	HIGH	1 Week

Security Findings by Azure Subscription

SUBSCRIPTION	CRITICAL	HIGH	MEDIUM	TOTAL	RISK DISTRIBUTION
AUTOZAMA SAS (3a658a26-399e-409d-9...	33	—	56	95	<div style="width: 35%; background-color: #c0392b;"></div>



Compliance & Regulatory Framework Alignment

Regulatory Framework Impact

Addressing these security recommendations helps maintain compliance with common security frameworks and regulatory requirements. These findings may impact your organization's ability to meet compliance obligations.

ISO 27001

Information Security Management

NIST CSF

Cybersecurity Framework

CIS Controls

Critical Security Controls

SOC 2 Type II

Trust Service Principles

HIPAA

Healthcare Data Protection

PCI DSS

Payment Card Standards

Security Remediation Roadmap

Phase 1: Critical Response (24 Hours)

1. **Emergency Triage:** Convene security team to review all 33 critical findings within 2 hours
2. **Immediate Mitigations:** Implement temporary security controls and workarounds
3. **Incident Response:** Activate procedures if any active exploitation detected
4. **Executive Notification:** Brief leadership on critical security posture
5. **Vendor Escalation:** Engage Microsoft support for critical Azure issues

Phase 2: Short-term Hardening (Week 1)

1. **High Priority Remediation:** Address all 33 high-priority findings
2. **Security Policy Updates:** Review and update policies, firewall rules, access controls
3. **MFA Enforcement:** Ensure multi-factor authentication for all privileged accounts
4. **Security Awareness:** Conduct targeted training for teams
5. **Enhanced Monitoring:** Implement additional security monitoring and alerting

Phase 3: Continuous Improvement (Month 1 & Ongoing)

1. **Complete Remediation:** Address all 56 medium-priority findings
2. **Security Automation:** Implement Azure Policy and automated guardrails
3. **Regular Assessments:** Establish weekly Azure Advisor security reviews
4. **Penetration Testing:** Conduct third-party security assessment
5. **Security Metrics:** Create executive dashboard tracking security KPIs
6. **Zero Trust Implementation:** Begin journey toward Zero Trust architecture

Immediate Action Items

Security Leadership Actions

1. **Emergency Review:** CISO/Security team review within 2 hours for critical findings
2. **Assign Ownership:** Designate security incident response team
3. **Stakeholder Communication:** Brief executive team and board on security posture
4. **Budget Allocation:** Secure emergency budget for critical improvements
5. **Third-party Assessment:** Consider engaging external security consultants
6. **Compliance Review:** Engage legal/compliance teams for regulatory implications
7. **Track Progress:** Implement daily stand-ups until critical issues resolved
8. **Post-mortem:** Conduct lessons learned and update security procedures

Security Disclaimer: This report was automatically generated from Azure Advisor recommendations. All data is sourced from Microsoft Azure Advisor as of October 26, 2025. Security findings should be evaluated by qualified security personnel before implementation. The security score is calculated based on Azure Advisor metrics and may not represent a comprehensive security assessment. We recommend conducting regular third-party security audits and penetration testing.

Azure Advisor Reports Platform

© 2025 | Powered by Microsoft Azure Advisor