Midpilot: security audit report

Created on 26 March 2026 @ 10:49

Midpilot wants to build trust by giving you insight in how it builds software in a secure manner. The report details how software development at Midpilot is being monitored and safeguarded from the developer's computer all the way to the infrastructure used for delivery.

This security report has been generated by Aikido Security based on real-time monitoring of Midpilot code and infrastructure.

ISO 27001:2022 compliance

A brief overview of the ISO 27001 requirements and any measures taken for these.

Title	Taken measures
A.8.2 - Privileged access rights	✓ Has checks in place for enforcing permissions
A.8.3 - Information access restriction	✓ Prevents public access to cloud resources ✓ Has proper access controls for cloud resources
A.8.5 - Secure authentication	✓ Requires MFA for cloud users ✓ Enforces encryption of data in transit
A.8.6 - Capacity management	✓ Uses load balancers correctly
A.8.7 - Protection against malware	✓ Prevents unwanted write operations to filesystems ✓ Uses Lockfiles to pin code dependencies
A.8.8 - Management of technical vulnerabilities	✓ Does not have any issues outside of their SLA
A.8.12 - Data leakage prevention	✓ Securely stores files ✓ Enforces encryption of data in transit ✓ Encrypts data at rest ✓ Prevents remote code execution ✓ Is protected against SSRF attacks ✓ Has measures against SQL injection attacks ✓ Prevents XSS attacks
A.8.13 - Backups	✓ Has backups for stateful cloud resources
A.8.15 - Logging	✓ Enabled security logging for cloud instances

A.8.18 - Use of privileged utility programs	✓ Enforces secure access for cloud users ✓ Prevents the exposure of sensitive data ✓ Has proper access controls for cloud resources ✓ Requires MFA for cloud users
A.8.20 - Network security	✓ Prevents ssh access to cloud resources from anywhere ✓ Prevents unauthorized network access
A.8.31 - Separation of development, test and production environments	✓ Has separate production and test environments
A.8.24 - Use of cryptography	✓ Enforces safe SSL protocol usage ✓ Uses secure cookies ✓ Uses up-to-date cryptographic libraries
A.8.9 - Configuration management	✓ Uses Lockfiles to pin code dependencies
A.8.16 - Monitoring activities	✓ Has connected a cloud environment ✓ Receives security alerts in real time
A.8.25 - Secure development lifecycle	✓ Uses a CI integration ✓ Has connected a code repository ✓ Has connected a cloud environment
A.8.28 - Secure coding	✓ Does not have any issues outside of their SLA
A.8.32 - Change management	✓ Tracks progress via an issue tracker
A.5.15 - Access control	✓ Applies the least privilege principle for cloud users ✓ Applies the least privilege principle for cloud resource ✓ Applies the least privilege principle to cloud resources ✓ Prevents the exposure of sensitive data
A.5.16 - Identity management	✓ Properly manages the identity of cloud users
A.5.28 - Collection of evidence	✓ Enabled security logging for cloud instances

A.5.33 - Protection of records	Prevents public access to cloud resources

SOC2 compliance

A brief overview of the SOC2 requirements and any measures taken for these.

Title	Taken measures
CC3.3: Consider the potential for fraud	✓ Applies the least privilege principle for cloud resource ✓ Applies the least privilege principle to cloud resources ✓ Enabled security logging for cloud instances ✓ Requires MFA for cloud users
CC3.2: Estimate Significance of Risks Identified	✓ Properly manages the identity of cloud users ✓ Does not have any severe surface monitoring issues ✓ Does not have any severe open source dependency issues ✓ Configured monitoring for code repositories ✓ Configured monitoring for domains
CC5.2: The entity selects and develops general control activities over technology to support the achievement of objectives	✓ Applies the least privilege principle for cloud resource ✓ Has deletion protection for cloud resources ✓ Properly manages the identity of cloud users ✓ Does not have any severe infrastructure as code issues
CC6.1: Restricts logical access	✓ Requires MFA for cloud users ✓ Applies the least privilege principle to cloud resources ✓ Enforces encryption of data in transit ✓ Encrypts data at rest ✓ Prevents the exposure of sensitive data ✓ Has measures against SQL injection attacks ✓ Is protected against SSRF attacks ✓ Is protected against command injections attacks ✓ Prevents XSS attacks
CC6.1: Consider network segmentation	✓ Prevents unauthorized public access to file storage ✓ Prevents unauthorized public access to database ✓ Prevents unauthorized access via ssh ✓ Has separate production and test environments
CC6.1: Restrict access to information assets	✓ Has secured load balancer access points

CC6.1: Manages credentials for infrastructure and software	✓ Has secured load balancer access points
CC6.1: Use encryption to protect data	✓ Encrypts data at rest ✓ Enforces encryption of data in transit ✓ Uses up to date cryptography libraries
CC6.6: Restrict Access	✓ Prevents public access to cloud resources
CC6.6: Require additional authentication or credentials	✓ MFA is enforced for cloud users
CC6.6: Implement boundary protection system	✓ Applies the least privilege principle for cloud resource
CC6.7: Use encryption technologies or secure communication channels to protect data	✓ Enforces latest TLS version ✓ Uses up to date cryptography libraries
CC6.8: Restrict application and software installation	✓ Protects unauthorized runtime access ✓ Prevents container orchestration takeover
CC6.8: Detect unauthorized changes to software and configuration parameters	✓ Enabled security logging for cloud instances
CC6.8 Use anti-virus and anti-malware software	✓ Aikido Malware Scanner is enabled
CC7.1: Monitor infrastructure and software	✓ Enabled security logging for cloud instances ✓ Configured SLAs to resolve issues ✓ Connected code repositories ✓ Connected cloud environment ✓ Connected public facing domain
CC7.1: Implement change detection mechanism	Monitoring, not fully compliant
CC7.1: Detect unknown or unauthorized components	✓ Does not have risky licenses

CC7.1: Conduct vulnerability scans	✓ Uses Lockfiles to pin code dependencies ✓ Does not have any issues outside of their SLA ✓ Connected code repositories ✓ Connected public facing domain
CC7.1: Implement filters to analyze anomalies	✓ Connected code repositories
CC7.1: Restores the affected environments	✓ Has no critical open source dependency issues
CC8.1: Protect confidential information	✓ Prevents the exposure of sensitive data
CC8.1: Track system changes	✓ Tracks progress via an issue tracker
CC10.3: Tests integrity and completeness of backup data	✓ Has backups for stateful cloud resources

GDPR compliance

A brief overview of GDPR rules and any measures taken for these.

Title	Taken measures
2.1 Principles Relating to Processing of Personal Data	✓ Encryption at Rest Enabled ✓ Use of Cryptography: Enforces SSL ✓ Enforces HTTPS traffic to cloud instances ✓ Use of Cryptography: Enforces TLS ✓ Use of Cryptography: Secure Cookies ✓ Use of Cryptography Libraries ✓ Runtimes are up to date
4.2 Data Protection by Design	✓ Enforces Multi-Factor Authentication (MFA) ✓ Proper Access Management for Users ✓ Proper Access Management for Resources ✓ Proper Access Management to Resources
4.5 Processor	✓ Encryption at Rest Enabled ✓ Use of Cryptography: Enforces SSL ✓ Enforces HTTPS traffic to cloud instances ✓ Use of Cryptography: Enforces TLS ✓ Use of Cryptography: Secure Cookies ✓ Use of Cryptography Libraries ✓ Runtimes are up to date
4.7 Records of Processing Activities	✓ Logging Enabled ✓ Backups Enabled
4.9 Security of Processing	✓ Encryption at Rest Enabled ✓ Use of Cryptography: Enforces SSL ✓ Enforces HTTPS traffic to cloud instances ✓ Use of Cryptography: Enforces TLS ✓ Use of Cryptography: Secure Cookies ✓ Use of Cryptography Libraries