Waypoint Platform Group: security audit report

Created on 13 August 2026 @ 22:33

Waypoint Platform Group wants to build trust by giving you insight in how it builds software in a secure manner. The report details how software development at Waypoint Platform Group 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 Waypoint Platform Group code and infrastructure.

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 ✓ Requires MFA for cloud users ✓ Applies the least privilege principle to cloud resources ✓ Enabled security logging for cloud instances ✓ Threat detection is enabled
CC3.2: Estimate Significance of Risks Identified	✓ Properly manages the identity of cloud users ✓ Threat detection is enabled ✓ 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 ✓ Threat detection is enabled ✓ Enforces encryption of data in transit ✓ 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
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	✓ DNS Domain transfer is locked ✓ 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	✓ Threat detection is enabled ✓ 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	✓ Alerting is enabled

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 ✓ Threat detection is enabled
CC7.1: Restores the affected environments	✓ Runtimes are up to date ✓ 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