Strategy Security Assurance Program

Certifications

- ISO 2700:2022 Certified for Strategy Managed Cloud Enterprise
- SOC1 Type II Assessment for Strategy Managed Cloud Enterprise
- SOC2 Type II Assessment for Strategy Managed Cloud Enterprise
- General Data Protection Regulation Compliant
- Data Privacy Framework Program Compliant
- PCI DSS Compliant Cloud Platform
- Strategy fully-managed HIPAA Compliant Cloud solution
- FedRAMP Moderate Authority to Operate
- GovRAMP Moderate Authorization
- ENS (Spain) High Certification
- BSI C5 (Germany) Assessment
- Corporate Financial System SOX Compliant
- Product Country of Origin: United States

Personnel Security

- Background checks performed on all employees
- Educational credentials validated
- Financial/credit history checked
- Criminal background checked

Security Training and Certifications for Employees

- Security principles
- Threat modeling
- Web, mobile and AI security
- Penetration testing

Secure Development

- Secure Coding Standards for all languages used
- Multiple-level code review
- SCA, SAST, DAST scanning across the SDLC

Strategy has a comprehensive security program focused on protecting your data. From engineering through vulnerability remediation, we are committed to ensuring that our products continually meet your business and security needs.

Strategy

Security Design Process

- Threat Modeling based on STRIDE and other internally developed models
- Application of security principles (e.g., “Defense in Depth”)
- Consideration of OWASP 10 vulnerabilities

Embedded Security Features

- User Authentication
- OIDC
- SAML
- SSO
- HTTPS/TLS protection for data in transit
- AES 256-bit encryption for data at rest
- Role based access control
- Row-level security
- CSRF, clickjacking, and HTML Output Encoding (for XSS prevention)

Third-Party Component Control

The use of third-party components is closely controlled. A formal process is enforced for the introduction of new components into the products. Independent confirmation of third-party components incorporated into the products is conducted via SCA tools. Components possessing security vulnerabilities are aggressively scheduled for upgrade or replacement.

Security Patches and Upgrades

Security is of the utmost importance at Strategy.

Vulnerabilities are treated as top priority issues and fixed in the next release. Therefore, keeping your software up to date is one of the simplest, but most important security precautions you can take to maintain your Strategy product’s security. In the event of a critical security issue outside of the regular update cycle, Strategy may issue an interim patch or workaround, but upgrading will still be required to keep your deployments as secure as possible.

Strategy₿

Internal Security Testing

Throughout the development cycle, Strategy conducts internal penetration tests to validate the security of new or modified features and to re-validate the security of the existing product suite to new threats. Such testing includes the risks identified in the OWASP-10 and other known weaknesses. Threat models developed during the product design provide additional guidance for this testing.

Independent Penetration Testing

We engage independent security firms to conduct annual penetration tests. Tests are comprehensive in scope and utilize black-box testing techniques as well as white-box testing which includes full access to the product source code. Issues identified during this testing are immediately scheduled for resolution in the product on a risk-prioritized basis. Subsequent re-testing is then conducted by the security firm(s) to verify that the issues have been successfully resolved.

Secure Release

A centralized code repository (GitHub Enterprise) is maintained for development. Repository check-ins undergo area-specific code review procedures. The building process is controlled by the DevOps team. All machines developing the product employ an enterprise-grade virus scanner updated with the latest signatures.

Reporting a Security Issue

Current Strategy customers may report potential security issues and queries via Strategy Technical Support.

Researchers may submit issues via our reporting page at https://www.strategy.com/software/go/report-a-strategy-product-vulnerability

Strategy Inc
1850 Towers Crescent Plaza,
Tysons, VA 22182

Strategysoftware.com

Strategy