› White Paper

SAS® Software Security Framework: Engineering Secure Products

sas
THE POWER TO KNOW®

Contents

Across an increasingly interconnected marketplace, the impact of software security breaches on organizations and consumers is driving more investment in security. Technology analysts report software security as a top initiative that will get increasing attention and investment.

At SAS, ensuring the quality and security of our products is more than a goal. It's a requirement that drives the way that we develop and test technology. To create the most stable and secure products possible, we develop, test and deliver technology using proven methodologies for secure software development. We know that keeping data and software secure is a fundamental expectation for our customers.

Organizations are establishing dialogues and building partnerships with their vendors to focus on security requirements. They want to know how the software they purchase can meet those demands. SAS welcomes that partnership with its customers, especially since feedback from the field is critical to delivering high-quality and secure software that exceeds customer expectations and industry requirements.

This document provides an overview of the SAS Software Security Framework. It explains the structures, processes and procedures that SAS has in place to deliver secure software for our global customer base.

The SAS® Software Security Framework

The SAS Software Security Framework defines the SAS software development process and provides principles for the development, delivery and support processes used to build and support SAS software. The framework includes a process for continuous learning and awareness of global security activities and standards – and incorporating them into SAS development practices.

The components of the framework include:

- **Education** – At its core, the SAS Software Security Framework is based on building a team trained to meet today's security challenges. SAS software engineers receive education on current and emerging industry security threats, and they leverage that information to design, develop and support products that are built with security requirements in mind.
- **Secure architecture and design** – SAS implements a security architecture that provides strong authentication, authorization, availability, data integrity and confidentiality.
- **Secure development standards** – SAS developers work with standards and guidelines that provide the foundation for building secure software. These coding guidelines and examples help SAS developers and the services staff create and implement secure software.
- **Security testing and validation** – The SAS Software Security Framework includes testing and validation processes that provide checks for security throughout the development process. SAS runs industry-standard security scanning software during the development cycle. These scans are designed to detect security vulnerabilities, and SAS follows up to evaluate and address identified issues before completing product development.
- **Product security response and remediation** – SAS recognizes that some security issues or questions occur after products are released. The SAS Software Security Framework includes a method to provide clear updates about these issues. After identifying a vulnerability, SAS will deliver workarounds and fixes as appropriate – and announce those fixes publicly through the appropriate customer communications channels.

Figure 1: The SAS Software Security Framework uses broad-based education to train the development staff on security issues – and how to apply best practices throughout the SAS software development life cycle.

Education

Education is the foundation for our efforts to identify and resolve security issues. The SAS Software Security Framework helps everyone responsible for creating, testing and implementing SAS technology to share knowledge of the scope and importance of security topics. The education element of the framework takes a number of forms, including:

- Development, test and support organizations receive training classes, refresher training, and peer mentoring for security topics.
- SAS security teams provide guidelines and coding examples associated with development standards.
- SAS internal IT teams collaborate with SAS development to provide insight into the security challenges faced by IT, and to guide choices based on proven practices and internal consistency.
- SAS development and test engineers strive to implement and validate a consistent set of protections and features across SAS products. The education program allows these teams to recognize and avoid potential vulnerabilities during the software development life cycle. Additionally, the technical support staff receives training on how to identify and handle security issues after software release so that issues are resolved quickly and communicated to customers.

Secure Architecture and Design

Delivering secure software begins with a product design based on standards and processes. SAS developers work with the architecture team to conduct design reviews. Checkpoints throughout the development process help SAS engineers prioritize secure design concepts in product development tasks.

Overseeing the architecture and design efforts is an internal, specialized security architecture team that consults with developers during design and development phases. This design phase provides a framework for planning new features that are built on strong security architecture options. The architectural design guides developers to maintain security for processes like authentication, authorization, availability, integrity and confidentiality. Security features implemented by many SAS products may include role-based access control, single sign-on integration, audit logging, and encryption of data in transit and at rest.

Secure Development Standards

The SAS Technology Office monitors current and evolving security trends and standards as input to the SAS Software Security Framework. From this, the team creates specific coding guidelines and best practice examples to guide SAS software development.

SAS development standards employ industry standards. The standards used by SAS development include the Open Web Application Security Project (OWASP) list of the top 10 critical web security flaws and the CWE/SANS Top 25. These lists provide awareness of common security vulnerabilities in software as well as the methods to avoid them during development and testing.

At SAS, security extends beyond the code being developed. SAS developers work in a secure environment. In addition to infrastructure security maintained by the SAS IT organization, SAS source code is accessible only to those who have a legitimate need for access. Once access is granted, password policies are strictly enforced. For more information about campus and code security, see the Quality Imperative, which provides a guide to SAS' commitment to product quality and customer satisfaction.

Security Testing and Validation

SAS performs a variety of security tests, including authentication testing, authorization (access) testing and web application vulnerability testing. SAS performs vulnerability testing before delivering feature releases and maintenance releases. This testing reinforces development standards to support secure software throughout the process.

In addition to scanning web applications and the web application server environment (using guidance from leading security organizations), SAS employs a suite of tests specific to SAS technology. Depending on the type of software being tested, the tests can include:

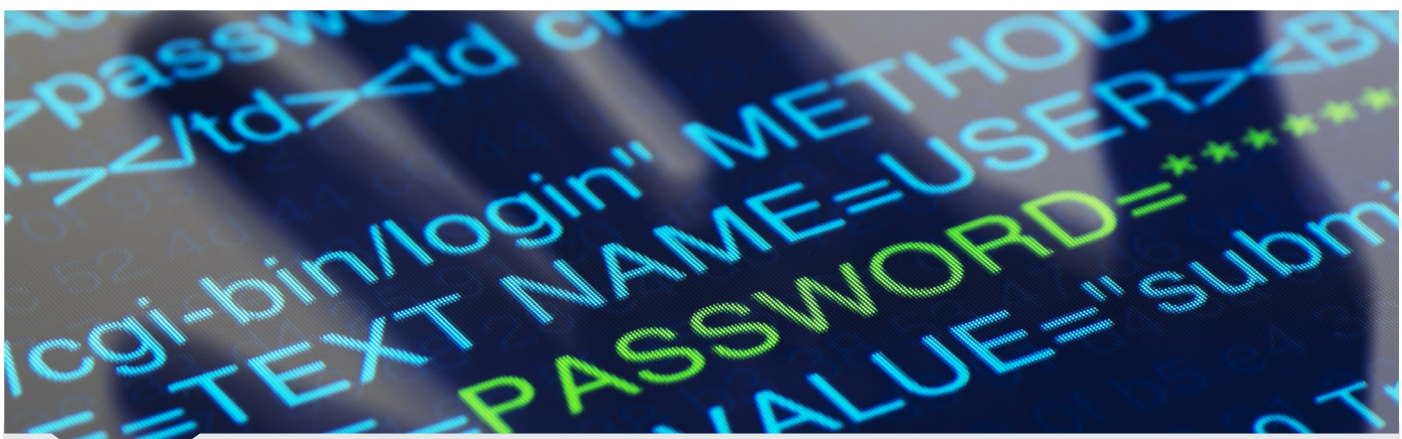
- Testing with users who have different security levels to make sure that each has the appropriate access levels.
- Confirming data access permissions, based on row-level permissions, to confirm that data authorization is applied appropriately for each user.
- Validating password and encryption security for SAS and for SAS Scalable Performance Data Server data sets.
- Testing SAS/ACCESS® engines for connectivity security (such as user ID and password) during connection testing.
- Testing appropriate user authorization and error handling.
- Testing web applications via static-source scanning and external security assessments, along with assessments using guidance from OWASP and SANS Institute.

Test teams use third-party dynamic vulnerability scanning tools to focus on classes of vulnerabilities that have been the root cause of known security issues in web-based software. These tools and test cases help developers focus on eliminating security vulnerabilities such as the OWASP Top 10 and the CWE/SANS Top 25. Issues found during a scan are entered into a defect tracking system and evaluated for appropriate response and remediation.

As part of the SAS Software Security Framework, our testing processes, strategies and tools are kept up to date with current security requirements. The testing and validation process for SAS products combines both internally-developed and third-party scanning and vulnerability tools. In addition, SAS continually expands the test suites for our software.

SAS recognizes that organizations use a variety of testing tools to scan for vulnerabilities. When customer-driven assessments raise potential security issues, customers should contact SAS Technical Support for response and feedback.

Results of vulnerability tests and scans conducted by SAS are company confidential. By policy, SAS does not share the tests or the individual results. The SAS security bulletins page provides updates about security issues, and security fixes for released products are highlighted through the standard technical support process for hot fixes. Customers can sign up for the support newsletter to receive regular updates about hot fixes and other important news from SAS. Visit the technical support hot fixes site for more information.



SAS performs a variety of security tests, including authentication testing, authorization (access) testing and web application vulnerability testing.

SAS Product Security Response and Remediation

SAS recognizes that some security issues emerge after products are released. As a result, the SAS Software Security Framework includes processes to assess vulnerabilities and provide clear and timely updates about their status. Customers with questions about security, including potential security vulnerabilities, should use the SAS Technical Support process to start a dialogue and get more information.

Once a security question surfaces, a multidivisional team helps respond to questions and assess potential vulnerabilities. Like most technology vendors, SAS has a Product Security Incident Response Team (PSIRT) process that investigates security vulnerability incidents and mobilizes resources to address identified incidents. Incidents are prioritized based on the potential severity of the vulnerability. SAS leverages the Common Vulnerability Scoring System (CVSS) during the vulnerability assessment.

After the initial investigation, SAS provides updates to our customers through SAS Technical Support. Depending on the severity of the security situation, SAS may communicate responses via one or more channels, such as software release notes, bulletins, support forum updates or direct customer outreach emails. Some resolutions may require configuration changes or deployment of software fixes. Ultimately, the resolution of a reported incident may require customers to upgrade to a more current version of SAS software.

Throughout the assessment and remediation processes for reported vulnerabilities, SAS is committed to clear and consistent communication with affected customers. The SAS Technical Support team provides one-on-one support around the world, including support for security incidents. In addition, SAS publishes updates and summaries of known problems on the SAS security bulletins page.

The SAS® Commitment to Security

Maintaining software security requires diligence and commitment. The SAS Software Security Framework applies industry-standard best practices for secure development life cycles to all organizations that perform SAS product engineering and maintenance processes. This helps SAS deliver and maintain products designed to meet the business needs and security requirements of our customers.

To contact your local SAS office, please visit: sas.com/offices

107607_S134871.0315