WHITE PAPER

SAS® Software Security Framework: Engineering Secure Products

THE POWER TO KNOW®

Contents

SAS builds quality software that is secure and privacy-preserving. Our products are built to be resistant to misuse and known cybersecurity threats. SAS guides its architects and developers based on our software security framework (see Figure 1). At the highest level of the framework, we have defined a software security policy structure that supports product security governance. This model applies to each phase of a product's software development life cycle (SDLC).

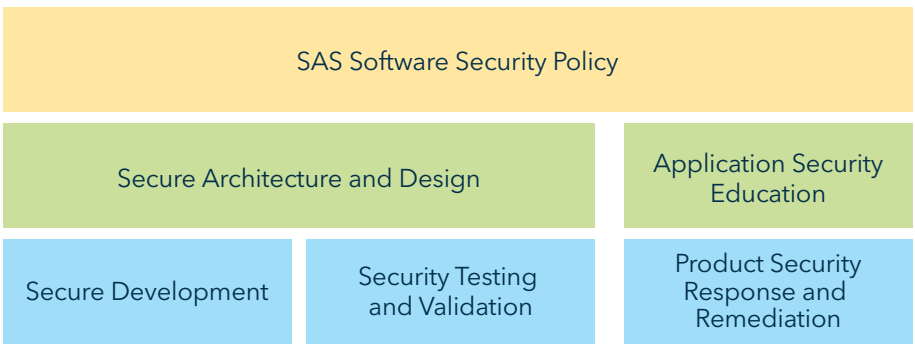

Figure 1: The SAS Software Security Framework.

SAS® Software Security Policy

Secure software development is governed by the product security office of the SAS research and development (R&D) division. Its mandate is to develop application security policies, secure architecture design patterns and ensure software code meets a standard of excellence.

In developing SAS policy (see Figure 2), we take into consideration industry best practices and standards that are developed by the US National Institute of Standards and Technology (NIST), the International Standards Organization and the Open Web Application Security Project (OWASP). The structure of our policy reflects the technical requirements of these organizations with the intent of informing our software engineers of product security requirements, which ultimately empowers our customers in their own compliance journey.

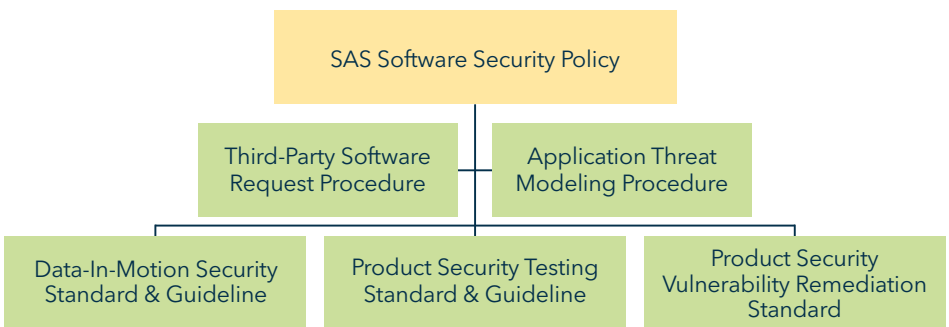

Figure 2: Structure of the SAS Software Security Policy.

Compliance with our software security policy standards and procedures is required by all R&D product teams. Additional guidelines provide detail and controls that can be implemented as required. Our policy includes:

- Ensuring that all open source code is reviewed for licensing and known security vulnerabilities (using software composition analysis tools) prior to integration with SAS product code.
- Reviewing new SAS products and features for theoretical attack surfaces using advanced application threat modeling techniques.
- Ensuring that SAS product teams conduct static and dynamic application security testing.
- Tracking and remediating product security vulnerabilities that are reported by customers.

Typical application security controls that are required by our policy include allowable encryption algorithm and cipher suite specification, authentication and authorization mechanisms, audit controls, error handling and session management. SAS provides engineering teams with detailed guidelines for secure coding and testing to ensure compliance with the SAS Software Security Policy.

Secure Architecture and Design

The SAS Platform uses a security architecture that provides strong authentication, authorization, confidentiality, availability and data integrity. We achieve a secure and reliable architecture through a secure-by-design philosophy.

Using advanced techniques such as application threat modeling, our engineers review solution architectures and software code to quickly identify and resolve potential security defects. We have integrated our threat modeling practice into the design phase of the SDLC and empower engineers with the tools and processes they need to evaluate new features for possible defects.

Threat modeling also enables SAS software testers with a priori knowledge of possible attack vectors and challenges them to test and validate any design assumption prior to implementation. SAS relies upon industry standard application security risk taxonomies (e.g., CWE, CAWE and CAPEC) to conduct product security evaluations. Our goal with threat modeling is to identify the software defects that the application code scanners cannot in order to secure the design at run-time.

Lastly, we complement our secure-by-design philosophy with an engineering product-level security review process to assure that each product has supporting internal documentation (i.e., objective evidence) on how it passed each of the requirements contained in our software security policy.

Application Security Education

SAS provides its employees with access to application security training resources that can be customized into a learning plan according to their role or their need to complete a specific security standard-related task. Security training is delivered through a central corporate learning management system (LMS) that empowers employees to be agile, lifelong learners. The SAS LMS connects individuals and teams with the knowledge resources that they need to solve application security problems. We also encourage team collaboration to create a shared understanding of the scope and impact of detected security weaknesses.

Our LMS provides a variety of delivery modes that includes self-paced e-learning, instructor-led workshops and labs, and a complete virtual learning environment with access to SAS software. Software developers also have access to advanced application security coaching modules within their development environments to help detect and resolve common weaknesses and exposures in real time as they are writing code.

Secure Development

SAS engineers design and build software according to industry best practices for secure coding and open protocol standards for secure authentication and network communication. At each phase of the secure SDLC, we ensure that engineers prioritize the development and testing of functional and non-functional security requirements. We build and test our products against accepted industry guidance:

- OWASP Top Ten Project
- SEI CERT Secure Coding Standards
- Common Weakness Enumeration (CWE)
- Internet Engineering Task Force Standards
- OWASP Software Assurance Maturity Model
- Common Architectural Weakness Enumeration (CAWE)
- Common Attack Pattern Enumeration and Classification (CAPEC)

SAS engineers work in trusted and secure development and build environments, which are centrally monitored and maintained by our global IT service delivery and support division. All development build systems and release pipelines are secure and only accessible to those who have legitimate and authorized need for access. For more details on our build process, please refer to the SAS Quality Imperative white paper.

Customers need to be cognizant of their security risk tolerance and often that means understanding how SAS products are built to support different levels of security. SAS products are designed to be highly configurable and adaptable to customer requirements and environments. One example is the use of encryption capabilities and the ability to select cipher suites that are compliant with NIST Federal Information Processing Standards.

Security Testing and Validation

Continuous security testing is an integral part of the SAS Software Security Framework. SAS employs a customized suite of security tests that are specific to the range of available SAS technologies. Depending on the type of product, the security tests can include exploitation of OWASP Top Ten weaknesses, CWEs, CVEs, encryption mechanisms, error handling, input handling and application programming interface security. SAS makes extensive use of commercial and open source tools for:

- Software composition analysis (SCA).
- Static application security testing (SAST).
- Dynamic application security testing (DAST).

We have automated the process of monitoring the quality of our code as it moves from development to build to release environments to ensure that it is following our software security policy before and after release. Each type of code scan (i.e., SCA, SAST and DAST) is performed by trained engineers to identify, confirm and remediate software weaknesses as they are found at different phases of the SDLC.

SAS also engages third parties to perform independent testing on our software products to determine its resiliency to attack and misuse. Specially constructed virtual environments are used to simulate customer deployments in the cloud and on-site. If weaknesses are identified in product or architecture deployments, then they are entered into a defect tracking system and worked to resolution. Importantly, SAS considers all product security testing tools, methods, models and results to be company confidential, and therefore details cannot be disclosed.

It is not uncommon for SAS to respond to our customers' security and internal audit teams to verify the results of their own security testing. SAS technical support (sas.com/support) works with organizations to understand the significance and impact to environments that any findings pertain to. We are committed to ensuring the successful and secure deployment of SAS products.

Product Security Response and Remediation

SAS is a proud member of the Forum of Incident Response and Security Teams (FIRST). We are committed to responsible reporting of security incidents and managing vulnerabilities identified in our software and integrated third-party components.

The SAS product security incident response team (PSIRT) is responsible for working with SAS technical support, customers and industry partners to create an informed understanding of the applicability, severity and impact that a security finding may have and then driving its remediation to closure.

Customers who have a valid SAS support contract should report suspected security issues by opening a track with SAS technical support. Security researchers or others who do not have a support contract can contact the SAS PSIRT directly by sending email to psirt@sas.com. Information about security vulnerabilities should be encrypted by using our PGP public key.

The SAS PSIRT process includes a structured approach to program management and vulnerability scoring as it applies to both investigating vulnerabilities and driving them to remediation according to the requirements of the SAS Software Security Policy. Often the scope of vulnerabilities can be cross-divisional and the PSIRT acts as the designated responder for SAS product security incidents.

SAS provides the following public communication channels to disseminate security-related announcements:

- SAS Security Bulletins.
- Downloads and Hot Fixes.
- SAS Notes With Security Vulnerabilities.
- Communities: SAS Hot Fix Announcements.

The security bulletins page provides official SAS statements and advisories on the applicability of major CVE announcements and our recommended resolution. SAS Notes provide in-depth analysis of vulnerabilities and a cross-reference to SAS product release fixes which are communicated through SAS user communities.

By following the SAS Hot Fix Announcements, customers can receive real-time notifications of software upgrades, fixes and, when applicable, recommended configuration changes. The security bulletins page also includes special topics such as Java support.

You Can Count on SAS

Our solutions and their deployments are complex and highly adaptable to the security configuration requirements of our customers. We have integrated industry best practices for software vulnerability detection throughout each phase of our secure SDLC. We also employ advanced threat modeling techniques during design and operations phases to continuously analyze and improve the resiliency of our software against today's emerging cybersecurity threats. SAS is committed to delivering and maintaining secure analytics solutions.

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