Veritas Application Security Assurance Program (ASAP)

The Veritas Application Security Assurance Program (ASAP) is based on Microsoft's Secure Development Lifecycle for Agile Developers. Over time, Veritas has evolved the Microsoft method to address real-world challenges and requirements of U.S. Presidential Executive Order 14028. When the order was announced in May 2021, Veritas verified that we already followed the majority of the Secure Software Development Framework (SSDF) as outlined in NIST SP 800-218.

The Veritas Product Security Group (PSG) incorporates security practices throughout the entire development cycle to ensure that each product follows a secure development lifecycle. Veritas ASAP aligns with NIST SP 800-218.

Application Security Assurance Pillars

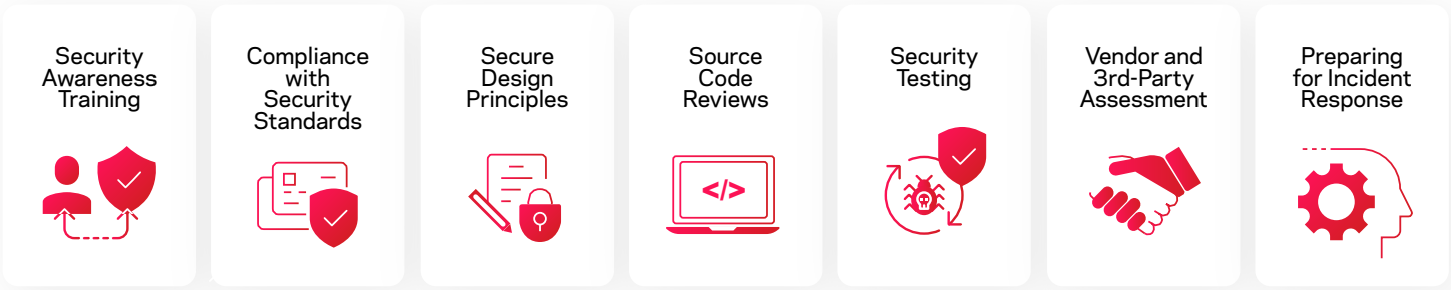

Figure 1. ASAP Pillars

Security Awareness Training

Veritas ensures that product development teams receive:

- Regular security awareness training to stay up-to-date with the latest security threats and mitigation techniques
- Role-based training for awareness of attack vectors and secure coding techniques
- Cyber-range awareness training in which developers play the attacker's role to better understand threats and mitigation

Security Standards Compliance

Veritas evaluates that products:

- Follow secure design principles, such as least privilege, defense in depth, and secure defaults
- Have undergone threat modeling to identify potential security risks and vulnerabilities
- Enforce Executive Order 14028 for items such as multi-factor authentication, encryption for data at rest and in transit (FIPS 140-2), Zero Trust architecture, and software bill of materials (SBOMs)
- Align best practices and security requirements with the SSDF

Secure Design Principles

Veritas works to ensure that:

- Products adhere to relevant security standards, regulations, and best practices; these include ISO 27001, NIST Cybersecurity Framework, or industry-specific security requirements
- Each product has undergone thread modeling to identify potential security risks and vulnerabilities
- Product teams follow the Security by Design principles defined by the Cybersecurity and Infrastructure Security Agency (CISA)
- Each product has an extensive cryptography review

Source Code Reviews

Veritas ensures:

- Product code reviews occur and identify security flaws such as injection vulnerabilities, authentication bypass, or insecure data handling
- A control analysis tool is executed and identified issues addressed

Security Testing

Veritas verifies that the product has undergone rigorous security testing, including:

- Penetration testing
- Vulnerability scanning
- Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) hardening
- Container scanning
- Fuzz testing

Veritas PSG provides product teams with vendors or internal help for each area. For example, internal penetration testing teams do testing along with third-party vendors.

Vendor and Third-Party Assessment

PSG works with each product team to:

- Ensure that all vendors assess third-party components and dependencies for potential security vulnerabilities or weaknesses
- Enforce secure configuration management practices, such as storing credentials securely, protecting sensitive data, and implementing secure communication protocols

Incident Response Preparedness

Preparation includes validating that each product team has an established plan, including procedures for security incidents, incident reporting, and communication channels.

Veritas releases monthly security patches to ensure that its customers have the latest fixes. Veritas has also built REDLab, an isolated lab to study ransomware and malware attacks firsthand.

Executive Order 14028

Veritas enforces the Executive Order 14028 requirements with all product teams. Product releases are not made generally available unless PSG has approved the SBOM.

Veritas PSG generated a tool that uses heuristics to do basic validation of the SBOM delivered. The tool provides views of the data to simplify human review. The tool also identifies issues for reporting in the Plan of Action and Milestones. The product team and PSG review the tool results; human intervention is crucial in generating an SBOM. The SBOMs are delivered in machine-readable format, specifically, Software Package Data Exchange (SPDX).

Veritas is exploring third-party validations for SBOMs and attestations for product compliance with the SSDF.

Vulnerability Policy and Transparency

Veritas uses multiple automated security tools and manual techniques to find vulnerabilities in our products in accordance with Executive Order and CISA requirements. Veritas scores the severity of vulnerabilities using an industry standard system (Common Vulnerability Scoring System v3.1) to guide remediation urgency and public notifications. Dedicated product security leads meet with PSG bi-weekly to review their application security.

Learn more about the Veritas Vulnerability Management Commitment and Disclosure Policy >

Veritas solutions are designed to protect, detect, and recover rapidly at enterprise scale. Our technology delivers the fundamental capabilities needed to strengthen your cybersecurity posture and keep your data and applications safe and resilient across any environment. Learn more about advanced cyber resiliency solutions.

VERITAS

2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

For global contact information visit:
veritas.com/company/contact

V1989 11/23