Veritas™ Application Security Assurance Program (ASAP) Whitepaper

This whitepaper is addressed to Information Technology (IT) decision makers, security personnel & IT auditors, and is directed to readers that are familiar with basic security concepts in the area of application security, data storage, networking, operating systems, data encryption, and operational controls in production IT environments.

Customers that have additional questions or comments regarding document can email Veritas Global Security Office (GSO) Customer Trust at DL-VTAS-GSO-CustomerTrustOffice@veritas.com stating the document title.

Forward-looking Statement: Any forward-looking indication of plans for products is preliminary and all future release dates are tentative and are subject to change at the sole discretion of Veritas. Any future release of a product or planned modifications to product capability, functionality, or feature are subject to ongoing evaluation by Veritas, may or may not be implemented, should not be considered firm commitments by Veritas, should not be relied upon in making purchasing decisions, and may not be incorporated into any contract. The information is provided without warranty of any kind, express or implied.

© 2018 Veritas Technologies LLC. All rights reserved. Veritas, the Veritas Logo, NetBackup, Backup Exec, Enterprise Vault, InfoScale, and Velocity are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.
Table of Contents
Executive Summary ........................................................................................................................................ 3
Governance: ASAP Roles and Responsibilities ..................................................................................... 3
Software Development Lifecycle .............................................................................................................. 4
Secure Development Training ................................................................................................................ 5
Requirements .......................................................................................................................................... 6
Design ..................................................................................................................................................... 6
Implementation ....................................................................................................................................... 6
Verification ............................................................................................................................................... 7
Deployment ............................................................................................................................................... 7
Operations ............................................................................................................................................... 7
Monitoring and Reporting: driving security maturity ........................................................................... 7
   Measured Application Security Assurance Processes (from the ground up): ..................................... 8
Software Supply Chain Security .............................................................................................................. 9
Penetration Testing ................................................................................................................................ 9
Privacy ................................................................................................................................................... 10
Conclusion ............................................................................................................................................... 10
Executive Summary
Veritas believes that information security and data safety are of utmost importance to our customers, who have chosen Veritas as a world leader in enterprise data protection products and services. Application security is a fundamental requirement that helps protect critical data assets from accidental or deliberate theft, leakage, integrity compromise (including ransomware) and deletion.

Veritas understands that safeguarding the integrity of data-protection products and services is critically important to our customers. We recognize that products must meet robust security standards so customers can deploy them with confidence. To meet this need, Veritas has established governance and policy structures that identify and mitigate potential product security risks during development and drive security awareness across the enterprise. Veritas maintains comprehensive and rigorous software development processes and procedures that are consistent with industry standards to identify and address potential vulnerabilities, while reducing risks to critical infrastructure, intellectual property, and sensitive information posed by the constantly evolving cyber-threat landscape.

This white paper provides an overview of our risk-based, software assurance process; a program that demonstrates Veritas’ commitment to building customer trust through the delivery of world-class data protection software.

Governance: ASAP Roles and Responsibilities
Starting with our people - clearly defined roles and responsibilities help our product teams know what to expect and how to meet those expectations. Security is “owned” at the top of the organization, while product teams are empowered to make the right risk-based decisions where security is concerned.

Product Security Group
The Product Security Group (PSG) is a dedicated cross-functional team within the Central Product Office that supports delivery of secure products. The PSG, in close partnership with the Global Security Office (GSO) and Legal teams, has a mission to ensure product security across the company; to verify that Veritas solutions are free from exploitable vulnerabilities, to identify and mitigate threat vectors, and to reduce cybersecurity risks to an acceptable level for Veritas and our customers. PSG teams assess security features throughout our product development lifecycle. From the gathering of requirements in New Product Initiatives, to the supporting of GA products, to end-of-life decisions – PSG is focused on reducing risk and answering the needs of our customers.

The PSG is responsible for leading, promoting, training, and setting expectations for application security best practices across the Veritas product organization. In addition, the ‘PSG Presents’ brown bag training activities and ‘PSG Bulletins’ provide timely awareness of current security news, events, and emerging regulations.

Product Security Leads
Following the Building-Security-In-Maturity-Model (BSIMM) framework, product security leads (or satellites) are the embedded security leads within each product team. Each team has at
least one primary security lead and one secondary. The security leads collaborate directly with the PSG on regular intervals to review dashboard metrics, discuss emerging threats, and promote security best practices across their teams.

**Product Security Managers**

Product Security Managers adhere to standards and best practices as directed by the leads and the PSG, and can escalate issues to senior management as needed. The product security managers are responsible for communications to all internal stakeholders regarding product release schedules and security deliverables.

**Developers**

Developers work ‘in the trenches’ to directly implement ASAP best practices in the software development and release cycles.

**Testers**

The QA test role has traditionally been to help ensure the functional capability of the product, but in the Veritas ASAP program (as described below) the testers are trained to think outside that traditional box by exploring the negative test cases (e.g., how a hacker might try to break an application), and then apply that ‘attacker-centric’ thinking to their test plans.

**Product Managers/Product Owners**

Product Managers and Product Owners are required to go through in-depth application security training providing education on potential risks to the products they own and deliver. When working with product teams, it is critical for product managers/owners to communicate between technology and business leaders to define security requirements in alignment with customer expectations.

**Scrum Masters**

Scrum masters play a critical role integrating security as a part of the Agile Scrum process. Scrum masters ensure teams have appropriate ‘epics’ and ‘user stories’ for security, and that the ASAP security activities are part of the ‘definition-of-done’ criteria for teams.

**Product/Software Development Lifecycle**

The Veritas Application Security Assurance Program (ASAP), evaluates application security best practices throughout the product/software development lifecycle (“PLC”).

The ASAP program’s goal is to shift security to the early phases of a project through identification and mitigation of risks utilizing industry standard methodologies. In industry terms, this is called “shift left,” where security practices are delivered proactively early in the software development lifecycle.

The ASAP program identifies seven key phases of application security activities within the product lifecycle for software development teams to follow:

1. Training
2. Requirements
3. Design
4. Implementation
5. Verification
6. Deployment
7. Operations

Figure 1.1: ASAP Secure Development Lifecycle

Application Security Assurance Program Phases

Secure Development Training
Secure development training is identified as its own phase in the program, but also considered across all phases. The key to effective training is that it be timely, meaningful, and easily applied.

Core SDL Training
The PSG ‘Security Warrior’ belt-system application security training and awareness program help ensures that roles in the ASAP program receive relevant and targeted role based training, at a minimum, on an annual basis. The training program starts with basic application security awareness, then - depending on the job role - moves into more advanced technical topics (such as “Secure Coding in Java”, “Threat Modeling”, and “Cryptography”).

Figure 1.2: Veritas Security Warrior Belt System
**Supplemental (Brown-Bag) Training**
In addition to the Security Warrior program, the PSG also delivers Brown Bag training session on key security topics on a regular basis and holds monthly meetings with all the security leads to highlight and help them understand the latest security issues or concerns.

**Requirements**
The requirements phase of PLC at Veritas includes a comprehensive analysis of security risk, where security concerns guide design and implementation decisions made by development team, rather than simply providing a checklist of required features. In this phase, teams review and classify the sensitivity of the various ‘data types’ that the application will be handling to determine appropriate controls, or countermeasures.

The Requirements phase also includes review of third party or open-source software used in the application for compliance with the Veritas policies. Product development teams will identify a project date/milestone to complete third-party updates to maintain compliance as the project proceeds.

During the requirements phase, teams identify security-training needs and allot time for members to complete the necessary curriculum.

**Design**
Software development teams are encouraged to use industry standard accepted security design patterns, such as NIST or ISO/IEC standards, in order to leverage validated defensive capabilities in the product line. In an Agile development approach, teams may continually revisit the design to maximize the defensive characteristics of the system as part of a defense-in-depth approach.

Design-phase key activities include:

- Creating an up-to-date threat model.
- Developing or revising user and service authentication, authorization and audit mechanisms documentation.
- Completing a Veritas Cryptographic Review Survey for encryption technologies utilized within the product.

**Implementation**
Implementation is the phase of PLC when the team is actually creating the product. This could be writing new software, upgrading existing software, integrating third party software, and other activities focused on building a customer-ready shipping product. All teams are required to follow Veritas Secure Coding Standards that implement industry best practices for the given technologies and programming language.
Automated Static Code Analysis (SCA) is performed in this phase and where possible implemented in an automated build/break fashion. The goal is to scan-early, scan-often, to identify and remove vulnerabilities as early as possible.

For business-logic stability, teams perform manual code reviews on the most critical functions to help ensure proper implementation based on the design.

To protect both our customers and Veritas from reverse engineering, teams are required to comply with the Veritas Source Code Handling Policy.

**Verification**

During the verification, phase teams perform Dynamic Application Security Testing (DAST) generally using more than one scanning tool to detect any vulnerabilities in the running product.

To support a risk-based focus, teams use risks identified during threat modeling as a part of the test plan to help ensure critical areas receive appropriate attention.

Veritas also works with several penetration testing vendors or providers to perform third party penetrations tests on a regular basis.

**Deployment**

Deployment or release phase includes the final steps before the product is ready to be released, whether that be on premise or cloud-based.

The PSG works with development teams to perform a final security review that analyzes each activity across the ASAP SDL. At this point, teams also update any security related documentation to inform customers of changes in the release and security best practices for the product.

**Operations**

The operations phase covers the range of newly released product to End-of-Life (EOL) product and expectations of the product team to support any product in production.

If a vulnerability is discovered during operations, teams are required to follow the Veritas Product Vulnerability Management Policy to address vulnerabilities in a timely manner, including both proprietary software and third party software included in the product.

**Monitoring and Reporting: driving security maturity**

ASAP program metrics are reported to senior management on monthly and quarterly reporting cycles via the ‘PSG Dashboard’.

Additionally, the PSG utilizes the Building Security in Maturity Model (BSIMM) framework for aligning to, and measuring against, industry standard best practices.
Measured Application Security Assurance Processes (from the ground up):

- **Application Security Assurance Program (drives Secure Development Lifecycle)**
  - The Application Security Assurance Program provides a framework to help ensure that our products are developed, delivered, and supported throughout their lifecycle in alignment with industry best practices.

- **Threat modeling and security checklist review by Architectural Review Board (ARB)**
  - The architectural process at Veritas includes threat modeling activity and security review checklists required for review by the ARB prior to greenlight.

- **Software security training for Architects, Engineers, and Product Managers**
  - The PSG ‘Security Warrior’ product security training and awareness program provides our Architects, Engineers, and Product Managers with relevant and targeted role based training, at a minimum, on an annual basis. The ‘PSG Presents’ brown bag training activities and ‘PSG Bulletins’ provide timely awareness of current security news, events, and emerging regulations.

- **Static Application Security Testing (SAST)**
  - During the implementation phase of the Secure Development Lifecycle (SDL), product teams are required to perform static analysis on their code to catch coding vulnerabilities as early as possible.

- **Dynamic Application Security Testing (DAST)**
  - During the verification phase of the Secure Development Lifecycle (SDL), product teams are required to perform dynamic security testing to again identify vulnerabilities prior to release.

- **Open-source software management**
  - The PSG team actively manages third party and open-source software utilized within the Veritas cloud product service offerings to promote utilization of the most up-to-date versions, and that vulnerabilities are: identified, patched, and remediated in a timely manner according to Veritas policy.

- **Cryptography reviews and adherence to standards**
  - The PSG team conducts regular and ad-hoc reviews of cryptographic modules and algorithms used in Veritas products to safeguard utilization of current standards and
supported versions. Certain Veritas products utilize FIPS 140-2 standards, where applicable, in alignment with Common Criteria guidelines.

- **Annual 3rd party penetration testing (red team) and versioned vulnerability scanning**
  - Veritas products are generally pen tested by an independent third party red team at least once per year. The PSG also conducts internal scans whenever a new product version is released. PSG manages schedules for pen testing and internal vulnerability scans.

- **Vulnerability Management Policy covering all Veritas products**
  - Veritas product teams are required to adhere to the internally facing Veritas Product Vulnerability Management Policy, including remediation of vulnerabilities within a target SLA window based on severity.

**Software Supply Chain Security**

The global expansion of the software industry has increased the risk of product or service compromise by malicious code introduced during product development or maintenance. Technological innovation and changes in sourcing and supply chain strategies have made software supply chain security a global challenge. Threats associated with IP theft, third-party code, and open source components have driven an industry-wide increase in supply chain security controls. Veritas works proactively to maximize the security of our supply chain.

**Managing Supply Chain Risk**

Veritas maintains a formal supply-chain risk management program that is focused on secure sourcing of hardware, firmware, and software integration related to our products.

Veritas has established processes governing supply chain risk and the sharing of source code with third parties, including contractual review by Legal, GSO, and PSG teams. Veritas includes terms that set minimum software security standards in its OEM (original equipment manufacturer) and third-party software license agreements that align with industry best practices.

**Industry Participation**

Veritas is an active member of the BSIMM community, utilizes the BSIMM framework for the Veritas ASAP program, and has undergone a formalized BSIMM assessment. Veritas is also actively engaged in the security research engineering community, and its GSO, PSG, and Security Lead teams work to build relationships in the cybersecurity and software development communities.

**Penetration Testing**

Veritas utilizes trained and experienced internal staff as well as third parties to regularly conduct penetration tests of critical systems and applications. Veritas targets performing third party testing
annually. Findings from penetration testing are handled in the same manner as vulnerabilities as discussed above. Penetration test results are considered Veritas Highly Confidential Information, and are not shared outside of the organization.

Veritas utilizes both white and gray box testing to help ensure complete coverage. The gray box approach is a mixture of black box and white box testing. White box testing means that all the source code is available, where black box testing means that the pen test executes without any source code access. The gray box method enables the third party performing the pen test to have source code available to assist with penetration testing. Third-party vendors have signed NDA and confidentiality agreements with the Veritas.

**Privacy**

**Privacy Policy:** The Veritas Privacy Policy can be reviewed at: [https://www.veritas.com/company/privacy](https://www.veritas.com/company/privacy)

**Conclusion**

Veritas strives to build products that customers trust with the most critical operations of their enterprises. To promote this intent, Veritas has established programs to identify and mitigate potential product security risks during development. In addition, Veritas Global Security Office (GSO) has instituted programs and practices that drive software security initiatives and awareness across the enterprise.

Veritas’ product security strategy and our Application Security Assurance Program (ASAP) allow us to continuously evolve methods to protect sensitive customer information and infrastructure from product vulnerabilities.

In closing, this document represents the approach taken by Veritas to develop secure, enterprise-class data protection products and services.