VMware Product Security

An Overview of VMware's Security Programs and Practices

TECHNICAL WHITE PAPER

vmware®

Table of Contents

Executive Summary

VMware, the industry-leading virtualization software company, empowers organizations to innovate and thrive by streamlining IT operations. Radically transforming IT with technologies that make your business more agile, efficient and profitable, VMware software powers the world's most complex digital infrastructure. The company's compute, cloud, mobility, networking and security offerings provide a dynamic and efficient digital foundation to over 500,000 customers globally, aided by an ecosystem of 75,000 partners. Our unique solutions drive outstanding application interoperability and customer choice, benefiting both business and society.

VMware understands that the integrity of its cloud services and products (herein "products") is of utmost importance to our customers and recognizes that unless its products meet the highest standards for security, its customers will not be able to deploy them with confidence. To achieve this, VMware has established oversight procedures that identify and mitigate potential product security risks during development and has instituted programs and practices that support both the development of secure products and solutions and drive security awareness across the enterprise. In response to risks to critical infrastructure, intellectual property, and sensitive information posed by the constantly evolving threat landscape, VMware has developed comprehensive and rigorous software security assurance processes and procedures that demonstrate the integrity of its products and address potential vulnerabilities.

This white paper provides an overview of how our commitment to building trust with our customers is present in every facet of our comprehensive, risk-based software assurance process and is reinforced in our program structure.

VMware's approach to product and information security addresses potential vulnerabilities within areas such as:

- Software product development
- Software supply chain
- Technology partnerships and ecosystems

Software Product Lifecycle Management

The VMware Software Product Lifecycle includes the framework, governance, and set of executive checkpoint reviews, tools, artifacts, and guidance that enable VMware product business units (BUs) to ensure business readiness at the time of product availability and throughout the product lifecycle. Central to the framework is an integrated and predictable approach to product and cross-functional planning, release/program management, execution, measurement, risk management, and decision making at each phase of the product lifecycle.

The VMware Software Product Lifecycle provides the framework for addressing critical decision points as a product proceeds through the lifecycle phases from Concept to Sustaining state.

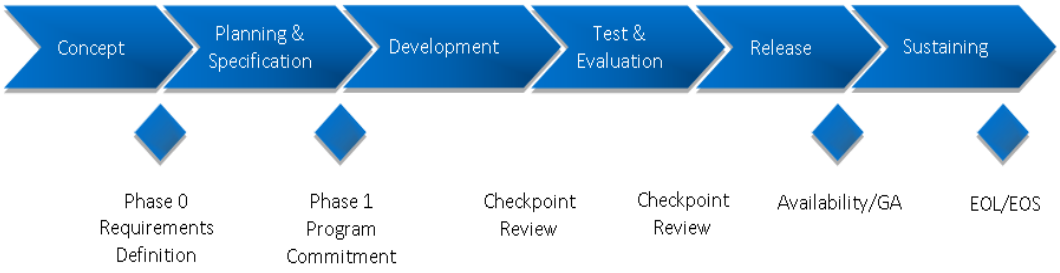

Figure 1 Enterprise Product Lifecycle Management Workflow

Privacy by Design

Building in appropriate security controls and safeguards in VMware products and services is integral to VMware's 'privacy by design' framework. The VMware security team and engineers work with the VMware privacy team during product development to evaluate security and privacy risks and implement safeguards to mitigate and minimize such risks and comply with applicable law. Further, as part of VMware's privacy program, VMware details the types of data collected in connection with its products and services in its Products and Service Notice, and the types of data VMware collects and uses to manage accounts and customer relations in its VMware Privacy Notice. The VMware Products and Services Notice contains information regarding the types of data collected and used in connection with VMware's provision of the Services.

Building Security into VMware Products and Practices

VMware has established programs and practices that identify and mitigate security risks during and throughout the software development process. Through these activities, VMware delivers secure products and solutions for its customers.

Based on industry-recognized best practices and standards, and developed in consultation with trusted industry participants, VMware's programs and practices focus on:

- Building secure software
- Protecting the intellectual property related to software products
- Managing software security supply chain risks
- Managing technology partner and ecosystem risks
- Delivering secure product support

Product Security

The Product Security group, VMware Security Engineering, Communications & Response (vSECR), develops and drives software security initiatives across all of VMware's R&D organizations to reduce and mitigate software security risks. Their goals and practices oversee a product development process that employs a comprehensive approach to assist in the delivery of secure products. The teams and efforts described in this section represent VMware's commitment to promoting a security-conscious approach and culture to foster positive cross-functional collaboration in security.

VMware has a comprehensive approach to security which includes collaboration with many teams across our organization, including Research and Development, Corporate Legal and Privacy, as well as Support and Field organizations. VMware also works closely with Industry Organizations, Security Analysts and Researchers, etc. to stay current on the Industry threat landscape and security best practices.

Figure 2 VMware Product Security

The vSECR group develops and drives software security initiatives across VMware's R&D organizations to reduce software security risks. The vSECR programs and engineering functions include:

- **VMware Security Development Lifecycle (SDL)** – A comprehensive program to identify and mitigate software security risks during the software development lifecycle. The program is supported by a security engineering team that performs security design reviews and thourough security testing.
- **Security Response Center (VSRC)** – Leads the analysis and remediation of security issues in VMware products, once products have been released to customers.
- **Security Certifications** – A program to drive key products through appropriate security certifications such as Common Criteria, FIPS 140-2, and DISA STIG
- **Security Evangelism** – A program to raise security awareness and competency within the broader VMware R&D community through formal and informal training

Security Development Lifecycle

VMware's Security Development Lifecycle (SDL) program is designed to identify and mitigate security risk during the development phase of VMware software products. The development of VMware's SDL has been heavily influenced by industry best practices and organizations such as SAFECode (the Software Assurance Forum for Excellence in Code) and BSIMM (Building Security In Maturity Model).

VMware is active in the broader software industry security community, becoming an early member of BSIMM in 2009 and a member of SAFECode (Software Assurance Forum for Excellence in Code) in 2014, an organization driving security and integrity in software products and solutions. VMware is also active in the security research community and works to actively cultivate relationships in this community. For example, VMware brings speakers from the research community onto VMware campuses to present technical talks on security topics. Furthermore, VMware hosts annual 2-day internal security engineering conferences at multiple VMware facilities globally, where external security researchers and internal security experts from across the globe present.

VMware SDL is periodically assessed for its effectiveness at identifying risk and new techniques are added to SDL activities as they are developed and mature.

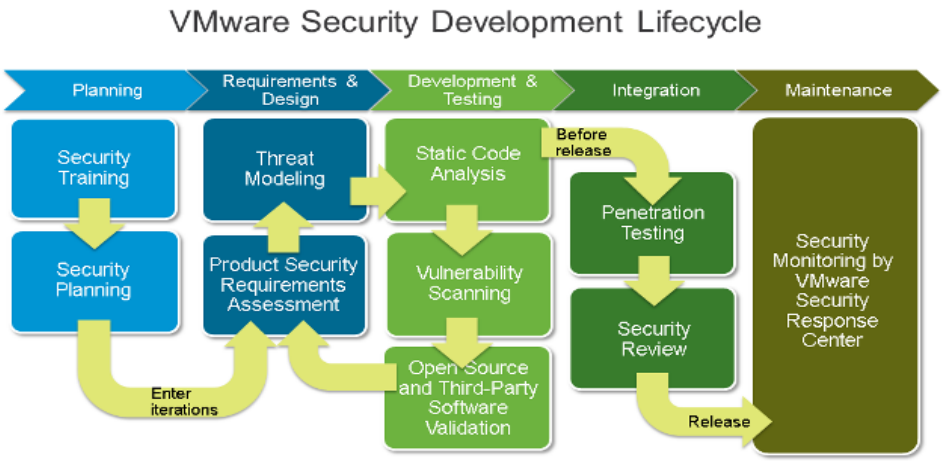

Figure 3 VMware Security Development Lifecycle

Current VMware SDL activities include:

- **Security Training –** vSECR maintains role-based technology-specific product security and privacy training curricula in VMware's central learning management system.
- **Security Planning –**SDL planning early in the development lifecycle forms the basis for the later Security Review activity, when a product's security profile is evaluated at development milestones.
- **Product Security Requirements Assessment –** This activity examines how a product adheres to VMware Product Security Requirements (PSR), which includes standards for:
  - Authentication
  - Authorization
  - Encryption
  - Certificates
  - Network security
  - Virtualization
  - Accountability
  - Software packaging and delivery
- **Threat Modeling –** This activity identifies security flaws and incorrect design assumptions present in the architecture of a product.
- **Open Source Software and Third-Party Software Validation (OSS/TPS) –** This activity highlights OSS/TP software components with known vulnerabilities so they can be fixed before being included in a product release.
- **Static Code Analysis –** This activity uses automated tools to detect defects and security flaws in code.
- **Vulnerability Scanning –** This activity uses automated tools to detect security vulnerabilities in running systems.
- **Penetration Testing –** This activity attempts to circumvent security controls and uncover implementation vulnerabilities in running environments.
- **Security Review –** This activity collects and examines the results of all the preceeding activities.

The vSECR group owns the definition and practice of SDL processes. The SDL is the secure software development methodology promoted by vSECR to help VMware product development groups identify and mitigate security issues early in the lifecycle so that their software is safe for release to customers.

The SDL's end-to-end set of lifecycle processes aim to help product development groups achieve these goals:

- Reduce their component's risk profile and attack surface
- Identify and remediate costly security-related design flaws early in the development process before much coding has taken place
- Discover and remediate security vulnerabilities prior to availability
- Educate their teams on security issues and security best practices

Figure 4 illustrates the timeline of SDL activities and product release milestones.

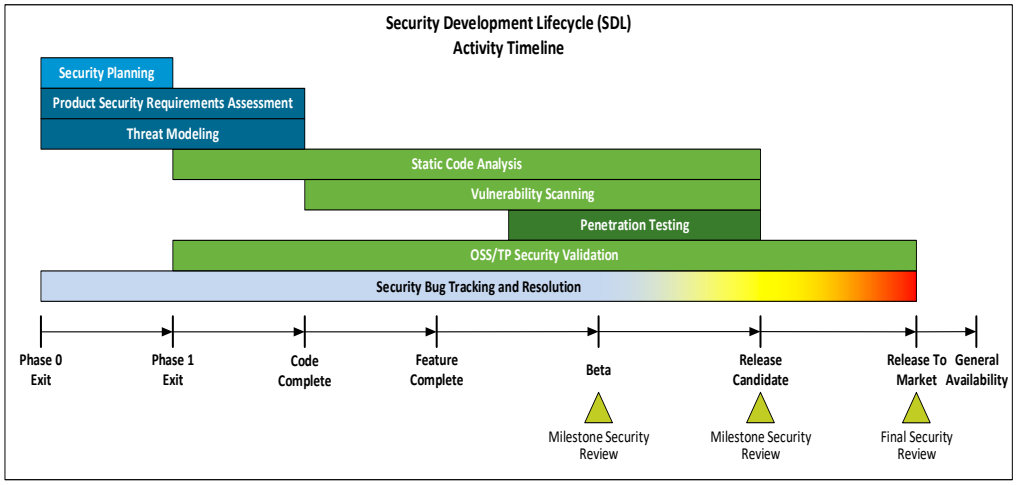

Figure 4 vSECR Security Development Lifecycle (SDL) Activity Timeline

The SDL processes include these activity phases:

Planning

During this phase, the development team documents its security plan (strategy, risks, initial schedule, etc.) for the release, utilizing the Security Development Lifecycle workflow.

As part of VMware's abiding commitment to ensuring support around security early in the development process, VMware offers courses for managers, developers, and quality engineers in:

- Security concepts
- Security design and testing
- Secure coding techniques for specific languages
- Various security tools

Design

During this phase, the development team utilizes the VMware Product Security Requirements (PSR) to identify and remediate security issues in VMware products before release.

Additionally, the development team formally develops a threat model that identifies potential security flaws and incorrect design assumptions present in the architecture of a software application or component. Threat modeling occurs early in the development process, and thus allows adequate time for teams to remediate any design-related security issues.

Implementation

During this phase, the development team utilizes automation tools as part of Static Code Analysis (SCA) to

detect defects, including security flaws, in software components that are not running or are "at rest".

Additionally, VMware requires that its development teams publish the names and release levels of each Open Source/Third-Party Software (OSS/TP) product or library that the team uses in building VMware products or components so they can update to the latest, fixed versions of the OSS/TP software in all product releases.

Validation

During this phase, the development team employs automated Vulnerability Scanning processes to identify security vulnerabilities in computing systems running in a network to determine the specific ways the system can be threatened and/or exploited.

Additionally, the development team uses Penetration Testing (pen test) assessments to determine if a malicious intruder can successfully attack a software product or solution. VMware conducts these tests on an isolated, mock customer environment. The tests include reviews of the product architecture and source code, and utilize various commercial and/or custom vulnerability detection tools.

Lastly, during this stage, the Security Review is conducted to establish whether the subject software has undergone the required SDL activities adequately, and has addressed security risks such that the software is suitable for release to customers. Formal Security Reviews occur before the Beta, Release Candidate (RC), and Release to Market (RTM) milestones.

Security Review

The Security Review establishes whether the subject software has undergone the required SDL activities adequately in order to identify security risks and addressed these risks such that the software is suitable for release to customers.

While the data that the Security Review evaluates is monitored throughout the entire security development lifecycle of the software, formal Security Reviews occur before the Beta, Release Candidate (RC), and Release to Market (RTM) milestones.

Production

When a VMware product has reached the general availability milestone, the product enters the production stage of its lifecycle, and remains in production until it reaches the end-of-life milestone.

The VMware Security Response Center (VSRC) is charged with monitoring the landscape for all reports of security issues concerning VMware products.

The internal role of VSRC is to investigate reported vulnerabilities and provide information on security issues to the appropriate teams. VSRC serves as a point of contact for security researchers, customers, partners, and other external parties with a point of contact for reporting vulnerabilities in VMware products (security@vmware.com). **Note:** We encourage use of encrypted email. Our public PGP key is found at kb.vmware.com/kb/1055.

When VSRC detects or receives a report of an issue with a VMware product, VSRC works with the development team to investigate the issue. VSRC continues to coordinate the remediation and communication of the issue with the appropriate product and support teams. VSRC is additionally responsible for communication and dissemination of all relevant VMware Security Advisories. VMware Security Advisories can be found at http://www.vmware.com/security/advisories/.

Security Response Center

Established in 2008, VSRC is responsible for managing and resolving security vulnerabilities in VMware products once products are released to customers. VSRC has a mature process for investigating reports, coordinating disclosure activities with researchers and other vendors when appropriate, and communicating remediation to customers via security advisories, blog posts, and email notifications. VSRC is well established within the security research community and participates in many external security events in order to foster strong working relationships with the security research community. For example, VMware participates in major security conferences such as RSA, Black Hat, DEF CON, and CanSecWest. Also, VMware is involved in the security community, including FIRST and ICASI, and hosts Moosecon, its own internal security conference, featuring internal and external speakers. VMware's security response policies are well established and are publicly documented on the VMware website at http://www.vmware.com/support/policies/security_response.html.

Security Evangelism

The long-term goal of the Security Evangelism team is to increase the level of software security awareness and competency within VMware's R&D community. This allows the SDL process to scale effectively. The team uses several programs to achieve this:

- An R&D wide, role-based technology-specific online software security training program
- Participation as speakers at VMware's annual Research & Development Innovation Offsite (RADIO) conference
- Software security challenges, competitions, and hackathons focused on VMware products
- Moosecon, an internal 2-day VMware security conference that involves industry-recognized speakers from both academia and the security research community as well as speakers from within VMware

Security Certifications

VMware has a long history of participating in FIPS and Common Criteria standards with the first VMware cryptographic module validated in 2007 and first VMware product being certified in 2008. The Security Certifications team drives the certification of major VMware products as well as the validation of cryptographic modules used in those and other products. The team, also, actively participates and contributes in the development of the standards and various Protection Profiles by continuously engaging with various WGs/TCs/iTCs.

For a complete list of VMware's Common Criteria certified products, visit http://www.vmware.com/security/certifications/common-criteria.html

For a complete list of VMware's FIPS 140-2 validated modules, visit https://www.vmware.com/security/certifications/fips.html

Software Supply Chain Security

With global expansion of the software industry, security concerns have increased that a product or service could be compromised 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 ranging from risks associated with using third-party code and open source components to IP theft have dramatized the vulnerability of this new risk domain. VMware is actively engaging in proactive measures to minimize the occurrence of these risks and has launched several initiatives to address the security of our supply chain.

Managing Supply Chain Risk

VMware utilizes a Supply Chain Risk Management program that focuses on secure sourcing and hardware, firmware, and software integration relating to building solutions. It includes use of an approved vendor list for several of its BUs and functions.

- VMware's recycle program for hardware products addresses supply chain risk by securely recycling equipment that may hold information sensitive to the supply chain. For example, hard drives that are at end of life and were used in the source control systems are properly recycled to ensure that the data from the source control systems is removed.
- VMware has established processes around partnerships with entities deemed to be of increased supply chain risk and around the sharing of source code with third-parties
- With respect to partnerships, VMware has an established process to determine if a partner is

considered to be of increased security risk. If a partner meets certain criteria, they may be excluded from certain programs that permit direct access to VMware IP.

- Both inbound and outbound contracts with software supply chain security implications are reviewed by the Legal and Product Security teams. VMware includes terms that set minimum software security standards in its OEM (Original Equipment Manufacturer) and third-party software license agreements that are in keeping with or exceed industry best practices.

Industry Participation

VMware is active in the broader software industry security community. As mentioned earlier, VMware is a participant in the BSIMM process and a member of the SAFECode organization. VMware is also active in the security research community and works to actively cultivate relationships in this community. VMware also actively engages with the Open Source community through contributions to existing community-based projects as well as developing, releasing, and leading new open source projects and initiatives.

Protecting Product Source Code

Product source code managed by the Source Code Management (SCM) team follows processes designed to safeguard the integrity of VMware's product-related intellectual property while providing engineers access to source code required to develop and maintain its products. Also, the SCM team manages the source code systems environments.

Code Integrity

These controls can allow for code integrity problems to be identified and remediated in a timely manner for perpetual software.

TABLE 1 CODE INTEGRITY CONTROLS

Control	Current Process
Code review	Well-adopted practice within teams
U.S.-Based Builds	All products TAA compliant
Security Reviews	Security Reviews conducted prior to release
Risk Management of Open Source Software (OSS)/Third-Party Software (TPS) supply chain	Contract provision to allow security testing of TPS

The following sections describe processes aimed at supporting product integrity for a VMware product that achieved Common Criteria Certification. The process extends to other VMware products.

Source Code Management

Source code control protects the security and integrity of code that is written, developed, tested, and evaluated. Source control covers code creation, modifications, deletion, and incorporation of the code into larger parts. Audit controls within the source control system automatically track what changes have been made, who made them, when a change was made, as well as other consequences of those changes. Access to the source code is controlled by a network access and is controlled on a per-user basis, by means of user permissions and roles.

The product source code is stored on centrally managed servers in a secure area and protected behind a network firewall.

Secure Delivery

Several procedures are necessary for VMware to maintain security when distributing the product to a customer's site. For a valid delivery, the product received must correspond precisely to the product master copy, without tampering, or substitution of a false version. The delivery procedures ensure that the integrity and authenticity of the product are maintained and that they are verifiable by the customer and by VMware after delivery has been completed. The product is delivered via VMware's websites by electronic distribution only. The end user is supplied with the product, product documentation, and product license.

Issue Remediation

Customers report security issues to VMware's Product Security group (security@vmware.com) when a problem is encountered in the normal operation of the product. Product issues are also reported, captured, and filed through VMware's Global Support Services (GSS). Internal wiki pages are used to track security related bugs reported from the security@vmware.com mailing list.

Any bug discovered during product development, design change, testing, or by a customer must be triaged, documented, and a solution offered before the bug report can be closed. These bugs include suspected and/or confirmed security flaws.

Providing Secure Product Support Services

VMware's Global Support Services (GSS) organization is global and as part of standard practice engages the necessary resources wherever they are in the world. VMware has established a variety of process and procedures to protect data while working to resolve customer support issues. For a more in-depth overview of Global Support Services and more on their expertise in Virtualization and Cloud Infrastructure, see http://www.vmware.com/files/pdf/support/VMware-Support-GSS-BR-EN.pdf.

Vulnerability Management

VMware has a Vulnerability Management program backed by approved and tested policies and procedures. Vulnerability scans are performed regularly on VMware developed products and Cloud Services.

System and application owners are required to address critical and high vulnerabilities with a plan of corrective action. Responsiveness requirements are dependent on vulnerability severity.

Risk analysis and acceptance are performed on vulnerabilities to confirm the vulnerability, and to determine the appropriate means of addressing the vulnerability. Senior management within the applicable BU – as well as IT and Information Security senior management – are required to approve the existence of all risks associated with vulnerabilities that are not patched with vendor provided fixes.

Penetration Testing

VMware utilizes trained and experienced internal security engineering staff to periodically perform penetration testing of critical systems and applications. Findings from penetration testing are handled in the same manner as vulnerabilities as discussed above. Penetration test results are considered VMware Private/Protected information and are not shared outside of the organization.

In order to achieve more meaningful test results, VMware uses both white and gray box testing. A gray box approach is a mixture of black box and white box testing. White box testing means that all the source code will be made available and black box testing means that the actual pentest will be performed without any source code access. The gray box method enables the security engineer performing the pentest to have source code available to assist with penetration testing. This results in a more robust set of tests because the penetration testers can achieve deeper and broader access since they spend less time breaking into targeted assets.

Conclusion

VMware strives to build products that its customers trust in the most critical operations of their enterprises. To promote this, VMware has established oversight procedures that identify and mitigate potential product security risks during development and has instituted programs and practices that drive software security initiatives and awareness across the enterprise.

VMware's focus on product security strategy and our security development lifecycle ensure our ability to continuously protect sensitive customer information from product vulnerabilities.

In closing, this document represents VMware's innovative, cooperative approach to security for its world-class virtualization software products and solutions. As such it also represents VMware's continuing commitment to its customers' success.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 1-877-486-9273 Fax 650-427-5001 www.vmware.com