VMware Trust & Assurance

TECHNICAL WHITE PAPER

Table of Contents

Introduction

As an industry-leading virtualization software company, VMware appreciates that the integrity, reliability, and security of its products are of utmost importance to its partners and customers.

The relentlessly advancing threat landscape over the last few years has yielded unprecedented cyber exploits which not only pose acute potential risk to critical infrastructure, intellectual property, and sensitive information, but can also erode a company's reputation. VMware is addressing the environment we now live in with innovative programs designed to get ahead of these problems and anticipate threat trends, along with keenly crafted assurance practices that engender customer trust.

VMware understands what matters to today's customer and is committed to furthering our insights through our well-established, candid customer dialogue and our growing transparency about the measures we take to ensure that our products and services continue to meet and exceed expectations on quality, performance and safety.

The VMware Trust and Assurance framework was created to drive this initiative of preserving and enhancing the trust customers place in VMware, our products and our services. We define trust as the demonstrable ability to execute on our commitments consistently over time--it is transparent, integrated, and proactive. Likewise, we are eager to communicate our proactive approach to reducing our risk landscape as well as activities ranging from development to security in support of providing comprehensive assurance--or proof--that our product offerings are secure, reliable, high quality, and trustworthy. This white paper discusses the teams, programs and practices that represent VMware Trust and Assurance's guiding principles of reliability, integrity, security and commitment.

Reliability

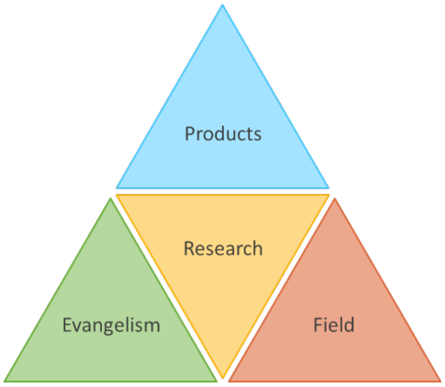
Quality and performance are key stakes in today's Infrastructure software and services. Our virtualization offerings have earned renown for high quality and high performance. In fact, we have led the creation of industry virtualization benchmarks for measuring workload performance. We take proactive measures to ensure we stay ahead in the area of both quality and performance to ensure our customers can continue to rely on us as we move into the next generation of virtualization software and cloud-based services.

Performance

The Performance Engineering team's mission is to ensure that VMware products and solutions perform competitively and scale optimally. As critical contributors at every stage of the product lifecycle, this team cultivates a culture where everyone owns performance as an ongoing key differentiator from on-premise to hybrid cloud to end user solutions. This aim is driven by core performance engineering values, which are commitment, collaboration, curiosity, customer focus, and excellence. These principles are illustrated in each of the Performance team's four main areas of focus: products, research, evangelism, and field.

For product performance, the team works to ensure VMware products and services perform excellently and scale optimally. Performance engineers:

- Ensure new products are architected and designed to perform
- Drive performance improvements for VMware products



- Evaluate progress across releases and competitors
- Prototype and develop product performance enhancements

A component of this effort is improving product performance via improved tier 1 application performance and relentless demonstration that all workloads virtualize. Improving performance also means opening new market opportunities, such as creating low latency for financials and online game hosting, as well as providing improved management product performance.

Evangelism and Education

The Performance Engineering team is committed to evangelizing and educating on Performance practices across the entire VMware ecosystem and beyond by developing and driving benchmarks, including industry leader and a cloud-based benchmark. The team teaches “The Performant Way” to VMware developers, partners, and customers, which results in everyone’s enablement to own performance via practical guidance, which consists of 15 crisp examples across architecture, design, and test. This includes:

- Extending performance knowledge internally and externally
- Driving performance best practices into VMware products
- Developing leading cloud and virtualization benchmarks
- Engaging through VMworld, blogs, and internal and external conferences

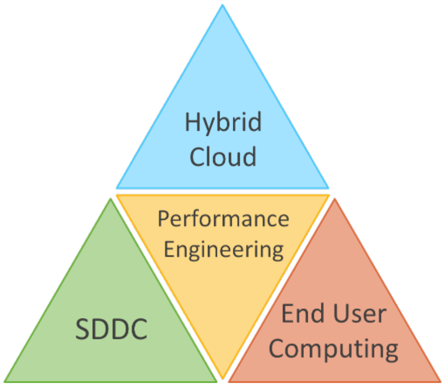
Research

Performance Engineering embodies a major component of the “R” in R&D at VMware. Exploring and researching opportunities for improvement and innovation in collaboration with developers, universities, and industry groups, this team drives deep-dive investigations into products and features. These relationships with thought-leaders and academics enhances this team’s exploration of emerging technologies and innovations with performance impact. Research likewise informs the development of tools and visualizations for analysis and revelation, illustrated by this team’s growing library of patents, papers, and publications, including twenty-five patent applications in 2014 alone.

Field Engagement

Another key vector that the Performance Engineering team pursues is enabling customers, partners, and VMware communities with performance expertise. This team facilitates VMware pre-sales by providing white papers, blogs, and hero numbers, and supports customers post-sale for the more complicated performance problems.

Performance Engineering continues to optimize IT outcomes across all products in the software defined datacenter (SDDC) with performance scorecards for every product. The team develops tools for sizing and analysis, and draws heavily on metrics with end-to-end impact across development, test, and integration. Their outcomes are also advanced by emerging research and differentiating technologies.



End User Computing is supported by improved desktop and mobile products, technologies, solutions, and benchmarks. Additionally, the Performance team is expanding virtualized desktop capabilities, such as EUC and ESX, and is exploring new technologies such as vCUDA, 3D, and containers.

Quality

Structural Quality
Customer Perception

Quality has always been a bedrock principle for VMware. Ensuring that our customers deploy new releases and updates in confidence, and all VMware products reliably interoperate as expected are key facets of our quality vision.

VMware has a quality process in place for each of our software products consisting of test plans, test designs, test procedures, and test exit criteria. These documents are updated and revised for each new version and serves as the plan of record for the project. Requirements and designs are documented and tracked as part of the software development lifecycle process. Multiple phase checkpoints during the development lifecycle that require stakeholder sign-off of quality criteria are conducted to ensure that the program is tracking to plan and if adjustments are needed, they are assessed and implemented accordingly. Always conscious of customers' perspective, quality teams are focused on root cause analysis of customer issues. VMware strives for continuous process improvements, and tracks metrics for product release against prior versions of the product.

VMware has training programs in quality that include bootcamp and refresher training for all quality test engineers. The entire R&D organization has specific training for employees on standard tools and processes.

Independent internal audits, reviews and checkpoints are conducted company wide, encompassing products and processes. Code reviews are conducted as part of the software development process, and reviews and checkpoints are conducted at various milestone points to ensure that entry and exit criteria are being satisfied.

In a continued effort to strengthen its customer-centric perspective, VMware has also created a quality effort team, which works to understand quality issues at VMware, and consults with teams across the enterprise to get an in-depth understanding of what quality means to VMware customers. Examples of this collaboration include working with Customer Advocacy to understand the customer view of quality, and conferring with the Global Support Services (GSS), Continuing Product Development (CPD), and Ecosystems teams to understand their quality concerns and review their metrics and processes. The Quality System team closely works with R&D teams to review processes and metrics and provide feedback, and reviews industry quality standards like CMM. Accordingly, this team works to improve quality through process changes within R&D, GSS, and CPD teams, tracking releases using predictive metrics, and sharing quality practices.

Integrity

Our software is developed, built, and delivered with integrity so that our customers, who include all of the Fortune 100, continue to entrust critical workloads to VMware. Our rigorous software development lifecycle and release management ensure product readiness and consistency, while our Compliance and Cyber Risk Solutions program helps customers foster a compliant-capable, audit ready posture. We manage Supply Chain security issues through a program that addresses risk associated with the use of third-party code and our IP sharing practices.

Release Management

The Release Management (RM) team's mission is to drive product teams through efficient and measurable Software Development Life Cycle (SDLC) processes to deliver high quality product releases that implement the company goals for Suite and Cloud. RM works with all business units and all cross-functional groups and is responsible for delivering all VMware releases, which exceed 400 each year. As the team is centrally hosted, it is optimally situated to drive consistency in release execution and in process compliance, maintain independence in status reporting and in escalation paths, and embed with engineering and quality teams.

RM provides active project management of VMware product releases, which includes driving product teams to build and release high quality products and services, using metrics to measure progress and to ensure release compliance to quality standards. RM additionally drives reporting and visibility on the state of releases and the release portfolio. Broadcasting metrics-driven release status updates provides invaluable information for the organization to stay at a competitive vanguard, while highlighting issues that require attention ensures the product or service is in an optimal condition before it is released.

RM establishes and improves release process best practices, and works with product teams to increase adoption of and consistency around release processes. It maintains the readiness of the product checklist, which ensures release compliance with legal requirements (open source, EULA, export compliance, country-of-origin, etc.), as well as ensuring compliance with accounting standards and federal certifications. For more information on our federal certifications, please see the VMware Product Security white paper at http://www.vmware.com/files/pdf/VMware-Product-Security.pdf.

The VMware Software Development Lifecycle (SDLC)

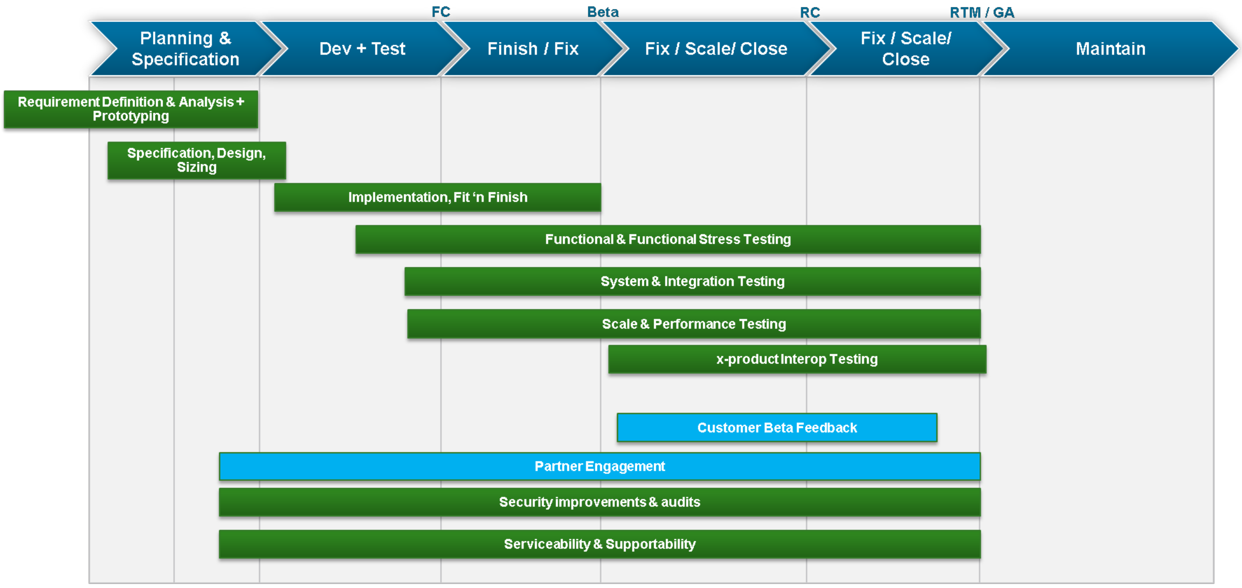
The VMware SDLC defines a clear and repeatable process and creates a structured and organized execution that helps enable us to deliver secure, high-performing products, services, and solutions. The SDLC integrates best practices into the development process so that developers can focus on creating innovative products. It spans the product lifecycle end-to-end, and includes:

- Requirements and product definition
- Development
- Testing
- Legal requirements
- Documentation
- Security
- Performance
- Globalization and Localization
- Release
- Supportability
- Pre-release user testing, including dogfooding (VMware-internal hands-on usage), alpha testing, and beta testing

SDLC processes are executed by cross-functional release teams, and operate following either an agile/scaled agile or waterfall methodology. The processes are:

- Agile, mostly scrum for small and medium-sized product teams
- Waterfall for larger product teams

Oversight is exercised at multiple stages of release planning and execution, and the executive team is actively engaged in approving transitions between release phases.


FC
Beta
RC
RTM / GA
Planning & Specification
Dev + Test
Finish / Fix
Fix / Scale/ Close
Fix / Scale/ Close
Maintain
Requirement Definition & Analysis + Prototyping
Specification, Design, Sizing
Implementation, Fit 'n Finish
Functional & Functional Stress Testing
System & Integration Testing
Scale & Performance Testing
x-product Interop Testing
Customer Beta Feedback
Partner Engagement
Security improvements & audits
Serviceability & Supportability

Release Lifecycle: Key Activities

Ongoing SDLC Dynamics

Current SDLC dynamics reflect the fact that increasingly, teams are looking for ways to accelerate their release cadence and are likewise working on transformations to deliver SaaS. Some SaaS teams are also adopting continuous delivery approaches, deploying smaller increments of capability at a higher frequency (weekly, daily).

Release Life Cycle: Metrics

A powerful tool for communicating and planning, metrics can provide valuable insight into processes, goal attainment, and what the future may hold. At VMware, metrics are at the center of tracking, reporting on and making decisions on releases. Metrics and related goals (release criteria) are locked down as part of release planning, and criteria are defined for each key release milestone. Metrics and criteria are defined by area:

- Testing (Functional, System/Integration, Functional Stress, Interop)
- Scale
- Performance
- Security
- Readiness for Support / Maintenance

Release Life Cycle: Readiness

Finally, prior to release, product/service increments need to comply with a number of mandatory readiness and compliance aspects. Product engineering teams are directly responsible for ensuring this compliance by taking action throughout the release cycle, and audits are conducted at various intervals in the release cycle to validate compliance. Key readiness aspects for product releases include:

- Security compliance
- Open Source license compliance
- EULA / Copyright / Trade Export Compliance
- Globalization / Internationalization
- Usability review
- Accessibility / 508c compliance
- Training / knowledge transfer to field and support personnel

Compliance & Cyber Risk Solutions

Today's government and business executives are familiar with the benefits that come from improving their information technology operations by using server virtualization when moving to the cloud. Those benefits--the ability to respond rapidly, isolate applications from one another during a cyberattack, and maintain business continuity while keeping resource costs low--have been proven. However, executives chartered with maintaining continuous compliance practices continue to be concerned about managing risk, particularly in regulated environments, such as PCI, FedRAMP, FISMA, HIPAA or CJIS.

Assessing risks and then developing adequate controls can be difficult in evolving environments. With complexity comes rising costs: the costs of audits and remediating the findings; the longer time needed to develop and implement new offerings; and the costs of maintaining and operating the environment as new vulnerabilities are discovered.

With this in mind, and in collaboration with the VMware partner ecosystem, VMware has developed the Compliance Reference Architecture Framework (RAF), which allows organizations in regulated IT environments to automate and orchestrate technology and policy enabling more effective cyber risk management. VMware delivers regulation specific guidance, which includes validated compatible software and hardware solutions enabling a Compliant Capable, Audit Ready Platform.

For more information, please visit VMware Compliance and Cyber Risk Solutions, where full compliance Reference Architecture documents for PCI, CJIS, FedRAMP and HIPAA are available. Please contact the Compliance and Cyber Risk Solutions team at compliance-solutions@vmware.com for details on the Compliance and Cyber Risk Solutions Program.

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 of 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 sharing 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. Partners are carefully vetted prior to gaining access to programs.
- Both inbound and outbound contracts with software supply chain security implications are reviewed by Legal and Information 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.

Privacy

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.

Security

As industry exploits attest, security cannot be bolted on just before a project is shipped--it must be an integral part of development from Day One. VMware builds our products with security from the ground up using leading security development tools, processes and methodology. VMware products are built on a comprehensive Security Development Lifecycle (SDL) methodology. Our VMware Security Response Center continuously monitors the security ecosystem and responds quickly to remediate vulnerabilities affecting our products and to mitigate risk for our customers.

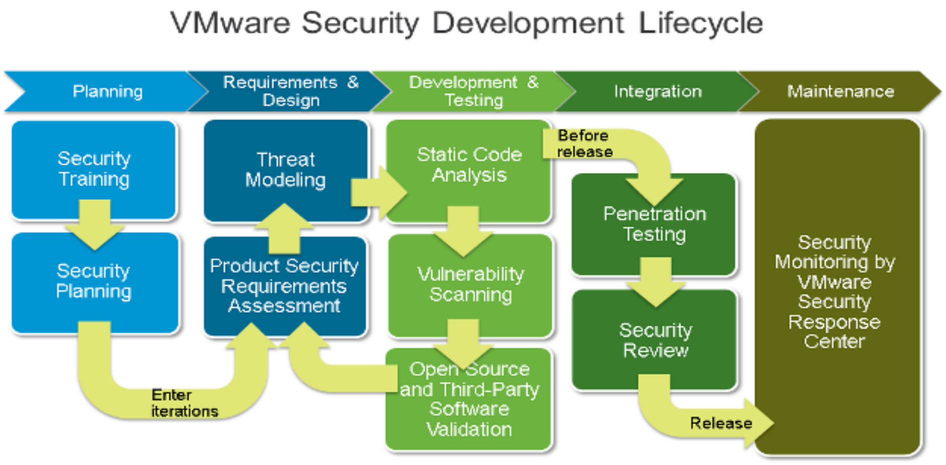
Product Security

VMware's Product Security team, internally known as the vSECR--VMware Security Engineering, Communication and Response--is responsible for protecting the VMware brand from a software security perspective. Its mission is to identify and mitigate security risk in VMware products and services. To achieve this, VMware has established oversight procedures that identify and mitigate potential product security risks throughout the development lifecycle. VMware has likewise 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.

VMware is active in the broader software industry security community, becoming an early member of BSIMM (Building Security In Maturity Model) 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 its Security Evangelism team works to actively cultivate relationships in this community. For example, VMware regularly brings speakers from the research community onto VMware campuses to present technical talks on security topics. VMware also hosts annual two-day internal security engineering conferences at multiple VMware facilities globally which include external security researchers and internal security experts from across the globe.

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 vSECR group owns the definition and practice of SDL processes. It is continuously assessed for its effectiveness at identifying risk and new techniques are added to SDL activities as they are developed and mature.



VMware Security Development Lifecycle

The SDL is the software development methodology promoted by vSECR to help VMware product development groups identify and mitigate security issues early in the lifecycle so that the development group's 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

Security Response Center (VSRC)

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 to investigate reports, coordinate disclosure activities with researchers and other vendors when appropriate, and communicate 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 at major security conferences such as RSA, Black Hat, DEF CON, and CanSecWest, and is involved in the Bay Area security community. 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.

To learn more about the Security Development Lifecycle stages, the Security Response Center, Security Engineering, and Security Certifications, please see the VMware Product Security white paper at http://www.vmware.com/files/pdf/VMware-Product-Security.pdf

IT Information Security

The IT Information Security team maintains a formal, approved, resourced, and robust Information Security Program with the full support of the VMware executive leadership team which protects the Confidentiality, Integrity and Availability of any and all data within the VMware networks and systems.

Industry standard processes and controls are implemented and maintained in an up-to-date and secure manner. These fall into three main areas:

Operational:

- 24x7x365 live monitoring of security events and response
- Robust and thoroughly tested Computer Security Incident Response Team which has dedicated procedures for incident handling involving sensitive information and Breach Notification policies in accordance with applicable state, federal and international laws
- Stateful packet inspection firewalls with appropriate inbound and outbound rule sets
- Signature and anomaly based intrusion detection systems
- Application whitelisting controls on critical servers
- Operational intelligence monitoring for VMware, key partners and vendors and supply chain
- Centralized logging and monitoring with industry standard tools
- Regular patching of systems for security vulnerabilities
- Formal vulnerability management and penetration testing processes
- Whole disk encryption of key laptops and desktops
- Data Loss Prevention processes
- Periodic Third Party testing of the entire VMware infrastructure

Architectural:

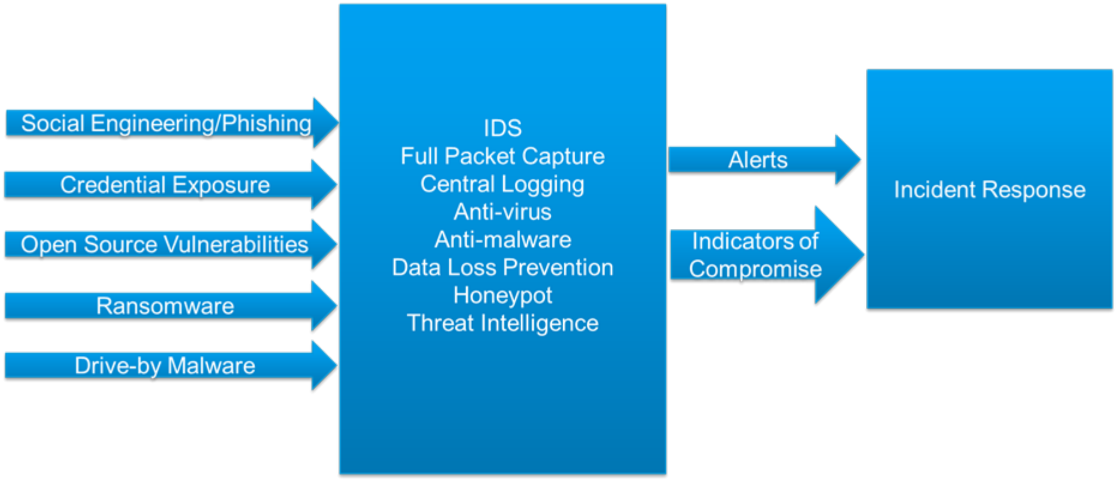
- Design concepts such as Least Privilege, Separation of Duties, and Defense in Depth for Security Controls
- Separation of production and development environments with prohibitions on utilizing production data within development environments
- Multi-factor authentication for remote access

GRC (Governance, Risk and Compliance):

- Policies, procedures, and standards that are reviewed regularly and approved by senior management--such as the Data Classification Policy, Information Security Policy, Incident Response Policy, Remote Access Policy, and password policies requiring regular changing of passwords meeting complexity requirements
- Use of a Service Catalog approach to providing “Information Security as a Service” to the broader organization--definition and scope of each service offered, Service Level Agreements, and associated reporting and metrics
- Information security awareness training for key security topics through various delivery methods – videos, regular email notifications, and in-person events in VMware office locations
- Holistic assessments of risk across VMware and prioritization of risk mitigation efforts based on risk-ranking
- Overall governance of the Information Security Program utilizing a framework based on ISO 27001 principles and including appropriate components all the way from senior or executive management reporting (as well as the Audit Committee to the Board) down to operational metrics capture and dashboards
- Compliance controls design, monitoring and testing for key requirements such as Sarbanes-Oxley, HIPAA, PCI, and FedRamp

The following graphic illustrates VMware IT Information Security measures to address a variety of threats:

Response: VMware Security "Stack"



Social Engineering/Phishing

Credential Exposure

Open Source Vulnerabilities

Ransomware

Drive-by Malware

IDS
Full Packet Capture
Central Logging
Anti-virus
Anti-malware
Data Loss Prevention
Honeypot
Threat Intelligence

Alerts

Indicators of Compromise

Incident Response

Commitment

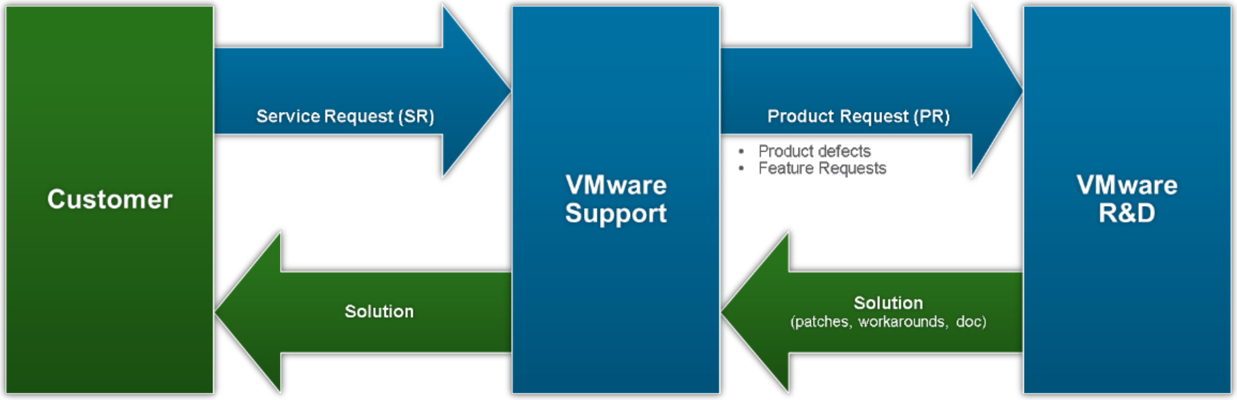
VMware's deep commitment to our customers' success is well represented by strategically aligned teams that focus on addressing issues and enabling infrastructure. We draw upon many resources to help solve our customers' challenges by providing a large, virtualization-specialized, Global Support Services (GSS) organization, and a growing ecosystem of certified solution and technology partners.

Managing Critical Customer Issues

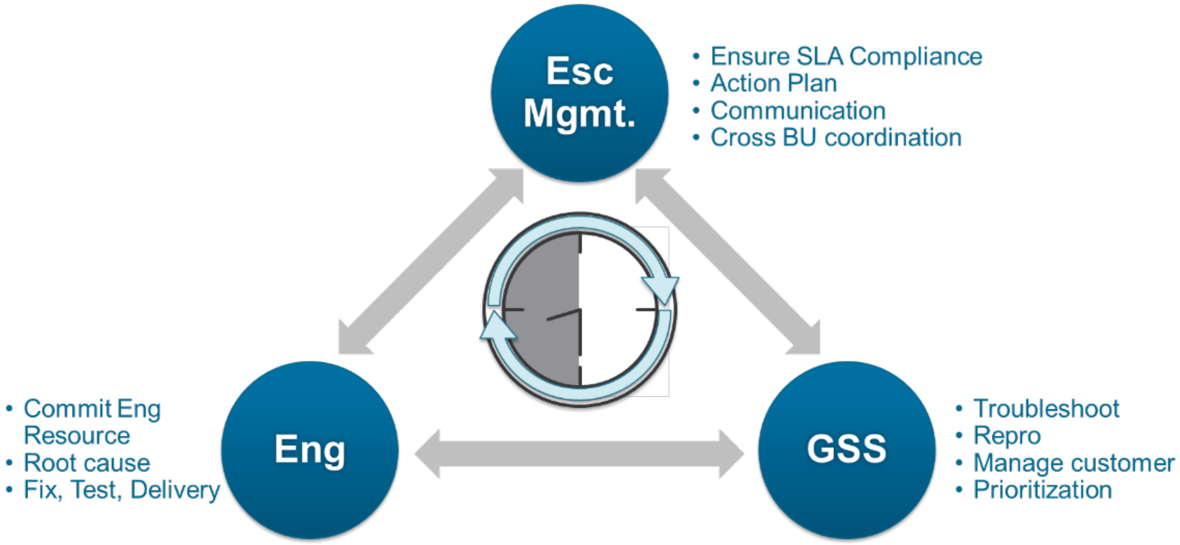
All development organizations provide escalation management along with the dedicated engineering focus to drive customer satisfaction and success through outstanding continuous product development. The following list of service offerings to customers is a value commitment.

Customer Management	Escalation management
	GSS Interface
Customer Engagement	Service Request (SR) –Product Request (PR) handling, 24x7, SLA management
	Repro, Hot Patches
Premier Support	Repro, Hot Patches
	Align with GSS offering
Maintenance Releases	Payload: SR-PRs, Stabilization bugs, GOS Enablement
	Qualify and deliver maintenance releases
Enhanced Maintenance	Incremental product features, HW and SW enablement
	RPQ, Extended Support

The following graphic presents an end-to-end view of supporting customers, illustrating the engineering escalation process and engineering escalation execution:



Engineering Escalation Process

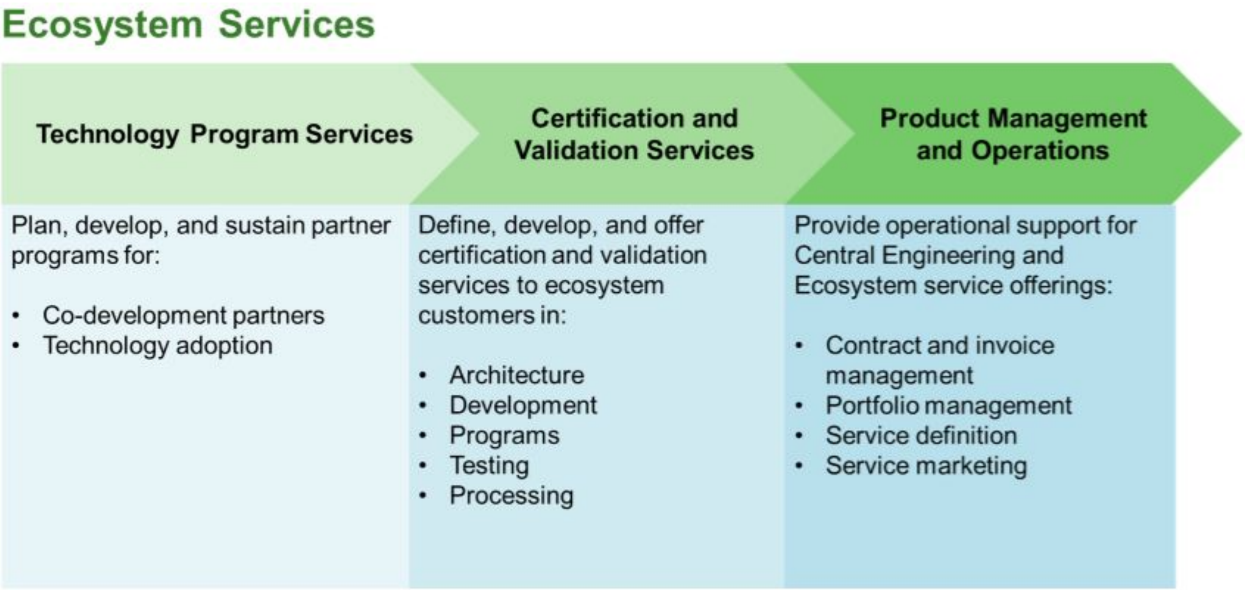


Escalation Execution

Ecosystem Services

The VMware Ecosystem Services team’s vision is to enable a healthy and growing ecosystem that provides a best-in-class cloud services experience for VMware customers. Their programs and practices bring strategic and essential value to our company-wide initiative of engendering customer trust in our products and solutions. This team offers over forty unique programs for over five hundred partner companies worldwide, resulting in more than twelve hundred TAP (Technical Alliance) partners with 13,000+ VMware Certified products.

The Ecosystem Services team’s mission is to accelerate delivery and adoption of quality, compliant, and validated VMware products and services. This involves representing partners internally, VMware representation externally to partners, protecting and promoting the company brand, and optimizing the VMware ecosystem practices, processes, and tools though automation and simplification.



Ecosystem Services

Technology Program Services	Certification and Validation Services	Product Management and Operations
Plan, develop, and sustain partner programs for: • Co-development partners • Technology adoption	Define, develop, and offer certification and validation services to ecosystem customers in: • Architecture • Development • Programs • Testing • Processing	Provide operational support for Central Engineering and Ecosystem service offerings: • Contract and invoice management • Portfolio management • Service definition • Service marketing

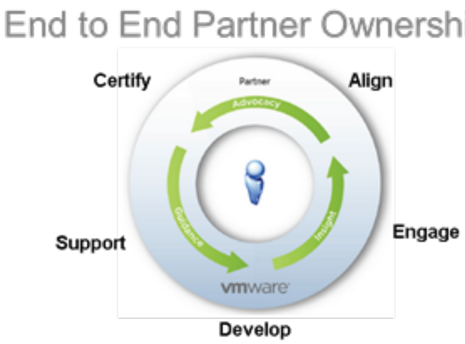
In partnering with the business units, the Ecosystem team's activities cover the full spectrum of support and collaboration. The technical facet of the program encompasses software--SDLC, product knowledge and access (pre-release), and technology enablement with scale.

Partner-facing activities include relationship management, expectation management, and roadmap alignment.

The business imperatives incorporate marketing, pricing and packaging, change management, and contract and legal.

Always critical, the team also oversees scaled communication, processes, and operations as applied to business flows (contracts, payment, support, utilization early access), project management (leadership, metrics), tools (DCPN, VCG, Developer Center, VMware Integration Validation (VIVa) etc.), and Certification.

The Ecosystem team's engagement with partners covers the entire spectrum of activities in the program life cycle:



Customer Advocacy

Why VMware Puts Customers First

Customers are core to VMware's "EPIC2" company values – the "C" stands for our Customers. At VMware, we seek to provide a world class customer experience from the inside out, which begins with a strong customer-centric culture. We aim to empower each employee with the insights, resources, and independence necessary to make choices that are in the best interests of both VMware and its customers. We strive to ensure that each employee understands his or her ability (and responsibility!) to impact the customer experience.

Customer Advocacy

The Customer Advocacy team's focus is to represent the customer, partner and employee voice across the globe to champion a customer-centric culture. This team is laser-focused on the mission to ignite systemic business improvements across VMware that optimize the customer, partner and employee experience.

This team lives by a 'listen + act' philosophy: they deeply value customer input, are always listening, and are driving change based on what VMware customers tell them.

Insights from customers, partners, and employees enable this team to pinpoint strengths and, more importantly, translate those insights into concrete business actions. They seek to understand stakeholder's perspectives and perceptions of the VMware brand, services and solutions through a variety of formal and informal listening posts, including:

- **Live Conversations:** The Customer Advocacy team engages in direct conversations with VMware's customers and partners to better understand how to enable them.
- **The Inner Circle:** The Inner Circle is an online community of select customers & partners, to facilitate rapid cycle research efforts that shape VMware's priorities.
- **Surveys:** The customer, partner and employee voices are fundamental to building VMware's strategy and shaping company priorities. Survey programs enable VMware to consistently listen to stakeholders across the globe.

At VMware we listen, but more importantly we act. Customer Advocacy works directly with VMware's leadership to address improvement opportunities in the areas most critical to customers and partners. Based on recent feedback, we've focused on four key areas to take action:

- **Product Satisfaction:** Focusing on product consistency and functionality to satisfy customer needs
- **Strategy and Product Plans:** Increasing clarity and transparency around our company strategy and product plans
- **Engagement with VMware:** Enhancing sales and services engagements to ensure you get the most out of your VMware relationship
- **Partner Relationship:** Enabling VMware's partners to deliver the best possible solutions to customers

VMware Global Support

VMware Global Support Services (GSS) is the world's largest virtualization support organization with fifteen years of experience supporting complex production and development environments. Working as a comprehensive unit, the team's mission is to provide outstanding levels of technical support using in-depth virtualization and cloud expertise. With support relationships with 100% of the Fortune 100, and 99% of Fortune 500 companies, this team delivers on aggressive resolution times and fast response times. GSS provides global coverage 24/7, 365 days/year, and follow-the-sun support for Severity 1 Issues. This large and important customer base underscores that VMware and our solutions have been widely trusted. It likewise reaffirms that our expert support organization is committed to maintaining and extending this trust into the future.

Conclusion

Due to the ever-increasing complexity of modern infrastructure software, recent high-publicity component vulnerabilities, and high-profile data breaches and privacy concerns, there is a growing need for corporations to be more transparent about their products and processes in order to engender trust with their customers. VMware is meeting and anticipating these rapidly emerging threat trends and increasing customer transparency through the VMware Trust and Assurance framework, which aims at answering the most pressing customer concerns and showcasing why customers can rely on VMware to be their most trusted IT infrastructure vendor.

The programs and practices presented in this document have been designed to create high quality, secure products and solutions that VMware’s customers can trust in the most critical operations of their enterprises. These initiatives have been tuned to advance and adapt to the frontline of our customers’ evolving IT infrastructure needs, and attest to VMware’s continuing commitment to our customers’ success.

Appendix

Privacy Resources

- VMware Privacy Policy: http://www.vmware.com/help/privacy.html
- US-EU Safe Harbor List: https://safeharbor.export.gov/companyinfo.aspx?id=22608
- VMware Safe Harbor Notice: http://www.vmware.com/safeharbor.html

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 VMTA 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 to the development of standards and various Protection Profiles by continuously engaging with various Working Groups (WGs)/NIAP Technical Committees (TCs)/International Technical Committees(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

More Information

For more information about VMware's product security programs and practices, see our Product Security white paper: http://www.vmware.com/files/pdf/VMware-Product-Security.pdf

Customer Advocacy website: https://www.vmware.com/support/customer-advocacy.html

VMware Trust and Assurance website: http://vmware.com/trustvmware

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