VMware vShield 5

General FAQ

Q. Why is VMware developing and selling VMware vShield™ security products?

A. VMware is dedicated to providing a trusted cloud infrastructure while maintaining the benefits of cloud agility. By building virtualized security that is built-in and not "bolted on", VMware enables customers to meet this objective.

Q. Why is the vShield product number now 5.0 when the prior release was 1.0?

A. By aligning with VMware vSphere™ version numbers, it will be easy for customers to know if they are selecting a vShield release that is compatible with their vSphere environment.

Q. What is incrementally new in the vShield 5.0 release relative to the 1.0 release?

A. There are two new products – vShield App with Data Security, and vShield Bundle – as well as numerous capability enhancements:

- vShield App with Data Security (new product) provides visibility into sensitive data stored within virtualized and cloud environments. Using proven Data Loss Prevention (DLP) technology, the solution scans virtualized workloads for sensitive data such as credit card information and reports violations of regulations (such as PCI-DSS), enabling IT organizations to quickly assess the state of compliance with regulations from around the world. Deployment and operation of this solution is optimized for virtual datacenters through use of proven vShield Endpoint technology.
- vShield Bundle (new product) provides vShield Edge, vShield App with Data Security, and vShield Endpoint in one easy to order bundle.
- Adaptive trust zones with Layer 2 firewall protect against password sniffing, dynamic host configuration protocol (DHCP) snooping/poisoning attacks, address resolution protocol (ARP) spoofing, and more.
- Flexible IP addressing, including the ability to use the same IP address in multiple tenant zones, simplifies provisioning without requiring that applications be reconfigured.
- Application-aware firewalling improves security by only opening ports and sessions when needed for common applications, such as Oracle DB, MS Exchange, and MS RPC.
- Role-based access control (RBAC) enables clear separation of workflow for virtual infrastructure and security administrators. RBAC provides flexibility in delegating administration across resource pools and security groups, improving security of applications and data.

Q. What is the migration path for vShield release 1.0 products to 5.0?

A. vShield 1.0 customers who are current on their support agreements will be able to download and use vShield 5.0 on or after General Availability. For more information on technical requirements for upgrade, please refer to respective product documentation.

Q. Are there upgrade paths between the different vShield products?

A. Yes. For customers who have transitioned to the 5.0 release, the following upgrade SKUs are available:

SKU	UPGRADE PATH
VS-VCD-EG5-UG-C	Upgrade: VMware Cloud Director to vShield Edge 5 (25 VM Pack)
VS-EP5-APDS5-UG-C	Upgrade: VMware vShield Endpoint 5 to vShield App 5 with Data Security (25 VM Pack)
VS-EP5-AP5-UG-C	Upgrade: VMware vShield Endpoint 5 to vShield App 5 (25 VM Pack)
VS-APP-APDS-UG-C	Upgrade: VMware vShield App 5 to vShield App 5 with Data Security (25 VM Pack)

Q. Are there any downgrade options available in case of software or hardware incompatibilities?

A. There is no specific downgrade guidance, but VMware is providing a compatibility matrix between the previous vShield components and the new vShield 5.0 components.

Product Functionality FAQs

Q. Does vShield App with Data Security quarantine the file and/or the VM that is out of compliance?

A. This solution doesn't currently provide a user interface to define policy that would automatically move a non-compliant virtual machine into a quarantine zone. Creation of quarantine zones has been supported since vShield 1.0, where vShield App can be used to create custom groupings (or zones) of virtual machines and then apply firewall rules to these zones.

As of vShield 5.0, there are two options for moving virtual machines into quarantine zones:

- Administrator manually moves the non-compliant virtual machine into a quarantine zone, using the vShield App UI.

- Administrator runs scripts using vShield App with Data Security REST APIs to move these non-compliant virtual machines into quarantine zones. For further automation, two other VMware solutions can be leveraged:
  - VMware vCenter™ Configuration Manager can be used to check data security scan results for non-compliant virtual machines.
  - vSphere Orchestrator can then be used to automate the movement of these virtual machines to the quarantine zones.

Q. Can viruses discovered with an antivirus solution running with vShield Endpoint be either quarantined or deleted?

A. The ability to quarantine or delete a virus, or other malware, is determined by the partner antivirus solution. vShield Endpoint provides the necessary integration options to partner solutions to enable these actions.

Q. Which types of files can – and cannot – be scanned by vShield App with Data Security?

A. In general, file types in common use by organizations can be scanned, such as .doc, .xls, .pdf, .txt, .zip and more. For a more detailed list of which file types are supported, please refer to the product documentation.

Q. What is the relative positioning of vShield App with Data Security and vCenter Configuration Manager (vCM)? Are both needed? For what use cases?

A. vCM is not required but can be used for control of selected functions. For example, when a scan performed using Sensitive Data Discovery identifies a resource that violates a policy (e.g., a file with unencrypted credit card numbers), vCM can be used to identify this policy violation and report it through a broader set of compliance reporting features. Think of vShield App with Data Security as implementing the control (scan for sensitive data) and vCM as aggregating this control with other controls to provide more comprehensive IT compliance reporting.

Q. What management tools are provided with the vShield products?

A. Each vShield product is managed by vShield Manager, which is included with the purchase of any vShield product.

Q. Where are more detailed, product-specific FAQs available?

A. See the public web for the vShield products http://www.vmware.com/products/vshield/overview.html. Go to the product of interest, then click on the FAQ section.

Pricing and Licensing FAQs

Q. How is the product licensed?

A. All vShield products are licensed on a per VM basis, in increments of 25 VMs in a license.

Q. How is the number of VMs to be licensed determined?

A. Each protected VM requires a license. For example, if vShield Edge protects the periphery of a port group, then all VMs within that port group need a vShield Edge license. Similarly, the number of vShield App with Data Security licenses required is based on the number of VMs that will be scanned for sensitive data.

Q. Can the Trend Micro Deep Security solution for vShield Endpoint be purchased from VMware?

A. The Trend Micro Deep Security Anti-malware product is purchased from Trend Micro or its sales channel partners; it is not sold by VMware.

Q. For customers that currently have Trend Micro Deep Security licenses, how do they transition to using their licenses with vShield Endpoint?

A. Please contact Trend Micro, or an authorized reseller, for details.

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