VMware vShield

Virtualization-Aware Security for the Cloud

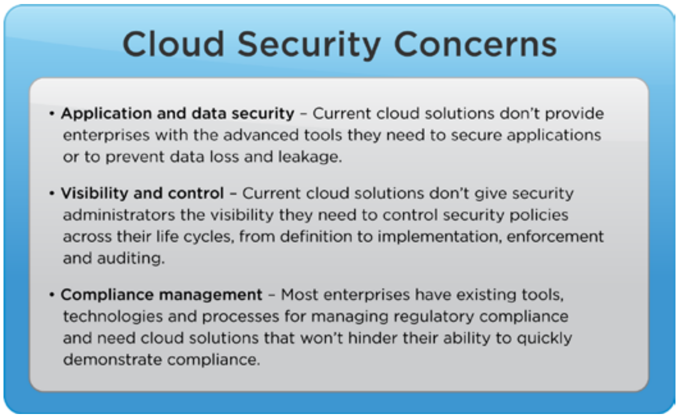
BROCHURE

At a Glance

For organizations that want to leverage the benefits of cloud computing without sacrificing security, control or compliance, the VMware vShield family of security solutions provides comprehensive protection for virtual datacenters and cloud environments. vShield enables customers to strengthen application and data security, improve visibility and control, and accelerate IT compliance efforts across the organization.

Cloud Security Challenges

Many organizations are considering cloud computing solutions and services as a way to increase agility and reduce the cost of owning and operating IT. However, the recent customer surveys on cloud computing unanimously cite security, control and compliance as the primary concerns preventing adoption. Consequently, organizations are looking for ways to address these issues so they can leverage the benefits of cloud computing without compromising security, control or compliance management efforts.



Cloud Security Concerns

- **Application and data security** – Current cloud solutions don't provide enterprises with the advanced tools they need to secure applications or to prevent data loss and leakage.
- **Visibility and control** – Current cloud solutions don't give security administrators the visibility they need to control security policies across their life cycles, from definition to implementation, enforcement and auditing.
- **Compliance management** – Most enterprises have existing tools, technologies and processes for managing regulatory compliance and need cloud solutions that won't hinder their ability to quickly demonstrate compliance.

Secure the Cloud with VMware vShield

Just as virtualization is indispensable for transitioning legacy applications to new cloud infrastructure, it is a key security enabler for cloud environments. As the global leader in virtualization, VMware has delivered secure, reliable virtualization solutions for more than a decade. Today, VMware is helping customers unlock the benefits of cloud computing with the new VMware vShield family of security products for virtual datacenters and private clouds.

Key Benefits

Go Beyond the Limitations of Physical Security

vShield provides adaptive security that travels with virtual machines as they migrate from host to host so that customers can securely support the virtual machines in dynamic cloud environments. This approach also helps to ensure that applications run efficiently within cloud environments while maintaining trust and network segmentation of users and sensitive data.

Improve and Simplify Security Management in a Single Framework

vShield provides a single comprehensive framework for securing virtual datacenters and cloud environments at all levels—host, network, application, data and endpoint. vShield ensures that the proper segmentation and trust zones are enforced for all application deployments on VMware-based clouds. vShield also provides a comprehensive set of capabilities to introspect and protect hosts and virtual machines. These capabilities, along with trusted solutions from VMware partners, ensure that VMware-based clouds provide the strongest possible protection for applications and data.

Reduce Complexity and Eliminate Bottlenecks

vShield helps to reduce the complexity of virtualization security by enabling customers to consolidate their security infrastructures and eliminate the sprawl associated with software agents, security policies, dedicated security appliances and air-gap solutions. vShield also prevents bottlenecks associated with endpoint security agents by eliminating the need to install antivirus software on individual virtual machines.

Improve Visibility and Accelerate Compliance

vShield leverages the unique introspection capabilities of the VMware vSphere™ platform to help identify hard-to-detect problems precisely and efficiently. vShield also enables controls such as file integrity monitoring, rootkit protection and data leak prevention, and helps to accelerate compliance efforts with detailed logging that can be exposed to existing auditing and IT compliance management solutions.

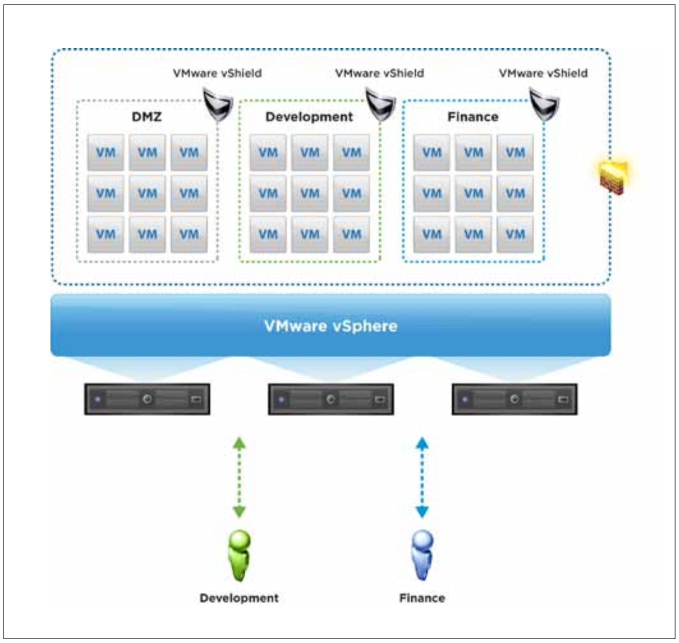
Leverage Existing Security Solutions

vShield is designed to work seamlessly with existing enterprise IT security measures through REST APIs that allow for customized integration of vShield capabilities into third-party security solutions. In addition, vShield includes an endpoint security API that enables integration with existing antivirus and anti-malware solutions, and interfaces into broader security solutions for security information and event management, data leak protection, change and configuration management, and auditing.

Using VMware vShield

Secure Business-Critical Applications

vShield solutions make it easy for customers to support applications belonging to different trust levels on the same virtual datacenter (e.g., production and development, finance and sales, classified and nonclassified applications, etc.). The hypervisor-level firewall in vShield ensures that proper segmentation and trust zones are enforced for all application deployments.

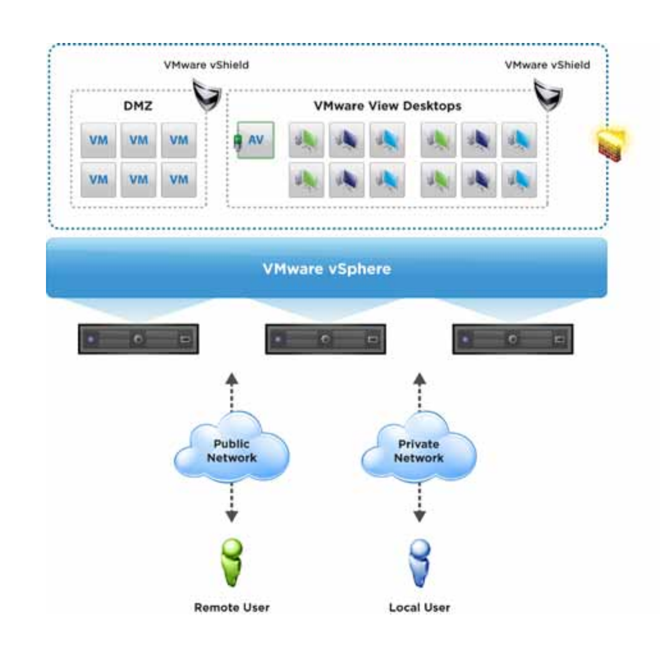


VMware vShield lets customers create business-based security groups and protect critical applications from network-based threats.

Secure Virtual Desktop Deployments

vShield integrates with VMware View™ to provide more efficient antivirus and anti-malware protection for virtual endpoints and applications by offloading antivirus and anti-malware functions from individual virtual machines to a secure virtual machine that protects the host and all virtual machines on it. This approach streamlines security management and provides added protection against antivirus storming, performance bottlenecks and botnet attacks.

vShield also helps organizations create logical security perimeters around virtual desktop infrastructures through complete network isolation and an array of network gateway services such as firewalls, VPN and DHCP.



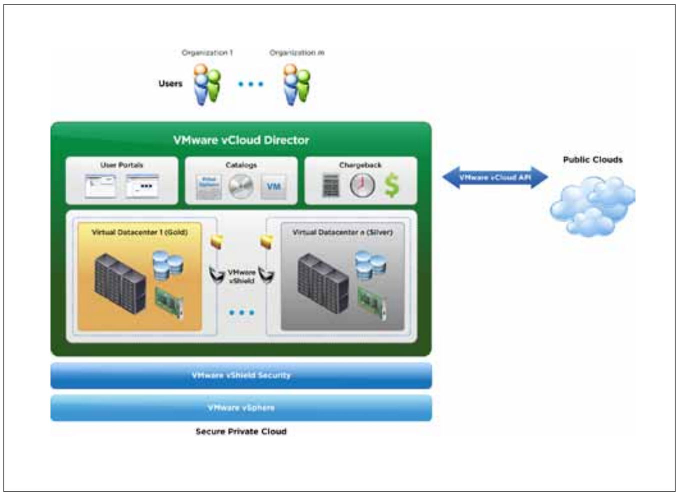
VMware vShield optimizes antivirus and anti-malware security for virtualized environments through a security virtual machine (provided by VMware partners).

Enterprise Partner Extranets

vShield lets enterprises extend their networks and application resources to branch offices, home offices and business partner sites through site-to-site VPN services that offer simplified provisioning, streamline administrative tasks and improve scalability. All traffic between sites is encrypted using IPsec to maintain the confidentiality and integrity of all site-to-site communications.

Secure Multi-Tenant Environments

vShield solutions make it easy for enterprises and cloud service providers to support multi-tenant IT environments and safely share network resources by creating logical security boundaries that provide complete network isolation for virtual datacenters. vShield also provides granular control and visibility over network gateway traffic, along with VPN services to protect the confidentiality and integrity of communications between virtual datacenters.



VMware vShield integrates with VMware vCloud Director to ensure security and network isolation in multi-tenant private clouds.

vShield Solutions

VMware vShield App

VMware vShield App protects applications in the virtual datacenter from network-based threats. vShield App gives organizations the ability to create and manage business-relevant policies that adapt to dynamic cloud environments. It also provides deep visibility into network communications between virtual machines and granular enforcement through security groups.

VMware vShield Edge

vShield Edge is a network gateway solution that protects the edges of the virtual datacenter with DCHP, network address translation, firewalling, load balancing, site-to-site VPN, port group isolation and other capabilities that help organizations maintain proper segmentation between different organizational units.

VMware vShield Endpoint

vShield Endpoint provides on-host antivirus and malware protection that reduces performance latency and eliminates the need to maintain individual security agents in each and every virtual machine, helping to simplify security administration while minimizing the risk of malware infections.

VMware vShield Manager

Included with all vShield products, vShield Manager provides a central point of control for managing, deploying, reporting, logging and integrating third-party security services. Working in conjunction with vCenter Server, vShield Manager also enables role-based access control and administrative delegation as part of a unified framework for managing virtualization security.

VMware vShield Zones

VMware vShield Zones, included with vSphere, provides basic protection from network-based threats in virtual datacenters, with application firewalling and policy management based on administrator-defined zones, using basic traffic information such as the source IP address, the destination port, and so on.

How to Buy

vShield App, vShield Edge and vShield Endpoint are available for purchase as standalone products. vShield Manager is included with all three solutions. VMware vShield Zones is available as a built-in feature of VMware vSphere.

Support and Services

VMware offers basic and production Subscription and Support (SnS) for all VMware vShield customers. Support for third-party antivirus and anti-malware solutions that leverage VMware vShield Endpoint is provided by the solution providers.

Find Out More

For information or to purchase VMware products, call 877-4-VMWARE (outside of North America dial 650-427-5000), visit www.vmware.com/products, or search online for an authorized reseller. For detailed specifications and systems requirements, refer to the VMware vShield documentation.

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