VMware vShield

The Foundation for Trusted Cloud Infrastructures

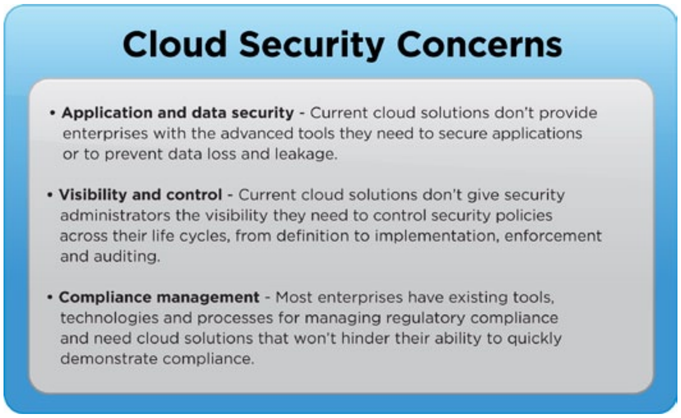
BROCHURE

At a Glance

For organizations looking 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 organizations to strengthen application and data security by providing protection against network intrusions, improving the performance of virus and malware protections for endpoints by more than an order of magnitude, improving visibility and control of sensitive data, and accelerating IT compliance across the enterprise.

Cloud Security Challenges

Many organizations are considering a cloud computing approach to increase agility and reduce costs. However, recent customer surveys on cloud computing unanimously cite security, control and compliance as the primary concerns preventing adoption. Consequently, organizations are seeking ways to address these issues so that they can leverage the benefits of cloud computing without compromising how they manage security, control or compliance.



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 Your 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. The global leader in virtualization and cloud infrastructure, VMware® has delivered secure, reliable virtualization solutions for more than a decade. Today, VMware is helping to unlock the benefits of cloud computing with the new VMware vShield family of security products for virtual datacenters and cloud environments. Only VMware enables your enterprise to adopt a cloud model that addresses your unique business challenges so that you can deliver the most important cloud—your cloud—securely.

Key Benefits

Go Beyond the Limitations of Physical Security

vShield solutions provide adaptive security that travels with virtual machines as they migrate from host to host so that enterprises can securely support their 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

Through a single, comprehensive framework, vShield secures virtual datacenters and cloud environments at all levels—host, network, application, data and endpoint. It helps to ensure that the proper segmentation and trust zones are enforced for all application deployments on VMware based clouds. vShield, together with the introspection capabilities of the VMware vSphere® platform, provide a complete set of capabilities to protect hosts and virtual machines. These features, along with trusted solutions from VMware partners, mean that VMware based clouds provide the strongest possible protection for applications and data.

Reduce Complexity and Eliminate Anti-Virus "Storms"

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

Protect Applications and Accelerate IT Compliance

vShield protects applications in the virtual datacenter from network-based attacks. Organizations gain visibility and control over network communications between virtual machines. Policy enforcement is agile, since it is based on logical constructs, including VMware vCenter™ containers and vShield security groups, and not just physical constructs such as IP address. vShield scans for sensitive data, such as credit card numbers, across virtualized resources. Policy violations are reported, enabling IT organizations to quickly assess the state of compliance with regulations from across the world.

Leverage Existing Security Solutions

vShield is designed to work seamlessly with existing enterprise IT security measures through Representational State Transfer (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, as well as interfaces into broader security solutions for security information and event management, data leak protection, change and configuration management and auditing.

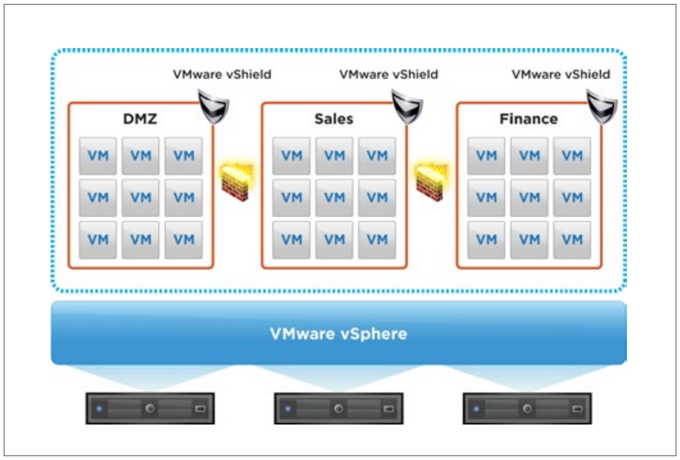
Using VMware vShield

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.

Secure Virtual Desktop Deployments

Through integration with VMware View™, vShield enables more efficient antivirus and anti-malware protection for virtual endpoints and applications. It does so by offloading antivirus and anti-malware functions from individual virtual machines to a secure virtual appliance that protects the host and all virtual machines on it. This approach streamlines security management and provides added protection against antivirus "storms," performance bottlenecks and botnet attacks.



VMware vShield allows organizations to create business-based security groups and protect critical applications from network-based threats.

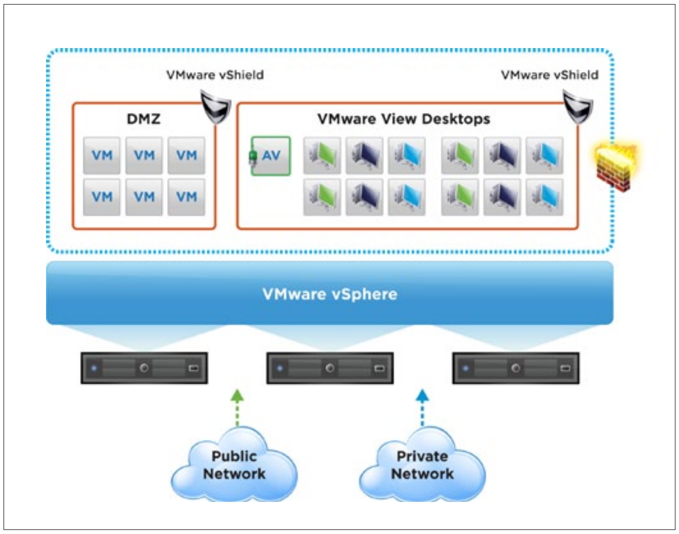
vShield also helps organizations to create logical security perimeters around virtual desktop infrastructure through complete network isolation and an array of network gateway services, such as firewalls, virtual private networks (VPNs) and dynamic host configuration protocol (DHCP).

Reduce Risk of Non-Compliance with Sensitive Data Discovery

Organizations can use vShield App with Data Security to accurately discover and report sensitive data in unstructured files. With more than 80 predefined templates for country- and industry-specific regulations, it quickly identifies and reports sensitive data exposures. In addition, it improves performance by offloading data discovery functions to a virtual appliance.

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 zones 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.



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

vShield Solutions

vShield Edge

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

vShield App with Data Security

vShield App with Data Security protects applications and data in the virtual datacenter from network-based threats. It 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. Discovery of unencrypted sensitive data, such as a credit card numbers, that might be stored in files resident in virtual machine containers is included. Administrators can meet regulatory compliance audits by using it to scan datacenters, clusters or resource pools for the presence of sensitive data. Administrators can use REST APIs to quarantine infected files.

vShield Endpoint

vShield Endpoint strengthens security for virtual machines while improving performance for endpoint protection by orders of magnitude. vShield Endpoint offloads antivirus and anti-malware agent processing to a dedicated secure virtual appliance delivered by VMware partners. The solution is designed to leverage existing investments by allowing organizations to manage antivirus and anti-malware policies for virtualized environments with the same management interfaces that they use to secure physical environments.

vShield Bundle

vShield Bundle includes the following products in the vShield family: vShield Edge, vShield App with Data Security, vShield Endpoint and vShield Manager.

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 enables role-based access control and separation of duties as part of a unified framework for managing virtualization security.

vShield Zones

vShield Zones, included with vSphere, provides basic protection from network-based threats in virtual datacenters. It delivers 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.

Supported Releases

For information about supported releases of vSphere, ESX and VMware View environments, please visit www.vmware.com/products.

How to Buy

vShield Edge, vShield App with Data Security, vShield Endpoint and vShield Bundle (which incorporates three vShield products) are available for purchase as standalone products. vShield Manager is included with each of the vShield products. vShield Zones is available as a built-in feature of vSphere.

Support and Services

VMware offers basic and production Subscription and Support (SnS) for all vShield customers. Support for third-party antivirus and anti-malware solutions that leverage 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