

VMware vShield App

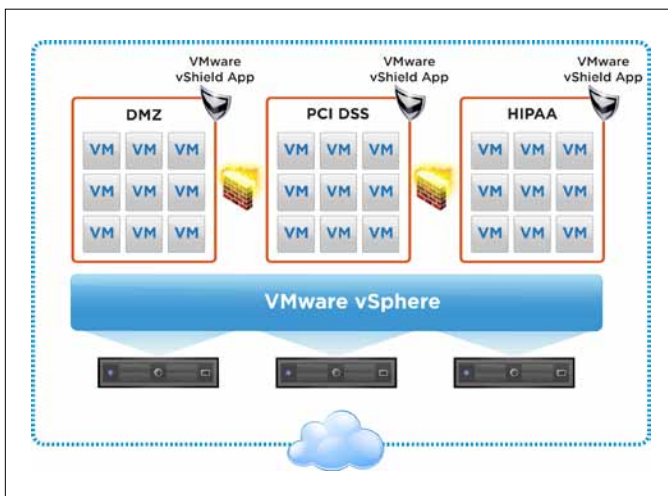
Protect Applications from Network-Based Attacks

AT A GLANCE

VMware vShield™ App, part of the VMware vShield family of virtualization security products, 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, because it is based on logical constructs such as VMware vCenter™ containers and vShield security groups—not just physical constructs such as IP addresses. vShield App eliminates dependence on hardware and legacy controls such as VLANs, resulting in reduced hardware and policy sprawl that is cost-effective and goes beyond the limitations of physical security. Also included is VMware vShield Endpoint, which offloads antivirus file scanning, minimizing antivirus “storms.”

KEY BENEFITS

- Increase visibility and control over network communications between virtual machines.
- Eliminate the need for dedicated hardware and VLANs to separate security groups from one another.
- Optimize hardware resource utilization while maintaining strong security.
- Simplify compliance through comprehensive logging of all virtual machine network activity.



vShield App enables granular policy enforcement using security groups.

What is vShield App?

vShield App is a hypervisor-based application-aware firewall solution for virtual datacenters. Administrators can meet regulatory compliance audits by using this product to scan datacenters, clusters or resource pools for sensitive data.

The product plugs directly into VMware vSphere® to protect against internal network-based threats and reduce the risk of policy violations within the corporate security perimeter. To accomplish this, vShield App uses application-aware firewalling with deep packet inspection and connection control based on source and destination IP addresses.

It also simplifies policy control by enabling IT to rapidly create business-relevant security groups, and its flow-monitoring controls help IT analyze virtual machine network traffic and dynamically enforce security group policies. Administrators can centrally manage vShield App through the included vShield Manager console, which integrates seamlessly with VMware vCenter Server to facilitate unified security management for virtual datacenters.

The product also eliminates dependence on hardware and legacy controls such as VLANs, resulting in reduced hardware and policy sprawl that is cost-effective and goes beyond the limitations of physical security.

How Does vShield App Work?

vShield App installs on each vSphere host, controlling and monitoring all network traffic on the host, even for packets that never cross a physical network interface card (NIC). vShield App can create and enforce policies based on administrator-defined, business-relevant security groups instead of physical boundaries or static assumptions about application deployments.

It also provides a centralized interface that leverages vCenter Server to consistently apply these policies across multiple vSphere hosts in the virtual datacenter.

How is vShield App Used?

- **Provide application-aware protection** – Administrators can define and enforce granular policies for all traffic that crosses a virtual NIC, increasing visibility over internal virtual datacenter traffic while helping to eliminate detours to physical firewalls.
- **Maintain change-aware protection** – Firewall protection is continuous as virtual machines migrate from host to host, helping to ensure that network topology changes do not impact application security.

- **Efficiently manage dynamic policies** – Administrators have a rich context for defining and refining internal firewall policies as business needs evolve over time.
- **Reduce botnet risks** – Security administrators can protect against botnets and other attacks by dynamically allocating ports to trusted applications.
- **Control access to shared resources** – Security administrators can restrict access to shared services such as storage and backup on vSphere hosts according to IP address.
- **Accelerate IT compliance** – Visibility and control over virtual machine network security increases, and logging and auditing controls enable enterprises to demonstrate compliance with internal policies and external regulatory requirements.

Key Features

Firewalls

- Hypervisor-level firewall provides inbound and outbound connection control enforced at the virtual NIC level through hypervisor inspection, supporting multihomed virtual machines.
- Layer 2 firewall (also known as a transparent firewall) protects against multiple types of attacks, such as password sniffing, DHCP snooping, Address Resolution Protocol (ARP) spoofing or poisoning attacks. It also provides complete isolation of SNMP traffic.
- Protection can be enforced according to network, application port, protocol type (TCP, UDP) or application type.
- Protection is dynamic as virtual machines migrate.
- IP-based stateful firewall and application layer gateway supports a broad range of protocols, including Oracle, Sun Remote Procedure Call (RPC), Microsoft RPC, LDAP and SMTP. The gateway improves security by opening sessions (ports) only as needed. For a complete list of supported protocols, see the VMware vShield Administration Guide.

Flow Monitoring

- Administrators can observe network activity between virtual machines to help define and refine firewall policies, identify botnets, and secure business processes through detailed reporting of application traffic (application, sessions, bytes).

Security Groups

- Administrators can define business-relevant groupings of any virtual machines by their virtual NICs.

Policy Management

- vShield Manager provides control of product features, many of which are also accessible through the vCenter Server interface.
- Administrators can enforce policies on security groups, vCenter Server groupings and TCP-5 tuple (source IP, destination IP, source port, destination port, protocol).
- Representational State Transfer (REST) APIs provide a programmable interface for management and policy enforcement.
- vShield App supports integration with enterprise security management tools.

IP Addressing

- Flexible IP addressing includes the ability to use the same IP address in multiple tenant zones to simplify provisioning.

Logging and Auditing

- Logging is based on industry-standard syslog format.
- REST APIs and vShield Manager provide access to logging and auditing tools.
- Administrator defines logging on and off for firewalls at rule level.

Supported Releases

For information on supported releases of vSphere environments, visit <http://vmware.com/products>.

Related Products

The vShield family of security products also includes VMware vShield Edge for perimeter security; vShield App with Data Security for discovery of sensitive data; vShield Endpoint for enhanced endpoint security and performance; vShield Manager; and vShield Bundle, which includes all products.

Find Out More

For information or to purchase VMware products, call 877-4-VMWARE (outside North America, +1-650-427-5000), visit <http://www.vmware.com/products>, or search online for an authorized reseller. For detailed product specifications and system requirements, refer to the VMware vShield Administration Guide at http://www.vmware.com/pdf/vshield_41_admin.pdf.

For additional information on vShield products, visit <http://vmware.com/products>.

