VMware vShield Bundle

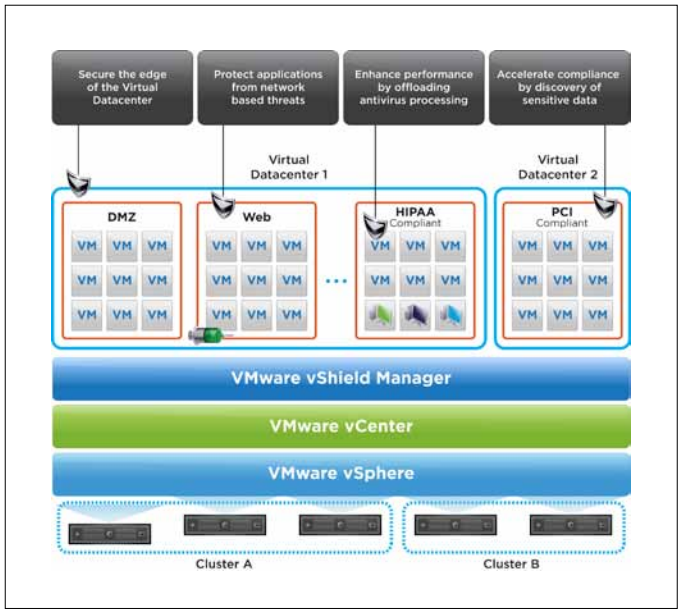
The Foundation for Trusted Cloud Infrastructures

AT A GLANCE

VMware vShield™ Bundle is the foundation for trusted cloud infrastructures. vShield Bundle delivers integrated, adaptive and cost-effective security services and management that protect virtual datacenters and cloud environments at all levels—network edge, applications and data, and endpoint. vShield Bundle works in concert with VMware vSphere®, VMware vCenter™ Server and VMware vCloud™ Director.

KEY BENEFITS

- Secure virtual datacenters and cloud environments at all levels—network edge, applications and data, and endpoint
- Reduce cost and complexity
- Eliminate antivirus and anti-malware "storms" via agentless deployment
- Reduce risk of non-compliance and reputation damage by discovery of sensitive data
- Adaptive trust zones to form groups of applications and data that have common security policy and access requirements



VMware vShield enables granular policy enforcement using security groups.

Overview of VMware vShield Bundle Functionality

vShield Bundle offers better than physical security for virtualized datacenters. It brings together the advanced capabilities of four vShield products to deliver integrated, adaptive and cost-effective security services and management that protect virtual datacenters and cloud environments from the network edge to applications and data through to endpoints.

Network Edge

With its edge network security solution to protect the perimeter of virtual datacenters, vShield Bundle provides essential security capabilities such as network security gateway services and Web load balancing for performance and availability. The solution plugs directly into VMware vSphere and leverages built-in features including fault tolerance and high availability for unparalleled resiliency.

vShield Bundle also works in concert with VMware vCloud Director to automate and accelerate the secure provisioning of virtual datacenters in multitenant cloud infrastructures. Separation of duties for security and virtual infrastructure administrators limits access only to authorized resources.

Deployed as a virtual appliance, vShield Bundle provides network security gateway functions such as firewall, virtual private network (VPN), Web load balancer, network address translation (NAT) and dynamic host configuration protocol (DHCP) services to monitor packet headers for source and destination IP addresses. Depending on policy, it can deny or allow connections, initiate and terminate VPN sessions, perform network address translation or inspect data by source-destination port and protocol type (transmission control protocol [TCP] or user datagram protocol [UDP]).

Applications and Data

vShield Bundle provides a hypervisor-based, application-aware firewall solution for virtual datacenters. It enables dynamic discovery of sensitive data, such as credit card data, that might be stored in unstructured data files resident in virtual machine containers. Administrators can meet regulatory compliance audits by using this product to scan datacenters, clusters or resource pools for the presence of sensitive data.

The product plugs directly into vSphere to protect against internal, network-based threats and reduce the risk of policy violations within the corporate security perimeter. It does so by using application-aware firewalling with deep packet inspection and connection control based on source and destination IP addresses. It also simplifies policy control by enabling administrators to rapidly

create business-relevant security groups. vShield Bundle creates and enforces policies based on administrator-defined, business-relevant security groups instead of physical boundaries or static assumptions about application deployments. It includes flow monitoring to analyze virtual machine network traffic and dynamically enforce security group policies.

vShield Bundle provides an administrator console for policy management of sensitive data discovery. A "policy" is created by selecting applicable regulations to scan across target virtual machine containers—datacenters, clusters and resource pools. Files to scan can be further filtered by file extension, size or date modified. Scan outputs include the identification of datacenter, cluster, virtual machine and file names that are not compliant with the selected policies. Administrators can use Representational State Transfer (REST) APIs to remediate non-compliant files.

Endpoint

The endpoint solution uses a revolutionary architectural approach to optimize antivirus, sensitive data discovery and other endpoint security capabilities delivered by VMware partners for use in vSphere and VMware View™ environments.

For antivirus implementations, vShield Bundle improves performance by offloading antivirus scanning activities to a secure virtual appliance that has a scanning engine, as well as the stored antivirus file signatures. For antivirus and anti-malware functions, this architecture eliminates the software agent footprint in virtual machines, frees system resources, improves performance and eliminates the risk of antivirus "storms" (overloaded resources during scheduled scans and signature updates). Since the secure virtual appliance does not go offline, it is able to continuously update antivirus signatures, providing continuous protection to the virtual machines on the host. In addition, new virtual machines are immediately protected with the most current antivirus signatures. With vShield Bundle, virtual infrastructure administrators have a vastly reduced set of tasks since there are no antivirus agents in each virtual machine to manage. Instead, administrators use the partner's management console to manage the secure virtual appliance. This approach avoids the need for frequent updates to be administered per virtual machine.

Enhancing security with a hardened, tamper-proof secure virtual appliance (delivered by VMware partners) that leverages the robust and secure hypervisor introspection capabilities in vSphere, vShield Bundle reduces the vulnerability of the antivirus and anti-malware service itself.

vShield Bundle also provides VMware partner companies with interfaces to implement file, memory and process scanning. The architecture supports multiple security solutions simultaneously, such as sensitive data discovery in one secure virtual appliance and an antivirus solution in another secure virtual appliance.

Organizations can demonstrate compliance and satisfy audit requirements through detailed activity logging from the antivirus or anti-malware service.

Management

Administrators centrally manage vShield Bundle through the included management console, vShield Manager. It integrates seamlessly with VMware vCenter Server to facilitate unified security management for virtual datacenters.

How is vShield Bundle Used?

vShield Bundle is deployed to deliver security services and management that protect virtual datacenters and cloud environments at all levels.

Network Edge

vShield Bundle includes a comprehensive set of edge network gateway security solutions that provide essential capabilities to

- **Consolidate edge security hardware** – Provision edge security services using existing vSphere resources, eliminating the need for purpose-built hardware appliances to "air gap" vSphere hosts.
- **Rapidly and securely provision virtual datacenter perimeters** – Easily create secure, logical, hardware-independent perimeters ("edges") around virtual datacenter environments, making it easier to leverage shared network resources in multitenant IT infrastructures.
- **Protect data confidentiality over shared networks** – Provide a site-to-site VPN with 256-bit encryption to protect the confidentiality of all data transmitted across virtual datacenter perimeters.
- **Ensure performance and availability of Web services** – Efficiently manage inbound Web traffic across virtual machine clusters and use Web load balancing capabilities that can be deployed with edge security or on their own.
- **Facilitate compliance management** – Deploy the necessary controls, such as detailed event logging and flow statistics, needed to demonstrate compliance with corporate policies, as well as industry and government regulations.

Applications and Data

vShield Bundle includes an application aware firewall that can be used to

- **Meet data compliance audits on virtualized hosts** – Perform scans, invoked manually or programmatically via REST APIs, to validate compliance with selected policies.

- **Provide application-aware protection** – Define and enforce granular policies for all traffic that crosses a virtual network interface card (NIC), increasing visibility over internal virtual datacenter traffic while helping to eliminate detours to physical firewalls.
- **Maintain change-aware protection** – Establish continuous firewall protection for virtual machines as they migrate from host to host to help ensure that network topology changes do not impact application security.
- **Efficiently manage dynamic policies** – Simplify policy definition and provide administrators with a rich context for defining and refining internal firewall policies as business needs evolve over time.
- **Reduce botnet risks** – Protect against botnets and other attacks by dynamically allocating ports to trusted applications.
- **Control access to shared resources** – Allow security administrators to restrict access based on IP address to shared services, such as storage and backup, on vSphere hosts.
- **Accelerate IT compliance** – Increase visibility and control over virtual machine network security with the logging and auditing controls needed to demonstrate compliance with internal policies and external regulatory requirements.

Endpoint

vShield Bundle includes endpoint capabilities that

- **Streamline antivirus and anti-malware deployment** – Deploy the enterprise antivirus engine and signature file only to a single secure virtual appliance instead of on every individual virtual machine on a vSphere host.
- **Improve virtual machine performance** – Securely achieve higher consolidation ratios by offloading activities such as antivirus and anti-malware agents scans from individual virtual machines to a single secure virtual appliance on each vSphere host.
- **Prevent antivirus "storms" and bottlenecks** – Implement antivirus and anti-malware scans and updates on a single secure virtual appliance to prevent antivirus "storms" and bottlenecks.
- **Protect antivirus security software from attack** – Deploy and run the antivirus and anti-malware client software in a hardened secure virtual appliance to prevent attacks that target antivirus and anti-malware solutions.

Key Features

vShield Bundle includes the following key features and components:

For Network Edge

Firewall

- Perimeter (Layer 3) firewall, which does not require network address translation (NAT)
- Stateful inspection firewall, with inbound and outbound connection control rules based on the following parameters:
  - IP address – source/destination IP address
  - Ports – source/destination port
  - Protocol – type (TCP or UDP)

Network Address Translation

- IP address translation to and from the virtualized environment
- Masquerading of virtual datacenter IP addresses to untrusted locations

Dynamic Host Configuration Protocol

- Automatic IP address provisioning to virtual machines in vSphere environments
- Administrator-defined parameters (such as address pools, lease times and dedicated IP addresses)

Site-to-Site VPN

- Secure communication between virtual datacenters (or edge security virtual machines)
- Internet Protocol Security (IPsec) VPN with support for certificate authentication, as well as shared key, based on the Internet Key Exchange (IKE) protocol

Web Load Balancing

- Inbound load balancing for all traffic including Web traffic (HTTP)
- Round-robin algorithm
- Support for "sticky" sessions

Edge Flow Statistics

- Metering of virtual datacenter resource utilization, with attribution back to the tenant
- Statistics accessible through REST APIs and leveraged in service provider chargeback applications

Policy Management

- Full-featured management through vShield Manager; many features also accessible through vCenter Server interface
- Customizable interface for management using REST APIs
- Support for integration with enterprise IT security management tools

Logging and Auditing

- Based on industry-standard syslog format
- Accessible through REST APIs and vShield Manager user interface
- Administrator-defined logging on and off for key edge security events (errors, warnings, etc.):
  - Firewall: at rule level
  - NAT: at rule level
  - VPN: site-to-site connection name
  - Web load balancer: at pool level, specific Web requests including URL or folder
  - DHCP: at service level, bindings (release and renewals)

For Applications and Data

Sensitive Data Discovery

- Policy management console lets administrators select regulations to be used in compliance scans
- More than 80 templates of regulations, such as PII (Personally Identifiable Information), PCI-DSS (PCI-Data Security Standard) cardholder data, PHI (Protected Health Information), and others from around the world (North America, EMEA, Asia Pacific)
- Output report identifies which scanned resources contain data that violates selected compliance regulations
- Functionality can be programmed using REST APIs or the operator console
- Infected virtual machines are quarantined and remediated through VMware vCenter Configuration Manager

Firewalls

- Hypervisor-level firewall provides inbound and outbound connection control enforced at the virtual NIC level through hypervisor inspection, supporting multi-homed 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 Simple Network Management Protocol (SNMP) traffic
- Protection can be enforced according to network, application port, protocol type (TCP, UDP) or application type
- Dynamic protection of virtual machines as they migrate
- IP-based, stateful firewall and application layer gateway supports a broad range of protocols including Oracle, Sun Remote Procedure Call (RPC), Microsoft RPC, Lightweight Directory Access Protocol (LDAP) and SMTP, improving 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 and bytes)

Security Groups

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

Policy Management

- vShield Manager provides control over product features, many of which are also accessible through the vCenter Server interface
- Policy enforcement of security groups, vCenter Server groupings and TCP-5 tuple (source IP, destination IP, source port, destination port and protocol)
- REST APIs provide a programmable interface for management and policy enforcement
- Support for integration with enterprise security management tools

IP Addressing

- Flexible IP addressing, including 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

For Endpoint

Antivirus and Anti-Malware Offloading

- Offloads virus scanning activities via the vShield Bundle ESX module to a secure virtual appliance where the virus scanning engine, as well as the stored antivirus signatures are located
- File, memory and process scanning, as well as other tasks, are offloaded from virtual machines to a secure virtual appliance via a thin client agent and partner ESX module

- Endpoint Security (EPsec) manages communication between virtual machines and the secure virtual appliance using introspection at the hypervisor layer
- Antivirus engine and signature files are updated only within the secure virtual appliance, but policies (administrator-defined collections of regulations) can be applied across all virtual machines on a vSphere host

Trigger Remediation by Secure Virtual Appliance

- Retains partner's antivirus engine policies to dictate whether a malicious file should be deleted, quarantined or otherwise handled
- Thin agent used for file remediation activity within the virtual machine

Partner Integrations

- Integration with secure virtual appliance solutions from VMware partners is facilitated through the vShield Bundle EPsec API for introspection into file activity via the hypervisor layer

vShield Manager, Policy Management and Automation

- Provides full-featured configuration of endpoint deployment
- REST APIs allow customized and automated integration of endpoint capabilities into solutions
  - Monitoring reports provided
  - vShield Manager can be leveraged as a vCenter plugin

Logging and Auditing

- Event logging is based on industry-standard syslog standard

Supported Releases

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

Related Products

The vShield family of security products includes vShield Edge for perimeter security; vShield App with Data Security to protect applications from network-based attacks and discover sensitive data; vShield Endpoint to enhance endpoint security and performance for virtual datacenters; and vShield Manager. vShield Bundle includes vShield Edge, vShield App with Data Security, vShield Endpoint and vShield Manager.

Find Out More

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

For additional information about vShield products, please visit http://www.vmware.com/products.

vShield Bundle includes

- **vShield Edge** – A network gateway solution, it secures the virtual datacenter perimeter.
- **vShield App with Data Security** – Adds dynamic discovery of sensitive data to vShield App, providing support for regulatory compliance audits.
- **vShield Endpoint** – Offloads antivirus and anti-malware agent processing to a dedicated secure virtual appliance, strengthening security for virtual machines and improving performance for endpoint protection.
- **vShield Manager** – A central point of control for managing, deploying, reporting, logging and integrating third-party security services.

vmware

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