

MEDIA BACKGROUNDER

VMware vShield™: Better-than-physical security for virtual and cloud environments

Overview

[Announced Aug. 31, 2010 at the VMworld 2010 conference in San Francisco](#), the VMware vShield™ family of products supports a new approach to securing data and applications in dynamic virtual and cloud environments with security levels that surpass those of traditional, physical deployments.

Security and compliance top the list of enterprise concerns about cloud computing and represent significant barriers to the mainstream adoption of this new approach to IT. Current approaches to security are anchored to physical infrastructure elements, requiring agents, dedicated hardware and brittle “air-gapped” configurations. The dynamic nature of cloud environments, where applications and services are mobile and leverage shared infrastructure, requires a new approach.

Virtualization, the foundation of cloud computing architectures, allows compute, storage and network resources to be pooled and leveraged by multiple applications and services. First, the new VMware vShield products virtualize network security services, including firewall, VPN and load balancing, in order to decrease the cost and complexity of security. Second, the VMware vShield products make security policies adaptive and allow them to “travel” with applications as they move across physical infrastructure boundaries. As a result, VMware-virtualized and cloud environments are more secure than traditional, physical deployment models at a fraction of the cost.

Customers can achieve this new, higher-level of security even as they are adopting a hybrid cloud computing model that spans on-premise infrastructure and off-premise infrastructure from the ecosystem of [vCloud service provider partners](#). VMware vShield also delivers an open approach and works in conjunction with leading security products from VMware’s partners, including Cisco, McAfee, RSA, Symantec and Trend Micro.

VMware vShield Features and Benefits

The VMware vShield product family provides a single framework to protect the cloud environment. From the edge to the application and endpoint, the VMware vShield product family enables customers to consolidate security infrastructure and eliminate sprawl associated with software agents, security policies, security appliances and “air-gapped” solutions.

- **Secure the Virtual Datacenter (VDC) Edge with VMware vShield Edge** – In virtual and cloud environments, the “edge” is no longer defined by the physical boundaries of the datacenter. VMware vShield Edge allows organizations to easily create secure, logical, hardware-independent perimeters (edges) around virtual datacenters, making it possible to create multi-tenant IT infrastructures. Deployed as a virtual appliance, VMware vShield Edge provides firewall, VPN, Web load balancer, NAT and DHCP services, allowing customers to provision all these edge security services while eliminating the need for multiple special-purpose appliances. With VMware vShield Edge, enterprises and service providers can offer secure, multi-tenant cloud services, isolating traffic between tenants, protecting the tenant applications and data, and ensuring compliance.
- **Application Protection for Virtual and Cloud Environments** – VMware vShield App is a hypervisor-based, application-aware firewall solution that installs on each VMware vSphere™ host, creating and enforcing logical, dynamic application boundaries – security groups – based on policies, rather than physical boundaries. Unlike traditional firewalls, VMware vShield App monitors the network communications between virtual machines and dynamically enforces security group policies, eliminating the need for dedicated hardware and VLANs to separate different security groups and offering a cost-effective solution that helps customers achieve better-than-physical application security.

- **Optimize End-Point Security for Virtual Environments** – VMware vShield Endpoint, in tandem with VMware’s partner solutions, protects virtual machines and their hosts against malware, viruses and other intrusions by optimizing antivirus and other host and endpoint security for use in VMware-virtualized and cloud environments. VMware vShield Endpoint eliminates the need for antivirus agent footprints by enabling the offloading of antivirus and anti-malware functions to hardened, tamper-proof virtual machines delivered by VMware’s security partners. VMware is collaborating with leading security vendors such as McAfee, Symantec and Trend Micro to integrate and deliver full endpoint protection solutions based on VMware vShield.
- **Provide Basic Protection for the Virtual Datacenter** – Included with VMware vSphere, VMware vShield Zones provides basic protection from network-based threats in virtual datacenters, with application firewalling based on administrator-defined zones.

All of the VMware vShield products include the VMware vShield Manager Console – the “command center” for security management – which integrates seamlessly with VMware vCenter™ Server to facilitate centralized security management for virtualized and cloud environments. VMware vShield Manager enables role-based access and views into all aspects of the security framework so that cross-functional IT teams – VI administrators, network and security – can easily coordinate tasks and functions, and is also the centralized point of logging, auditing, reporting and third-party integration

“VMware vShield™ will dramatically simplify security by freeing it from the constraints of physical infrastructure,” said Bogomil Balkansky, vice president, product marketing, virtualization and cloud platforms, VMware. “The result is security services that are cost effective and adaptive to the dynamic nature of cloud environments. VMware vShield will eliminate one of the biggest barriers to cloud computing and give our customers confidence that any environment built on VMware is protected and compliant.”

Pricing and Availability

The VMware vShield product family is currently available and is licensed per VM starting at \$50 per VM.

Industry Support

“As datacenters become more dynamic and adaptive, security must also evolve. Today’s static security infrastructure is an inhibitor to agility and an organization’s ability to adopt cloud-based computing services,” said Neil MacDonald, vice president and [Gartner](#) Fellow. “Virtualized, not physical, security controls will secure workloads within the next-generation data center with policies based on logical, not physical, attributes – such as application and user identity. This allows workloads to move as the business requires within private clouds and, in the future, to and from public cloud computing environments without compromising security.”

Partner Support

Cisco

“Cisco and VMware are committed to helping customers easily protect their applications in the datacenter from network-based threats as well as delivering a level of protection for virtual machines that exceeds the physical server deployments. To support this commitment, Cisco and VMware are collaborating to develop an integrated solution that leverages VMware vShield™ Manager as a point of integration between VMware vSphere™, VMware vCloud™ Director and Cisco network services and devices.”

—Ed Bugnion, vice president and CTO, Server Access and Virtualization Technology Group, Cisco

McAfee

"As the demand for secure virtualization and cloud computing environments increases, McAfee and VMware will work together where the McAfee ePolicy Orchestrator platform can extend, enrich and enforce threat protection, compliance and policy intelligence."

—*Dave Scholtz, senior vice president of global alliances at McAfee*

RSA

"The VMware vShield™ family of products will bring positive transformation to how security is implemented and operated for VMware-virtualized environments. . By offering intuitive, built-in security controls to virtualization administrators, VMware has made it possible for security to be integral to how virtual infrastructure is operated, resulting in better security. RSA and VMware are collaborating to further advance this value by integrating VMware-virtualized environments into enterprise security infrastructure. We've worked together on interoperability between the RSA® enVision SIEM platform and VMware vShield so that security events from the virtual infrastructure can be collected, analyzed and reported centrally along with security events from physical IT infrastructure. These events further inform security dashboards with the RSA® Archer eGRC platform."

—*Tom Corn, Chief Strategy Officer, RSA, The Security Division of EMC*

Symantec

"Securing the virtual infrastructure remains a serious concern for enterprises today. Symantec is working closely with VMware to deliver best-of-breed security solutions, optimized for virtual environments, for hardening servers, securing endpoints and enforcing security policies. Symantec is committed to helping customers realize the benefits of Secure Private Clouds more quickly, more easily and with greater confidence."

—*Art Gilliland, vice president of product management, Symantec*

Trend Micro

"VMware vShield™ Endpoint is a dramatic leap forward for enterprises that want to ensure the security of their virtualized computing environments, while maximizing operational efficiency, system performance and cost savings. Our new agentless anti-malware solution, which leverages VMware vShield Endpoint and is tightly integrated with other VMware technologies and products, has received strong positive feedback from customers. VMware vShield Endpoint further demonstrates VMware's commitment to delivering better-than-physical security and maximizing customer value."

—*Steve Quane, chief product officer, Trend Micro*

Additional Resources

- Learn more about [VMware vShield](#)
- Read VMware sr. director of product marketing, [Venu Aravamudan's blog on VMware vShield](#)
- Get [product information, datasheets and screenshots](#)
- Learn more about [VMware's cloud infrastructure strategy](#)
- Learn more about [VMware's Vision for Next Decade of Information Technology](#)
- See what's happening at [VMworld 2010](#)

#

VMware, VMware vCenter, VMware vCloud, VMware vSphere and VMware vShield are registered trademarks and/or trademarks of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. The use of the word "partner" or "partnership" does not imply a legal partnership relationship between VMware and any other company.

Contacts:

Leah Bibbo
VMware Global Communication
lbibbo@vmware.com
(650) 427-1097

Alex Kirschner
OutCast Communications for VMware
alex@outcastpr.com
(415) 345-4783