VMware Integrated Partner Solutions for Networking and Security

vmware

VMware Integrated Partner Solutions for Security and Compliance

VMware vCloud® Networking and Security is the leading networking and security virtualization platform that enhances operational efficiency, unlocks agility and is extensible to rapidly respond to business needs. It provides a broad range of services in a single solution, including virtual firewall, VPN, load balancing and VXLAN extended networks while also providing a comprehensive framework to integrate 3rd party solutions.

Networking and security are complex, dynamic areas, and VMware recognizes the vital role our technology partners play in helping our customers as they transition to virtual and cloud architectures. VMware vCloud Ecosystem Framework provides service insertion at the vNIC and the virtual edge level. This allows any partner solution to access both traffic flows and workload context without significant software development. Customers can easily take advantage of a new vendor's technology and integrate operations with the existing systems and procedures, leading to improved levels of service and performance.

Below is a list of VMware integrated partner networking and security solutions. Integrated networking and security solutions from VMware and our partners unlock the benefits of cloud computing, lower costs, and accelerate IT agility. We invite you to visit our partner's web sites to learn more about how these solutions help make VMware the platform of choice for your journey to the cloud.

Bitdefender	**Security for Virtualized Environments**	Bitdefender Security for Virtualized Environments integrates with VMware vShield Endpoint to centralize antimalware functions and increase consolidation ratios in virtualized server or desktop environments.
CA	**CA ControlMinder for Virtual Environments**	CA ControlMinder for Virtual Environments integrates with VMware vCenter™ and vCloud Networking and Security App to provide comprehensive privileged identity management for both the hypervisor and virtual machines.
Catbird	**Catbird vSecurity**	Catbird vSecurity is now integrated with VMware vCloud Networking and Security App to broaden access control capabilities for compliance enforcement. Catbird vSecurity, a 4-time Best of Show Finalist at VMworld, together with vCloud Networking and Security App monitors and protects organizations regulated by specifications such as PCI, HIPAA and NIST.
Checkpoint	**Security Gateway VE**	Checkpoint Security Gateway VE is integrated with VMware to ensure organizations can secure inter-VM traffic and external networks with granular firewall policies and integrated intrusion prevention capabilities to protect against malicious and unwanted network activity.
EMC/RSA	**Security Management for Virtual Infrastructure**	EMC Storage Advisor + Network Config Manager and vCenter Configuration Manager feed compliance results for Storage, Network and Compute up through RSA Archer dashboard and support drill down in context into each of these solutions.
	Data Loss Prevention	Data classification technology powered by RSA Data Loss Prevention (DLP) is embedded within vCloud Networking and Security to enable organizations to classify sensitive data natively. In addition, RSA DLP is certified with VMware View technology to empower organizations to monitor data flow and enforce real-time controls.
	Governance, Risk and Compliance (GRC)	RSA Archer is integrated with VMware vCenter to provide visibility into the compliance status of the virtual infrastructure for various regulations, helping organizations manage risk and compliance audits for their virtual infrastructure.
	Authentication	RSA SecurID two-factor authentication integrates with VMware View to provide an added layer of security. This ensures that the permitted users can access the right hypervisor or the relevant virtual sessions within the virtual desktop environment securely.

	Infrastructure Protection	RSA enVision is tested and certified with VMware vSphere, View and ESX to collect, store, manage, and correlate logs and events generated for security monitoring and compliance retention and reporting.
HP TippingPoint	**vController IPS/IDS for Virtual Environments**	Hardware and software solution that combines HP TippingPoint vController with VMware vCloud Networking and Security App and Edge protection to simplify enterprise security. The HP TippingPoint IPS vController and VMware vCloud Networking and Security solution is a comprehensive firewall and IPS security offering that protects across physical and virtual environments.
HyTrust	**HyTrust Appliance**	HyTrust Appliance integrates with VMware to manage privileged access, ensure accountability, and enforce compliance for VMware vSphere™ based infrastructure.
IBM ISS	**IBM Security Virtual Server Protection for VMware**	IBM Security Virtual Server Protection for VMware helps meet regulatory compliance by limiting access to critical data, tracking user access and providing reporting for the virtual infrastructure. Provides defense-in-depth, dynamic security with VM rootkit detection and virtual infrastructure auditing and monitors traffic with VMsafe™ integration. Helps to accelerate and simplify PCI DSS audit and achieve compliance with security and reporting functionality.
Juniper Networks	**vGW Virtual Gateway**	Juniper vGW Virtual Gateway is a comprehensive virtualization security solution for virtualized data centers and clouds that gives full visibility and granular access control over all traffic flowing through virtual machines. vGW includes a high -performance hypervisor-based stateful firewall, integrated intrusion detection, compliance monitoring and enforcement, and virtualization-specific antivirus protection. vGW synchronizes with VMware vCenter™ and uses VMware APIs to provide the highest levels of security and performance.
Kaspersky	**Kaspersky Security for Virtualization**	Kaspersky Security for Virtualization delivers agentless anti-malware security, architected for VMware vSphere™ Endpoint, to alleviate the increasing security threats for virtualized data centers, servers and desktops, based on Kaspersky Lab's advanced, award-winning anti-malware engine. Kaspersky delivers the first unified "single pane of glass" management console for all virtual, physical and mobile devices across a wide range of platforms allowing immediate response to security events.
Logrhythm	**LogRhythm's next-generation SIEM platform**	LogRhythm's next-generation SIEM platform, with integrated File Integrity Monitoring, includes comprehensive deployment and log collection support for VMware technologies. With robust multi-tenant capabilities, broad out-of-the-box compliance packages, and advanced multi-dimensional Big Data analytics, LogRhythm enables enterprises and MSSPs to automate and assure compliance, detect and respond to advanced cyber-threats, and address operational challenges, in large-scale virtual, physical and hybrid environments.
McAfee	**McAfee MOVE AV**	McAfee MOVE AV provides strong anti-malware protection seamlessly at the initiation of a virtual machine and integrates with VMware vShield Endpoint to offload key antivirus and anti-malware functions to a hardened, tamperproof security virtual appliance, eliminating agent footprint. VMware VMs are instantly protected without having a McAfee agent in each Guest VM.

Reflex Systems	**Virtualization Management Center**	The vTrust component in Reflex System's Virtualization Management Center integrates with VMware to provide dynamic policy enforcement and management, virtual segmentation, quarantine and networking policies
SafeNet	**SafeNet ProtectV**	SafeNet ProtectV solution integrates with VMware vCenter to provide high assurance security by enabling organizations to encrypt and secure the entire contents of their virtual machines, protecting sensitive assets from theft or exposure. ProtectV has achieved VMware Ready™ status, VMware's highest level of endorsement.
Sourcefire	**Next-Generation Intrusion Prevention System (NGIPS)**	The Sourcefire Next-Generation Intrusion Prevention System (NGIPS) monitors real-time network and user activity in a virtual environment, detecting policy violations such as the use of unauthorized applications on non-standard ports or unpermitted access to a critical host. When a violation is identified, Sourcefire uses VMware vCloud Networking and Security APIs to dynamically configure vCloud Networking and Security App or vCloud Networking and Security Edge to restrict the activity causing the violation.
	SourceFire FireAMP Virtual	FireAMP Virtual protects VMware virtual machines from advanced malware and stops threats that bypass other security layers. Designed for VMware environments, FireAMP Virtual increases efficiency through integration with the agentless VMware vShield architecture. Customers deploying FireAMP Virtual benefit from having seamless visibility and control to identify and remediate advanced malware across their entire environment.
Symantec	**Critical System Protection**	Critical System Protection integrates VMware vSphere protection and hardening policies to monitor and prevent configuration file tampering, limit inbound/outbound communications and access, stop unauthorized services from running and prevent zero day attacks against unpatched or vulnerable systems.
	Control Compliance Suite	Control Compliance Suite integrates vSphere hardening policies allowing for scheduled automated scans to report on vSphere platform state as well as perform vulnerability scans of critical vSphere assets.
	Symantec Endpoint Protection	Symantec Endpoint Protection integrates with VMware vShield Endpoint to secure your high density business critical environments with uncompromising effectiveness and high performance.
	Security Information Manager	Security Information Manager provides an integrated vCloud Networking and Security log collector to extend visibility into the advancing virtual infrastructure for unparalleled context to potential threat activity with advanced telemetry between internal physical, virtual and external threat landscape intelligence to prioritize risk.
	Managed Security Services	Symantec's Managed Security Service utilizes an integrated vCloud Networking and Security collector to provide new threat-based context to advancing virtual infrastructures combined with 7x24 GIAC-certified Security Analyst expertise to assist with incident remediation.
	Data Loss Prevention	Symantec Data Loss Prevention integrates with vCloud Networking and Security to discover sensitive data residing in virtual datacenters and automatically quarantine virtual machines that violate data security policies.

	Web Gateway	The Symantec Secure Web Gateway provides reputation and policy-based web filtering, and now integrates with vCloud Networking and Security App to enforce network-based protection of virtual servers. Using vCloud Networking and Security, Secure Web Gateway automatically isolates the traffic of virtual machines and prevents communication with untrusted or malicious Internet destinations.
TIBCO LogLogic	**Log and Security Intelligence Platform**	LogLogic provides a scalable log and security intelligence solution for your VMware-based enterprise and Cloud Big Data requirements. The solution collects all your logs and IT data, enriches it with meaningful and contextual knowledge, and provides you with intelligent reports, alerts, and dashboards for making the right decisions while compressing and storing the raw data in its unaltered form for compliance.
	Compliance Manager and Compliance Suites	LogLogic delivers a virtualized environment compliance suite with direct support for VMware vCloud Director, VMware vCenter, VMware ESX Server, and VMware vCloud Networking and Security Edge. Both enterprise and cloud providers can now automate compliance needs with LogLogic and ensure coverage for the vCloud Datacenter.
Trend Micro	**Deep Security Antivirus**	Deep Security for vShield Endpoint integrates with the VMware APIs to provide agentless anti-malware protection for VMware virtual machines with zero in-guest footprint. Helps avoid security brown-outs commonly seen in full system scans and pattern updates.
	Deep Security Integrity Monitoring	Agentless File Integrity Monitoring, through the same Deep Security Virtual Appliance that already provides agentless anti-malware and agentless intrusion prevention in a virtual environment, removes integrity scan storms and significantly lowers the operational complexity.

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

Item No. VMW-CH-RSA-Partner-A4-111 02/13