Trend Micro Deep Security for VMware Mobile Secure Desktops

Trend Micro Optimizes and Secures the VMware View Mobile Secure Desktop Across Devices and Locations

Key Benefits

This joint solution protects Mobile Secure Desktop environments from the latest threats, while delivering:

- **Higher Density** by offloading security scans from individual virtual machines to a single security virtual appliance on each vSphere host
- **Optimized Resources** by eliminating antivirus storms and resource contention from multiple security agents
- **Simplified Management** by eliminating agents and the need to configure and update each one
- **Stronger Security** by providing instant-on protection for new virtual machines and tamper-proof security coordinated by the dedicated security appliance

Securing the New Mobile Workforce

Today's employees are increasingly transient and consumer products such as laptops, desktops, tablets, and smartphones are driving user expectations at home and in the office. This consumerization of IT is forcing many IT departments to scramble to balance consumer trends and needs with IT requirements to protect corporate assets.

VMware has worked with key partners such as Trend Micro to develop a solution to address the new mobile workforce challenge—the Mobile Secure Desktop. With the Mobile Secure Desktop, VMware® and Trend Micro are transforming stationary workstations into secure, stateless mobile workspaces leading to increased employee productivity and satisfaction, enhanced security and compliance, and lower total cost of ownership.

The Mobile Secure Desktop holds the promise of a new way to work, enabling Bring Your Own Device (BYOD) programs and delivering a seamless experience for virtual desktop users. Securing this new way to work demands a new approach as well, and as a result, Trend Micro and VMware have partnered to deliver agentless security for virtualized datacenters and desktop virtual machines. Traditional agent-based security solutions that are not designed for virtualization can result in a number of significant operational security issues. VMware and Trend Micro's agentless security resolve these challenges.

Unique Challenges in Virtual Desktop Environments

Both physical and virtual desktops need antimalware protection, but virtual desktop anti-malware security must be designed for a shared resource environment. If traditional physical security is deployed, the anti-malware across all of the individual virtual desktop instances can create performance degradation on the host—sabotaging the improved efficiencies you're trying to achieve with virtual desktops. And the ease of virtual desktop provisioning can make it difficult to keep virtual desktop security current. Only virtualization-aware security can combat these virtual desktop security challenges:

- **Resource Contention** – In virtual desktop deployments, numerous desktops share the host's hardware resources, often at a ratio of 60-to-1 or higher. Simultaneous security updates and full-system scans can result in a dramatic loss of desktop performance – limiting availability or reducing VM consolidation ratios.
- **Instant-On Gaps** – Virtual desktops can quickly be provisioned, cloned, reverted to previous instances, paused, and restarted, all relatively easily. Vulnerabilities or configuration errors may be unknowingly propagated, and dormant desktop images can be reactivated with out-of-date security.
- **Antivirus (AV) Storms** – When traditional AV solutions simultaneously initiate scans or scheduled security updates on all VMs on a single physical host, an "AV storm" can result, creating an extreme load on the system and reducing performance.
- **Compliance and Data Privacy** – With the ease of provisioning and mobility of virtual desktops, it can be difficult to maintain an auditable record of the security state of a virtual desktop at any given point in time. Yet, many regulations require proof of current antimalware protection.

Securing the Mobile Secure Desktop

The VMware View Mobile Secure Desktop solution provides an innovative way for IT to support device diversity and BYOD initiatives by improving user access and mobility, streamlining application updates, enhancing data security and delivering the highest-fidelity user experience.

As the security component of the VMware View™ Mobile Secure Desktop solution, VMware vShield™ and VMware View products, together with Trend Micro Deep Security, allow IT to offload AV to secure virtual machines. This provides high levels of isolation between resource pools and networks, allowing IT to apply policies across VMs and pools of users.

Within a Mobile Secure Desktop Environment, Deep Security components are located on Virtual Desktop ESX hosts as the Deep Security Virtual Appliance and on the Management Cluster as the Deep Security Manager. The Deep Security Virtual Appliances provide the agentless security services to the hypervisor while the Deep Security Manager manages these Deep Security Virtual Appliances and stores all configuration settings and events.

Deep Security Virtual Appliance – Transparently enforces security policies on VMware vSphere virtual machines for agentless anti-malware, IDS/IPS, integrity monitoring, web application protection, application control, and firewall protection — coordinating with Deep Security Agent, if desired, for log inspection and defense in depth.

Deep Security Manager – Powerful, centralized management enables administrators to create security profiles and apply them to servers, monitor alerts and preventive actions taken in response to threats, distribute security updates to servers, and generate reports. Event tagging functionality streamlines the management of high-volume events.

Solution Elements

Trend Micro Deep Security with VMware vShield Endpoint and VMware View maximize virtual desktop protection and performance. Key solution elements include:

VMware vShield Endpoint

vShield Endpoint is a unique solution that optimizes host and endpoint security for use in vSphere™ and View environments. vShield Endpoint provides the intermediary for anti-malware and deep packet inspection. This allows IT to enhance endpoint performance across the desktop environment by offloading virus scanning to secure virtual machines—effectively eliminating the need to install complex antivirus agents inside each individual virtual machine. This advanced solution frees up system

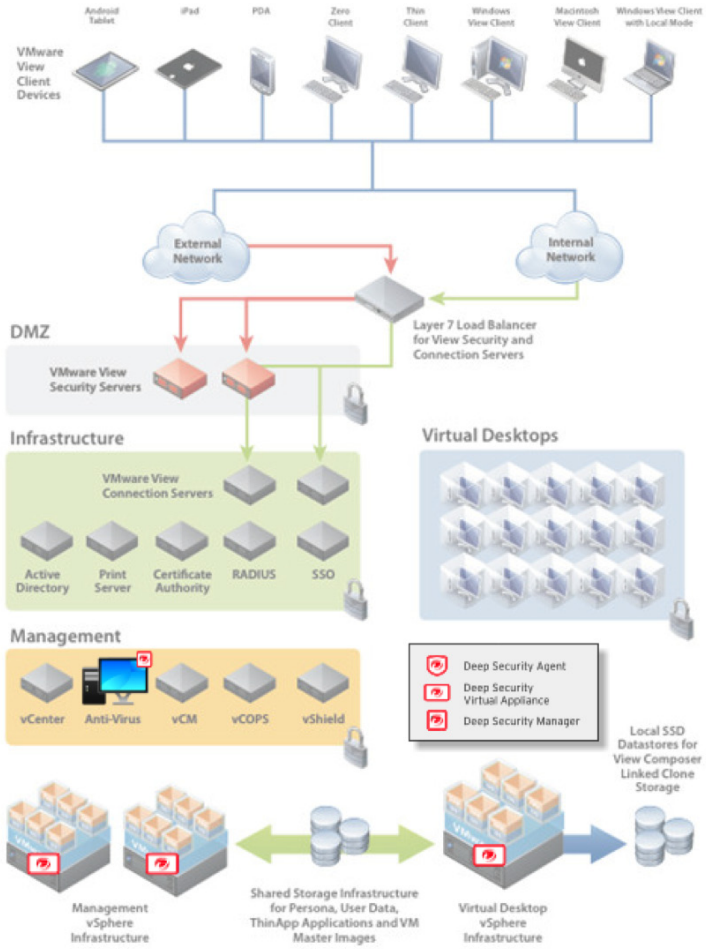

Figure 1: Deep Security Components within the Mobile Secure Desktop Environment

resources, improves performance, and eliminates the risk of security "storms" (overloaded resources during scheduled scans and signature updates).

Trend Micro Deep Security

Trend Micro Deep Security provides a comprehensive server security platform integrated with the Mobile Secure Desktop solution. Trend Micro was the first security vendor to integrate with VMware vShield APIs to provide you with better protection, less administrative complexity, and increased performance through cutting-edge agentless technology. Built to handle the rigors of virtual desktop environments, VMware and Trend Micro solutions maximize protection and security while preserving performance and increasing ROI.

Tightly integrated modules easily expand the platform to ensure server, application, and data security across physical, virtual, and cloud servers, as well as virtual desktops. Deep Security provides a wide range of security options for VMware virtual machines:

- **Anti-Malware** – Integrates new VMware vShield Endpoint 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. Additionally, Web Reputation functionality prevents users from accessing malicious websites and downloading malware.
- **Intrusion Detection and Prevention** – Shields known vulnerabilities from unlimited exploits until they can be patched. Helps achieve timely protection against known and zero-day attacks. Uses vulnerability rules to shield a known vulnerability—for example those disclosed monthly by Microsoft—from an unlimited number of exploits. Offers out-of-the-box vulnerability protection for over 100 applications, including database, web, email, and FTP servers. Automatically delivers rules that shield newly discovered vulnerabilities within hours, and can be pushed out to thousands of servers in minutes, without a system reboot.
- **Integrity Monitoring** – Detects malicious and unexpected changes. Leverages an agentless configuration to add greater security to virtual machines without additional footprint. Event tagging and cloud-based whitelisting reduce the complexity of administrative operations. Also includes real-time, on-demand, or scheduled detection of change and provides auditable reports.
- **Application Control** – Increases visibility into, or control over, applications accessing the network. Identifies malicious software accessing the network and reduces the vulnerability exposure of your servers.
- **Firewall** – Centralizes management of server firewall policy using a bi-directional stateful firewall. Supports virtual machine zoning and prevents Denial of Service attacks. Provides broad coverage for all IP-based protocols and frame types as well as fine-grained filtering for ports and IP and MAC addresses.
- **Log Inspection** – Collects and analyzes operating and application logs for suspicious behavior, security events, and administrative events across the datacenter.
- **Web Application Protection** – Enables compliance with PCI Requirement 6.6 for the protection of web applications and the data that they process. Defends against SQL injections attacks, cross-site scripting attacks, and other web application vulnerabilities. Shields vulnerabilities until code fixes can be completed.

Summary

The Mobile Secure Desktop from VMware is a managed solution that integrates technology from VMware and Trend Micro to ensure a secure and seamless experience for virtual desktops, allowing IT to provide the new mobile workforce access to their desktops, applications, and data anywhere, any time, on any device.

Learn More about the Mobile Secure Desktop

For additional information about Trend Micro Deep Security for VMware View including the Mobile Secure Desktop Solution, please visit www.trendmicro.com/deepsecurity or for contact phone numbers, see http://www.trendmicro.com/us/about-us/locations/index.html.