Trend Micro™

DEEP SECURITY ACCELERATION KIT

Virtualization security software and services for midsize businesses

Virtualization and cloud computing have changed the face of today's data center. Yet midsized businesses on the cutting edge of virtualization are not seeing the expected gains because legacy security is holding them back. Legacy security was not designed to function in virtualized environments–resulting in operational overhead, application outages, even exploits and data breaches. Midsize businesses need a comprehensive security solution architected specifically for their virtual environments to help them address these challenges.

Deep Security is the industry's leading physical, virtual, and cloud server security solution designed by Trend Micro in collaboration with VMware for virtual and cloud environments. This comprehensive, virtualization security is available to midsize businesses in acceleration kits designed specifically to enable operational ease of use, business continuity, and protection from sophisticated threats.

Although it can be deployed in the form of an integrated agent, Deep Security is an agentless security solution that allows a single virtual appliance to secure the entire virtualized host without in-guest security agents. This flexible, agentless deployment simplifies security operations while accelerating the ROI of virtualization. Deep Security Acceleration Kits for midsize businesses feature tightly integrated modules including anti-malware, web reputation, integrity monitoring, and intrusion prevention for virtual patching. This enables advanced server security, application security, and data security from sophisticated threats across virtual machines (VMs). To get you up and running quickly, the acceleration kits also include remote deployment services for expert assistance.

With Deep Security, you gain an easy-to-use, advanced, virtualization security solution that optimizes the performance and availability of your business applications while protecting your VMware environment from sophisticated threats.

Accelerates Virtualization ROI

- Provides a lighter, more manageable way to secure VMs with the industry's first and most comprehensive agentless security solution built for VMware environments
- Unparalleled agentless security performance with improved resource efficiency via ESX scanning deduplication
- Improves resource utilization and delivers higher VM densities than legacy anti-malware solutions, by orders of magnitude
- Improves the manageability of security in VMware environments by reducing the need to continually configure, update, and patch agents

ADVANTAGES

Simplifies Manageability

- Reduces complexity with tight integrations to management consoles from Trend Micro andVMware, and directory services such as active directory
- Provides vulnerability protection to prioritize secure coding, and cost-effective implementation of unscheduled patching
- Eliminates the cost of deploying multiple software clients with a centrally managed, multi-purpose software agent or virtual appliance
- Reduces management costs by automating repetitive and resource intensive security tasks, reducing false-positive security alerts, and enabling workflow of security incident response
- Significantly reduces the complexity of managing file integrity monitoring with cloud-based event whitelisting and trusted events

Prevents Data Breaches

- Detects and removes malware in real time with minimal performance impact
- Blocks malware that attempts to evade detection by uninstalling or otherwise disrupting the security program
- Shields known and unknown vulnerabilities in web and enterprise applications and operating systems
- Detects and alerts suspicious or malicious activity to trigger proactive, preventative actions
- Leverages the web reputation capabilities of one of the largest domain-reputation databases in the world to protect users from accessing infected sites

Supports Business Continuity

- Prevents unplanned downtime from emergency patching by virtually patching (shielding) critical vulnerabilities and zero-day attacks
- Combines multiple protection modules to provide multi-layered defense from threats and mitigates application outage from infections
- Virtualization-aware architecture ensures optimized performance and prevents application slowdown

DEEP SECURITY ACCELERATION KIT MODULES

Anti-Malware

- Integrates VMware vShield Endpoint APIs to protect VMware virtual machines against viruses, spyware, trojans and other malware with zero in-guest footprint
- Delivers an anti-malware agent to extend protection to other hypervisors as well as physical and cloud servers
- Improves performance through ESX level caching and deduplication.
- Optimizes security operations to avoid performance degradation (antivirus storms) commonly seen in full system scans and pattern updates
- Tamper-proofs security from sophisticated attacks in virtual environments by isolating malware from anti-malware

Web Reputation

- Integrates with the Trend Micro™ Smart Protection Network™ for web reputation capabilities that block access to compromised web sites to strengthen protection for servers and virtual desktops
- Provides agentless web reputation on the same virtual appliance as agentless anti-malware and intrusion prevention for greater virtual server security without added footprint

Intrusion Prevention and Firewall

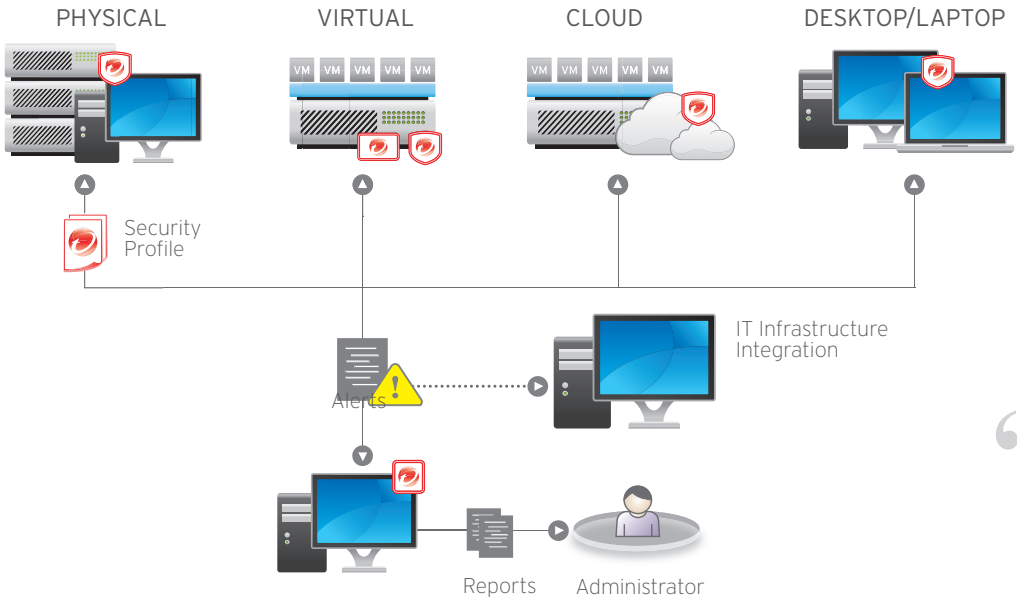
- Protects against known and zero-day attacks by virtually patching (shielding) known vulnerabilities from unlimited exploits
- Examines all incoming and outgoing traffic for protocol deviations, policy violations, or content that signals an attack
- Automatically shields newly discovered vulnerabilities within hours, pushing protection to thousands of servers in minutes without a system reboot
- Assists compliance (PCI DSS 6.6) to protect web applications and the data they process
- Defends against SQL injection, cross-site scripting, and other web application vulnerabilities
- Shields against vulnerabilities until code fixes can be completed
- Includes out-of-the-box vulnerability protection for all major operating systems and over 100 applications, including database, web, email, and FTP servers
- Provides increased visibility into, or control over applications accessing the network
- Decreases the attack surface of physical, cloud, and virtual servers with fine-grained filtering, design policies per network, and location awareness for all IP-based protocols and frame types
- Centrally manages server firewall policy, including templates for common server types
- Prevents denial of service attacks and detects reconnaissance

Integrity Monitoring

- Monitors critical operating system and application files, such as directories, registry keys, and values, to detect and report malicious and unexpected changes in real time
- Employs Intel TPM/TXT technology to perform hypervisor integrity monitoring. Monitors for any unauthorized changes to the hypervisor, thereby extending security and compliance of virtualized systems to the hypervisor.
- Reduces administrative overhead with trusted event tagging that automatically replicates actions for similar events across the entire data center
- Simplifies administration by greatly reducing the number of known good events through automatic cloud-based whitelisting from Trend Micro Certified Safe Software Service

> "Through the concept of the agentless virtual appliance, Deep Security simplifies security processes considerably and allows for more efficient utilization of resources, especially when compared to conventional anti-malware solutions... With its centralized approach, Deep Security is the only way for us to offer our customers a truly secure environment that performs well."

Holger Schmieder, CEO
SCHMIEDER it-solutions,
Baden-Württemberg, Germany



BUILT FOR VMWARE VIRTUAL AND CLOUD ENVIRONMENTS

Deep Security is specifically designed for virtual environments. Its agentless architecture provides comprehensive protection from advanced threats, minimizes operational complexity, improves business continuity and allows organizations to accelerate virtualization and cloud adoption. Developed in close collaboration with VMware, Deep Security is the first product in its category to offer support for VMware vSphere 5.1 and VMware vShield Endpoint 5.1. Deep Security also provides full backward compatibility with vSphere 4.1 and 5.0 environments.

> "Deep Security has been a very good fit in our data center and provides excellent protection for our virtualized servers and desktops and our continually changing environment. I love it."
>
> Orinzal Williams, Executive Director
> **United Way of Atlanta, Georgia, US**

SOLUTION ARCHITECTURE

Deep Security Virtual Appliance. Transparently enforces security policies on VMware vSphere virtual machines for agentless anti-malware, web reputation, intrusion prevention, and integrity monitoring, protection–coordinating with Deep Security Agent, if desired, for log inspection and defense in depth.

Deep Security Agent. This small software component deployed on the server or virtual machine being protected enforces the datacenter's security policy (anti-malware, web reputation, intrusion prevention, and integrity monitoring).

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.

Smart Protection Network. Deep Security integrates with this cloud-based security infrastructure that delivers global threat intelligence and real-time protection from emerging threats by continuously evaluating and correlating threat and reputation intelligence for websites, email sources, and files.

> "I did the Deep Security deployment myself–it was less than a day for the roll out across 100 virtual machines. Overnight, I saw our memory resource utilization go down by 27%."
>
> Nick Casagrande, Director of IT
> **Southern Waste Systems LLC, Florida, US**

DEPLOYMENT AND INTEGRATION

Deep Security Remote Deployment Services

These services are included with your Deep Security Acceleration Kit. Trend Micro or certified partner consultants with extensive security deployment experience will provide assistance using remote deployment tools to ensure Deep Security is set up ideally for your VMware environment. You'll benefit from expert knowledge that will fully optimize your virtualization security solution.

The service components include:

- One Deep Security Manager Console installation
- Up to 25 agents/VMs on one ESX Host installation
- VMware vShield installation

SOLUTION ARCHITECTURE

Microsoft® Windows®

- XP (32-bit/64-bit)
- XP Embedded
- Windows 7 (32-bit/64-bit)
- Windows Vista (32-bit/64-bit)
- Windows Server 2003 (32-bit/64-bit)
- Windows Server 2008 R2 (64-bit)

Linux

- Red Hat® Enterprise 5, 6 (32-bit/64-bit)[1]
- SUSE® Enterprise 10, 11 (32-bit/64-bit)[1]

Solaris™

- OS: 8, 9, 10 (64-bit SPARC), 10 (64-bit x86)[1]

UNIX

- AIX 5.3, 6.1 on IBM Power Systems[2]
- HP-UX 11i v3 (11.31)[2]

VIRTUAL

- VMware®: ESX/ESXi 3.x3, vSphere 4.04, vSphere 4.1/5.05, View 4.5/5.05
- Citrix®: XenServer[3]
- Microsoft®: HyperV[3]

[1] Anti-malware not available
[2] Only Integrity Monitoring available on this platform
[3] Protection via Deep Security Agent and Virtual Appliance for intrusion prevention, via Agent only for other modules

Deep Security Acceleration Kits

Trend Micro™ Deep Security Acceleration Kits have everything you need to deploy virtualization security quickly, including expert remote deployment services to get you off to the right start:

- Anti-malware
- Web reputation
- Integrity monitoring
- Intrusion prevention and firewall (option to add-on)

The result is that you will have an easy-to-use, advanced virtualization security solution that will optimize the performance of your business applications while protecting your VMware environment.

Deep Security Acceleration Kits for midsize businesses (100-1000 employees) are available through Trend Micro channel partners nationwide. To find a reseller visit: www.trendmicro.com/mbvirtualization.

Key Certifications and Alliances

- Common Criteria EAL 4+
- PCI Suitability Testing for HIPS (NSS Labs)
- Virtualization by VMware
- Microsoft Application Protection Program
- Microsoft Certified Partnership
- Oracle Partnership
- HP Business Partnership
- Certified Red Hat Ready
- Certified for vBlock systems

TREND MICRO™

Securing Your Journey to the Cloud