

Trend Micro™

## Deep Security 6 Software

Adding Server and Application Protection to Dynamic Datacenters

Enterprises increasingly rely on their Internet-based business, and no matter what the purpose—connecting partners, personnel, suppliers, or customers—Web applications face a growing danger of cyber attacks. These targeted threats are greater and more sophisticated than ever before, and data security compliance becomes more stringent every day. Your company needs uncompromising security that doesn't reduce performance—streamlined, integrated products, services, and solutions that cost-effectively protect sensitive data and minimize risk. Trend Micro and its partners have answers for your Web security needs.

With Trend Micro™ Enterprise Security solutions, your business quickly and simply acquires, deploys, and manages security solutions—minimizing risk and cost by rapidly identifying threats and offering superior, unified protection. As a result, you stay ahead of content security threats, protecting customer relationships, Web-generated revenue, market reputation, and employee productivity. Our strong relationship with industry-leading security providers, including Third Brigade, enables us to work together to offer an in-depth approach to Web-based security. One such solution is Third Brigade Deep Security 6 software.

### SELF-DEFENDING SECURITY

Third Brigade Deep Security is comprehensive server and application protection software that enables physical and virtualized servers—and cloud computing environments—to become self-defending through these software modules:

- Deep Packet Inspection
  - IDS/IPS
  - Web Application Protection
  - Application Control
- Firewall
- Integrity Monitoring
- Log Inspection

### KEY FEATURES

#### Deep Packet Inspection (DPI) Enables Intrusion Detection and Prevention, Web Application Protection, and Application Control

- The software features a high-performance deep packet inspection engine that examines all incoming and outgoing traffic for protocol deviations, content that signals an attack, or policy violations
- It can operate in detection or prevention mode to protect operating systems and enterprise application vulnerabilities, defending Web applications against application-layer attacks including SQL injection and cross-site scripting

- Detailed events provide valuable information, including who attacked, when they attacked, and what they attempted to exploit. Administrators can be notified automatically via alerts when an incident has occurred

#### Intrusion Detection and Prevention (IDS/IPS) Shield Vulnerabilities Until They Can Be Patched

- Provides protection against known and zero-day attacks
- Vulnerability rules shield known vulnerabilities from an unlimited number of exploits. Automatically shields newly discovered vulnerabilities within hours. Protection can be pushed out to thousands of servers in minutes without a system reboot
- Includes out-of-the-box vulnerability protection for over 100 applications, including database, Web, email, and FTP servers
- Smart rules provide zero-day protection from unknown exploits that attack an unknown vulnerability, by detecting unusual protocol data containing malicious code
- Exploit rules stop known attacks and malware and are similar to traditional antivirus signatures in that they use signatures to identify and block individual, known exploits

### KEY BENEFITS

#### Prevents Data Breaches and Business Disruptions

- Provides a line of defense at the server itself, whether physical, virtual, or in the cloud, preventing data breaches and business disruptions
- Shields known and unknown vulnerabilities in Web and enterprise applications, as well as operating systems, and blocks attacks to these systems
- Enables businesses to identify suspicious activity and behavior and to take proactive or preventive measures

#### Helps Comply with PCI and Other Regulations and Standards

- Addresses six major PCI compliance requirements—including Web application-layer firewall requirements such as file integrity monitoring, Web application-layer firewall, and network segmentation along with a wide range of other compliance requirements
- Provides detailed, auditable reports that document prevented attacks and policy compliance status, and reduces the preparation time required to support audits

#### Achieves Operational Cost Reductions

- Provides security to enable organizations to fully leverage virtualization or cloud computing and to realize the cost reductions inherent in these approaches
- Provides vulnerability protection so that secure coding efforts can be prioritized and unscheduled patching can be implemented more cost-effectively
- Delivers comprehensive protection in a single, centrally managed software agent, thus eliminating the need for, and costs associated with, deploying multiple software clients

### Web Application Protection

- Assists with compliance with PCI Requirement 6.6 for the protection of Web applications and the data that they process
- Offers Web application protection rules that defend against SQL injection attacks, cross-site scripting attacks, and other Web application vulnerabilities, and shield these vulnerabilities until code fixes can be completed

### Application Control Rules to Provide Increased Visibility into, or Control over, the Applications Accessing the Network

- These application control rules can also be used to identify malicious software accessing the network, or to reduce the vulnerability exposure of your servers

### A Firewall Designed to Decrease the Attack Surface of Your Physical and Virtual Servers

- An enterprise-grade, bidirectional stateful firewall providing centralized management of server firewall policy, including predefined templates for common enterprise server types
- The firewall's powerful features and benefits include virtual machine isolation, fine-grained filtering (IP and MAC addresses, ports), coverage of all IP-based protocols (TCP, UDP, ICMP, GGP, IGMP, etc.) and all frame types (IP, ARP, etc.), prevention of denial of service (DoS) attacks, design policies per network interface, location awareness, and detection of reconnaissance scans

### Integrity Monitoring of Files, Systems, and Registry for Changes

- Monitors critical operating system and application files, such as directories, registry keys, and values, to detect malicious and unexpected changes
- Enables on-demand or scheduled detection; extensive file property checking, including attributes (PCI 10.5.5); monitor-specific directories; flexible and practical monitoring through includes/excludes; and auditable reports

### Log Inspection to Ensure Visibility into Important Security Events Buried in Log Files

- Collects and analyzes operating system and application logs for security events while log inspection rules optimize the identification of important security events buried in multiple log entries

- Forwards events to a security information and event management (SIEM) system or centralized logging server for correlation, reporting, and archiving
- Includes suspicious-behavior detection, collection of security-related administrative actions, optimized collection of security events across your datacenter, and advanced rule creation using OSSEC rule syntax

firewall changes typically needed for centrally managed systems

- Software distribution, with agent software that can be deployed easily through standard software distribution mechanisms such as Microsoft® SMS, Novel Zenworks, and Altiris

## ARCHITECTURE

### Third Brigade Deep Security Software Consists of:

- Deep Security Agent, a small software component deployed on the server or virtual machine being protected. It enforces the datacenter's security policy (IDS/IPS, Web application protection, application control, firewall, integrity monitoring, and log inspection)
- Deep Security Manager, a powerful, centralized management system enabling 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
- Security Center, a dedicated team of security experts who help customers stay ahead of the latest threats by rapidly developing and delivering security updates that address newly discovered vulnerabilities, together with a customer portal for accessing these security updates and information. These updates are delivered to the Deep Security Manager system for deployment

## DEPLOYMENT AND INTEGRATION

### Deep Security Software Can Be Deployed Rapidly, Leveraging Existing IT and Security Investments:

- VMware integration with VMware Virtual Center (vCenter) and ESX Server enables organizational and operational information from vCenter and ESX nodes to be imported into Deep Security Manager, and detailed security to be applied to an enterprise's VMware infrastructure
- SIEM integration. Detailed, server-level security events are provided to a SIEM system, including ArcSight™, Intellitactics, NetIQ, RSA Envision, Q1Labs, Loglogic, and other systems through multiple integration options
- Directory integration so that it integrates with enterprise directories, including Microsoft Active Directory
- Configurable management communication, as either the Manager or the Agent can initiate communication. This minimizes or eliminates

**PLATFORMS PROTECTED**

- Microsoft® Windows®:
  - 2000 (32-bit)
  - XP (32-bit/64-bit)
  - XP embedded
  - Windows Vista (32-bit/64-bit)
  - Windows Server 2003 (32-bit/64-bit)
  - Windows Server 2008 (32-bit/64-bit)
- Solaris™ OS: 8, 9, 10 (64-bit SPARC, x86)
- Linux:
  - Red Hat® Enterprise 3.0 (32-bit), 4.0, 5.0 (32-bit/64-bit)
  - SUSE® Enterprise 9, 10 (32-bit)
- UNIX\*: AIX 5.2, HP-UX 10, 11i v2

\* Integrity Monitoring and Log Inspection

**KEY CERTIFICATIONS AND ALLIANCES**

- In addition to a partnership with Trend Micro, Deep Security software leverages these valuable certifications and alliances with Third Brigade:
- Common Criteria EAL 3+
  - PCI Suitability Testing for HIPS (NSS Labs)
  - ICSA Firewall
  - Virtualization by VMware
  - Microsoft Application Protection Program
  - Microsoft Certified Partnership
  - Novell
  - Oracle Partnership
  - HP Business Partnership
  - It is also certified Red Hat Ready

**Trend Micro™ Enterprise Security**

OfficeScan™ and Intrusion Defense Firewall are key components of Trend Micro™ Enterprise Security. Powered by our unique Trend Micro™ Smart Protection Network—Trend Micro Enterprise Security minimizes the time to protect your organization from content security risks, delivering better protection with less complexity.

**ONLINE RESOURCES**

Trend Micro-Third Brigade Web page: <http://us.trendmicro.com/us/partners/strategic-partners/third-brigade/>

**VIRTUALIZATION**

- VMware®: VMware ESX Server (guest OS)
- Citrix®: XenServer Guest VM
- Microsoft®: HyperV Guest VM
- Sun: Solaris 10 OS partitions

Deep Security Modules						
Datacenter Requirement	Deep Packet Inspection			Firewall	Integrity Monitoring	Log Inspection
	IDS/IPS	Web Application Protection	Application Control			
Server Protection	○			○	○	●
Web Application Security	○	○			●	○
Virtualization Security	○	●		○	○	●
Suspicious-Behavior Detection	●		○	○	○	○
Virtual Machine Isolation				○		
Cloud Computing Security	○	●		○	○	○
Compliance Reporting	●	○	●	●	○	○

○ = Essential ● = Advantageous

Trust a Security Industry Leader with a Proven Track Record. A global leader in Internet content security, Trend Micro focuses on securing the exchange of digital information. Trend Micro continues to provide innovation with the Trend Micro Smart Protection Network, correlating real-time data on new and unknown threats and delivering continuously updated protection. Based on extensive content security expertise, Trend Micro provides over five billion dynamically rated Web sites, spam sources, and files every day. Since 1988, Trend Micro has held a singular focus on Internet content security. Meanwhile, other vendors have become distracted as they grow, and some are too narrowly focused on point products. That is why thousands of companies continue to put their trust in Trend Micro—a company with 20 years of experience dedicated to content security and expertise based on a history of innovation. To learn more about Trend Micro Enterprise Security and the Trend Micro Smart Protection Network, contact your Trend Micro representative or visit us online at trendmicro.com.

Third Brigade specializes in server and application protection for dynamic datacenters. Its advanced software and vulnerability response service enables virtual machines and physical servers to become self-defending—safe from the latest online threats. This comprehensive, proven protection helps customers prevent data breaches and business disruptions. It helps with compliance, supports operational cost reductions, and addresses the dynamic nature of datacenters, including virtualization and consolidation, new service delivery models, and cloud computing. Third Brigade also owns and maintains OSSEC, the Open Source Host Intrusion Detection Project, actively used in 50 countries around the world.



© 2009 Trend Micro, Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo, OfficeScan, and Trend Micro Control Manager are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.  
DS01TBDS\_090119

[www.trendmicro.com](http://www.trendmicro.com)