Devising a Server Protection Strategy with Trend Micro

A Trend Micro White Paper

Trend Micro, Incorporated

» Trend Micro's portfolio of solutions meets and exceeds Gartner's recommendations on how to devise a server protection strategy.

How Trend Micro does this is detailed in this white paper.

Executive Summary:

With so many Information Technology solutions available to choose from today, many organizations put their trust in the experience, insight and advice of Gartner, and their industry-leading analysts.

Trend Micro's endpoint solutions, server and client, are consistently rated highly by Gartner and are often featured in the "Leaders' Quadrant" section of the Gartner "Magic Quadrant for Endpoint Protection Platforms". In the latest issue, published on January 16th 2012, Gartner states, "Trend Micro should be considered a strong vendor that's suitable for any enterprise."

Neil MacDonald and Peter Firstbrook, of Gartner published a research note, "How to Devise a Server Protection Strategy" on December 6th, 2011, strongly validating Trend Micro's approach to server security, and specifically acknowledges Trend Micro's leadership in virtualization and cloud security.

Trend Micro's unique, industry first, agentless server security solution has been field-proven for 18 months, and deployed at well over 1000 customer sites – including VMware. Trend Micro provide agent-less integrity monitoring, antivirus, IDS/IPS, firewall and VMware's datacenter protection for increased security with less resource footprint.

Trend Micro's portfolio of solutions meets and exceeds Gartner's recommendations on how to devise a server protection strategy. Precisely how Trend Micro does this is detailed in the sections below.

Devising a Server Protection Strategy with Trend Micro

In the "How to Devise a Server Protection Strategy" overview section, Gartner states that: "Preference should be given to endpoint protection platform vendors that offer a portfolio of capabilities that address all endpoint needs, servers desktops and laptops". Trend Micro's portfolio of solutions provides these capabilities, and more.

Gartner lists 13 server protection priorities along with 12 desktop protection priorities. The 12 desktop priorities are a subset of the 13 server priorities. All 13 are listed below in descending order of server protection importance. All 13 priority technologies can be provided by Trend Micro.

Server Priority (High to Low)	Trend Micro Capability
Security Configuration Management	Yes
Patch Management	Yes
Application control	Yes
File Integrity Monitoring (FIM)	Yes
Antimalware (file servers)	Yes
Deep Packet Inspection based HIPS	Yes
Antimalware (Windows)	Yes
Behavioral HIPS	Yes
Application Firewalling	Yes
Traditional Host Based Firewall	Yes
Device Control	Yes
Full Drive Encryption	Yes
Removable Device Encryption	Yes

1. Security Configuration Management

Trend Micro Vulnerability Management Services enable you to automate the process of your vulnerability management and policy compliance across the enterprise, providing network discovery and mapping, asset prioritization, vulnerability assessment reporting, and remediation tracking according to business risk. Policy compliance features also allow security managers to audit, enforce and document compliance with internal security policies and external regulations.

Additionally Trend Micro Deep Security provides a “Recommendation Scan” which analyses your operating systems and applications, then provides recommendations for virtual patches to apply to shield your systems from vulnerabilities. It offers vulnerability protection for over 100 applications, including database, web, email and FTP servers.

2. Patch Management

Trend Micro Deep Security shields known vulnerabilities from exploits until they can be patched, helping to achieve timely protection against known and zero-day attacks. It uses vulnerability rules to shield a known vulnerability, for example those disclosed monthly by Microsoft, from an unlimited number of exploits. Rules that shield newly discovered vulnerabilities within hours are delivered automatically and can be pushed out to thousands of servers in minutes, without a system reboot.

3. Application Control

Deep Security identifies malicious software accessing the network and increases visibility into, or control over, applications accessing the network. It can identify malicious software accessing the network and reduce the vulnerability exposure of your servers.

4. **File Integrity Monitoring (FIM)**

Again, Deep Security can detect and reports malicious and unexpected changes to files and systems registry in real time. It detects malicious and unexpected changes and uses an agentless configuration to add greater security to virtual machines without additional footprint. Event tagging and cloud-based white listing reduce the complexity of your administrative operations and real-time, on-demand, or scheduled detection of change, all with auditable reports.

5. **Antimalware (file servers)**

Deep Security integrates with VMware environments for agentless protection, or provides an agent for physical servers and virtual desktops in local mode.

It integrates the new VMware vShield Endpoint APIs to provide agentless anti-malware protection for VMware virtual machines with zero in-guest foot print to help avoid security "brown-outs" or "AV storms" commonly seen in full system scans and pattern updates. Gartner recognise that Trend Micro are "well ahead in their virtualization-optimized solutions".

6. **Deep Packet Inspection (DPI) based Host Intrusion Prevention (HIPS)**

Rules are delivered automatically to Deep Security which shield newly discovered vulnerabilities and can be pushed out to thousands of servers in minutes, without a system reboot.

7. **Antimalware (Windows)**

Deep Security also provides agent-based anti-malware to protect physical servers, Windows, Hyper-V and Xen-based virtual servers, public cloud servers, as well as virtual desktops in local mode. It coordinates this protection with both agentless and agent-based form factors to provide adaptive security to defend your virtual servers as they move between the data centre and public cloud.

8. **Behavioural HIPS**

Deep Security uses application-layer protocol decoding to detect and stop invalid behaviour.

9. **Application firewalling**

Deep Security can defend against web application vulnerabilities and enable compliance with PCI Requirement 6.6 for the protection of web applications and the data that they process. It also defends against SQL injections attacks, cross-site scripting attacks, and other web application vulnerabilities. Deep Security also shields vulnerabilities until code fixes can be completed.

10. **Traditional host based firewall**

Deep Security decreases the attack surface of your physical and virtual servers and centralises the management of server firewall policy using a bi-directional stateful firewall. It supports virtual machine zoning and prevents Denial-of-Service attacks. Deep Security provides broad coverage for all IP-based protocols and frame types, as well as fine-grained filtering for ports and IP and MAC addresses.

11. Device control

Trend Micro Endpoint Encryption helps secure server data by offering granular port and device control to prevent unauthorised access and use of private information.

12. Full drive encryption

Trend Micro SecureCloud provides data protection for public and private clouds and your VMware vSphere virtual environments. It protects and controls your confidential information. SecureCloud is an efficient and easy-to-use encryption service that ensures your data is kept privately and helps you meet your regulatory compliance requirements. Additionally, Trend Micro Endpoint Encryption offers enterprise-wide, full disk, file/folder, and removable media encryption.

13. Removable device encryption

Trend Micro Endpoint Encryption allows you to manage both hardware and software encryption for entire hard drives, specific files, folders, removable media, and storage devices with the flexibility to seamlessly transition between multiple forms of encryption.

Other server protection technologies

Gartner also recommend Secure Web and Mail Gateways and specific Collaboration server security solutions, and again, Trend Micro can provide award-winning solutions for all of these protection points, underpinned by our unique Smart Protection Network to secure your infrastructure and provide safe, real-time collaboration to employees, partners, and customers.

Conclusion:

Trend Micro's portfolio of industry leading solutions meets and exceeds Gartner's recommendations on how to devise a server protection strategy. Gartner have highly rated Trend Micro's Endpoint solutions, which have featured consistently in the "Leaders' Quadrant" in the "Magic Quadrant for Endpoint Protection Platforms".

Gartner has recognised Trend Micro as a leader in Virtualization and Cloud Security with our unique agentless server security solution, which has been field-proven for 18 months and currently protects 250,000 virtual machines.

So, no matter what you need to secure, or how narrow or broad your requirements, Trend Micro has the security solution designed to protect your vital data and provides you with the confidence that you are following the advice and recommendations of the leading industry analysts:

"Trend Micro should be considered a strong vendor that's suitable for any enterprise"
Gartner: Magic Quadrant for Endpoint Protection Platforms (Published: January 16, 2012)

TREND MICRO™

Trend Micro Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our Web site: www.trendmicro.com.

TREND MICRO INC.
U.S. toll free: +1 800.228.5651
phone: +1 408.257.1500
fax:+1408.257.2003

www.trendmicro.com.