Trend Micro Deep Security

Server Security

Protecting the Dynamic Datacenter

A Trend Micro White Paper | August 2009

I. SECURITY IN THE DYNAMIC DATACENTER

The purpose of IT security is to enable your business, not impede it, but the challenges and complexity you face for your IT security grow every day. Compliance requirements impose security standards for data and applications on servers. Physical servers are replaced with virtual machines to save money, be green, and increase scalability. Cloud computing evolves the traditional IT infrastructure to increase cost savings while enhancing flexibility, capacity, and choice. Servers are no longer barricaded behind perimeter defenses, and like laptops before them, they're now moving outside the security perimeter and need a last line of defense. It's now vital to your defense-in-depth security strategy to deploy a server and application protection system delivering comprehensive security controls while supporting current and future IT environments. Trend Micro delivers answers to these challenges, including the Deep Security solution.

SERVERS ARE UNDER PRESSURE

According to the Verizon Business Risk Team's 2008 Data Breach Investigations Report, 59% of recent data breaches were the result of hacking and intrusions. The TJX and Hannaford breaches underlined the potential for system compromises to negatively impact the reputation and operations of any business in significant ways. Organizations continue to struggle to balance the need to protect their resources with the need to extend access to those same resources to more business partners and customers.

Current Payment Card Industry Data Security Standards (PCI DSS) recognize that traditional perimeter defenses are no longer sufficient to protect data from the latest threats, and that they now require multiple layers of protection beyond appliance-based firewall and intrusion detection and prevention systems (IDS/IPS). Wireless networks, encrypted attacks, mobile resources, and vulnerable Web applications all contribute to the weakness that exposes enterprise servers to penetration and compromise.

Within the past five years, datacenter computing platforms, which largely had been based on physical servers, have undergone a major technology change. The traditional datacenter footprint is shrinking to enable cost savings and "greener" IT through server consolidation. Nearly every organization has virtualized some or all of its datacenter workloads, enabling multitenant uses of what previously had been single-tenant or single-purpose physical servers. The Gartner Group expects that between now and 2011, the installed base of virtual machines will expand more than tenfold—and it is expected that by 2012, the majority of x86 server workloads will be run within virtual machines.

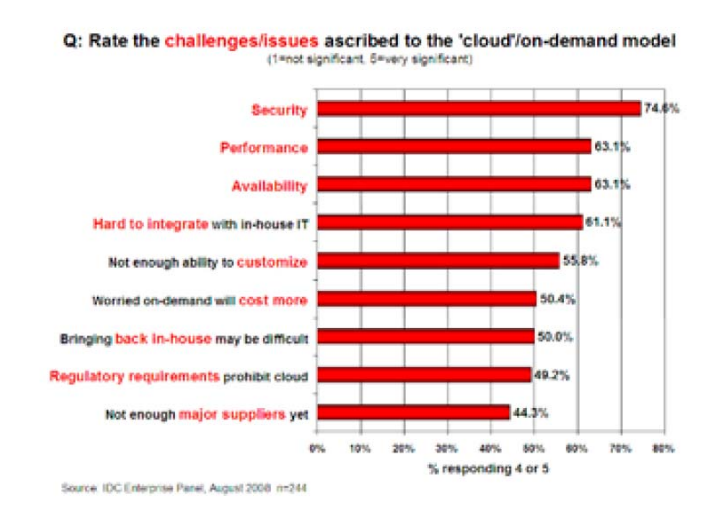
SERVERS ARE MULTIPLYING RAPIDLY AND IN MOTION

The significant benefits IT virtualization offers organizations have led to widespread adoption. Virtualization increases capacity and responsiveness to corporate demands, and more efficient use of hardware and software licenses results in continued consolidation of server workloads. In virtual environments, strict separation between network devices and servers diminishes—these are now combined within virtualization platforms. However, since network security appliances are blind to traffic sent between virtual machines, hosting workloads of different sensitivities opens up the opportunity for attacks. Motion tools—critical for managing planned downtime, effective use of virtualization resources, and application availability—result in additional workload sharing on the server, impacting compliance history management and virtual security appliances.The inevitable "sprawl" of virtual machines also increases the likelihood of exposure to malicious traffic for those without the latest patches. IT personnel must closely examine the methods used to protect virtual instances of enterprise servers.

SERVERS OPEN IN THE CLOUD

Cloud computing extends an enterprise's ability to meet the computing demands of its everyday operations. With the growing number of organizations taking advantage of cloud computing, and service providers building public clouds, the security model is further challenged to effectively host these virtualized workloads. Security is the area that causes the greatest hesitation in organizations when it comes to moving business workloads into public clouds. When IDC recently conducted a survey of 244 IT executives/CIOs and their line-of-business (LOB) colleagues to gauge their opinions and understand their companies' use of IT cloud services, security ranked first as the greatest cloud computing challenge.

When a server is moved to public cloud resources, the datacenter perimeter offers no protection, as these virtualized servers now provide administrative access directly over the Internet. Problems already faced in the datacenter, such as patch management and compliance reporting, become commensurately more complex as a result. The only relevant protection in the cloud is the lowest common denominator that the vendor can provide on its perimeter—or whatever an organization can equip its virtual machine with to defend itself, since it is hosted on servers alongside other organizations' workloads.



Source: IDC Enterprise Panel, August 2008 n=244

"By far, the #1 concern about cloud services is security. With their businesses' information and critical IT resources outside the firewall, customers worry about their vulnerability to attack."

—Frank Gens, Senior Vice President and Chief Analyst, IDC

II. OVERVIEW: TREND MICRO DEEP SECURITY

The Trend Micro Deep Security solution is server and application protection software that unifies security across virtual, cloud computing, and traditional datacenter environments. It helps organizations prevent data breaches and business disruptions, enable compliance with key regulations and standards including PCI, and help reduce operational costs as the current economic climate requires. The Deep Security solution enables systems to become self-defending and is optimized to help protect your confidential data and ensure application availability. The Deep Security solution provides comprehensive protection, including:

- Deep packet inspection enabling Intrusion detection and prevention (IDS/IPS), web application protection, and application control
- Stateful firewall
- File and system integrity monitoring
- Log inspection

III. COMPREHENSIVE, MANAGEABLE SECURITY

The Deep Security solution uses modules to address key server and application protection requirements:

	Deep Security Modules					
Datacenter Requirement	Deep Packet Inspection			Firewall	Integrity Monitoring	Log Inspection
	IDS/IPS	Web Application Protection	Application Control			
Server protection – Protection against known and zero-day attacks – Shield vulnerabilities until patching	●			●	●	○
Web application protection – Protection against Internet attacks such as SQL injection, cross-site scripting, and brute force attacks – Meets PCI DSS requirement 6.5 — Web-application firewall	●	●			○	●
Virtualization security – Protection against known and zero-day attacks – Shield vulnerabilities until patching – VMware vCenter integration enhances visibility and management	●	○		●	●	○
Suspicious-behavior detection – Protection against reconnaissance scans – Detection of allowed protocols over inappropriate ports – Alert on OS and application errors that could signal an attack – Alert on critical OS and application changes	○		●	●	●	●
Cloud computing security – Use firewall policies to isolate virtual machines – Protection against known and zero-day attacks – Shield vulnerabilities until patching	●	○		●	●	●
Compliance reporting – Visibility and audit trail of all changes to critical servers – Inspection, correlation, and forwarding of important security events to logging servers for remediation, reporting, and archiving – Reports on configurations, activity detected and prevented	○	●	○	○	●	●

● = Essential ○ = Advantageous

IV. BENEFITS

Datacenter server security architectures must address changing IT architectures, including virtualization and consolidation, new service delivery models, and cloud computing. For all of these datacenter models, Deep Security solutions help to:

- Prevent data breaches and business disruptions by:
  - Providing a line of defense at the server itself—whether physical, virtual, or cloud
  - Shielding known and unknown vulnerabilities in Web and enterprise applications, as well as in operating systems, and blocking attacks to these systems
  - Empowering you to identify suspicious activity and behavior and to take proactive or preventive measures
- Enable compliance by:
  - Addressing six major PCI compliance requirements—including Web application security, file integrity monitoring, and server log collection—along with a wide range of other compliance requirements
  - Providing detailed, auditable reports documenting prevented attacks and policy compliance status, reducing the preparation time required to support audits
- Support operational cost reductions by:
  - Offering vulnerability protection so that secure coding efforts can be prioritized and unscheduled patching can be implemented more cost-effectively
  - Providing the security necessary for organizations to fully leverage virtualization or cloud computing and to realize the cost reductions inherent in these approaches
  - Delivering comprehensive protection in a single, centrally managed software agent—eliminating the need for, and costs associated with, deploying multiple software clients

V. MODULES AND FUNCTIONALITY

The Deep Security solution enables you to deploy one or more protection modules, engaging just the right amount of protection to meet your changing business requirements. You can opt to create self-defending servers and virtual machines by deploying comprehensive protection, or start with the Integrity Monitoring module to uncover suspicious behavior. All modular functionality is deployed to the server or virtual machine by a single Deep Security Agent, which is centrally managed by Deep Security Manager software and unified across physical, virtual, and cloud computing environments.

DEEP PACKET INSPECTION (DPI) ENGINE

Enabling Intrusion Detection and Prevention, Web Application Protection, and Application Control
The solution's high-performance deep packet inspection engine examines all incoming and outgoing traffic, including SSL traffic, for protocol deviations, content that signals an attack, and policy violations. It can operate in detection or prevention mode to protect operating systems and enterprise application vulnerabilities. It protects Web applications from 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. DPI is used for intrusion detection and prevention, Web application protection, and application control.

INTRUSION DETECTION AND PREVENTION (IDS/IPS)

Shields Vulnerabilities in Operating Systems and Enterprise Applications Until They Can Be Patched, for Timely Protection Against Known and Zero-Day Attacks

Vulnerability rules shield a known vulnerability—for example, those disclosed on 'Microsoft Tuesday'—from an unlimited number of exploits. The Deep Security solution includes out-of-the-box vulnerability protection for over 100 applications, including database, Web, email, and FTP servers. Rules shielding newly discovered vulnerabilities are automatically delivered within hours, and they can be pushed out to thousands of servers in minutes without a system reboot:

- Smart rules provide zero-day protection from unknown exploits attacking unknown vulnerabilities, by detecting unusual protocol data containing malicious code.
- Exploit rules stop known attacks and malware and are similar to traditional antivirus software in that they use signatures to identify and block known individual exploits.

As a result of being an inaugural member of the Microsoft Active Protections Program (MAPP), the Deep Security solution receives vulnerability information from Microsoft in advance of their monthly security bulletins. This advance notice makes it possible to anticipate emerging threats and to provide mutual customers with more timely protections effectively and efficiently via security updates.

WEB APPLICATION SECURITY

The Deep Security solution enables compliance with PCI requirement 6.6 for the protection of Web applications and the data they process. Web application protection rules defend against SQL injection attacks, cross-site scripting attacks, and other Web application vulnerabilities, shielding these vulnerabilities until code fixes can be completed. The solution uses smart rules to identify and block common Web application attacks. A SaaS datacenter deploying Deep Security was able to shield 99% of all high-severity vulnerabilities discovered in its Web applications and servers, through a customer-requested penetration test.

APPLICATION CONTROL

Application control rules provide increased visibility into, or control over, the applications that are accessing the network. These rules can also be used to identify malicious software accessing the network, or to reduce the vulnerability of your servers.

FIREWALL

Decreasing the Attack Surface of Your Physical and Virtual Servers

The Deep Security Firewall software module is enterprise grade, bidirectional, and stateful. It can be used to enable communications over ports and protocols necessary for correct server operation and to block all other ports and protocols, reducing the risk of unauthorized access to the server. Its features include:

- Virtual machine isolation: enabling virtual machines to be isolated in cloud computing or multitenant virtual environments, providing virtual segmentation without modifying virtual switch configurations.
- Fine-grained filtering: filtering traffic with firewall rules on: IP addresses, Mac addresses, ports, and more. Different policies can be configured for each network interface.
- Coverage of all IP-based protocols: Supporting full-packet capturing simplifies troubleshooting and provides valuable insight into understanding raised firewall events—TCP, UDP, ICMP, and more.
- Reconnaissance detection: detects activities such as port scan. Non-IP traffic such as ARP traffic can also be restricted.
- Flexible control: The stateful firewall is flexible, enabling complete bypass of inspection in a controlled manner when appropriate. It addresses ambiguous traffic characteristics that can be encountered on any network, due to normal conditions or as part of an attack.
- Predefined firewall profiles: grouping common enterprise server types—including Web, LDAP, DHCP, FTP, and database—ensuring rapid, easy, consistent deployment of firewall policy, even in large, complex networks.
- Actionable reporting: With detailed logging, alerting, dashboards, and flexible reporting, the Deep Security Firewall software module captures and tracks configuration changes—such as what policy changes have been made and who made the changes—providing a detailed audit trail.

INTEGRITY MONITORING

Monitoring Unauthorized, Unexpected, or Suspicious Changes

The Deep Security Integrity Monitoring software module monitors critical operating system and application files—such as directories, and registry keys and values—to detect suspicious behavior. Its features include:

- On-demand or scheduled detection: Integrity scans can be scheduled or performed on-demand.
- Extensive file property checking: Files and directories can be monitored for changes to: contents, attributes—such as owners, permissions, and size—and time-and-date stamp using out-of-the-box integrity rules. Additions, modifications, or deletions of Windows registry keys and values, access control lists, and log files can also be monitored and alerted. This capability is applicable to the PCI DSS 10.5.5 requirement.
- Auditable reporting: The Integrity Monitoring module can display integrity events within the Deep Security Manager dashboard, generate alerts, and provide auditable reports. It is also able to forward events to a security information and event management (SIEM) system via Syslog.
- Security profile groupings: Integrity monitoring rules can be configured for groups or individual servers, to simplify deployment and management of monitoring rulesets.
- Baseline setting: Baseline security profiles can be established and used to compare for changes, to initiate alerts and determine appropriate actions.
- Flexible, practical monitoring: The Integrity Monitoring module offers flexibility and control to optimize the monitoring activities for your unique environment. This includes the ability to include/exclude files or wildcard filenames and include/exclude subdirectories in scan parameters. It also gives the flexibility to create custom rules for unique requirements.

LOG INSPECTION

Finding and Learning from Important Security Events Buried in Log Files

The Deep Security Log Inspection software module provides the ability to collect and analyze operating system and application logs for security events. Log inspection rules optimize the identification of important security events buried in multiple log entries. These events are forwarded to a SIEM system or centralized logging server for correlation, reporting, and archiving. The Deep Security Agent will also forward the event information to the Deep Security Manager. Some of the benefits of the Log Inspection module include:

- Suspicious-behavior detection: The module provides visibility into suspicious behavior that might occur on your servers.
- Collecting events across your environment: The Deep Security Log Inspection module is able to collect and correlate: events across Microsoft Windows, Linux, and Solaris platforms; application events from Web servers, mail servers, SSHD, Samba, Microsoft FTP, and more; as well as custom application log events.
- Correlate different events: Collect and correlate diverse warnings, errors, and informational events, including system messages—such as disk full, communication errors, services events, shutdown, and system updates—application events—such as account login/logout/failures/lockout, application errors, and communication errors—and administrative actions—such as administrative login/logout/failure/lockout, policy changes, and account changes.
- Auditable reporting for compliance: A complete audit trail of security events can be generated to assist with meeting compliance requirements such as PCI 10.6.

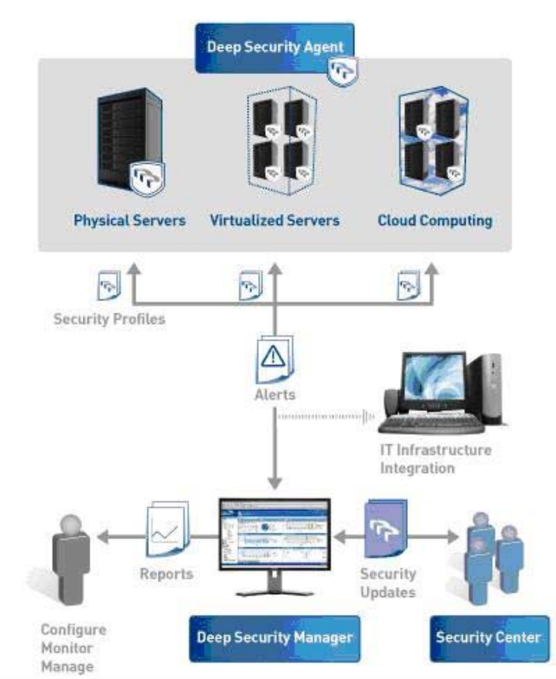
VI. DEEP SECURITY SOLUTION ARCHITECTURE

The Deep Security solution architecture comprises three components:

- Deep Security Agent, which is deployed on the server or virtual machine being protected.
- Deep Security Manager, which provides centralized policy management, distribution of security updates, and monitoring through alerts and reports.
- Security Center, a hosted portal where a dedicated vulnerability research team develops rule updates for emerging threats—these updates are periodically pulled by the Deep Security Manager.

HOW IT WORKS

The Deep Security Agent receives a security configuration, typically a security profile, from the Deep Security Manager. This security configuration contains the deep packet inspection, firewall, integrity monitoring, and log inspection rules enforced on the server. The rules to be assigned to a server can be determined simply by performing a recommendation scan, which scans the server for installed software and recommends the rules required to protect the server. Events are created for all rulemonitoring activities, and these events are sent to the Deep Security Manager and optionally to a SIEM system. All communication between Deep Security Agents and the Deep Security Manager is protected by mutually authenticated SSL.



The Deep Security Manager initiates polling of the Security Center to determine whether a new security update is available. When a new update is available, it is retrieved by the Deep Security Manager and either manually or automatically applied to the servers requiring the additional protection that the update provides. Communication between the Deep Security Manager and Security Center is also protected by mutually authenticated SSL. The Deep Security Manager also connects to other elements of the IT infrastructure to simplify management. The Deep Security Manager can connect to VMware vCenter, as well as to directories such as Microsoft Active Directory, to obtain server configuration and grouping information. The Deep Security Manager also has a Web services API, which can be used to programmatically access functionality.

The Security Center monitors both public and private sources of vulnerability information in order to protect the operating systems and applications in use by customers.

DEEP SECURITY MANAGER

The Deep Security solution provides practical, proven controls that address difficult security problems. Operational and actionable security gives your organization knowledge—not just information—about a security event. In many cases, this is about supplying the “who, what, when, and where” so that events can be properly understood and subsequent actions can be taken—beyond what is performed by the security control itself. Deep Security Manager software addresses both security and operational requirements, with features including:

- Centralized, Web-based management system: Create and manage security policies, and track threats and preventive actions taken in response to them, from a familiar, explorer-style UI.

- Detailed reporting: A wide selection of detailed reports document attempted attacks and provide an auditable history of security configurations and changes.
- Recommendation scan: Identify applications running on servers and virtual machines and recommend which filters should be applied to these systems, ensuring the correct protection with minimal effort.
- Risk ranking: Security events can be viewed based on asset value as well as vulnerability information.
- Role-based access: Enable multiple administrators, each with different levels of permission, to operate different aspects of the system and to receive information appropriate to them.
- Customizable dashboard: Enable administrators to navigate and drill down to specific information and to monitor threats and preventive actions taken. Multiple personalized views can be created and saved.
- Scheduled tasks: Routine tasks—such as reports, updates, backups, and directory synchronization—can be scheduled for automatic completion.

DEEP SECURITY AGENT

The Deep Security Agent is a server-based software component of the Deep Security solution, enabling IDS/IPS, Web application protection, application control, firewall, integrity monitoring, and log inspection. It defends the server or virtual machine by monitoring incoming and outgoing traffic for protocol deviations, content that signals an attack, or policy violations. When necessary, the Deep Security Agent intervenes and neutralizes the threat by blocking the malicious traffic.

SECURITY CENTER

The Security Center is an integral part of the Deep Security solution. It consists of a dynamic team of security experts who help customers stay ahead of the latest threats by providing a timely and rapid response to a broad range of new vulnerabilities and threats as they are discovered, together with a customer portal for accessing security updates and information. Security Center experts apply a rigorous, six-step, rapid response process supported by sophisticated and automated tools:

- Monitor: Over 100 sources of public, private, and government data are systematically and continuously monitored to identify and correlate new relevant threats and vulnerabilities. The Security Center researchersleverage relationships with different organizations to get early and sometimes prerelease information on vulnerabilities, so that timely and accurate protection can be delivered to customers. These sources include Microsoft, Oracle, and other vendor advisories; SANS; CERT; Bugtraq; VulnWatch; PacketStorm; and Securiteam.
- Prioritize: The vulnerabilities are then prioritized for further analysis, based on an assessment of risk to customers along with service-level agreements.
- Analyze: An in-depth analysis of the vulnerabilities is conducted to identify the necessary protection.
- Develop and test: Software filters that shield the vulnerabilities, and rules that recommend filters, are then developed and extensively tested to minimize false positives and ensure that customers can deploy them quickly and smoothly.
- Deliver: The new filters are delivered to customers as security updates. Customers receive immediate notice via an alert in Deep Security Manager when a new security update is released. These filters can then be automatically or manually applied to the appropriate servers.
- Communicate: Ongoing communication with customers is provided through security advisories, which provide detailed descriptions of the newly discovered security vulnerabilities.

PROACTIVE RESEARCH FURTHER ENHANCES PROTECTION

In addition, the Security Center team conducts ongoing research to improve overall protection mechanisms. This work is strongly influenced by results and trends uncovered during the vulnerability and threat response process. These results also impact both how new filters and rules are created and the quality of existing protection mechanisms, ultimately improving overall protection.

PROTECTING A BROAD RANGE OF VULNERABILITIES

The Security Center develops and delivers filters protecting commercial off-the-shelf applications as well as custom Web applications. Exploit and vulnerability filters are reactive, in that they are used in response to the discovery of a known vulnerability. In contrast, smart filters provide proactive protection. Integrity monitoring filters check various system components and their specific properties, and they alert the administrator when specific triggering conditions are met. Some of the components that can be monitored include system directories, files, Windows registry, user accounts, ports, and network shares. Log inspection filters parse logs from operating system and third-party applications, and they alert the administrator when specific events have occurred.

SECURITY CENTER PORTAL

The Security Center portal provides customers with a single, secure point of access to product-related information and support, including:

- Security updates
- Security advisories
- CVSS score information in vulnerabilities
- Alert summaries for Microsoft Tuesday
- Advanced search for vulnerabilities
- Full disclosure of vulnerabilities, including those not protected by Third Brigade
- Patch information for each vulnerability
- RSS feeds
- Trouble tickets
- Software downloads
- Product documentation

VII. DEPLOYMENT AND INTEGRATION

The Deep Security solution is designed for rapid enterprise deployment. It leverages and integrates with existing infrastructure and investments to help achieve greater operational efficiency and to support operational cost reductions.

- VMware integration: Tight integration with VMware vCenter and ESX Server enable 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 through multiple integration options to SIEM, including ArcSight, Intellitactics, NetIQ, RSA Envision, Q1Labs, LogLogic, and other systems.
- Directory integration: Integrates with enterprise directories, including Microsoft Active Directory.
- Configurable management communication: The Deep Security Manager or Deep Security Agent can initiate communication. This minimizes or eliminates firewall changes typically needed for centrally managed systems.
- Software distribution: Agent software can be deployed easily through standard software distribution mechanisms such as Microsoft SMS, Novell Zenworks, and Altiris.
- Optimized filtering: Advanced capabilities for dealing with streaming media, such as Internet protocol television (IPTV), to help maximize performance.

VIII. THE DEEP SECURI TY DIFFERENCE

Trend Micro server and application protection addresses the challenging operational security and compliance needs of today's dynamic datacenter. We provide comprehensive protection, greater operational efficiency, superior platform support, and tighter integration with existing investments, and we are more responsive to customer requirements. With Deep Security solutions, you can obtain:

- Deeper protection: including stateful firewall, intrusion detection and prevention, application-layer firewalling, file and system integrity monitoring, and log inspection—in a single solution.
- Greater operational efficiency: Deploying quickly and widely, and automating many key tasks—including the recommendation of appropriate protection to be applied to each server—the solution can be managed more efficiently, with minimal impact on existing IT resources.
- Superior platform support: Providing full functionality across more platforms, and supporting current versions of these platforms more quickly, enables you to continue to adopt the newest virtualization platforms and operating system releases without sacrificing protection.
- Tighter integration: Offering tighter integration with IT infrastructure, including directory and virtualization platforms—and other best-of-breed security investments such as SIEM—helps ensure effective enterprise deployment and continued vendor flexibility.

For more information please call or visit us at.
www.trendmicro.com/go/enterprise
+1-877-21-TREND