VISIBILITY INTO DATA CENTER SECURITY AND OPERATIONS MANAGEMENT WITH TREND MICRO AND VMWARE

VMware and Trend Micro have partnered to deliver the first security and operations management solution designed for virtualized environments. Today, most organizations are highly virtualized on VMware, and this has produced significant savings. VMware and Trend Micro are committed to creating solutions that optimize security, manageability, and business continuity, while allowing IT to meet service level agreements (SLAs).

CHALLENGES

SECURITY

Most organizations are running a legacy agent-based antivirus product in their virtual environment. In the fast-changing virtual environment, it is difficult to keep this agent-based security up to date. Also, antivirus as a technology is insufficient to protect against today's sophisticated threats. However, the burden of managing more security agents (in addition to antivirus) causes most organizations to live with an inordinate level of risk to the virtual environment.

MANAGEABILITY

Administrators need to provision security agents in new virtual machines. Continuously reconfiguring these agents as virtual machines move around or change state and rolling out pattern updates on a regular basis, can be extremely time consuming.

BUSINESS CONTINUITY

When traditional antivirus solutions initiate scans simultaneously, or when security updates run on all virtual machines on a single physical host—an "antivirus storm" can cause application slowdowns and loss of business continuity.

MEETING SERVICE LEVEL AGREEMENTS

Many organizations are in reactive mode and lack the ability to analyze performance trends, proactively identify abnormalities, and identify the root cause of problems in dynamic virtualized environments.

CAPACITY PLANNING

Without capacity utilization tools, organizations frequently under- or over-provision, negatively impacting their virtualization savings.

SOLUTION OVERVIEW

VMware and Trend Micro have partnered to deliver the first security and operations management solution designed for VMware® vSphere environments.

The joint solution includes the following components:

- **vCenter Operations Manager** is VMware's recommended solution to proactively ensure performance, utilization, and availability of infrastructure and applications running on vSphere, Hyper-V, Amazon, or hardware—using predictive analytics and policy-based automation.
- **Trend Micro™ Deep Security**, the market leader in security for virtualization and cloud, provides a next-generation server security platform specifically designed for virtual and cloud environments. Its agentless architecture delivers comprehensive protection from advanced threats, minimizes operational complexity, improves business continuity, and allows organizations to accelerate virtualization and cloud adoption. Deep Security provides a hardened security virtual appliance that integrates with vSphere at the hypervisor level to offer agentless antivirus, web reputation, integrity monitoring, and intrusion prevention for VMware virtual machines.
- **Trend Micro Deep Security Management Pack for vCenter Operations** allows the operations team to see the security status, security related events and overall health of the virtual data center from a single view. This allows the operations team to correlate system activity with security activity and address problems in the virtual data center holistically.

ENHANCING VIRTUALIZED DATA CENTER OPERATIONS WITH SECURITY MANAGEMENT

Trend Micro Deep Security Management Pack for vCenter Operations gives the virtualization operations team the ability to see virtual machine security status and operational status from a single view. This allows the operations team to correlate system activity with security activity and address problems in the virtual data center holistically. Image 1 depicts the view within vCenter Operations Manager v5.8.x (Advanced edition) once the Deep Security management pack adapter has been activated. It immediately provides information such as the list of computers that Deep Security is protecting along with an overview of each computer's overall health. Note that to leverage the integration with Deep Security, you must have access to the Advanced edition of vCenter Operations Manager v5.8.x.

Key Benefits for Businesses

Trend Micro Deep Security with VMware vCenter Operations (Advanced edition) delivers unique benefits including:

- a real-time unified dashboard that allows the operations team to correlate IT and security incidents in their environment and be more effective in responding to these events
- correlation between security incidents and virtual machine operations that can save hours or days of debugging and prevent costly downtime of decommissioned VMs
- increased visibility into security events on computers protected by Deep Security
- a quick visual representation, through a heat map, that shows which computers have had security events triggered
- an Intuitive metric-graph that shows what events are being triggered and the peak numbers and times of these events
- a Top 'N' Analysis report of computers that have had security events triggered

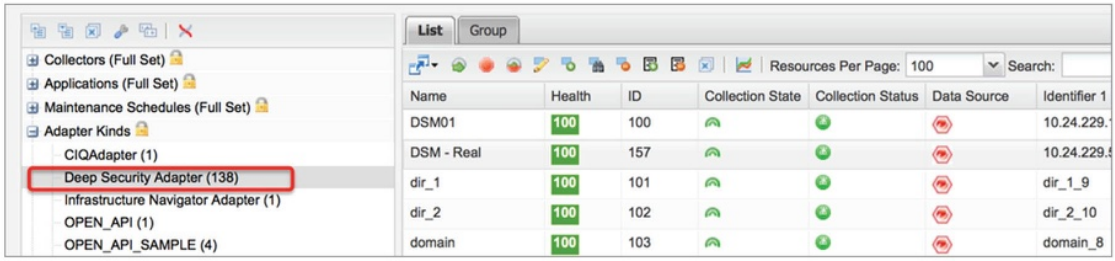

IMAGE 1: VMware vCenter Operations (Advanced edition) with Trend Micro Deep Security

PERFORMANCE ANALYSIS

Trend Micro Deep Security with VMware vCenter Operations Manager v5.8.x (Advanced edition) enables organizations to compare security event activity with performance activity. For example (image 2), we are looking at SQL server (top left) activity. We can see that at the CPU Demand is at 30 percent and then increases sharply to 88 percent. The security event metrics (bottom left) show that the number of security events has also gone up. The detailed information for the security activity (right) shows that these events were due to firewall and malware events being triggered. The jump in security activity and possible threats is likely impacting the performance and causing the spike. The operations team can now inform the security team of their findings and the machines with security events can be examined in detail.

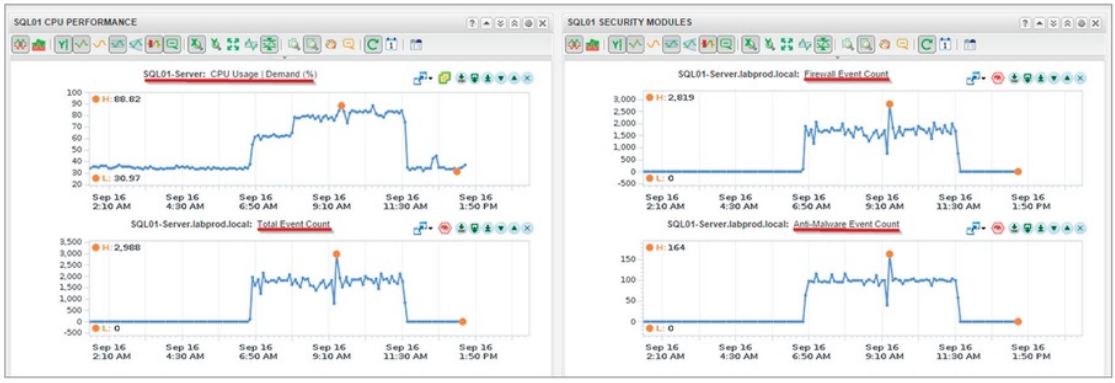

IMAGE 2: Performance Analysis

SECURITY ANALYSIS

The Deep Security Heat Map (image 3) quickly lets you see which computers are under attack the most at any given time. Like other vCenter Operations Heat Maps, green indicates fewer events occurring on a particular computer while red indicates more security events triggered. These events can be any of the events in Deep Security Manager; Anti-Malware, Intrusion Prevention, Integrity Monitoring, Firewall, and Web Reputation.

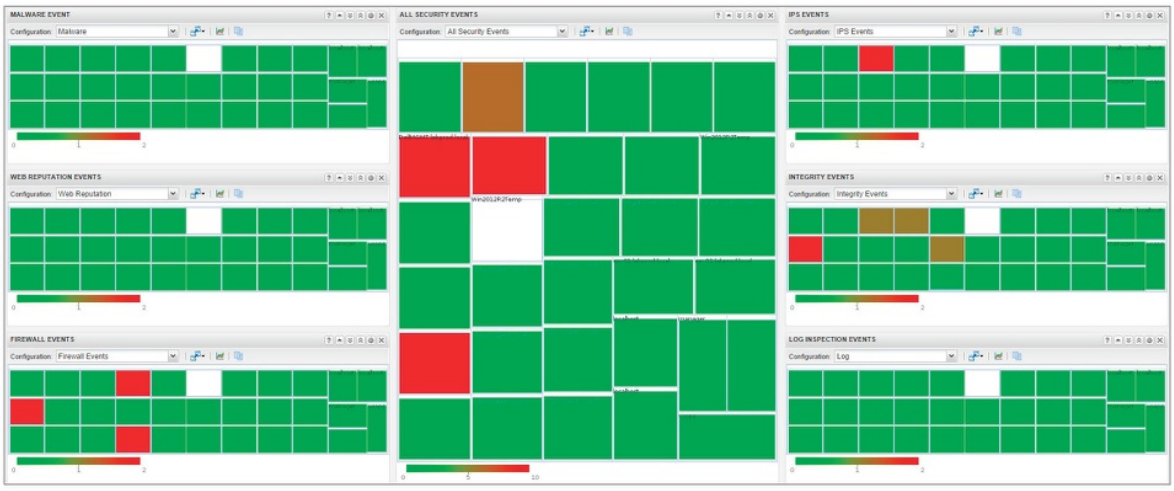

IMAGE 3: Security Analysis—Heat Map

Clicking on the Heat Map will give you the Metric Graph (image 4) for that particular machine. Operations teams can see individual graphs for each type of security event: Anti-Malware, Intrusion Prevention, Integrity Monitoring, Firewall, and Web Reputation. These graphs share critical information such as total events over time and highest/lowest event counts. This enables a quick overview of the peak time events are being triggered, as well as the specific security events being triggered.

IMAGE 4: Security Analysis—Metric Graph

SIMPLIFIED SECURITY WITH TREND MICRO DEEP SECURITY

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

It combines multiple, tightly integrated modules including anti-malware, web reputation, integrity monitoring, log inspection, and intrusion prevention to prevent data breaches. This enables advanced server security, application security, and data security across virtual machines (VMs).

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 consuming fewer system resources and supporting higher VM densities.

With Deep Security, you gain:

- comprehensive virtualization security with multilayered protection—with four modules that protect the entire virtual environment
- orders-of-magnitude better manageability due to the single virtual appliance, rather than up to hundreds of in-guest agents to provision, maintain, patch, and update
- improved business continuity through mitigation of application outages from infections, prevention of antivirus storms, and virtual patching to shield vulnerabilities from exploits and prevent unplanned downtime from emergency patching
- a lighter, more manageable way to secure VMs that delivers more efficient resource utilization and higher VM densities than traditional agent-based solutions

The Deep Security agentless architecture has been market tested in thousands of real-world customer deployments including large enterprises and midsize businesses. Trend Micro users consistently cite strong improvements in security and manageability. In addition, our customers have been able to achieve breakthrough VM densities of about 300 VMs/host, up to seven times higher than what was previously possible with an agent-based security product.

vmware®

www.vmware.com/go/vrops

TREND MICRO™

www.trendmicro.com/datacenter

Get More Information

BLUE IT SOLUTIONS

Vía Borelli 201 Col. Fuentes del Valle
San Pedro Garza García, N.L. 66224
www.blueitsolutions.com
marketing@blueitsolutions.com
T. (81) 8174-0500