Technology Partner

Dell and Trend Micro Boost VM density with AV Design for VDI

As enterprises move to virtual desktops, they quickly learn that VDI environments are quite different from physical environments. The conventional antivirus solutions used within physical desktops to keep the corporate network safe simply do not work well in a VDI environment.

Using traditional AV poses significant performance challenges on the shared VDI server hardware, leaving end-users negatively impacted. In the end, enterprises are forced to choose between poor VDI Return on Investment (ROI) or compromised security configurations along with a potential lack or regulatory compliance.

Dell understands the unique challenges of VDI deployments and the importance of properly securing virtual desktop environments. That's why they are partnering with Trend Micro, a leader in virtualization security, and tested the Trend Micro Deep Security solution for VDI.

Simplifying VDI Deployments

Deep Security can improve the overall management of VDI deployments. With an agentless AV solution, administrators can manage a single virtual appliance, rather than hundreds of VMs, allowing them to focus on other opportunities to support business goals.

In addition to delivering superior performance for Dell VDI customers, Trend Micro Deep Security offers powerful capabilities to simplify security and ensure compliance:

- Integrity Monitoring
- Intrusion Detection and Prevention
- Web Application Protection
- Application Control
- Firewall
- Log Inspection

Test Results Highlight Increased AV/AM Virtual Machine Density

To measure the effectiveness of Deep Security's agentless AV solution for VDI, Dell researchers compared it to a traditional, agent-based AV solution. The validation test was performed on a VMware View 5 and ESXi 5 VDI stack, which consisted of a management host, compute host, Force10 S60 Network Switch and an Equalogic PS4100. The VDI pool for the validation test consisted of 120 VMs, all configured for a "basic" workload.

Three testing categories were used for the validation: no AV standard, agent-based AV and Trend Micro Deep Security agentless AV. In addition, a scheduled "scan" was performed with both standard agentless AV and Deep Security AV. The results show that Deep Security's agentless AV solution's VMdensity supported more than twice as many VMs as agent-based AV in basic mode. The results also show that Deep Security supported more than three times as many VMs with a standard mode, and seven times more in premium mode.

	Basic	Standard	Premium
No AV	138	110	81
Agent-based Desktop AV	50	25	10
Virtualized Trend Micro	120	96	70

Tested to determine how many VMs the environment could support.

Basic – The basic User workload profile consists of simple task worker workloads. Typically a repetitive application use profile with a non-personalized virtual desktop image. Sample use cases may be a kiosk or call center use cases which do not require a personalized desktop environment and the application stack is static. In a virtual desktop environment the image is dynamically created from a template for each user and returned to the desktop pool for reuse by other users. The workload requirements for a basic user is the lowest in terms of CPU, memory, network and Disk I/O requirements and will allow the greatest density and scalability of the infrastructure.

Standard – The Standard User workload profile consists of email, typical office productivity applications and web browsing for research/training. There is minimal image personalization required in a standard user workload profile. The workload requirement for a Standard User is moderate and most closely matches the majority of office worker profiles in terms of CPU, memory, network and Disk I/O. This will allow moderate density and scalability of the infrastructure.

Premium – The Premium User workload is an advanced knowledge worker. All office applications are configured and utilized. The user has moderate – to-large file size (access, save, transfer requirements). Web browsing use is typically research/training driven, similar to Standard Users. The Premium User requires extensive image personalization, for shortcuts, macros, menu layouts etc. The workload requirements for a Premium User are heavier than typical office workers in terms of CPU, memory, Network and Disk I/O. This will limit density and scalability of the infrastructure.

These results clearly illustrate that using the traditional, agent-based approach to securing virtual desktops limits the amount of VMs that can be run concurrently, which can impair user experience and reduce the benefits of VDI.

A VDI-aware solution implemented to take advantage of VMware vShield Endpoint API-such as Deep Security – dramatically improves the overall VDI density per ESX host. By simultaneously sharing resources without degrading performance, Deep Security's agentless, virtual appliance approach enables much higher VM density that traditional agent-based AV.

About Trend Micro Inc.

Trend Micro, a global leader in security software and solutions, strives to make the world safe for exchanging digital information. For the past 25 years, its employees have been inspired to protect individuals, families, businesses and governments as they look to harness the potential of emerging technologies and new ways of sharing information.

In today's organizations, information has become the most strategic asset; embodying competitive advantage and powering operational excellence. With the explosion of mobile, social and cloud technologies, protecting this information has become more challenging than ever. Organizations need smart protection of information, with technology that is simple to deploy and manage, and security that fits an evolving ecosystem. Trend Micro solutions enable a smart protection strategy for organizations. Smart. Simple. Security that fits.

Trend Micro provides layered content security for mobile devices, endpoints, gateways, servers and the cloud. Leveraging these solutions, organizations can protect their end users, their evolving data center and cloud resources, and their information threatened by sophisticated targeted attacks.

All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For additional information, visit www.trendmicro.com.

The Dell Technology Partner Program

Trend Micro Inc. is a Dell Technology Partner and Deep Security is certified by Dell to run on the Dell platforms specified in the technical architecture section.

The Dell Technology Partner program is a multi-tier program that includes ISVs, IHVs and Solution Providers. This global program helps partners build innovative and competitive business solutions using Dell platforms. Program resources keep customer costs low and help sustain competitiveness.

The program has a structured and streamlined process that combines technology and business strategies with Dell Solution Center expertise to onboard and test partner products on Dell platforms. This testing process helps ensure that products have met the technical requirements to perform well on Dell platforms.