Eric Ogren
92 Robert Road
Stow, MA 01775
m: 978•618•9240
eric@ogrengroup.com

Endpoint Security: Become Aware of Virtual Desktop Infrastructures!

An Ogren Group Special Report

May 2011

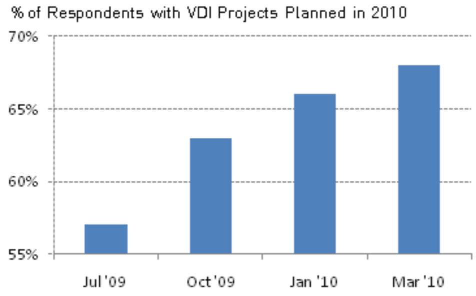
Executive Summary

Virtual desktops infrastructures, VDI, present IT with the unique opportunity to fundamentally improve the way desktops are purchased, deployed, managed, and secured. Organizations are attracted to VDI's promise to reduce operating costs, provide users with wide choices of devices, improve application performance, and enhance corporate security against malware and loss of sensitive data. The benefits are compelling, with survey data showing approximately 70 percent of CIOs reporting VDI projects planned for 2010.

However, enterprises find while scaling from proof-of-concept projects to full deployment that desktop security software that is not optimized for VDI causes storage and network contention that significantly degrades virtual machine densities. The Ogren Group recommends the following guidelines in selecting endpoint security to help organizations preserve the benefits of VDI:

- **Choose endpoint security that is specifically designed for VDI performance.** Endpoint security needs an architecture that avoids performance drags from storage and network resource contention as tens of desktop virtual machines, VMs, populate a physical server.
- **Require intelligent use of cloud-based security to keep agent bloat from affecting VDI density.** The discovery rate of new attacks is absolutely exploding. Evaluate approaches that scale by blocking attacks in the cloud, and do not steadily increase processor demands for VM-based endpoint security.
- **Insist on VDI-aware approaches allowing endpoint security to simplify administration of virtual and physical desktops.** Since organizations will need to operate a mix of physical and virtual endpoint security, the security software should be optimized for each environment for user satisfaction, and ease of administration.

CIO Interest in Desktop Virtualization has Increased Steadily over the Past Year



Source: Morgan Stanley CIO Surveys

Trend Micro's OfficeScan and Deep Security products are designed for use in VDI environments. The Ogren Group finds that Trend Micro exceeds requirements for protecting the business while enabling IT to realize the benefits of virtual desktop infrastructures. This special report, commissioned by Trend Micro, presents the case for endpoint security that is specifically architected to be VDI-aware, enabling organizations to securely evolve from physical desktops to virtual desktop infrastructures. Information in this report derives from independent Ogren Group research and interviews with enterprise security officers of global organizations.

Preserve VDI performance with VDI-aware security

The resource sharing nature of virtual desktops can lead to contention for storage and network resources when the number of desktops per server is scaled up to production levels. Traditional endpoint security that is completely contained within each desktop VM aggregates file scanning and pattern file update loads across each server. The performance degradation of the cumulative load leads IT teams to cut densities in less than half – requiring more servers and reducing operational cost savings from VDI. The Ogren Group recommends that organizations test the performance of endpoint security with fully loaded servers, and evaluate vendor features for VDI support such as:

- **Scan scheduling to disperse storage system loads.** Balance the load of file scans across desktop VMs to avoid contention and performance spikes.
- **Acquire pattern file updates efficiently – avoid the "9 AM problem".** Reduce the number of pattern file updates requested by each physical server to avoid network contention that can sap VDI performance.
- **Ensure that increased pattern matching loads are not replicated within each virtual desktop.** With the number of identified threats increasing every day, require that VDI-aware security share resources in filtering attacks – either in the cloud or as a security VM for the physical server. For example, Trend Micro's Smart Protection Network blocked 5 billion threats in 2010, *before* the threats reached corporate networks.

Competitive solutions approach the VDI-aware problem with desktop agents that randomize scan activity and pattern file updates, and some postpone security functions when the server is stressed by high CPU loads. These approaches are still vulnerable to concurrency issues affecting VDI performance, and worse they may result in desktop VMs operating with non-compliant security pattern files. Trend Micro's VDI-aware offerings minimize the processing required by each desktop VM with an architecture that can scale as both the number of virtual desktops and the number of identified threats increase.

Cover the spectrum of users and security

Endpoint security that is VDI-aware detects when the desktop is virtualized, and acts to leverage shared resources on the physical server. The ability to detect the operating environment is critical as organizations migrate from physical to virtual desktops and the VDI use cases evolve. The main use cases to consider span the spectrum from full desktop replacement, to shared workstations and locally-hosted virtual desktops – all of which must be integrated with physical desktop security.

- **Replace desktops.** Instead of maintaining a distributed infrastructure of physical desktops, IT centralizes desktop processing on servers in the data center. Security is challenged to recognize when it is operating on a device that is shared with other desktops.

- **Offer shared workstations.** Shared devices, with limited Web connectivity and application choices, provide cost-effective interfaces to virtual desktops.
- **Secure checked out desktops.** The ability to stream virtual desktops to personal devices is critical for supporting remote users. Since no security assumptions can be made about the operating environment, checked out virtual desktops must be self-reliant with "full-strength" security.
- **Integrate security with physical desktops.** As organizations evolve to increase the mix of virtual desktops, endpoint security must also evolve to protect the business against malware and data loss.

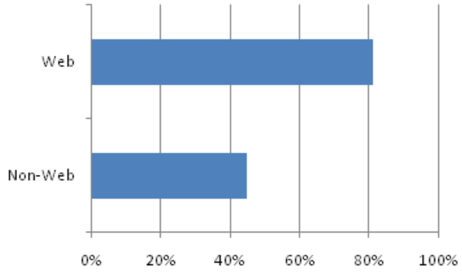
Replace physical desktops with full security

Organizations embrace VDI for enhancements in performance and security, such as to ensure compliant endpoint configurations, keep sensitive data secure in the data center, provide users wide choices of computing devices, and optimize transaction performance to data center resident applications and databases. The "replace physical desktops" use case entails persistent desktop VMs with full Internet access. Users require comprehensive endpoint security within each desktop VM, with features that are able to:

- **Optimize protection against Web, email, and file threats.** The Web is the now the source of most attacks, accounting for 80 percent of identified attacks, with file based attacks accounting for 40% (with allowances for hybrids).
- **Control sensitive data.** Inspecting content for the presence of regulated data or intellectual property with data leakage protection (DLP) technology is required to protect the organization against compliance violations and public disclosure events.
- **Plug vulnerabilities.** A key layer of defense is to close vulnerabilities before they are exploited. Virtual patching eliminates the time gap between identification of a vulnerability and deployment of a patch to desktop virtual machines.

VDI Security Needs Balanced
Protection Against Web and Non-Web Threats

Infection Vector Profile of the Top 30 Malware from
April to September 2010 (Web vs. Non-Web)



Source: Trend Micro ThreatTrends 2010

- **Monitor activity to detect zero day attacks.** The last line of defense is to monitor desktop VM activity for signs of inappropriate behavior that signals the presence of a zero day attacks or advanced persistent threat (APT).
- **Integrate firewall features.** Users require full Internet access in desktop replacement scenarios, necessitating firewall features to block unauthorized communications.

Check out locally-hosted desktops

Many users will have a need access to their desktops from remote locations, and cannot rely on high performance network connectivity to the desktop VM hosted in the corporate data center. These users "check out" their desktop virtual machine, installing a temporary copy onto their laptop or remote device. The VDI-aware endpoint security supports the locally hosted use case by operating full-strength security within the desktop VM as if it were protecting a physical endpoint.

Share workstations between users

At the other end of the spectrum from physical desktop replacement, is the use case of users sharing workstations. In the shared workstation scenario, users typically have a limited selection of approved applications, may have restricted Web connectivity, the desktop VMs have short life spans, and sensitive data is cleaned to leave a pristine state for the next user. While users require best-of-breed security, the transitory nature of virtual desktops in shared workstation scenarios creates additional requirements, including:

- **Simplify management with one security VM per server.** It is easier to administer the bulk of endpoint security in a security VM, without the requirement to support remote users and persistent desktops.
- **Keep security memory and CPU footprints light to maximize desktop VM density.** Shared workstations located in tightly controlled environments can tune security policy enforcement to keep desktop virtual machines agile and responsive.
- **Tightly integrate with the virtualization infrastructure.** Security can scan dormant desktop VMs for infections, whitelist base images after scanning to increase performance, and take full advantage of hypervisor security services.

Integrate security of physical and virtual desktops

As organizations evolve to virtual desktop infrastructures, security will need to support a changing mix of virtual and physical desktops – it is unlikely that businesses will become 100 percent virtualized. There will always be physical desktops to secure; there will always be virtual desktops to secure. Security teams should not have to manage separate security products for virtual desktops and physical desktops. Integration of virtual and physical security approaches is critical for maintaining a compliant and secure infrastructure:

- **Require common administration for physical and virtual desktops.** Management of security and security reporting for compliance is simplified with a common administrative interface for both physical and virtual desktops.
- **Require automated VDI-aware security.** Endpoint security software must be able to identify and adjust to its environment – a physical desktop or virtualized on Citrix, Microsoft, or VMware servers.

Conclusions and recommendations

Businesses face a dual a challenge in re-architecting their approach to desktop management with virtual desktop infrastructures, and in effectively securing VDI implementations. Ogren Group research has found a surprising number of organizations with VDI projects that have stalled because traditional approaches to desktop security cause performance-killing contention for shared CPU storage, and network resources. Organizations require a VDI-aware architecture that leverages virtualization, allows virtual desktops to be locally hosted with full security, and integrates with protection of the physical infrastructure. Trend Micro has responded to the challenges of VDI-aware security with approaches that the Ogren Group recommends, with products such as:

- OfficeScan. Trend Micro's OficeScan product is a VDI-aware implementation that protects desktops from Web, email and file-based threats. Working in conjunction with the Smart Protection Network, OfficeScan lowers infection rates and can cut administrative costs by 40 percent.
- Deep Security. Trend Micro's Deep Security is designed specifically for the needs of servers in the data center. While OfficeScan protects virtual desktops, Deep Security protects the underlying physical server with intrusion detection and prevention, firewall, integrity monitoring, log inspection, and anti-malware defenses.
- Smart Protection Network. Trend Micro performance scales against the explosion of threats by detecting and blocking identified attacks in the cloud. Threats can be mitigated before the attacks penetrate the corporate infrastructure and before consuming desktop resources.

It is More Efficient to Stop Threats Before they Reach the Desktop VM

By the end of 2010, Trend Micro's Smart Protection Network will be blocking 5 billion threats daily.

Source: Trend Micro ThreatTrends 2010

The Ogren Group believes that Trend Micro has shown real industry leadership in its approach to securing virtual desktop infrastructures. Its VDI-aware OfficeScan protects desktop VMs, Deep Security adds protection without requiring real estate within the desktop VM, and Smart Protection Network prevents endpoints from being overloaded with security inspections. VDI provides tangible performance, cost savings, and user satisfaction benefits to the business – Trend Micro's security enables security teams to protect the business while those benefits are realized. The Ogren Group recommends Trend Micro to security teams evaluating solutions for secure virtual desktop infrastructures.