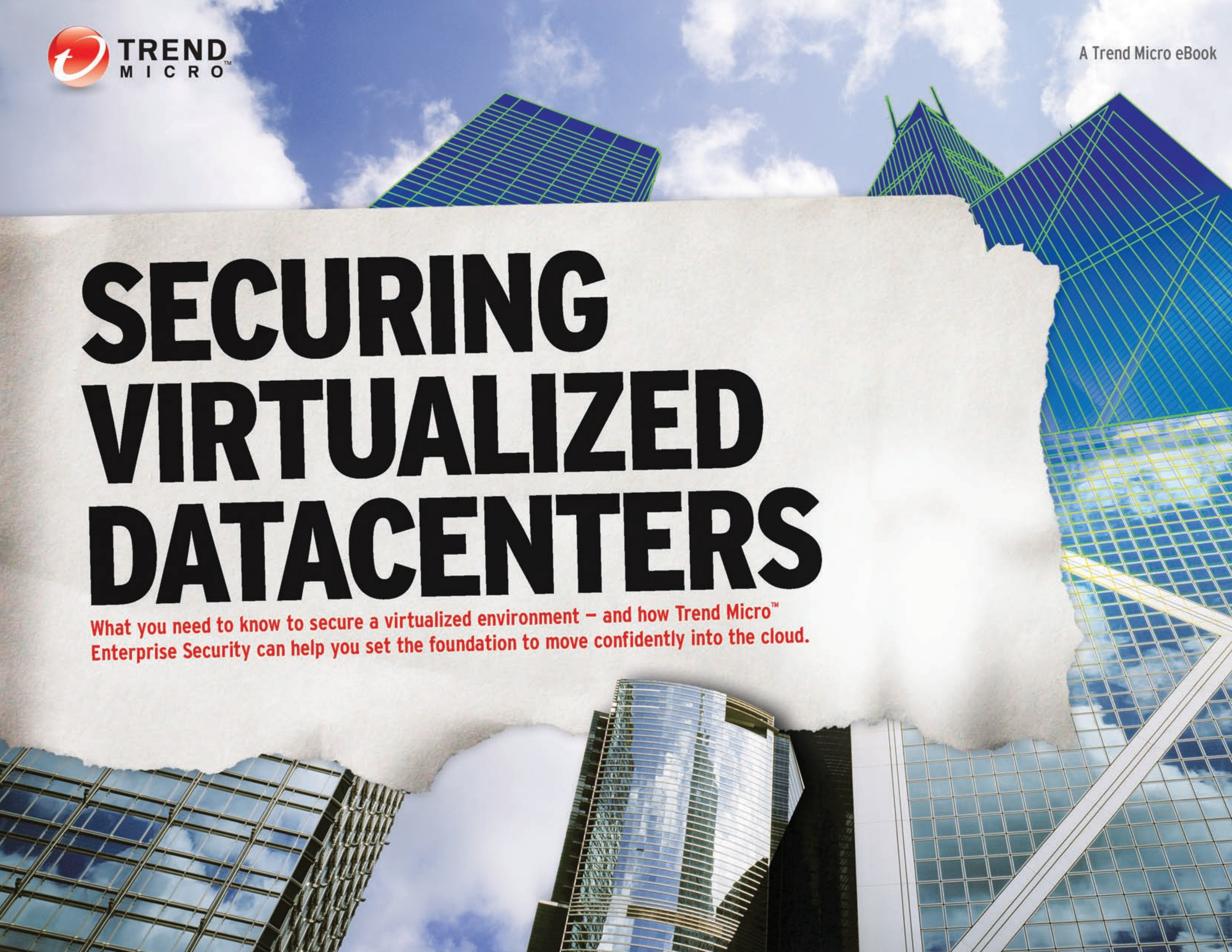
TREND MICRO™

A Trend Micro eBook

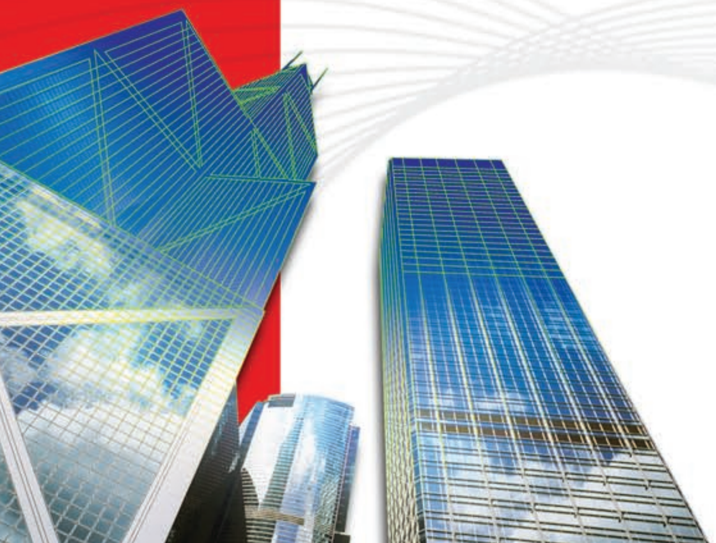
SECURING VIRTUALIZED DATACENTERS

What you need to know to secure a virtualized environment — and how Trend Micro™ Enterprise Security can help you set the foundation to move confidently into the cloud.



A Trend Micro eBook / 2009

Table of Contents



1 Introduction: Virtualization: You Can't Afford Not To...

There's been a quiet revolution in the datacenter over the past few years. No longer do you see IT staff rolling out new hardware every time a new application or service is needed. With today's budget constraints and the mandate to "go green,' organizations are demanding that their IT infrastructure be more lean, efficient and cost-effective than ever.

To meet these goals, IT groups have been consolidating their applications and storage onto fewer servers, reducing hardware footprints and energy usage. The key enabling technology for consolidation is virtualization, which allows you to run numerous "virtual machines" on a single physical server.

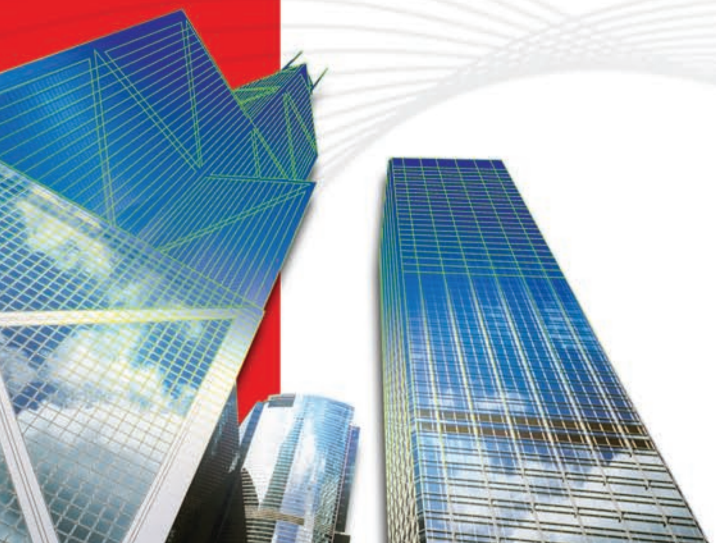
Virtualization not only lets you optimize utilization of assets, but also enables IT departments to fine-tune infrastructure to meet business demands. It's much easier to deploy new virtualized applications and workloads on an existing server than it is to procure, configure, and install new hardware. Virtualization enables the redundancy and quick provisioning that businesses need to compete effectively.

As a "green" technology, virtualization slashes power and cooling requirements in the datacenter. VMware, a leading provider of virtualization solutions, estimates that for every workload that is virtualized, a company will save more than $550 a year in power and cooling expenses. [VMware Market Opportunity Study, Server and Infrastructure Virtualization, January 2007.]

The appeal of the cost savings, flexible capacity, and failover that virtualization enables is undeniable. The big question is: Can today's datacenter balance this increased flexibility with the need to maintain security policies and control over applications, along with the ability to prove compliance?

Gartner found that a typical non-virtualized x86/x64 server environment uses less than 10 percent of its available computing power at any given time, causing significant power and cooling problems.
- Gartner, "Data Center Power and Cooling Scenario: Options for the Road Ahead," Pages 2-3, April 2007

North America and Europe deployed more virtual than physical servers in 2008. Read the article



2 A New Environment to Secure

The very concept of the datacenter and how to protect and secure the integrity of the infrastructure is being transformed. On the surface, virtualized datacenters appear to have all of the same vulnerabilities and security challenges as conventional datacenters. In a conventional datacenter, you can achieve a baseline of security by locking servers behind strong doors, protecting network access by a perimeter firewall and hardware-based intrusion detection and prevention systems.

With virtual machines, new challenges minimize the effectiveness of these protections. Virtual machines require more than perimeter security because of the dynamic way in which VMs can easily be moved, created and replicated among physical servers.

As virtual environments become more complex, it becomes more difficult to maintain security along with audit trails that enable compliance. Virtual management systems enable virtual machines to zoom across virtual networks, losing their security context and opening the possibility of VMs on the same server attacking each other.

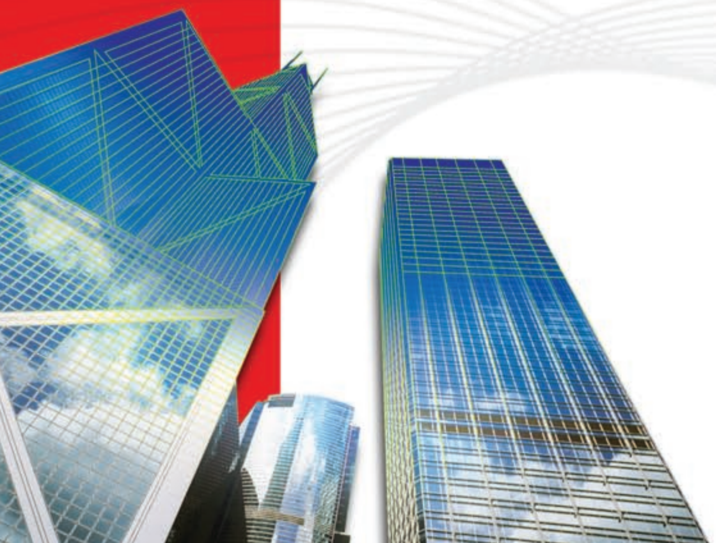
Enterprises are further challenged by the need to develop and enforce coherent security policies for servers that run virtualized mission-critical applications within dynamic environments.

Multiple Layers of Defense

To protect virtual environments, you need multiple layers of defense. Beyond the perimeter firewall and network intrusion devices, you have to ensure the security policies and protection mechanisms on all VMs can be maintained, so that your consolidation levels can increase.

You have to monitor overall system integrity and be able to detect suspicious activity across the ever increasing number of VMs. It is important that live migration of virtual machines does not compromise the security and compliance of production systems.

> Gartner predicts the number of deployed virtual machines will grow tenfold by 2012.
> - October 7, 2009 Virtual Machines and Market Share Through 2012, Thomas Bittman



3 Invisible Challenges of Virtualization Security

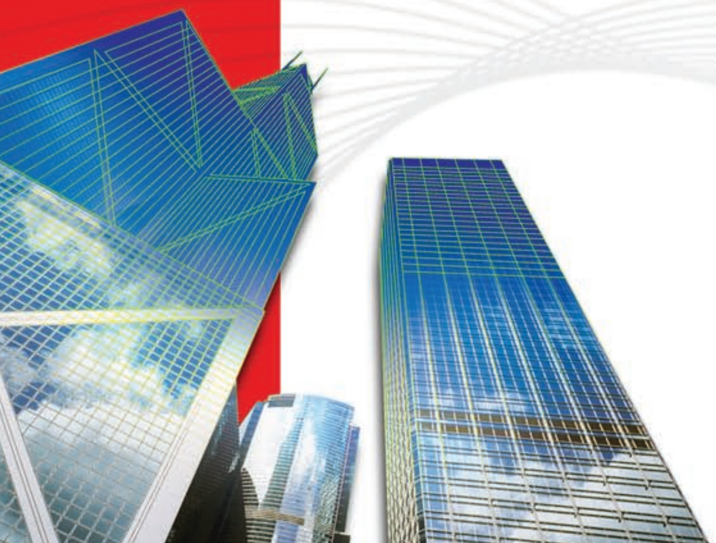
When an enterprise moves its applications and workloads to virtual servers, it expects to gain fast provisioning, instant additional capacity, and reduced costs in hardware, power and cooling. What it might not expect to get, however, are a host of new security challenges.

The difficulty in securing a virtual environment can be partly blamed on its complexity. The "server sprawl" of yesterday's datacenter is giving way to a new phenomenon – VM sprawl. Virtual environments that optimize resource allocations result in virtual machines that are in constant motion. By their nature, virtual machines are also inherently dynamic – pausing and restarting, reverting to previous instances, being cloned and moving among multiple physical servers.

In this dynamic environment, vulnerabilities and configuration errors can spread accidentally or undetected. It can also be difficult to monitor and maintain auditable records of the security states of these virtual machines. Regulatory compliance requirements and best practices demand that IT be able to prove the security of its systems, including those using virtual machines.

We've mentioned the risk of virtual machines on the same server attacking each other. Virtualized servers use the same operating systems and applications as physical servers. Attackers and malware can target VMs as easily as any other environment, and once a VM is compromised, there is greater risk of compromise for all VMs located on the same physical server. Combining the risk of inter-VM attack with the movement of VMs within the virtualized environment expands this risk exponentially.

60% of production virtual machines are less secure than their physical counterparts Read the article



4 The Risk of Dormant Virtual Machines

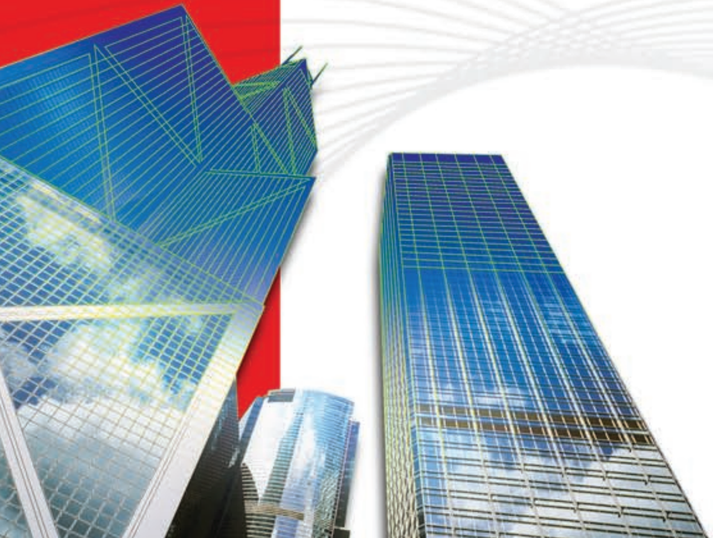
In the traditional datacenter, when a physical server is off, it does not change, it is safe from attack until it is brought back online. The same cannot be said in virtual environments. An offline VM may be paused, dormant or, worse, compromised.

Conventional anti-virus and anti-malware tools fall short in virtual environments. When a virtual machine is taken offline or is dormant, it loses the ability to run these conventional programs. Yet offline VMs are vulnerable to infection by any malware or infected applications that can access virtual machine storage over the network.

Also, sleeping VMs can be backed up or archived to other servers and storage devices for extended periods of time. This time lapse guarantees that patch levels or security programs will be out of date when the VM is restarted. Conventional tools are not able to meet this dynamic security challenge.

According to a recent study, 90 percent of known vulnerabilities that were exploited had patches available for at least six months prior to the breach. [2008 Data Breach Investigations Report, Verizon Business Risk Team]. Because of the difficulty in taking mission-critical systems offline for patching, and the fact that many legacy systems will never have patches available, some companies are turning to "virtual patching" or "vulnerability shielding" as a means to prevent the exploitation of known vulnerabilities.

Gartner VP Neil MacDonald: Virtualization will be the target of new security threats. Read the article



5 Lure of the Cloud

Even as virtualization is spreading rapidly among organizations seeking to become more agile and cut capital expenses, another phenomenon is taking hold: the move to cloud computing.

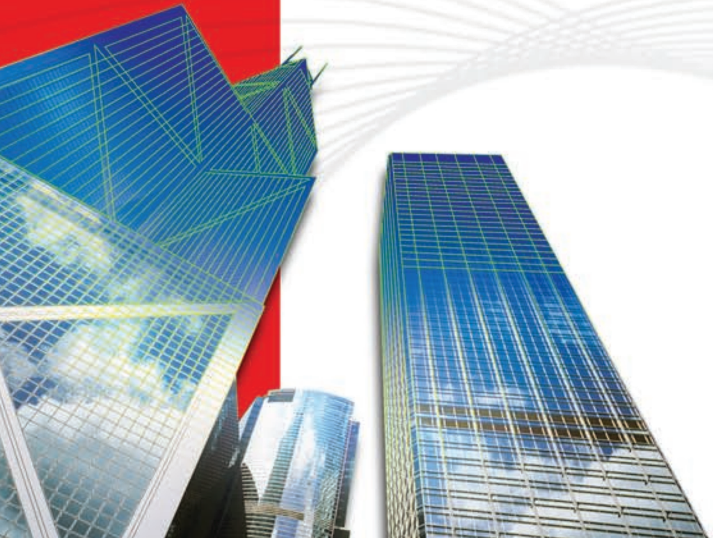
Cloud computing providers use virtualization for the same reasons as corporate datacenters - scalability, flexibility, and high asset utilization. Of course, cloud-services customers don't have to buy and maintain hardware, or pay for power and cooling. And it is easy to almost instantly expand computing capacity and provision new applications and services.

Many businesses prefer to manage their own IT environments using virtualization to optimize efficiency in a "private cloud." For peak demand periods, some of these companies will utilize public cloud computing services, renting the extra capacity as needed.

The Question of Security

But organizations make a big trade-off when they use cloud-based services - they outsource a level of control and responsibility for security to a third party. The particular challenges of securing virtual environments and maintaining an audit trail for compliance means that in all instances, the move to cloud computing must include a review of the potential impact on enterprise security.

Because it's so easy to access cloud computing - all you need is a credit card - IT departments are effectively competing with service providers in the cloud. To win this competition, IT groups will need to provision computing resources quickly and deliver responsive, high-quality, and secure service to their user groups.



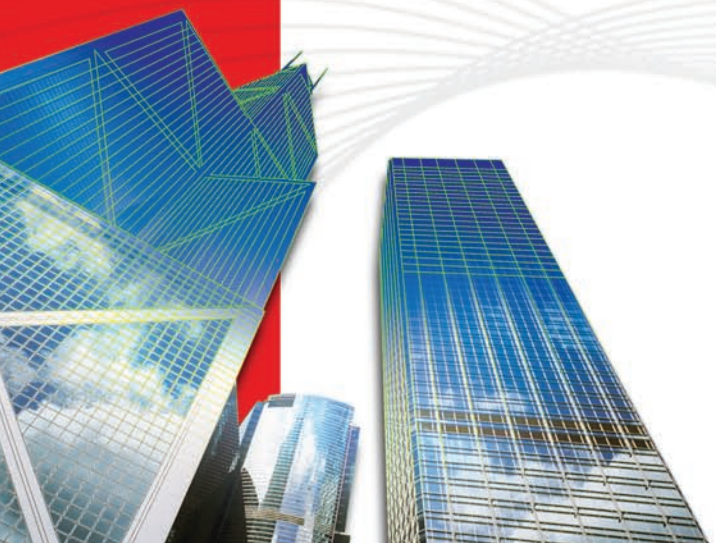
6 Private or Public, Cloud Can Be Secure

In the last year of media hype on cloud computing, security has emerged as the overwhelming concern preventing public cloud deployments. The lack of control over the network perimeter is just the start of the list of security challenges that should concern anyone considering cloud computing.

In cloud deployments we rely on administrative connectivity to servers and applications accessible only via the Internet. The potential for vulnerability exploits from co-located cloud servers and the need to ensure data protection and data integrity in these co-located cloud hosting environments is enough to keep any self-respecting CIO awake at night. They legitimately ask:

- *Who owns the logs?*
- *Where is my data?*
- *How do I prove to auditors that these resources are adequately protected?*
- *(and, perhaps the most important question:) What risks are being taken by others, both unmanaged and unidentified by my team?*

These are critical questions when considering public cloud deployments. Nearly all the same risks exist equally in private cloud deployments and virtualized datacenters. Thankfully, technologies are emerging that can address these security challenges and span the transformation of the datacenter, from physical to virtual and cloud computing servers.



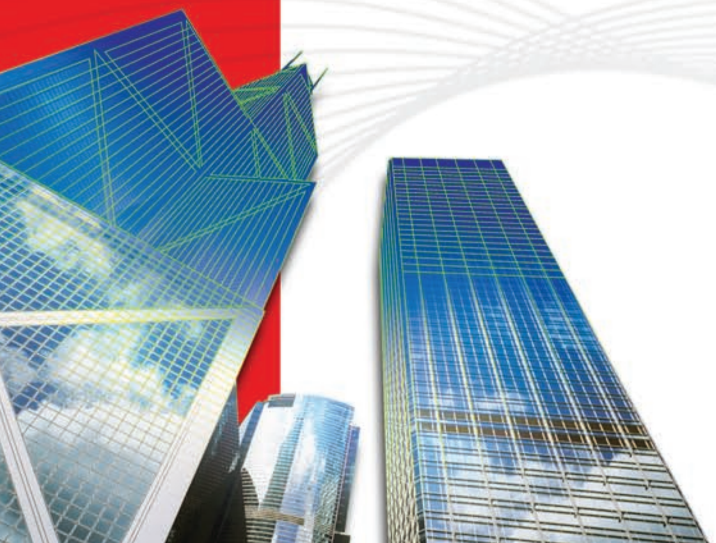
7 Protecting the Virtual Machine

Because virtualized environments are equally vulnerable to security breaches as physical servers, enterprises must take positive action to evolve their IT security to meet the dynamic nature of virtual machines.

To maintain the integrity of virtual machines, security must be a priority, with people, processes, and technologies aligned. All servers – whether physical, virtual or cloud – must have their own defenses activated from the moment they are booted.

Here's the secret: it is imperative to adapt your security perimeter and apply security mechanisms as close to the virtual machine as possible – **the server must be able to protect itself**. It is crucial to ensure that security maintains the performance and flexibility of virtual servers while delivering optimal protection.

Fortunately, this VM-centric focus allows you to achieve security without significant impact to your architecture. Applying comprehensive security mechanisms at the VM enables virtual machines to become self defending against the increasingly sophisticated attacks launched by for-profit hackers.



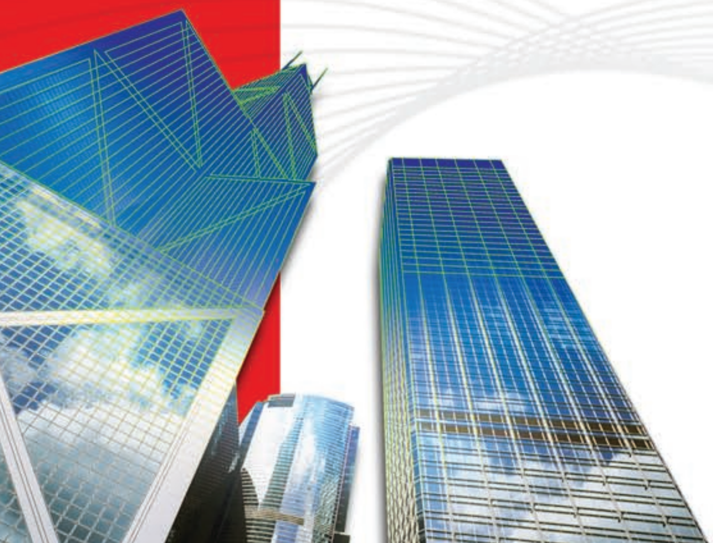
8 Appliances and Agents

The first step that enterprises moving to virtualization usually take is to try to adapt existing security technologies to the new virtualized environment. Organizations that have traditionally relied on network appliances to deliver firewall and intrusion detection and prevention (IDS/IPS) typically turn first to the equivalent virtual appliance (or virtual security appliance) to monitor traffic between virtual switches and guest VMs. However, this approach has significant limitations and can require extensive network configuration.

The first generation of virtual security appliances, which do not leverage hypervisor-aware security capabilities, cannot prevent attacks between VMs on the same vSwitch. Moreover, the security appliance is rendered ineffective if a VM is moved from one physical server to another, unless all appliances are configured for every possible destination of a VM – a process that is resource intensive and would impact performance.

Alternatively, enterprises that rely on host-based security mechanisms on physical servers, such as local firewalls and host intrusion prevention systems, can continue to install security agents on each virtual machine to achieve immediate protection for those VMs. This approach minimizes the potential performance impacts by removing security bottlenecks, and avoids the main shortcomings of first generation virtual security appliances.

However, the shortcomings of conventional software become apparent when faced with the dynamic nature of virtualized environments. As an example, although templates can aid in making sure that common security agents are installed in each virtual machine, it is still possible for non-secure VMs to be accidentally introduced to the production environment.



9 The Dark Side of Consolidation

Virtualization is designed to deliver better asset utilization, since multiple VMs can reside on a single physical server. In fact, the leading virtualization platforms have taken this concept a step further. As a prime example, VMware vMotion enables instant, live migration of virtual machines from one physical box to another to ensure instantaneous optimization of resource usage.

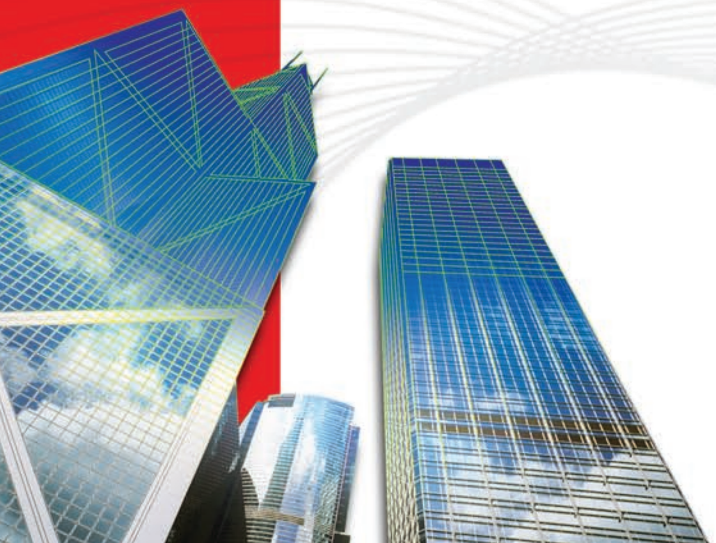
We previously mentioned the immediate security challenge this poses for virtual machines that do not carry their security posture from one physical environment to another. Security context and audit capabilities are lost in the act of migration.

Conventional security solutions, such as anti-virus and anti-malware, also present an additional challenge in consolidated and migrating environments. These solutions typically rely on two methods of scanning to maintain protection and identify malware to be cleaned from infected systems – light-weight, realtime scans, plus more resource-intensive, full-system scans.

The realtime scan is performed when an action occurs, such as opening an email or file, to ensure there is no malicious software or malware within the item. Full-system scans, which are typically scheduled (but can be manually activated) are resource intensive. Regardless of the security product, it is not uncommon to experience a performance impact on a system when a full-system scan occurs.

Now, consider the impact of multiple full-system scans activating simultaneously on multiple VMs. There will be performance degradation. In static virtual environments, it might be possible to schedule these full-system scans to run asynchronously. However, attempting to do so could restrict the total number of VMs able to be consolidated on the physical server to ensure only one full-system scan is performed at any given instant. Add to this limitation the complication of dynamic environments enabled by vMotion. Using conventional security tools, you are faced with either a scheduling nightmare or guaranteed performance degradation.

New virtualization-aware security technologies must integrate with the virtual infrastructure to remove these limitations and enable virtual environments to achieve optimal protection and intended scalability and performance.



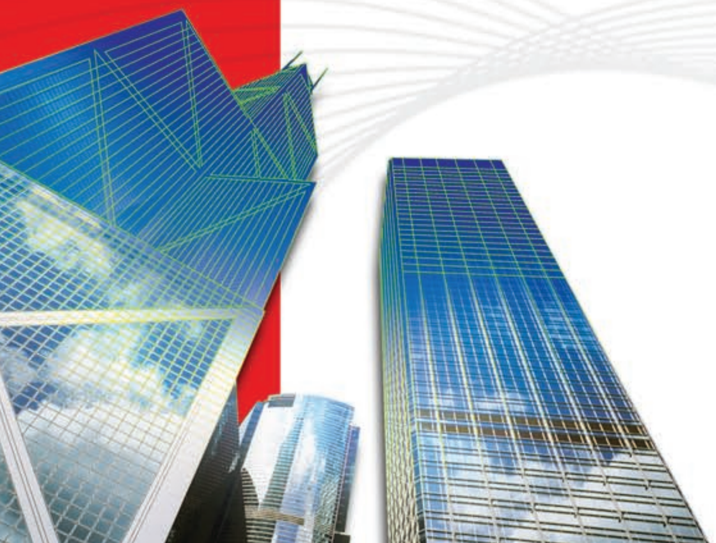
10 Integrating Security with the Virtual Infrastructure

On the previous pages, we mentioned several limitations of relying on conventional security tools to protect virtual machines. We also highlighted the potential risk of relying on newer virtual security appliances which can not adequately address the mobility, scalability and performance requirements of dynamic virtual environments.

Now, with VMware's VMsafe program, there's a new way of implementing security controls within a virtual environment: using hypervisor-aware security.

Hypervisor-aware security enables a dedicated VM with privileged access to hypervisor APIs to achieve tight integration with the virtual infrastructure to deliver faster, more effective protection to virtual machines. VMsafe APIs enable next-generation security software to provide a baseline of protection for all virtual machines, while eliminating many shortcomings, such as lack of transparency and the risk of inter-VM attack not addressed by earlier virtual security appliances.

By leveraging hypervisor-aware security software, such as a VMsafe API-based security appliance, enterprises can enable anti-virus, firewall and IDS/IPS functions across all VMs on a protected physical server. But there are performance trade-offs when compared to VM-centric security agents. Moreover, some security functions, such as handling encrypted traffic, accessing certain real-time information or the process of cleaning and removing malware from infected VMs will continue to require VM-based agents.

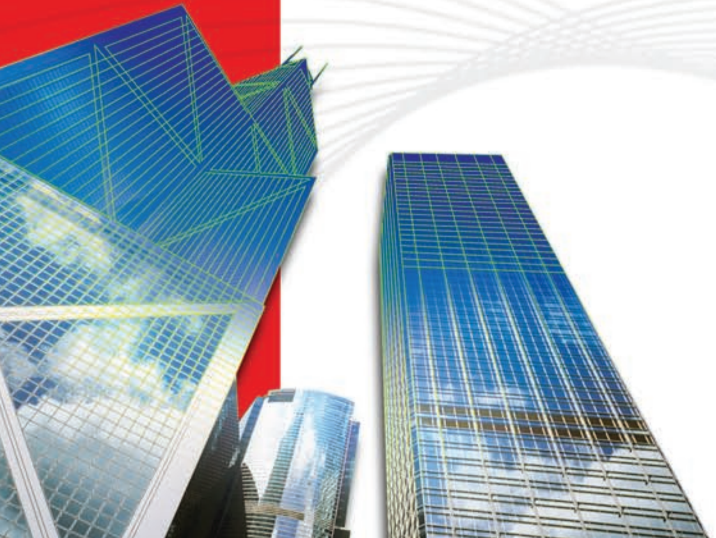


11 A Coordinated Approach

Given the performance issues of relying on security appliances, including hypervisor-aware security VMs, and the need to use VM-based agents for certain functions, a coordinated approach is the best way to protect virtual environments. VMsafe API-based security appliances are best for protecting noncritical assets; locally mounted software agents are ideal for protecting individual VMs.

Using this model, the hypervisor-aware security VM is notified whenever a guest virtual machine is activated, automatically checking and updating the software version and security configuration of the security agent it detects. In this way, guest VMs with IDS/IPS agents are protected and can safely send network traffic directly from the hypervisor to other VMs without incurring any performance delays. If the guest VM does not require an agent, the hypervisor-aware security VM applies IDS/IPS filtering to all data flowing through the VMsafe APIs.

For seamless protection, the IDS/IPS systems security management function should be linked to the centralized virtual management system, such as VMware vCenter Server, to keep current with configuration information about hosts and VMs.



12 Achieving Deeper Security in the Virtual World

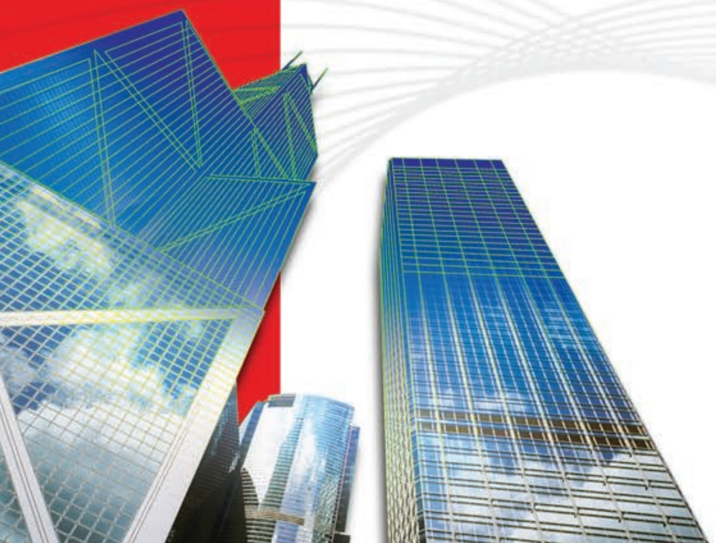
As your enterprise continues to deploy virtualized machines and adopt cloud computing, you need a single security solution that crosses physical, virtual, and cloud computing environments. Trend Micro Deep Security is an architecture that protects your infrastructure and delivers visibility at multiple levels:

Deep Security Virtual Appliance. The industry's first hypervisor-aware security VM that actively coordinates security with VM-based security agents, the Deep Security Virtual Appliance transparently enforces security policies on VMware vSphere virtual machines–coordinating with Deep Security Agent to deliver optimal protection and performance.

Deep Security Agent. Residing on each server or VM that needs protection, the Deep Security Agents enable IDS/IPS, Web application protection, application control, firewall, integrity monitoring, log inspection and anti-malware protection. Agents monitor traffic for protocol deviations, policy violations, and for indications of an attack, then block malicious traffic to neutralize the threat. Anti-malware protection includes real-time, scheduled and on-demand scanning.

Deep Security Manager. Providing centralized policy management, distribution of security updates, and monitoring through alerts and reports, Deep Security Manager simplifies and unites security management across physical, virtual and cloud computing servers. It maintains updated security configurations for all servers. The Deep Security Manager periodically scans servers for installed software, then recommends and assigns rules to protect those servers. These rules are sent to the Deep Security Agent - all communication between the Deep Security Manager and Deep Security Agent is protected by mutually authenticated SSL.

Deep Security Center. Keeping the Deep Security solutions up to date with the latest vulnerability research, the Deep Security Center is a dedicated vulnerability research team that provides security updates for the Deep Security solutions. These updates can automatically or under manual control be applied to those servers and VMs which require them.

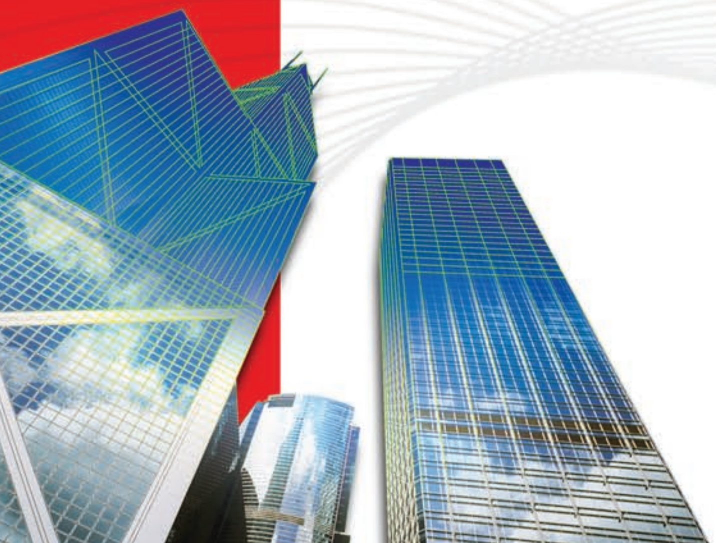


13 Self-Defense in the Virtual World

Trend Micro Deep Security's multi-layer defense strategy derails the targeted threats that are getting more sophisticated every year. It deploys security agents on servers and virtual machines, combined with powerful centralized management that allows IT staff to create and apply security profiles to servers, monitor alerts and preventative actions, and distribute security updates to servers. It proactively detects suspicious behavior, so you can take action before it is too late.

Trend Micro's approach is unique in the way it enables physical servers, virtual machines, and cloud environments to become self-defending. It is the first solution that coordinates security between local agents and hypervisor-aware security VMs that plug directly into VMware APIs. This coordinated approach delivers comprehensive protection while maintaining the optimum performance, mobility and scalability of virtual machines.

The Deep Security management console is optimized for datacenter environments spanning across physical, virtual and cloud computing servers. Integrating with enterprise-scale directories including Microsoft Active Directory, the VMware virtual infrastructures via VMware vCenter, and security information and event management systems (SIEM), Trend Micro solutions offer maximum protection, with minimum complexity to deliver security that fits into today's modern datacenter.

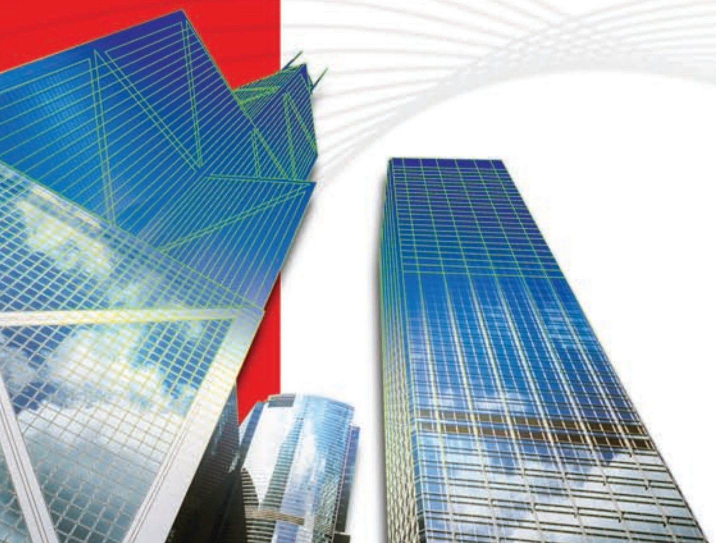


14 Practical Applications for Advanced Virtual Security

The Patch Before the Patch. With Trend Micro Deep Security, you can gain some relief when faced with meeting 30-day compliance deadlines for installing critical patches. As a member of the **Microsoft Active Protections Program**, Trend Micro works closely with Microsoft to be able to issue Vulnerability Shield Updates for Deep Security typically within two hours of Microsoft Security Advisories. These timely updates enable customers to buy time by “virtually patching” their systems against attacks on recently identified vulnerabilities. No longer do you need to decide between shutting down mission-critical systems and complying with patch updates.

Protecting Legacy Applications. Virtual patching has even greater advantages for legacy applications that are increasingly becoming preserved in virtual environments. These applications, both commercial and custom, do not have the luxury of patches to protect against attacks on vulnerabilities. In this case, comprehensive vulnerability shielding is the only effective method to prevent for-profit attackers from leveraging vulnerabilities to breach security.

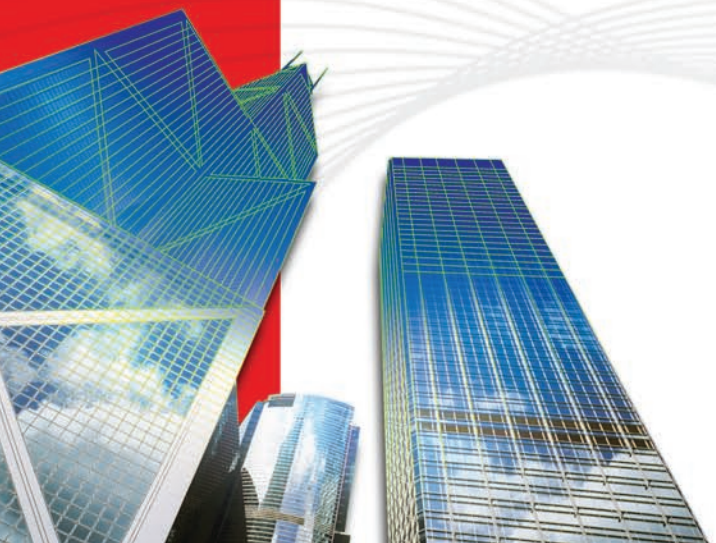
Finding Security Events in Logs. Reviewing server logs for security events is probably the most effective method to uncover suspicious activity, but it can be a real headache. Even downloading logs for all servers can be impractical, given network bandwidth limits. Trend Micro helps solve this problem by using the Deep Security Agent to sift through logs and uncover relevant events that could signal an attack. These events are then forwarded to a SIEM system (if you have one) and to the Deep Security Manager, which will set off the appropriate alerts based on the privileges and thresholds you can control.



14 Practical Applications for Advanced Virtual Security

Spanning Compliance Requirements. With data security compliance that encompasses standards, regulations, and internal mandates being both necessity and priority, it's good to know that Deep Security provides protection and facilitates audit processes on physical, virtual and cloud computing systems. It addresses six major PCI compliance requirements–including Web application-layer firewall requirements, IDS/IPS, file integrity monitoring, Web application-layer firewall, and network segmentation, along with a wide range of other compliance requirements.

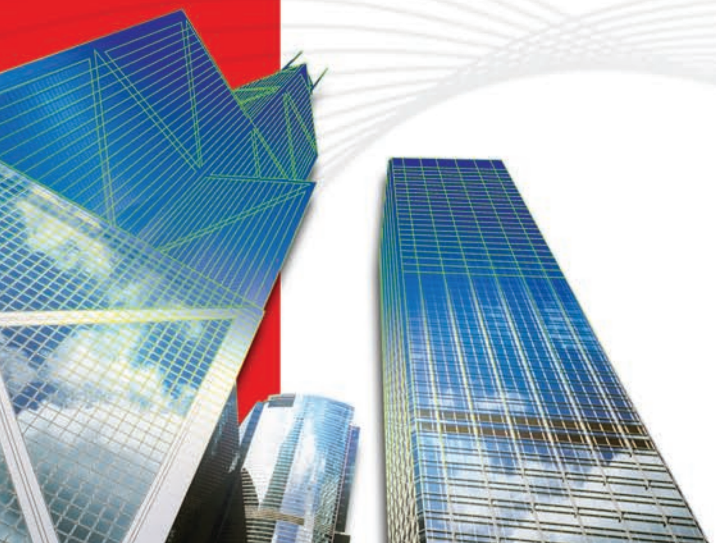
Stopping For-Profit Attackers. Deep Security protects against the most popular attack vectors used by for-profit hackers by preventing **SQL injection** and **cross-site scripting** attacks on web servers. Not only does Deep Security prevent web server data breaches, it provides detailed, auditable reports that document prevented attacks and policy compliance. As you continue to deploy web-facing servers in your virtualized datacenter, you'll appreciate the way Deep Security delivers comprehensive protection integrates with your existing infrastructure while not adversely affecting performance.



15 Looking Ahead Through Transformation

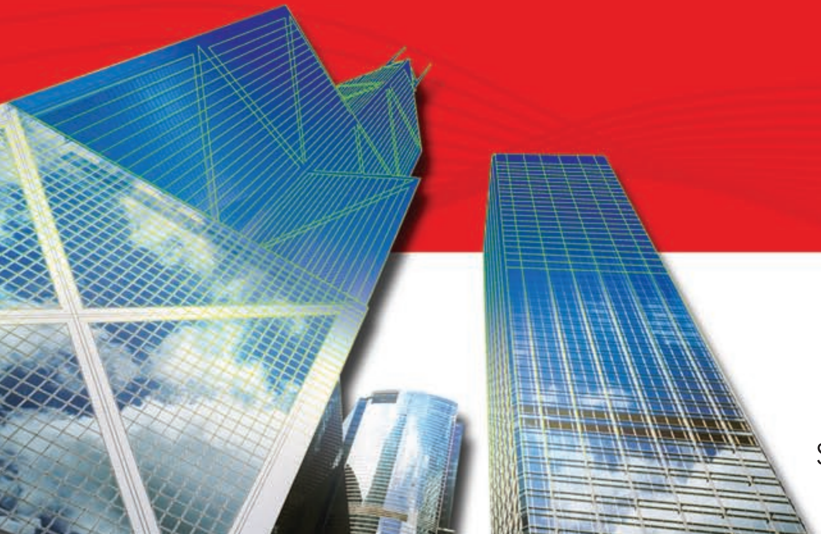
Your datacenter transformation is underway and a virtual desktop infrastructure (VDI) is likely on the horizon. As virtualization technology continues to develop, you will want to be sure your security solution keeps pace. That's why Trend Micro's multi-platform support is a critical advantage. No matter which virtualization platform you encounter – VMware, Microsoft, Citrix and more – Trend Micro will provide comprehensive protection across your enterprise's physical, virtual and cloud computing environments.

The move to virtualization and cloud computing doesn't need to be fraught with risk and danger. With the right tools and security strategy, you can neutralize attacks before they cause damage,



About Trend Micro

Trend Micro Incorporated, a global leader in Internet content security, focuses on securing the exchange of digital information for businesses and consumers. A pioneer and industry vanguard, Trend Micro is advancing integrated threat management technology to protect operational continuity, personal information, and property from malware, spam, data leaks, and the newest Web threats. Its flexible solutions, available in multiple form factors, are supported 24/7 by threat intelligence experts around the globe. A transnational company with headquarters in Tokyo, Trend Micro's trusted security solutions are sold through its business partners worldwide.



TREND MICRO™

Securing Your Web World