

Cost-effective Virtualization & Cloud Security

Safer Consolidation, Reduced Costs

Virtualization and cloud computing can help your organization achieve significant datacenter savings in hardware costs, operational expenditures, and energy demands—while achieving improvements in quality of service improvements and business agility. Yet many organizations don't realize that using their existing physical server security in virtual environments limits their ability to maximize their use of virtualization and cloud technologies. Even worse it leaves them exposed in ways they may not have anticipated—causing significant security gaps and even performance degradation during concurrent security operations. Trend Micro offers purpose-built virtualization security solutions designed to help you fully and safely utilize your virtualization environment.

Security Impediments in the Virtualization and Cloud Journey

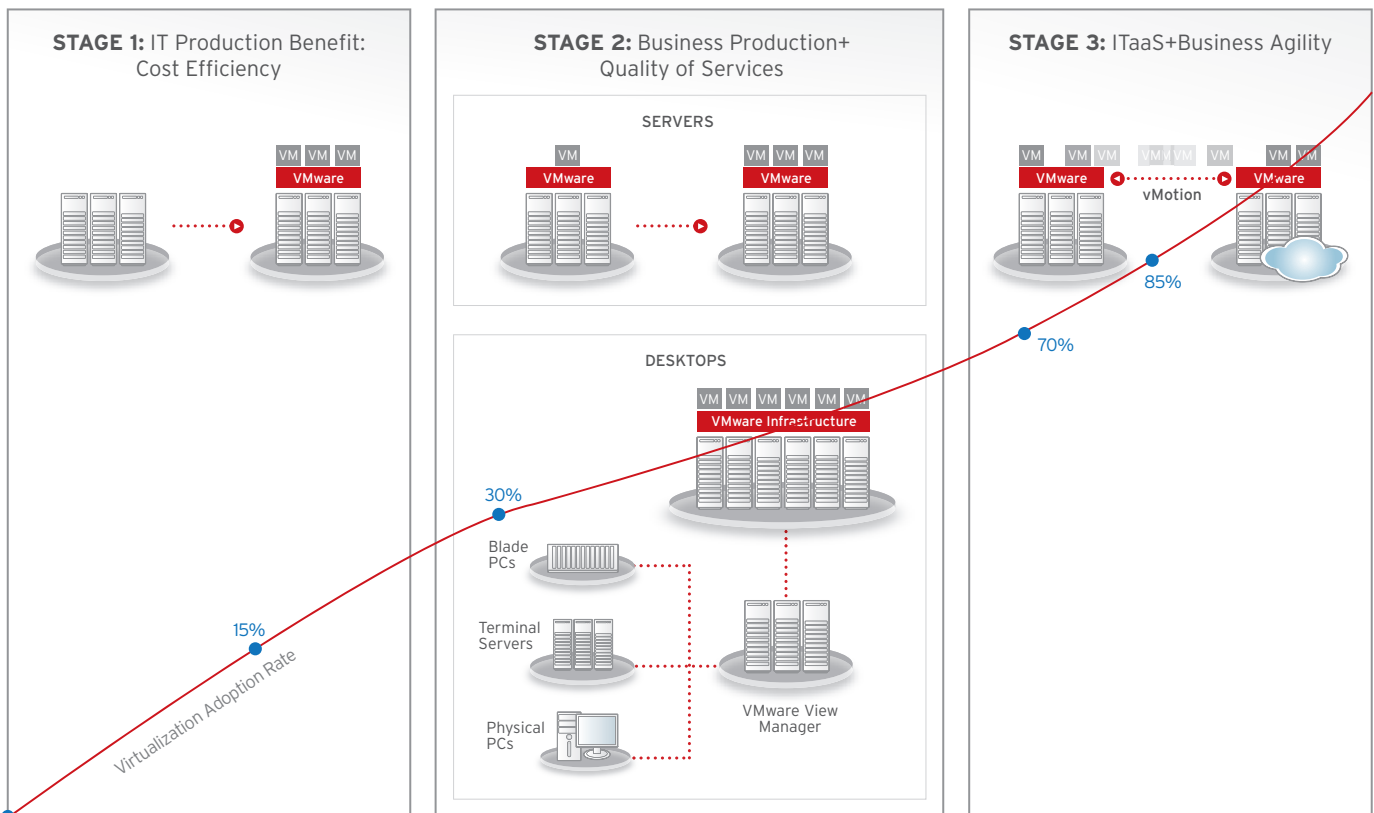
The typical customer virtualization journey happens in 3 stages:

Stage 1: Virtualization of IT systems—web servers, file and print servers, etc.

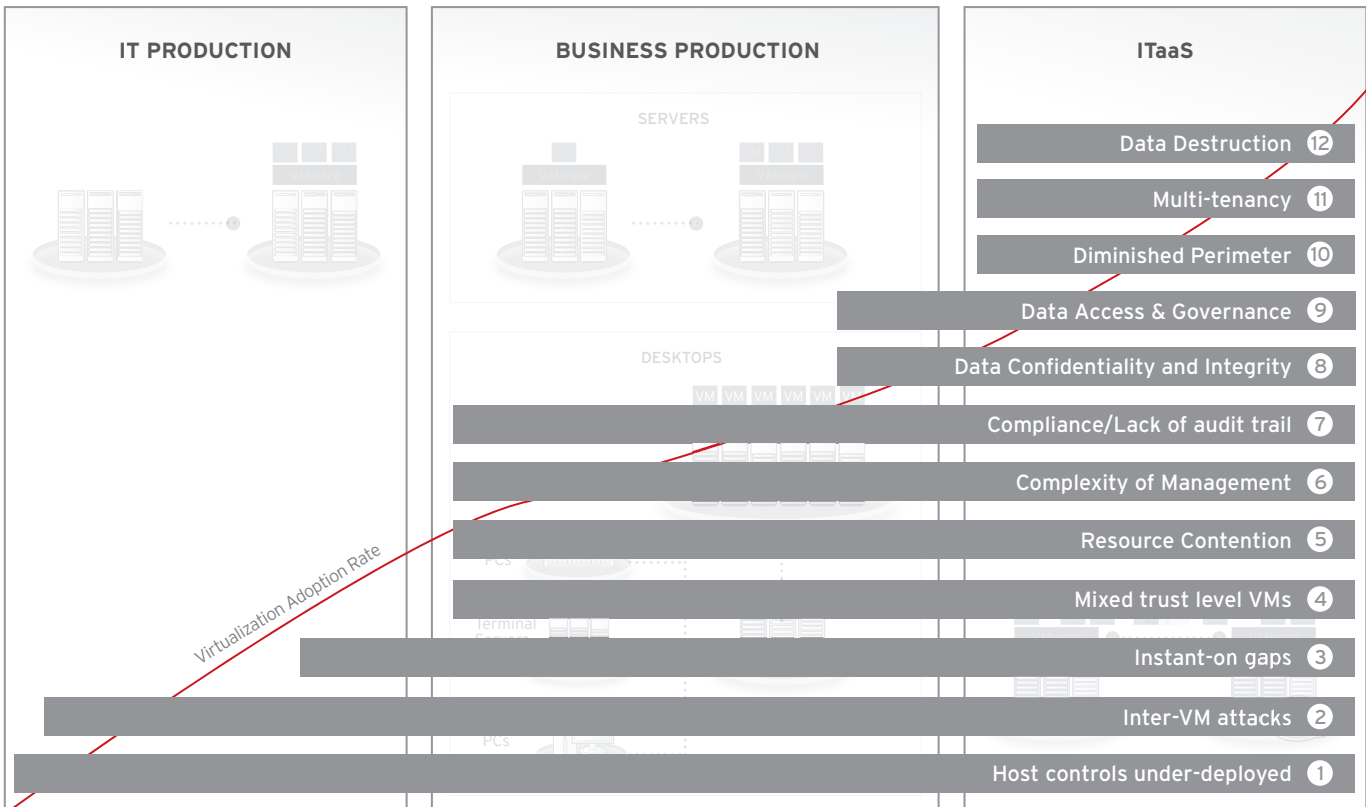
Stage 2: Virtualization of LOB systems—mission critical servers and tier-1 applications, plus desktops

Stage 3: Adoption of private or public clouds

Cost and efficiency benefits increase the further you progress in the virtualization journey. However leveraging traditional security solutions transposed from physical server environments can become a major obstacle in your progress—most predate X86 virtualization and were never designed to operate in this environment. Issues such as network blind spots, instant-ON gaps, mixed trust level workloads, antivirus storms are all new challenges unique to this environment that requires a new type of security designed specifically for this environment.

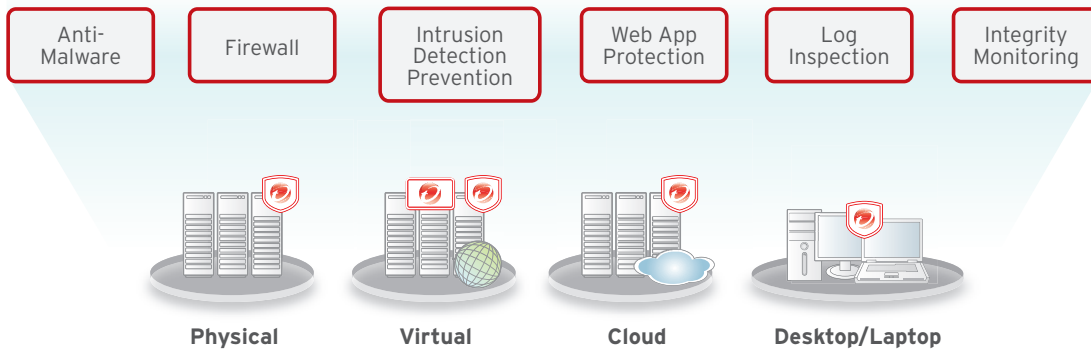


THE VIRTUALIZATION JOURNEY: SECURITY IMPEDIMENTS TO THE JOURNEY	
Security Challenge	Detail
Host-based controls under-deployed	File Integrity Monitoring, host IDS/IPS and anti-malware are often under-deployed, because of cost, complexity or performance
Inter-VM attacks	Traditional network security devices cannot detect or contain malicious inter-VM traffic
Instant-on gaps	It's all but impossible to consistently provision security to "instant-on" VMs, and keep it up-to-date. Dormant VMs can eventually deviate so far from the baseline that merely powering them on introduces a massive security hole
Mixed trust level VMs	Workloads of different trust levels are likely being consolidated onto a single physical server without sufficient separation
Resource contention	Resource-intensive operations (AV storms & pattern-file updates) can quickly result in an extreme load on the system
Complexity of management	Virtualization has led to the proliferation of more virtual machines (VM sprawl) than their physical predecessors, leading to increased complexity in provisioning security agents to each VM, and constantly reconfiguring, patch and rolling out patterns to each VM
Compliance/Lack of audit trail	Higher levels of consolidation put greater stress on the ability to ensure compliance, particularly amongst mission critical/Tier 1 applications. As well, virtualization makes it more difficult to maintain audit trails, and understand what, or by whom, changes were made
Data confidentiality & integrity	Unencrypted information in cloud environments is subjected to various risks including theft, unauthorized exposure and malicious manipulation
Data access & governance	RESTful-authentication* in the cloud can be susceptible to brute force and hijacking, attacks allowing unauthorized data access. Breakdown in the separation of duties might allow unauthorized vendor access to data (* REpresentational State Transfer)
Diminished perimeter	Security mechanisms are under the cloud service provider's control and perimeter security mechanisms are significantly diminished
Multi-tenancy	In cloud environments, your VMs exist with other unfamiliar, potentially hostile VMs with unknown security
Data destruction	Some cloud providers do not overwrite storage before recycling it to another tenant; in some cases where the storage is overwritten, data may be vulnerable after a system crash or unexpected termination



Enhanced Virtualization Security

Trend Micro has the broadest and deepest suite of security solutions designed specifically to secure virtual environments. Trend Micro Deep Security delivers advanced security software to protect operating systems, applications, and data on virtual, physical, and cloud servers as well as virtual desktops. Deep Security helps protect your virtualized datacenter from data breaches and business disruptions while enabling compliance. The solution also allows higher consolidation rates, maximizes performance, and increases operational flexibility. With Deep Security, your IT infrastructure receives comprehensive, integrated protection, which includes:




Solution Components

Deep Security comprises of the following solution components:

- **Deep Security Agent:** a small software component deployed on VMs or physical servers to protect them
- **Deep Security Virtual Appliance:** a packaged security VM that protects all other VMs on a VMware vSphere server
- **Deep Security Manager:** a powerful, centralized, customizable dashboard for managing agents or the virtual appliance
- **Security Center:** the portal that delivers security updates to the Manager, automatically or on-demand
- **Smart Protection Network:** the next-generation cloud-client infrastructure for delivering real-time malware protection to the virtual appliance

Deep Security Virtual Appliance and Agents



-  Deep Security Agent
-  Deep Security Virtual Appliance



Unparalleled Virtualization Security

Deep Security goes farther than any other product in the market in terms of securing virtual server and desktop environments.

- 1. Comprehensive security.** Deep Security consists of one integrated security solution with multiple advanced protection modules—firewall, intrusion detection and prevention, web application protection, file integrity monitoring, log inspection, and anti-malware.
- 2. Next-generation Architecture.** Deep Security integrates hypervisor APIs to offer agentless security for VMware vSphere environments. The Deep Security virtual appliance integrates the new vShield Endpoint APIs developed by VMware in collaboration with Trend Micro to offer the industry's first anti-malware solution designed specifically to protect the vSphere platform without requiring an agent in the VM. In addition, the same virtual appliance also uses VMsafe APIs to provide firewall, IDS/IPS, and web application protection for all virtual machines from outside the VM.
- 3. Ultimate flexibility.** The Deep Security virtual appliance works in coordination with any in-guest agents for maximum security coverage and scalability. Agents can be used in high-risk VMs to provide additional protection such as integrity monitoring and log inspection or with resource-heavy VMs to maximize overall system performance. Should the in-guest agent be removed, the virtual appliance will automatically step in and protect the VM.
- 4. Tight Integration with VMware.** Deep Security also integrates with VMware vCenter so it always aware of the inventory of virtual machines in the network and can automatically secure new virtual machines as they become active in the network. This close coordination also enables 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.
- 5. Immediate protection.** Deep Security is also integrated with the Trend Micro Smart Protection Network—a next-generation cloud-client infrastructure that combines sophisticated cloud-based technology and the expertise of Trend Labs researchers to deliver threat information in real-time to each system. No longer do large pattern files with shrinking shelf lives need to be continuously downloaded to each and every virtual machine on the network.
- 6. Built for the future.** Deep Security is not just built to provide security from the cloud, it also provides security for the cloud so enterprises are future-proofed in terms of security whenever they consider a move to this environment.

Protected Platforms

- VMware vSphere
- Citrix XenServer
- Microsoft Hyper-V

Related Products

- Core Protection for Virtual Machines
- OfficeScan™
- InterScan™ Web Security Virtual Appliance
- InterScan™ Messaging Security Virtual Appliance

Features and Benefits

- **Integrated suite of protection technologies:** Combines multiple modules to enable comprehensive cost-effective protection at the server
- **Inter-VM attack prevention:** Detects and prevents attacks targeting sensitive data—including attacks originating from other virtual machines on the same server—immediately alerting personnel of the attempt
- **Instant ON protection:** Ensures that virtual machines are automatically secure the instant they are ON—both newly emerging VMs and recently activated VMs—without requiring administrative action
- **Tamper-proof:** Isolates anti-malware from the machine being scanned to protect against malware that attempts to escape detection by uninstalling, inhibiting, or fraudulently patching antivirus security
- **Support for dynamic environments:** Protects mixed workload VM environments and multi-tenant cloud environments by creating a secure container around each VM
- **Improved performance:** Prevents AV storms and performance degradation by offloading resource-intensive operations such as full-system scans and pattern updates
- **Simplified manageability:** Simplifies management without requiring administrators to provision agents in each VM or constantly reconfigure, patch, and rollout patterns to each agent

