Cost-effective Virtualization & Cloud Security
Trend Micro™ Deep Security

Virtualization and cloud computing can help your organization achieve significant ROI as well as savings in hardware costs, operational expenditures, and energy demands—while achieving improvements in service quality and business agility.

Despite this potential, many organizations maintain their existing physical server security, unaware that this 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.

Security Impediments in the Virtualization and Cloud Journey
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, and antivirus storms are all new challenges unique to this environment that require a new type of security designed specifically for this environment.
<table>
<thead>
<tr>
<th>Security Challenge</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host-based controls under-deployed</td>
<td>File Integrity Monitoring, host IDS/IPS and anti-malware are often under-deployed, because of cost, complexity or performance</td>
</tr>
<tr>
<td>Inter-VM attacks</td>
<td>Traditional network security devices cannot detect or contain malicious inter-VM traffic</td>
</tr>
<tr>
<td>Instant-on gaps</td>
<td>It's all but impossible to consistently provision security to &quot;instant-on&quot; 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</td>
</tr>
<tr>
<td>Mixed trust level VMs</td>
<td>Workloads of different trust levels are likely being consolidated onto a single physical server without sufficient separation</td>
</tr>
<tr>
<td>Resource contention</td>
<td>Resource-intensive operations (AV storms &amp; pattern-file updates) can quickly result in an extreme load on the system</td>
</tr>
<tr>
<td>Complexity of management</td>
<td>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, patching and rolling out patterns to each VM</td>
</tr>
<tr>
<td>Compliance/Lack of audit trail</td>
<td>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</td>
</tr>
<tr>
<td>Data confidentiality &amp; integrity</td>
<td>Unencrypted information in cloud environments is subjected to various risks including theft, unauthorized exposure and malicious manipulation</td>
</tr>
<tr>
<td>Data access &amp; governance</td>
<td>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)</td>
</tr>
<tr>
<td>Diminished perimeter</td>
<td>Security mechanisms are under the cloud service provider’s control and perimeter security mechanisms are significantly diminished</td>
</tr>
<tr>
<td>Multi-tenancy</td>
<td>In cloud environments, your VMs exist with other unfamiliar, potentially hostile VMs with unknown security</td>
</tr>
<tr>
<td>Data destruction</td>
<td>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</td>
</tr>
</tbody>
</table>

---

**IT PRODUCTION**

**BUSINESS PRODUCTION**

**ITaaS**

- Data Destruction
- Multi-tenancy
- Diminished Perimeter
- Data Access & Governance
- Data Confidentiality and Integrity
- Compliance/Lack of audit trail
- Complexity of Management
- Resource Contention
- Mixed trust level VMs
- Instant-on gaps
- Inter-VM attacks
- Host controls under-deployed
Enhanced Virtualization and Cloud Security

Trend Micro has the broadest and deepest suite of security solutions designed specifically to secure virtual environments. Trend Micro Deep Security provides a comprehensive server security platform that delivers advanced protection for servers, applications, and data across virtual, physical, and cloud servers, as well as virtual desktops. Deep Security is a comprehensive server security platform designed to help protect your virtualized data center from data breaches and business disruptions while enabling compliance. This agentless solution accelerates virtualization and cloud ROI, allows higher virtual machine densities, maximizes performance, simplifies administration, and increases operational flexibility. With the Deep Security server security platform, your IT infrastructure receives comprehensive, integrated protection, which includes: Anti-malware, Web Threat Protection, Firewall, Intrusion Detection and Prevention (IDS/IPS), Web Application Protection, Integrity monitoring (includes hypervisor integrity monitoring), and Log inspection (available in agent-based form only).

These modules are also available in agent-based form, which is a useful form factor in public cloud environments, where you lack control of the hypervisor. With the multi-tenant environment creating a higher level of risk, these modules help servers in the cloud to become self-defending.

Solution Components

Deep Security is comprised 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, and includes capability of agentless protection.
- **Deep Security Manager**: a powerful, centralized, customizable dashboard for managing agents or the virtual appliance.
- **Smart Protection Network**: the next-generation cloud-client infrastructure for delivering real-time malware protection to the virtual appliance.
Unparalleled Virtualization and Cloud Security

1. Proven and comprehensive agentless security platform. Deep Security integrates with VMware vShield and other APIs to provide agentless anti-malware, web threat protection, integrity monitoring, intrusion prevention, and firewall in a single virtual appliance for the entire vSphere server. So you get stronger security for each VM without adding extra footprint, not to mention significantly easier manageability, greater resource efficiency, and higher levels of VM density. Thousands of real world deployments as well as third-party tests show that Deep Security's agentless architecture can support several times higher VM densities than traditional agent-based solutions.

2. Broadest and Deepest Integration for VMware. Deep Security is in its fourth generation of integration with VMware. In addition to its integration with VMware vShield, Deep Security also integrates with VMware vCenter for automatic and instantaneous security for new virtual machines in the network, and utilizes the TPM/TXT architecture for monitoring hypervisor integrity. The solution also integrates with VMware vCloud Director for enabling security in VMware-based clouds.

3. Extending to the Cloud. Deep Security integrates with VMware vCloud Director as well as with Amazon AWS enabling organizations to extend their corporate security policies to workloads in the public cloud, and manage both datacenter and cloud workloads through a single pane of glass. Deep Security also supports a true multi-tenant architecture allowing separate tenants or business units to manage policies independently and in self-service manner. Automated deployment of Deep Security components support elasticity and cloud-scaling of security infrastructure, and RESTful management APIs support integration into modern cloud management infrastructure.

4. Ultimate flexibility. Deep Security can be flexibly deployed in either virtual appliance or agent-based form factors to flexibly fit physical, virtual, private cloud and public cloud environments. The virtual appliance can also be deployed in coordination with select in-guest agents for defense in depth and scalability. Should the in-guest agent be removed, the virtual appliance will automatically step in and protect the VM.

5. Immediate protection. Deep Security is powered by 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.


Protected Platforms
- VMware vSphere
- Citrix XenServer
- Microsoft Hyper-V

Related Products
- OfficeScan™
- ServerProtect
- SecureCloud
- InterScan™ Web Security Virtual Appliance
- InterScan™ Messaging Security Virtual Appliance

Features and Benefits
- Integrated suite of protection technologies: Combines multiple modules to provide comprehensive cost-effective protection at the server
- Unparalleled agentless security performance: Improved resource efficiency via ESX scanning deduplication, and agentless AV, IPS, file integrity and more
- Self-defending servers: Multiple integrated modules provide a line of defense at the server—physical, virtual and cloud. Intrusion prevention detects and prevents attacks targeting sensitive data
- Integrity monitoring of the hypervisor: Utilizes Intel TPM/TXT technology to monitor for unauthorized changes to the hypervisor and meet evolving compliance needs
- Instant ON protection: Ensures that virtual machines in the datacenter or cloud are automatically secure the instant they are ON—both newly emerging VMs and recently activated VMs
- Integrated cloud security: Integrates with VMware vCloud Director and Amazon AWS to support unified management and common security controls across datacenter and cloud workloads
- Support for dynamic environments: Protects mixed workload VM environments and multi-tenant cloud environments by creating a secure container around each VM
- Simplified manageability: Agentless architecture eliminates the need to provision, update and patch agents in each VM. Multi-tenancy support simplifies management of cloud workloads