Trend Micro

HYBRID CLOUD SECURITY

Secure virtual, cloud, physical, and hybrid environments easily and effectively

INTRODUCTION

As you take advantage of the operational and economic benefits of virtualization and the cloud, it's critical to secure your virtualized data centers, cloud deployments, and hybrid environments effectively. If you neglect any aspect of security, you leave gaps that open the door to web threats and serious data breaches. And, to meet data privacy and compliance regulations, you will need to demonstrate that you have the appropriate security, regardless of your computing environment.

Trend Micro Hybrid Cloud Security solutions protect applications and data and prevent business disruptions, while helping to ensure regulatory compliance. Whether you are focused on securing physical or virtual environments, cloud instances, or web applications, Trend Micro provides the advanced server security you need for virtual, cloud, and physical servers via the Trend Micro™ Deep Security™ platform.

Trend Micro is the **#1 provider of server security for physical, virtual, and cloud environments**[1]— combining the most complete set of security capabilities with automated management to dramatically reduce both risk and cost.

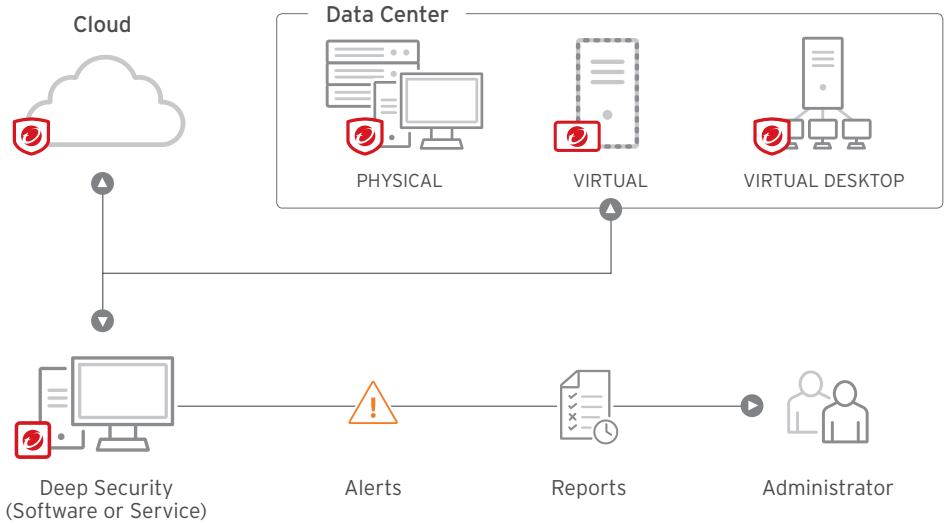
[1] IDC, Worldwide Endpoint Security Market Shares: Success of Midsize Vendors, #US40546915, Figure 5, Dec 2015

Why Trend Micro for hybrid cloud security?

- Secures physical, virtual, and cloud environments with one comprehensive solution
- Provides the most complete set of security capabilities available from the global market share leader in server security
- Saves resources/reduces costs with automated policy and lifecycle management with optimized security
- Available as software or as-a-service with central management across hybrid environments

DEEP SECURITY

With a single, comprehensive security solution, deployment and management are much faster and easier as you transition from physical and virtual environments to the cloud. Centralized management and vulnerability shielding help you save time and resources. Furthermore, our deep integration with VMWare optimizes virtual server performance without compromising on security.



Deep Security Agent
Deep Security Manager
Deep Security Virtual Appliance

> "Deep Security has been a very good fit in our data center and provides excellent protection for our virtualized servers and desktops and our continually changing environment. I love it."
>
> **Orinzal Williams**
> Executive Director
> United Way of Atlanta
> Georgia, US

TREND MICRO HYBRID CLOUD SECURITY SOLUTIONS

PROVEN VIRTUALIZATION SECURITY

Optimized security for the modern data center helps data center operators and architects control operating costs while improving performance with security optimized for virtual environments. Decrease risk, costs, and save time with automatic policy management, hypervisor-based security and central management.

ELASTIC CLOUD SECURITY

Automated security for the Cloud helps cloud architects meet shared security responsibility when deploying sensitive applications to the cloud. It provides elastic security for dynamic workflows running in Amazon Web Services (AWS), Microsoft Azure, and VMware vCloud Air.

> "I did the Deep Security deployment myself—it was less than a day for the roll out across 100 virtual machines. Overnight, I saw our memory resource utilization go down by 27 percent."
>
> **Nick Casagrande**
> Director of IT
> Southern Waste Systems LLC
> Florida, US

OPTIMIZED SECURITY FOR THE MODERN DATA CENTER

Trend Micro's market-leading security protects virtual desktops and servers, cloud, and hybrid architectures against zero-day malware and other threats while minimizing operational impact from resource inefficiencies and emergency patching.

Provisions full security capabilities automatically in the data center

To reap the benefits of virtualization and be efficient, a security solution built for virtual environments must be automated as part of the data center provisioning process. Trend Micro not only ensures physical servers and virtual machines (VMs) are protected the moment they are provisioned, it also recommends and applies only the policies that are relevant. Deep Security fits dynamic environments, by following VMs as they are brought up and down.

Deep Security's capabilities include:

- Anti-malware with web reputation to protect against constant malware attacks
- Network security, including intrusion detection and protection (IDS/IPS) to shield unpatched vulnerabilities, as well as a stateful firewall to provide a customizable perimeter around each server
- System security, including file and system integrity monitoring for compliance, as well as log inspection to identify and report important security events

Optimizes data center resources

Deep Security takes a better approach with hypervisor-based security. It is deployed at the hypervisor level so there is no need to install and manage a separate agent on every VM. This also means that individual servers and VMs are not cluttered with signature libraries and detection engines, which leads to tremendous improvements in management, network usage, speed of scans, host-wide CPU and memory usage, input/output operations per second (IOPS), and overall storage.

This central architecture also makes it possible to have a scan cache. The scan cache eliminates duplication in scanning across similar VMs, which can dramatically improve performance. Full scans complete up to 20 times faster, real-time scanning up to five times faster, and even faster logins for VDI.

To further simplify provisioning, Trend Micro solutions take advantage of the latest VMware platform innovations. Our tight integration with VMware allows automatic protection of new virtual machines as they are brought up, while automatically provisioning appropriate security policy and ensuring no security gaps.

This hypervisor-based approach is continued in the new NSX platform from VMware to ensure these performance advantages are preserved as organizations begin to migrate to the new architecture.

Manages security efficiently, even while transitioning to new environments

Managing security is easy with a single dashboard that allows continuous monitoring of multiple controls across physical, virtual, and cloud environments. Robust reporting and alerting help you focus on what's important so you can quickly identify issues and respond accordingly. Easy integration with other systems, such as SIEM, help incorporate security management as part of other data center operations. All controls are managed through a single virtual appliance so there is no need to manually keep agents up to date—an especially difficult task when rapidly scaling your operations. The dashboard includes information from cloud environments such as Amazon Web Services (AWS), Microsoft Azure, and VMware vCloud Air, making it painless to manage all your servers, regardless of location, from one central tool.

Achieves cost-effective compliance

Major compliance requirements for PCI DSS 3.1, as well as HIPAA, NIST, and SSAE 16 are addressed with:

- **Detailed, auditable reports** that document prevented vulnerabilities, detected attacks, and policy compliance status
- **Reduced preparation time and effort** required to support audits through centralized security controls and consolidated reporting
- **Support for internal compliance initiatives** to increase visibility of internal network activity
- **Proven technology** certified to Common Criteria EAL4+

Future proof your VMware investment with NSX

Organizations currently using VMware, and considering migrating to NSX, can take advantage of Trend Micro's unique ability to provide a single security solution to manage both current and future deployments. Trend Micro's modern data center security supports NSX with a comprehensive security platform designed to provide server, application, and data security across physical, virtual, and cloud servers.

AUTOMATED SECURITY FOR THE CLOUD

Cloud adoption is accelerating rapidly, driven by the cost savings, agility, and other advantages it offers. As you transition to the cloud, you must take care to ensure that you implement adequate security under the shared security responsibility model, and that your security solution meets internal and regulatory compliance rules.

Trend Micro Deep Security is optimized for leading cloud service providers (CSPs) including AWS, Microsoft Azure, and VMware vCloud Air. Deep Security makes using leading orchestration tools like Chef, Puppet, Salt, and Opworks easy, providing automated generation of policy scripts that enable security to be managed as part of cloud operations.

Prevents data breaches and business disruptions

Already selected by thousands of global customers to protect millions of servers, Trend Micro's market leading security capabilities help organizations to:

- Defend against network and application threats, leveraging proven host-based network security controls like Intrusion Detection & Protection (IDS/IPS)
- Protect against vulnerabilities, instantly shielding vulnerable applications and servers with a 'virtual patch' until a workload can be replaced
- Keep malware of workloads, ensuring that servers and applications are protected
- Identify suspicious changes on servers, including registry settings, system folders, and application files that shouldn't change

Reduces operational costs

Trend Micro provides advanced server security for cloud instances while simultaneously managing security on virtual and physical servers in the data center.

The integrated administrative console gives you a single, up-to-date view of the security posture for your entire cloud environment, reducing time and resource costs by making security management more efficient. Automated vulnerability shielding prevents the disruption of emergency patching.

In addition, Deep Security's tight integration with both AWS and Azure allows specific customizable policy templates to be applied based on instance metadata, ensuring the right policies are applied to the right servers automatically.

Achieves cost-effective compliance

Major compliance requirements for PCI DSS 3.1, as well as HIPAA, NIST, and SSAE 16 are addressed with:

- **Detailed, auditable reports** that document prevented vulnerabilities, detected attacks, and policy compliance status
- **Reduced preparation time and effort** required to support audits through centralized security controls and consolidated reporting
- **Support of internal compliance initiatives** to increase visibility of internal network activity
- **Proven technology** certified to Common Criteria EAL4+
- **Comprehensive set of tools** to eliminate need for multiple vendors

To learn more about our cloud and data center security solutions or to take a test drive, visit trendmicro.com/hybridcloud

> "Businesses face ever-growing and ever-changing threats on the Internet. By blocking threats, Deep Security protects the online experiences of our customers. This upholds our reputation and theirs."

Todd Redfoot
Chief Information Security Officer (CISO) at Go Daddy

TREND MICRO™

Securing Your Journey to the Cloud

Now available on awsmarketplace Windows Azure Marketplace