Virtualization and hybrid cloud computing can help your organization achieve significant savings in data center hardware costs, operational expenditures, and energy demands—while achieving improvements in quality of service and business agility. However, as data centers continue to transition from physical to virtual and now increasingly, cloud environments, traditional security can slow down provisioning, become difficult to manage, and cause performance lag. As you scale your virtual environment and adopt software-defined networking, evolving your approach to security can reduce time, effort, and impact on CPU, network, and storage.

Trend Micro’s modern data center security is optimized to help you safely reap the full benefits of your virtualized or hybrid cloud environment. Our virtualization-aware security offers many advantages including performance preservation, increased VM densities, and accelerated ROI. By leveraging Trend Micro™ Deep Security™, it offers a comprehensive set of security capabilities with the features you need to benefit from the efficiencies of virtualized environments and help meet compliance. This integrated solution protects physical, virtual, cloud, and hybrid environments.

Why Choose Trend Micro to protect your data center?

- Comprehensive set of security capabilities to protect sensitive applications and data
- Optimized for virtualized environments to improve performance and VM densities while reducing administrative effort
- Support for major virtualization platforms including network and file-based security controls for VMware NSX
- Single platform for physical, virtualized, and cloud instances to simplify security policy and infrastructure management
- First and only security architecture designed for service providers and enterprises with software-defined data centers, with support for multi-tenancy, auto-scaling, utility computing, and self-service
- Consistently ranked #1 in server security and chosen by thousands of customers to protect millions of servers

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

OPTIMIZED SECURITY FOR THE MODERN DATA CENTER: FEATURING DEEP SECURITY

A COMPREHENSIVE SET OF SECURITY CAPABILITIES

To be effective, security in your data center must be able to dynamically follow your servers, protect your unpatched servers from vulnerabilities, conduct real-time monitoring, and provide automatic protection. Trend Micro’s security for modern data centers, powered by Deep Security, has a broad set of security capabilities to support all of the above. This integrated solution protects your applications and data from attacks, optimizes data center resources, manages security efficiently, and helps achieve cost-effective internal and regulatory compliance.

PROTECTS YOUR MODERN DATA CENTER WITH COMPREHENSIVE SECURITY

- **Provides timely protection from constant malware attacks** including sandbox analysis that delivers advanced threat detection and remediation of suspicious objects through anti-malware and web reputation. Using the Trend Micro™ Smart Protection Network™, Deep Security deployments leverage the latest in global threat intelligence.

- **Shields unpatched vulnerabilities from attacks** with intrusion detection and prevention (IDS/IPS). Security policies update automatically to ensure the right protection is applied to the right servers at the right time.

- **Reduces exposure to attacks** with a host firewall. Blocks attacks and limits communication to only the ports and protocols necessary, with the ability to log and audit traffic for compliance reporting at the instance level.

- **Automatically detects and blocks** unauthorized software with application control at the server level.

- **Meets compliance file and system monitoring requirements** with integrity monitoring. Ensures unauthorized or out-of-policy changes are detected and reported—across files, ports, registries, and more.

- **Identifies important security events** buried in multiple log entries with log inspection. Forwards suspicious events to an SIEM system or centralized logging server for correlation, reporting, and archiving.

- **Scans web applications** for vulnerabilities and helps protect against them. Expert testing and false positive removal allow you to focus on high severity vulnerabilities and help to quickly mitigate them.

- **Automatically recognizes VMs** at launch. Automatically initiates security at start to dramatically reduce the risk of any instances going unprotected.

- **Protects Docker containers on the host** across all of their environments by detecting if containers are deployed onto a server and applying pre-defined policies to the host to protect the containers.

In addition to the ability to implement anti-malware functions separately on each server, we highly value the comprehensive security functions that Deep Security has, such as IPS/IDS.

Shuichi Hiraki
Associate Manager
Astellas Pharma, Inc.
Agentless security has been key. We know we cannot proceed with ‘traditional’ antivirus products, since the impact on performance is too much in terms of I/O, CPU, and memory.

Jussi Tarkkonen
System Specialist
City of Oulu, Finland

Switching to Trend Micro has raised the level of confidence in security.

Scott Forrest
Director
Networks and Infrastructure
Guess?, Inc
DEEP SECURITY PROVIDES AUTOMATED AND HIGHLY SCALABLE SECURITY

Deep Security has been chosen by thousands of global customers to protect millions of servers. Advantages include:

- **Comprehensive security capabilities** including anti-malware with web reputation, host-based firewall, intrusion detection/prevention, integrity monitoring, application control, and log inspection.

- **Reduced cost and complexity** with security optimized for virtual environments. Reduces operational impact with a single platform for management of security controls and policies across multiple environments: physical, virtual, cloud, and hybrid.

- **Agentless and agent-based architecture options** to support the leading virtualization platform VMware (including NSX). In addition, Trend Micro was the first to be certified for converged infrastructures like Cisco UCS, VCE vBlock and Nutanix.

- **Seamlessly extends security** to cloud environments including AWS, Microsoft Azure, and VMware vCloud Air.

TRENDS MICRO™ DEEP SECURITY™
Advanced server security for physical, virtual, cloud and hybrid environments

**Deep Security** protects enterprise applications and data from breaches and business disruptions. This comprehensive, centrally managed platform helps organizations simplify security operations while accelerating regulatory compliance. Automated security 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.

ABOUT TREND MICRO

As a global leader in cloud security, Trend Micro develops security solutions that make the world safe for businesses and consumers to exchange digital information. With more than 25 years of experience, Trend Micro delivers top-ranked security that fits customers’ needs, stops new threats faster, and protects data in physical, virtualized, and cloud environments.

Designed for Today’s Data Centers

Trend Micro Deep Security 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, and central management.

Visit [www.trendmicro.com/datacenter](http://www.trendmicro.com/datacenter) to learn more about our modern data center security for your virtualized or hybrid environment.

Deep Security is part of the Trend Micro Hybrid Cloud Security solution, powered by XGen™ security.