Trend Micro

SECURITY FOR THE MODERN DATA CENTER

Proven, efficient security for dynamic hybrid cloud environments

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.

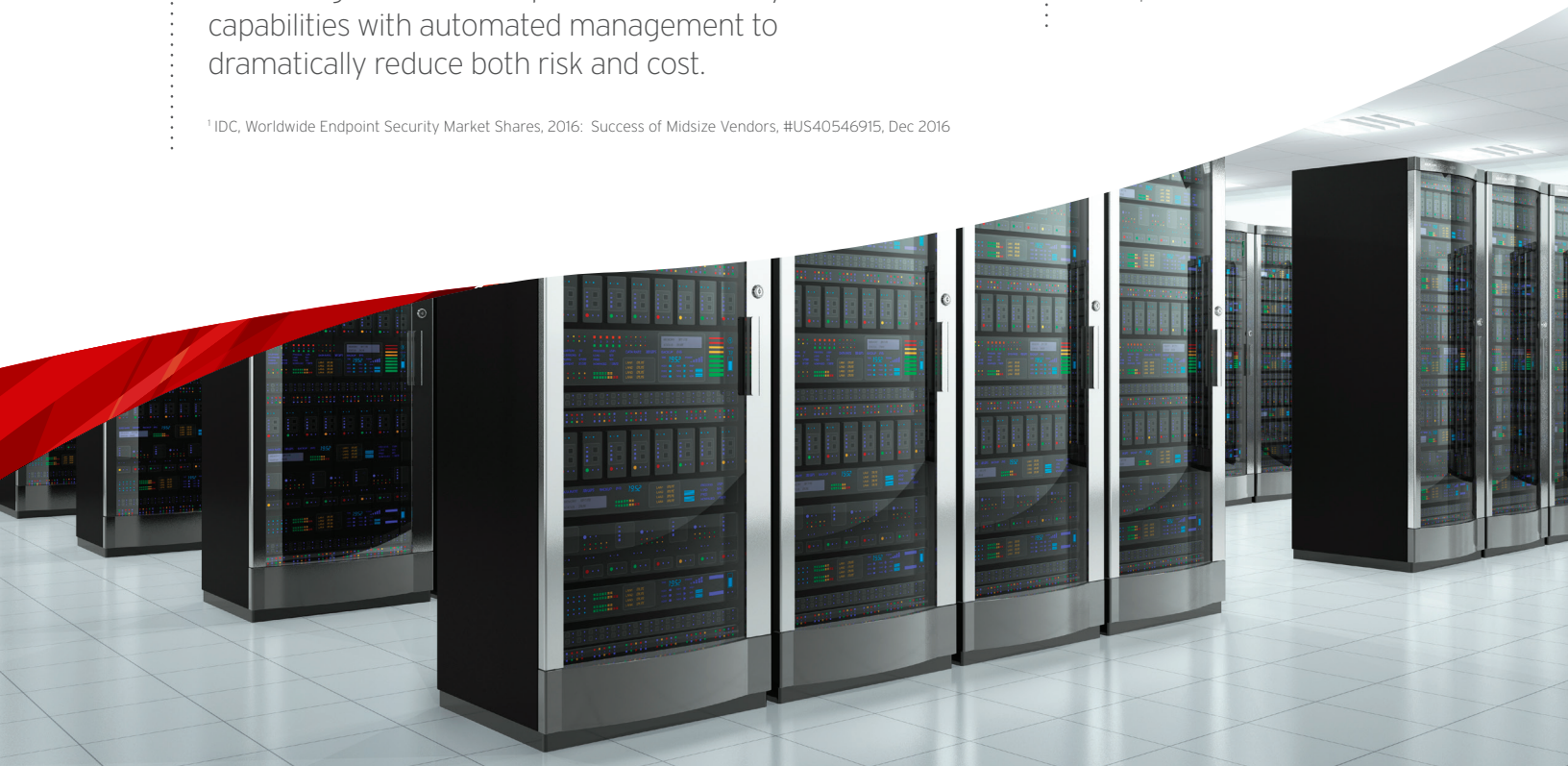
By leveraging **Trend Micro™ Deep Security™**, it offers a complete set of security capabilities with the features you need to benefit from the efficiencies of virtualized environments and help meet compliance. This integrated solution protects physical, virtual, cloud, and hybrid environments.

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

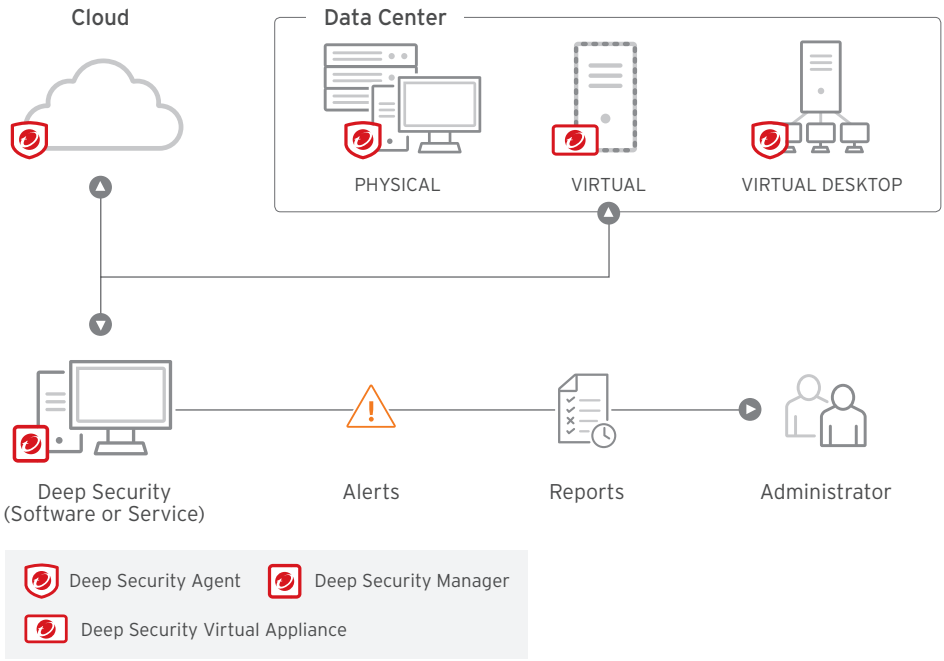
[1] IDC, Worldwide Endpoint Security Market Shares, 2016: Success of Midsize Vendors, #US40546915, Dec 2016

Why choose Trend Micro to protect your data center?

- Complete 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



OPTIMIZED SECURITY FOR THE MODERN DATA CENTER: FEATURING DEEP SECURITY



A COMPLETE 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 COMPLETE SECURITY

- **Provides timely protection from sophisticated malware attacks,** like ransomware, using advanced threat detection and remediation techniques such as behavioral monitoring, application control, predictive machine learning, and sandbox analysis. 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 multi-platform 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 and 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.

OPTIMIZES DATA CENTER RESOURCES WITH VIRTUALIZATION-AWARE SECURITY

Deep Security offers a wide range of security deployment options for your data center. It can be deployed at the hypervisor level with agentless security, or a light and lean, centrally-managed agent can be deployed at the VM level. This 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. VDI security is also maximized with agentless architecture, ensuring no extra footprint from a security agent impacts the virtual desktops and the underlying host.

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 policies.

> "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

MANAGES SECURITY EFFICIENTLY, ACROSS ALL ENVIRONMENTS

Managing security is easy with a single dashboard that allows continuous monitoring of multiple security controls across physical, virtual, cloud and hybrid environments. Robust reporting and alerting help you focus on what's important so you can quickly identify issues and respond accordingly. You can use Trend Micro™ Control Manager™ as your dashboard, or a third-party system such as VMware vRealize, Splunk, HP ArcSight, or IBM QRadar.

Deep Security supports multiple virtualization platforms such as VMware®, Microsoft® HyperV, and Citrix® XenServer. Plus, it integrates with cloud service providers such as Amazon Web Services (AWS), Microsoft Azure, and VMware Cloud™ on AWS, to provide a single dashboard for managing security across all environments, regardless of location, from one central tool.

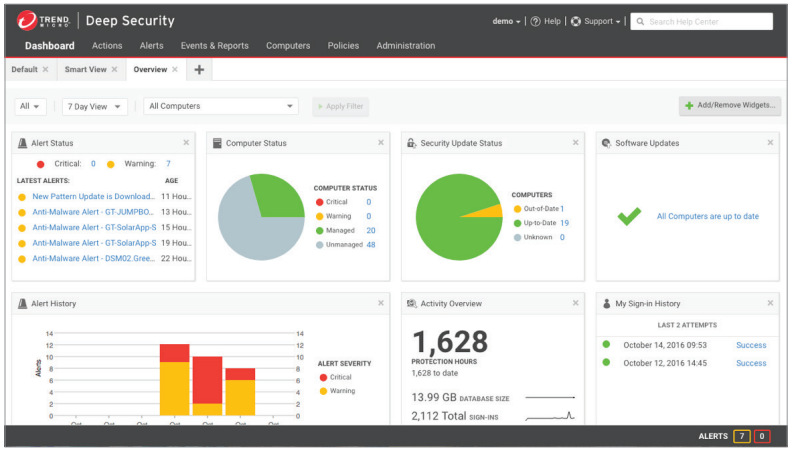
ACCELERATES COST-EFFECTIVE COMPLIANCE

The complexity and fluidity of virtualized and cloud environments pose regulatory and internal compliance challenges. Deep Security supports audits through centralized security controls and consolidated reporting, saving time and resources.

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

- **Detailed, auditable reports** that document prevented vulnerabilities, detected attacks, and policy compliance status
- **Continuous application scanning** to detect web application vulnerabilities
- **Support for internal compliance initiatives** to increase visibility of internal network activity
- **Proven technology** certified to Common Criteria EAL

> "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:

- **Complete security capabilities** including malware prevention with web reputation and behavioral monitoring, predictive machine learning, host-based firewall, intrusion detection/prevention, integrity monitoring, multi-platform 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 Cloud on AWS.

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. CIOs and CISOs can decrease risk, costs, and save time for their security administrators and development teams with automatic policy management, and central management across all environments.

Visit **www.trendmicro.com/datacenter** to learn more about our modern data center security for your virtualized or hybrid environment.

TREND 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 complete, centrally managed platform helps organizations, including DevOps engineers, and simplifies 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.

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

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.

TREND MICRO™

Securing Your Journey to the Cloud