Trend Micro

CLOUD AND DATA CENTER 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. Because 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 Cloud and Data Center 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.

Why Trend Micro for cloud and data center security?

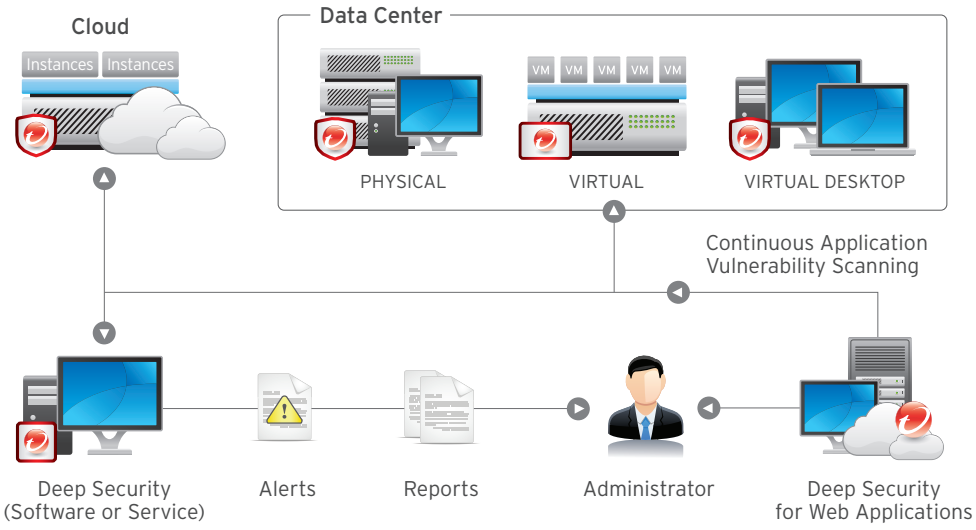
- Secures physical, virtual, and cloud environments with one comprehensive solution
- Provides the most complete set of security capabilities available from the global marketshare leader in server security
- Saves resources/reduces costs with automated policy and lifecycle management with optimized security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

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 2013-2017 Forecast and 2012 Vendor Shares, Figure 2, doc #242618, August 2013

DEEP SECURITY PLATFORM

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 agentless architecture optimizes virtual servers and increases performance, helping accelerate ROI.



Deep Security Agent
Deep Security Manager
Deep Security Agentless 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 CLOUD AND DATA CENTER 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, agentless operation and central management.

ELASTIC CLOUD SECURITY

Instant-On 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.

WEB APPLICATION SECURITY

Nonstop Security for Web Apps helps IT protect sensitive transactions and data on external web applications without false positives. Platform and application vulnerability scanning coupled with expert testing protect applications from sophisticated attacks.

> "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
- File and system integrity monitoring for compliance
- Intrusion detection and protection to shield unpatched vulnerabilities
- Stateful firewall to provide a customizable perimeter around each server
- Log inspection to identify and report important security events

Optimizes data center resources

Deep Security takes a better approach with agentless security. Because it is deployed at the hypervisor level, 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. VDI security is also maximized with agentless architecture, ensuring no extra footprint from a security agent impacts the virtual desktops and the underlying host.

And, 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—all without deploying an agent. This is another key method of eliminating security gaps.

This agentless 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. And because all controls are managed through a single virtual appliance, 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, 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 3.0, as well as HIPAA, NIST, and SAS 70 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+
- **Data protection** with FIPS 140-2 validated encryption for maximum privacy and secure data destruction capabilities

INSTANT-ON 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's Instant-On Cloud Security is optimized for leading cloud service providers (CSPs) including AWS, Microsoft Azure, and VMware vCloud architectures. Fast and easy to deploy tight integration with CSPs makes security efficient and elastic so you get the full benefit of the cloud's agility and cost savings. It's compatible with leading cloud deployment tools like Chef, Puppet, RightScale, OpsWorks, Salt, etc., so that security can be built into current elastic environments.

Prevents data breaches and business disruptions

Already selected by thousands of global customers to protect millions of servers, Trend Micro's Instant-On Cloud Security delivers a complete set of security capabilities including:

- Application scanning to detect vulnerabilities
- Anti-malware with web reputation to protect against constant malware attacks
- File and system integrity monitoring for compliance
- IDS/IPS to shield unpatched vulnerabilities
- Stateful firewall to provide a customizable firewall perimeter around each server
- Log inspection to identify important security events
- Encryption to protect sensitive data in transit and at rest

Reduces operational costs

Trend Micro's Instant-On Cloud Security 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, AutoSync 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 3.0, as well as HIPAA, NIST, and SAS 70 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+
- **Data protection** with FIPS 140-2 validated encryption for maximum privacy and secure data destruction capabilities
- **Comprehensive set of tools** to eliminate need for multiple vendors

> "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

> "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 (intrusion detection and prevention), and virtual patching."

Shuichi Hiraki
Associate Manager
Infrastructure, Information Systems
Astellas Pharma Inc.

NONSTOP SECURITY FOR WEB APPS

Web threats are rapidly intensifying in their relentless targeting of applications and the valuable data they access. Increasingly, these applications are being hosted not only in the data center, but also in the cloud, further compounding the complexity of keeping them secure. To fully protect your applications and data, you need to identify vulnerabilities and address them immediately. By the time you discover a weakness because of a successful attack, it's too late.

Detects and shields vulnerabilities

Trend Micro Deep Security for Web Apps provides intelligent application scanning for today's complex threat environment. Using both automatic scanning and hands-on testing by security experts, this complete solution continually protects web applications against the most complex attacks, while avoiding the false positives that would bog down your security team.

Integrated detection and protection; helps achieve PCI compliance

With integrated protection mechanisms like IPS, vulnerabilities are shielded from potential exploitation the moment they are discovered. Continuous scanning and shielding helps you maintain PCI compliance.

In addition, when application vulnerabilities are discovered, native Web Application Firewall (WAF) rules are generated for easy import into an already deployed WAF. These rules equip you to defend against application exploits before you are able to fix the code and configuration.

Unlimited SSL certificates

Deep Security for Web Apps helps you manage SSL requirements, while removing cost barriers to deploying the SSL certificates you need to secure online transactions with a globally trusted security partner. You can deploy unlimited SSL certificates cost-effectively, including Extended Validation (EV) certificates.

> "Trend Micro Deep Security for Web Apps gives us greater visibility into our vulnerabilities and allows us to quickly address those issues and focus our IT efforts more efficiently."

Mark Dunkerley
Team lead, messaging and domain services
Adventist Health System Information Services

Trend Micro Cloud and Data Center Security solutions protect your 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 Deep Security Platform delivers highly efficient agentless and agent-based protection for physical, virtual, and cloud servers. Deployed at the hypervisor level for maximum efficiency, agentless security protects your virtual servers and virtual desktop infrastructure (VDI) without the complexity of endpoint deployments. To integrate easily into your existing infrastructure, Deep Security is optimized for leading virtualization solutions and cloud services providers' architectures including **Amazon Web Services**, **Microsoft Azure**, **VMware Vcloud**.

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

TREND MICRO™

Securing Your Journey to the Cloud