

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, hybrid environments, and containers effectively. If you neglect any aspect of security, you leave gaps that open the door to threats and serious data breaches. And, to comply with data privacy and industry regulations, you will need to demonstrate that you have the appropriate security, regardless of your computing environment.

The **Trend Micro Hybrid Cloud Security solution, powered by XGen™**, protects applications and data on your server, prevents business disruptions, and helps to accelerate regulatory compliance. Whether you are focused on securing servers running applications in physical and virtual environments, or cloud and container workloads, Trend Micro provides the advanced server security you need for hybrid cloud security via **Trend Micro™ Deep Security™**.

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

<sup>1</sup> IDC, Worldwide Endpoint Security Market Shares, 2015: Currency Volatility Headwind, #US41867116, November 2016

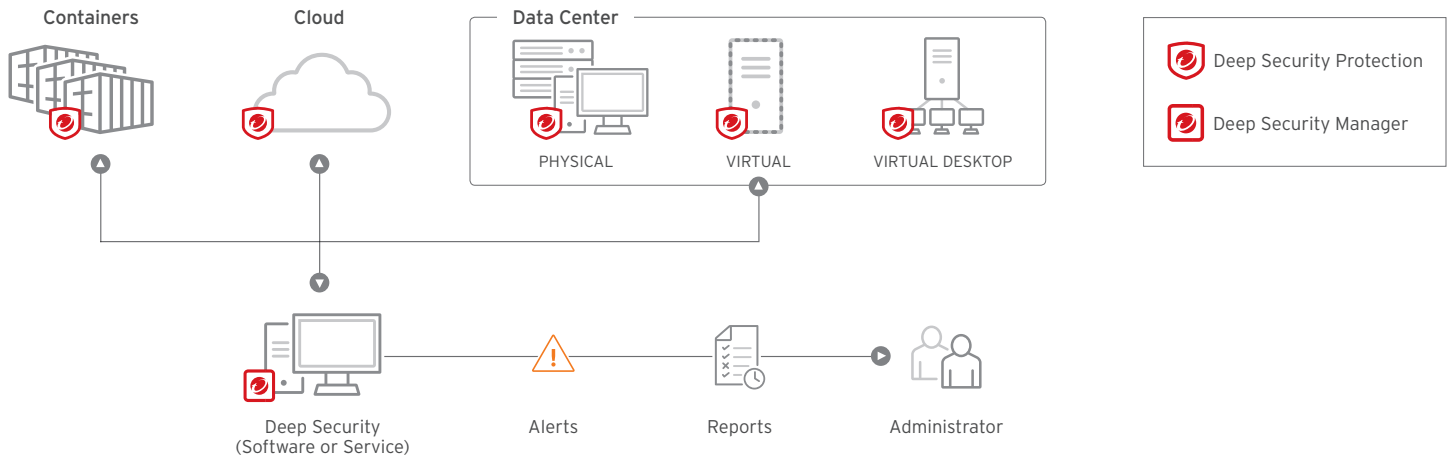
### Why Trend Micro for hybrid cloud security?

- Secures physical, virtual, cloud, and container environments with central visibility and control
- Provides the most complete set of security capabilities available from the global market share leader in server security
- Reduces the number of security tools you need to protect your hybrid environment and meet compliance requirements
- Saves resources and reduces costs with automated policy and environment-optimized security
- Available as software, as-a-service, or through the AWS and Microsoft Azure marketplaces
- Powered by XGen™ security, which offers a cross-generational set of security controls optimized for leading environments



## DEEP SECURITY

Delivering multiple security techniques in a single product, Deep Security makes the deployment and management of security faster and easier, simplifying the transition from physical to virtual, and to the cloud. It also includes support for micro-services architectures and Docker container protection, delivering a consistent way to secure your data center evolution. Deep Security includes centralized management, automated server discovery, and vulnerability shielding to save you time and resources, leveraging integration with environments like VMware, AWS, and Microsoft Azure that have been optimized for maximum performance without compromising on security.



## TREND MICRO HYBRID CLOUD SECURITY

### PROVEN VIRTUALIZATION SECURITY

**The Trend Micro Hybrid Cloud Security solution, powered by XGen™**, brings protection and visibility to your virtualized environments—including VMware Cloud™ on AWS—and removes the complexity and risk of managing security across multiple environments. It features Deep Security, which has been optimized for the virtualized data center, helping the operations and security teams to maximize security with minimal impacts on performance. It delivers decreased risk, lower operational costs, and rapid response to threats with automatic policy management, hypervisor-based security, and central visibility and control.

### AUTOMATED CLOUD SECURITY

**Deep Security helps to defend your cloud workloads**, addressing the need to protect what is deployed in the cloud as a part of the shared security responsibility for the cloud. It provides elastic security for dynamic workloads running in Amazon Web Services (AWS), Microsoft® Azure™, Google Cloud, and more. And for organizations embracing micro-services with containers, Deep Security protects Docker containers, extending frictionless host protection through to the container itself, allowing a secure and agile DevOps model.

“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

## SECURITY FOR THE MODERN DATA CENTER

Trend Micro's market-leading security protects virtual desktops and servers, cloud workloads, Docker containers, and hybrid architectures against zero-day malware—including ransomware—and advanced threats while minimizing the operational impact of security 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 with virtual and cloud workloads by following VMs as they are brought up and down and applying appropriate security.

### Deep Security's capabilities include:

- Malware prevention with web reputation, predictive machine learning, and sandbox analysis integration to protect against malware attacks, including ransomware and attacks like WannaCry and Erebus
- Network security, including intrusion detection and prevention (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, multi-platform application control for server lockdown and ransomware prevention, as well as log inspection to identify and report important security events

### Optimizes data center resources

Deep Security takes a better approach to virtualization security with integration at the hypervisor-level through VMware NSX. Automatically deployed with no downtime, it removes the 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 usage.

This centralized approach enables the use of a highly efficient malware scan cache. The scan cache eliminates duplication in scanning across similar VMs, which dramatically improves 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 like NSX and VMware Cloud on AWS. VMware NSX integration allows automatic protection of new virtual machines as they are brought up, while automatically provisioning appropriate security policy and ensuring no security gaps. And our unique integration with vRealize Operations Management enables organizations to have a single view of data center operations and security, further streamlining how security is managed in a virtual data center.

### 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 Security Information and Event Management (SIEM), help incorporate security management as part of other data center operations. And with security managed through a central integration point with NSX, there is no need to manually keep agents up to date—an especially difficult task when rapidly scaling your operations. The dashboard also includes information from cloud environments such as AWS, Microsoft Azure, Google Cloud and more, making it painless to manage all your servers, regardless of location, from one central tool. And with support for micro-services architectures and containers, you can securely evolve the way your data center runs.

Optimized for:

vmware®



Microsoft Azure

“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

## 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, the shared security responsibility model means that you must secure what you put IN the cloud, and that your security solution meets internal and regulatory compliance rules.

Deep Security is optimized for leading cloud service providers (CSPs) including AWS, Microsoft Azure, Google Cloud, and more. It makes using leading orchestration tools like Chef, Puppet, SaltStack, Ansible, and AWS Opworks easy, providing deployment examples and 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 and protection (IDS/IPS)
- Protect against vulnerabilities, instantly shielding vulnerable applications and servers with a 'virtual patch' until a workload can be replaced
- Lock down servers so that only authorized processes can run with application control for Windows and Linux
- Keep malware like ransomware off 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 workloads 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 workload discovery and security deployment, including specific customizable policy templates that can be applied based on instance metadata, ensuring the right policies are applied to the right servers automatically.

## ACCELERATE COMPLIANCE ACROSS THE HYBRID CLOUD

Compliance with major regulations like PCI DSS, HIPAA, NIST, SSAE-16, and GDPR span the data center and cloud. Deep Security helps 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 EAL2

To learn more about our hybrid cloud security capabilities or to take a test drive, visit [trendmicro.com/hybridcloud](https://trendmicro.com/hybridcloud)

Available on  **Microsoft Azure**

Trend Micro Hybrid Cloud Security solution is powered by XGen™, a smart, optimized, and connected security approach.



“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



Securing Your Journey to the Cloud

©2017 by Trend Micro Incorporated. All rights reserved. Trend Micro, and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice.  
(SB05\_HYBRID\_CLOUD\_SECURITY\_171101US)