

VIRTUALIZATION AND CLOUD COMPUTING

# THE JOURNEY TO THE CLOUD



Data Center Security



Securing Your Journey  
to the Cloud

# Abstract

**Trend Micro’s “journey to the cloud” started with the desire to build more defenses into its security solutions without increasing the on-premise security footprint. The lessons learned from the implementation and evolution of Trend Micro’s cloud have led the company to rethink security, and pioneer a new security model combining traditional protection approaches with innovations that extend security into virtualized and cloud environments.**

This paper tells the story of the Trend Micro global, private cloud, and how it is being used both operationally and for the delivery of products and services.

# Table of Contents

|   |    |
|---|----|
| Executive Summary .....   | 3  |
| The Changing Compute Model .....  | 4  |
| Rethinking Security .....   | 5  |
| Taking Advantage of the Cloud .....   | 6  |
| Securing Data That Travels Outside of the “Safe” Zone .....   | 7  |
| A Unique Cloud Platform for Operations and Delivering Protection.....                                   | 8  |
| Results of Trend Micro’s Own Journey: Lessons Learned For Securing Virtual and Cloud Environments ..... | 10 |
| Securing Every Step in the Enterprise’s Journey to the Cloud .....                                      | 11 |
| Why Choose Trend Micro for Your Journey? .....  | 14 |
| For More Information.....   | 15 |

# Executive Summary

Trend Micro's "journey to the cloud" started with the goal to build in more defenses to its security solutions without increasing the on-premise security footprint. Threats were increasing in numbers, types, and levels of sophistication and existing pattern-based solutions were placing a growing burden on endpoints. The company's security architects also recognized the need to adapt the security model for the unique requirements within virtualized data centers and cloud networks. These environments were changing the traditional network boundaries and perimeters, and called for rethinking security.

The Trend Micro™ Smart Protection Network™ infrastructure was created to address both of these objectives. As the industry's first cloud-based protection, it added the ultimate layer of defense with global correlated threat intelligence, shorter time to protection, and improved endpoint performance within a cloud-client security model.

While delivering security from the cloud, Trend Micro also took an active role in the advancement of security technologies for cloud computing environments and the development of a single security model for physical, virtual, and cloud environments.

Today, Trend Micro's products and services are differentiated from those of its competitors by the support of its very complex, high-scale, private cloud environment that currently handles more than 70-billion requests each day. The company's cloud is unique since it serves corporate operations as well as allows Trend Micro to accelerate delivery of products and services to its customers.

The implementation and evolution of Trend Micro's cloud have allowed the company to pioneer a consolidated approach to security that covers both traditional and virtualized environments. Smart Protection Network has proved the efficacy of cloud-based protection for overcoming the latest security challenges that stem from our Internet-intensive online world.

The lessons learned on Trend Micro's own journey to the cloud include the necessity for:

- Holistic, layered protection
- Avoiding server sprawl
- Blocking threats at the source
- The ability to automatically source, identify, and protect against unknown threats

These basic premises drive a broad offering of Trend Micro security solutions aimed at protecting enterprise resources and data at every step in a business' own journey to the cloud. By converging protection of data across physical, virtual, and cloud environments, Trend Micro gives these enterprises a safe journey to the cloud with minimized complexity.

# The Changing Compute Model

The world of computing is moving to the cloud. The benefits of the public cloud are compelling—shared infrastructure, shared systems, instant provisioning, and pay-as-you-go services. And users can enjoy anytime, anywhere access to services and their data. Increasing numbers of subscribers are taking advantage of cloud resources, and enjoying the freedom to access information using multiple “smart” devices. Online data and content continues to grow and move around in unprecedented volumes.

Cloud computing and virtualized environments raise questions about security, however. Are users secure within the new cloud environments? Are data assets protected as they move around in the cloud? The answer to both is yes—as long as the underlying security solution architecture has been designed for the cloud.

# Rethinking Security

Over the company's 20-year history, Trend Micro has significantly evolved the security model. Originally, the company pioneered a security model that protected data that remained inside the system and application, and systems and applications that remained inside the network. The company led the industry with security solutions that created layers of protection around systems and applications, preventing unauthorized access and theft.

This has been referred to as "perimeter defense" or a "defense-in-depth" security strategy. Anything from the outside is inspected and potentially blocked at the perimeter, if flagged as a threat. Multiple layers work together to stop threats at the earliest possible point in the network.

Over the last decade, however, Trend Micro security architects recognized several factors that called for reevaluating or evolving the traditional perimeter-based security model:

- Virtualization and cloud computing were redefining or stretching traditional boundaries and perimeters in networks.
- With threats increasing in numbers and types, traditional pattern-based methods required that scans be performed more often, which put an increasing burden on the processors and networks.
- The increasing size of the on-premise security software further taxed other endpoint resources such as memory and storage.
- Multiple threat vectors—from email, web, and files—and increasing levels of sophistication also complicated the battle to defend resources and asset

# Taking Advantage of the Cloud

Trend Micro quickly recognized in-the-cloud technologies as an opportunity for improving the defense-in-depth model. Today, cloud computing—one of the forces putting strain on the traditional network perimeters—has become part of the solution.

The cloud has led to a revolutionary shift in the security paradigm, and has also started Trend Micro on its own journey to the cloud. Initially, the company leveraged a cloud model to implement global email reputation collection and correlation. The in-the-cloud layer of protection was soon expanded to include web reputation checking, and later file reputation created a triad of global threat intelligence correlation.

The development of these cloud-based approaches evolved into the Trend Micro Smart Protection Network infrastructure. As the industry's first cloud-based layer of protection, it added the ultimate defense to the Trend Micro security model. This step into the cloud has allowed Trend Micro to bring immediate benefits to traditional enterprise environments. These benefits include global correlated threat intelligence, faster delivery of security, community feedback, and lighter-weight clients within a cloud-client security model.

While delivering security from the cloud, Trend Micro also took an active role in the advancement of security technologies for cloud computing environments and the development of a single security model for physical, virtual, and cloud environments.

# Securing Data That Travels Outside of the “Safe” Zone

As an early adopter of virtualization and cloud computing, Trend Micro gained a clear understanding of the security challenges for extending protection into the emerging cloud environments. Within virtualized data centers and cloud infrastructures, data is no longer tied to one server or even one group of servers, and it can be accessed from multiple devices simultaneously.

To protect data, therefore, security solutions cannot embrace a “lock-down” mentality, or rely solely on defense at traditional perimeters. Security solutions must evolve towards an integrated security approach that follows the data from physical to virtual to cloud environments.

Following and protecting the data requires that security take into account the context of the data. Context-aware protection shifts focus from defense inside a perimeter to smart data protection that takes into account data information such as user identity, type of data being accessed, geographical location, and more.

A data-centric security approach is ideally suited to the challenges of accelerated data flows precipitated by cloud computing and virtual machine data storms. This approach also supports consumerization, extending data protection to the multitude of mobile devices now used by employees, giving customers back control over their data, wherever it resides.

# A Unique Cloud Platform for Operations and Delivering Protection

Trend Micro's products and services are differentiated from those of its competitors by the support of a very complex, high-scale, private cloud infrastructure that currently handles more than 70-billion requests each day. The company's cloud is unique from other clouds in that it serves both an internal and external role, as an integral part of corporate operations as well as a delivery platform for customer products and services.

## **A Global Cloud Platform**

Trend Micro's global cloud ensures optimal availability and efficient network access for employees and customers. At the core of this cloud, the Smart Protection Network is comprised of several interlinked data centers that support complex multi-vector threat correlation. The data centers tie into a global network of more than 85,000 servers distributed across the Internet, and link to more than 100-million endpoints that generate real-time traffic for analysis and protection.

Smart Protection Network is a rare combination of a centralized cloud, a CDN/distributed cloud, and a fully distributed ambient cloud architecture within a single system. Trend Micro's advanced cloud infrastructure achieves a level of scale with amazing efficiency compared to most clouds.

## **Internal Operational Efficiencies**

The Trend Micro infrastructure currently extends to globally distributed offices and five corporate data centers. Every data center and major office makes use of virtualization and the personal cloud it enables, with more than 1,680 virtual servers currently deployed companywide. By 2012, data center virtualization will reach the target of 78% virtualization, with the European data center leading the way with 85% of its servers already virtualized.

## **A Light, Converged Layer of Protection**

With the evolution of its Smart Protection Network, Trend Micro has proved the efficacy of cloud-based protection for overcoming the latest security challenges that plague both traditional and cloud environments. By converging protection of data across physical, virtual, and cloud environments, Trend Micro gives enterprises a safe "journey to the cloud" with minimized complexity.

Trend Micro customers have been quick to take advantage of the Smart Protection Network. Today, an installed base of more than 100-million users is protected by the reputation intelligence of the Smart Protection Network. The Trend Micro cloud correlates all of the threat intelligence to track the current threats and help customers proactively block attacks at the source, stopping threats before they even enter customers' networks. (See Figure 1.)

The data centers hosting the Smart Protection Network services currently respond to 55-billion URL requests per day. With feedback loops that tie the user base into the Smart Protection Network, Trend Micro is able to intelligently crawl global infrastructures and correlate information from data feeds and feedback loops to efficiently identify emerging threats. The resulting threat blocking rates are impressive: billions of spam messages are blocked per week, along with billions of malicious URLs and files.

Besides improved protection rates, the Smart Protection Network has also provided an improved time to protect against threats unknown to Trend Micro. Using “Smart” feedback to source new potential threats and patent-pending correlation to analyze multiple threat vectors (web, email, file) in real-time, Trend Micro shrinks the window of opportunity for threats attempting to penetrate customers’ networks.

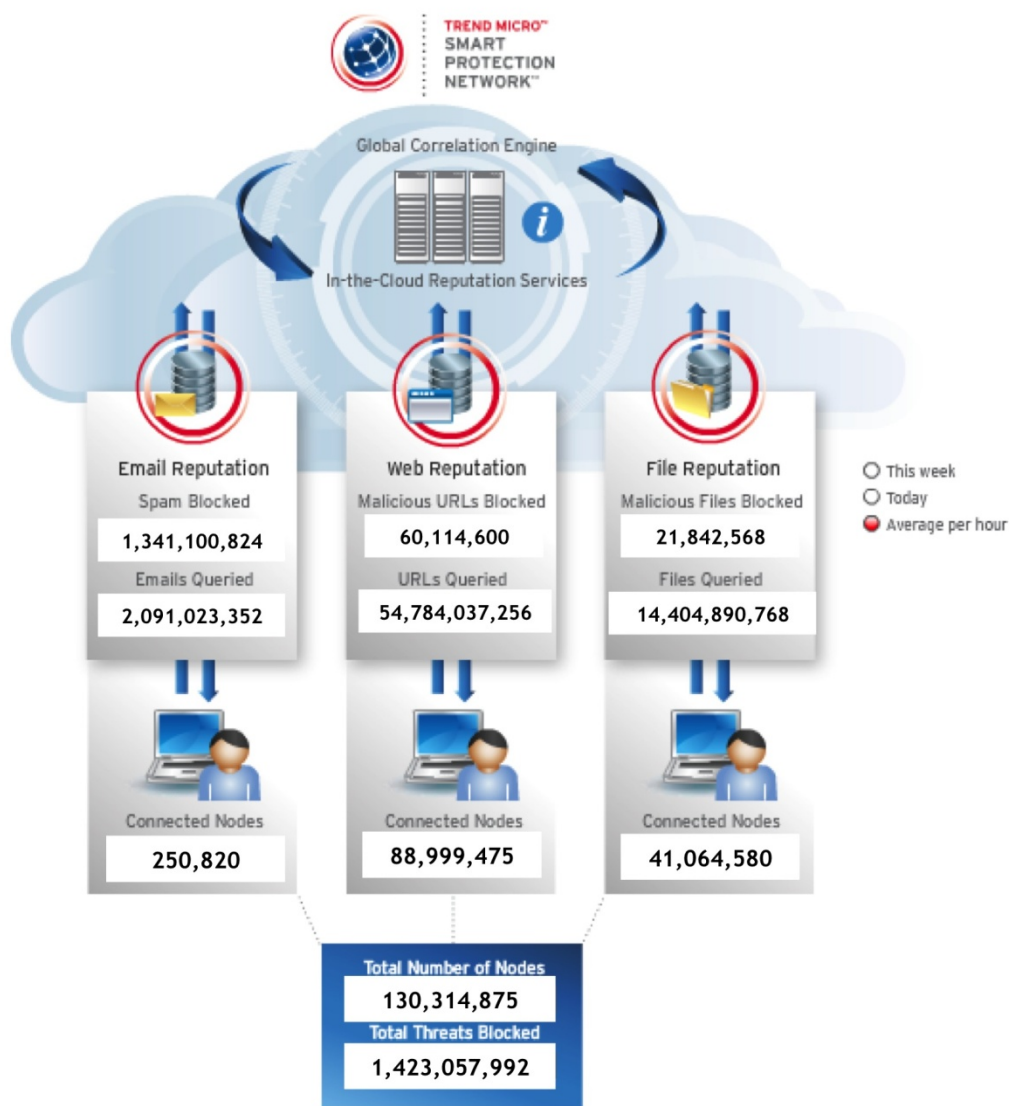


Figure 1. Smart Protection Network Threat Tracking

# Results of Trend Micro's Own Journey: Lessons Learned For Securing Virtual and Cloud Environments

By embarking on its own journey to the cloud as well as providing security from the cloud, Trend Micro has gained a decade of first-hand experience regarding the requirements for security solutions that protect virtualized and cloud environments. The lessons learned include the necessity for:

- Holistic, layered protection, including:
  - Web threat protection
  - Signature-based malware/virus detection
  - Behavior/heuristic detection/blocking
- Avoiding server sprawl and building cloud-aware security into servers:
  - Placing priority on appropriate server configuration management
  - Mandating virtual patching to protect from “instant-on” gaps
  - Enabling public/private cloud data security with policy-based encryption key management with server validation
  - Addressing mobile endpoint access from the cloud, which is inevitable and can become the most significant security weakness
- Blocking threats at the source:
  - Keeping threats completely off the customers' networks or computers
  - Eliminating bandwidth consumption for downloading malicious files
  - Improving computer resources, eliminating file scanning at the endpoints
- The ability to automatically source, identify, and protect against unknown threats:
  - Smart feedback, to improve threat intelligence
  - Correlation and analysis, to identify new threats faster
  - Cloud-client architecture, to provide faster protection to the user

These basic premises drive a broad offering of Trend Micro security solutions aimed at protecting enterprise resources and data at every step in the journey to the cloud. For some customers, the journey might start and end with a hosted service or virtualized servers (either on-premise or within a service provider's data center). For others, it might extend to the adoption of virtual desktop infrastructure (VDI) and a range of cloud services from third-party infrastructure providers.

Regardless of each company's or organization's path, a forward-looking security portfolio must address the changing infrastructures and data as businesses move into the cloud.

# Securing Every Step in the Enterprise's Journey to the Cloud

Trend Micro has applied the lessons learned from its own journey to the cloud such that it can now provide data-centric security, protecting business assets as they travel from the desktop to the data center and beyond.

## Endpoint Security

To give enterprises full access to the agility and cost savings provided by virtualization and cloud computing, a tightly integrated security solution must cover physical and virtual endpoints and servers. Security must be “light & lean” on all endpoints. Scans must not interfere with the real tasks at hand, and updates must be efficiently distributed without taking over local networks. For example, with Smart Protection Network enabled, Trend Micro endpoint security does not deploy signature files to physical or virtual endpoints. This avoids the risk of update-induced AV-storms, and also minimizes the memory footprint since pattern files are not stored on every endpoint or virtual machine (VM).

## Data Centers

Within data centers, virtualized servers and virtual desktop infrastructure require security that is fully “virtual aware.” Integration of security solutions with industry-leading virtualization platforms (e.g., VMware vShield Endpoint APIs) makes it possible for a single VM to protect all of the other VMs on the same hypervisor. This agentless malware protection scheme, currently only available with Trend Micro™ Deep Security, also simplifies automatic, always-up-to-date protection of new or reactivated VMs and minimizes the overall amount of memory and CPU cycles required for security.

Agentless security provides an excellent solution for environments where virtualization performance and density are at a premium. For environments that are not as concerned with density, and where the priority is managing more instances, an agent-based model is advantageous. Agent-based security is also required in the multi-tenant environment of the public cloud.

True virtualization awareness requires that the security solutions have the capability to communicate with the virtualization platform management modules (e.g., VMware vCenter or Citrix XenServer). The management servers can then determine whether endpoints are physical or virtual, such that virtual desktops can be treated appropriately. For example, desktop base images can be pre-scanned since they are largely identical; this avoids unnecessarily repeated scans of the same image for multiple virtual desktops.

The combination of integrated, light & lean virtual-physical endpoint security solutions and virtualization-aware data center security allows customers to preserve their consolidation ratios. Customers can accommodate more fully secured VMs per physical server, and therefore maximize savings from server consolidation.

## **Protecting the Data as it Travels into the Cloud**

As previously discussed, protecting the data requires rethinking traditional security models. In the case of the Trend Micro security model, data protection has evolved such that security can travel with the data. For example, Deep Security allows the implementation of security policies that travel with a VM whether it ends up being deployed on an on-premise server or in the cloud at a service provider's data center.

## **Data Encryption**

With the rapid provisioning and mobility of virtual and cloud data, businesses do not always know where their data is or who is accessing it. Data protection with encryption and policy-based key management provide another layer of protection to virtual and cloud environments, but must be easy to use and manage to ensure adoption. Trend Micro™ SecureCloud™ introduced a patent-pending approach that combines policy-based key management, industry-standard encryption, and virtual server validation to simplify data security in private or public cloud environments. This lightweight approach lets cloud users secure sensitive information without having to install a vastly more complex file infrastructure.

Enterprises also want assurances that encryption keys remain in their control, without the need to share them with cloud service providers. SecureCloud also gives users exclusive custody over their encryption keys, where other encryption solutions might share or keep custody of keys. This approach provides "separation of duties," allowing cloud customers the ability to leverage the efficiencies and benefits of cloud services while maintaining authority over the information within their environments. With customer-key ownership, businesses have the freedom to choose their cloud service and even move between cloud service providers, avoiding vendor lock in.

SecureCloud demonstrates that companies can take advantage of public cloud services without compromising compliance with security standards set in regulations like HITECH, PCI DSS, and GLBA. Sensitive and personally identifiable information can be safeguarded in the cloud with strong encryption techniques.

## **The Safe Use of Mobile Devices**

Smart devices have entered the workplace, whether or not companies are ready. The lure of anytime, anywhere access to data and applications makes them essential to today's generation of mobile tech-savvy users.

Today's security portfolios must include solutions that extend protection to the mobile users and devices, and should ideally go further to promote the safe sharing of information between mobile devices and on-network systems.

Trend Micro solutions for mobile users—Trend Micro™ Mobile Security, and Trend Micro™ SafeSync™ for Business—validate that protection can be extended from on-premise physical systems to mobile devices and out to the cloud. Files can be automatically protected and synchronized across multiple devices, with access controls giving users and businesses control over their data assets. With automatic updates, security can be always current. The ability to locate and wipe data from lost or stolen devices should also be considered an essential feature for a cloud-ready security solution for mobile users.

# Trend Micro's Ongoing Cloud Strategy

The threat landscape constantly changes and evolves, as criminals look for new ways to profit from electronic data. Trend Micro has never rested from its quest to provide the best protection from these evolving threats, and has increased efforts in several areas to keep ahead of threat trends:

- **Exhaustive in-house research:** internal deployments of Trend Micro solutions yield higher-quality products and predictable performance. Research and development teams also take advantage of emerging industry technologies, which recently have included cloud services and open source innovations. Trend Micro researchers routinely participate in industry discussions and collaborations, and share information that promotes accelerated development of security solutions and standards.
- **Evolving security:** Trend Micro's security model is being extended to include inside-out data protection as well as traditional outside-in threat protection. The changes address advanced persistent threats, data breaches, and more.
- **Partnering with best-in-class technology providers:** long-term relationships with VMware, Citrix, and other technology providers has allowed Trend Micro to introduce platform-ready solutions that are highly integrated into the environments they protect. By comparing technology roadmaps, Trend Micro and its partners optimize the alignment of security and platform solutions.
- **Industry leadership:** participation in the Cloud Security Alliance and other organizations that drive standards and innovation allows Trend Micro to increase awareness of security-related issues that result in faster time to market for viable solutions.

# Why Choose Trend Micro for Your Journey?

Trend Micro has led the industry in terms of helping customers safely exploit the benefits of cloud computing, and has invested heavily in security solutions both from the cloud and for the cloud. With a family of multi-layered protection for cloud and virtual environments, and after 20 years in the content security business, Trend Micro has become the largest independent security company. For cloud security, Trend Micro is #1 in terms of market share in server security (according to IDC, November 2010) as well as #1 in market share for virtualization security (according to Technavio, May 2011).

Last year, Trend Micro revealed its new tagline—“Securing Your Journey to the Cloud”—along with its commitment to become the top provider of cloud security. Today, Trend Micro offers a portfolio of integrated solutions that secures data out into the cloud. The unique hallmarks of the Trend Micro portfolio include:

- Security that supports the evolution of the data center, with VM and cloud protection that travels with servers to safeguard data
- Security that is designed for VDI to support better resource utilization and cost savings
- Security with better protection and performance, that is truly virtualization-aware
- Security that enables fully leveraging virtualization and cloud computing, while minimizing IT costs
- Security that supports consumerization, enabling businesses to support the multitude of mobile devices being used by employees today.

# For More Information

To learn more about Trend Micro security solutions that can secure your journey to the cloud, please visit [www.cloudjourney.com](http://www.cloudjourney.com).



Securing Your Journey  
to the Cloud

## About Trend Micro

Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years' experience, we deliver top-ranked client, server, and cloud-based security that fits our customers' and partners' needs, stops new threats faster, and protects data in physical, virtualized, and cloud environments.

Powered by the Trend Micro Smart Protection Network cloud computing security infrastructure, our industry-leading cloud-computing security technology, products, and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe.

Additional information about Trend Micro Incorporated and the products and services is available at [www.trendmicro.com](http://www.trendmicro.com).