Simplifying Network Security in the Cloud

How Trend Micro Cloud One™ makes it easy to bring network-layer security into your cloud environment
Enterprises are moving to the cloud to take advantage of its elasticity, flexibility, and scalability. However, reaping those benefits is becoming a challenge as cloud security becomes increasingly complex, with numerous different firewalls, load balancers, and other appliances having to be installed and managed to inspect traffic. This white paper explores how Trend Micro Cloud One™ – Network Security helps simplify security in multi- or hybrid cloud environments by bringing network-layer protection to the cloud without disrupting critical business applications.

Table of contents

Secure the Cloud Without Giving up the Benefits ................................................................................................................... 3
  A challenge to deploy ........................................................................................................................................................ 3
  Security designed for the cloud ......................................................................................................................................... 3

A Closer Look at Network Security in the Cloud ...................................................................................................................... 4
  Flexible deployment in action ........................................................................................................................................... 5
  A flow-based engine for transparent deployment ............................................................................................................. 5
  Comprehensive, active threat protection .......................................................................................................................... 5
  Centralized visibility across the cloud footprint ................................................................................................................. 6

Powered by Research Excellence ............................................................................................................................................. 6
  Trend Micro Zero Day Initiative ......................................................................................................................................... 6
  Trend Micro Smart Protection Network ............................................................................................................................. 6

Conclusion ................................................................................................................................................................................ 7
SECURE THE CLOUD WITHOUT GIVING UP THE BENEFITS

As more and more enterprises adopt multi- or hybrid cloud strategies, cloud architects and network security teams are struggling to protect business-critical assets across their many different cloud environments. They’re finding that what worked on-premises for security doesn’t necessarily translate to the cloud.

A challenge to deploy

Many existing network security solutions are painful to deploy because they’re not designed for the cloud. Some require extensive downtime to be inserted inline, some have outdated throughput-based licensing models, and others may be impossible to deploy within an enterprise’s existing cloud infrastructure. For example, agent/host-based solutions aren’t always feasible or desirable with the cloud. Enterprises may not have the right to deploy an agent on their cloud provider’s virtual server—or may not want to dedicate compute to an agent at the expense of other workloads.

There’s also the problem of complexity. An overwhelming number of appliances, load balancers, and other “moving parts” have to be installed and managed to inspect inbound and outbound traffic. If every virtual public cloud (VPC) needs its own firewall—and if an enterprise has hundreds of VPCs—the management burden and costs quickly add up.

Changes often have to be made to the network infrastructure itself to accommodate those additional components, with some security solutions requiring IP addresses to be changed or specific topologies to be deployed. New devices inserted in the network can also become “critical” going forward, meaning they can’t be easily (or cheaply) removed or modified. And as more pieces get added, they bring inefficiencies that can disrupt or slow down network traffic, affecting core business operations and processes.

There are cloud-native security solutions, of course, but these are often tied to specific platforms, such as Amazon Web Services (AWS) or Microsoft® Azure®. Having a different security solution for every cloud prevents enterprises from getting a centralized view of the threats they face. It also increases the risks of management dashboard/console overload, increasing the odds that important security alerts will be missed. These platform-specific cloud solutions also tend to lack key security features, such as virtual patching at the network layer, egress filtering, and deep packet inspection.

SECURITY DESIGNED FOR THE CLOUD

For enterprises seeking elasticity, flexibility, and scalability, these security challenges can undermine the very reasons for moving to the cloud in the first place. What’s needed, is a solution designed specifically for the cloud. It needs to have flexible, transparent deployment options that won’t disrupt the business, along with comprehensive, active protection for broad, network-layer security in the cloud, including all the capabilities of an on-premises intrusion prevention system (IPS).

Those criteria are the drivers behind Trend Micro Cloud One™ – Network Security.
A CLOSER LOOK AT NETWORK SECURITY IN THE CLOUD

Trend Micro Cloud One™ is a software-as-a-service platform that provides a flexible, all-in-one approach to physical, virtual, and cloud security. Its Network Security service is a transparently deployed, inline solution that quickly detects and prevents known and unknown attacks at the network layer, protecting VPCs at scale without disrupting business applications or network traffic.

Network Security can be deployed with either AWS or Azure. Its multiple deployment options make it insertable into existing cloud environments, whenever and wherever needed. It can also be deployed in multiple configurations, giving enterprises the freedom to choose how many instances are required, what traffic to inspect, how detected threats will be handled, and more.

With Transit Gateway, enterprises can use a single instance of Network Security to protect traffic across all of their VPCs. Through a hub-and-spoke architecture that centralizes inspection, traffic coming and going from the internet can be monitored from the same instance. And with each VPC no longer needing its own load balancer and firewall, enterprises can significantly reduce the number of components in their network architecture—saving both time and money. There’s just a single instance to manage in a single location.

Because some enterprises have not adopted Transit Gateway, AWS introduced VPC Ingress Routing in late 2019. It allows enterprises to define routing rules to redirect ingress traffic to third-party appliances, such as Network Security, before it reaches its final destination. Since VPC Ingress Routing is available to all AWS customers as part of their infrastructure—meaning no additional installation or configuration is required—it is a very quick and easy way to deploy Network Security in an AWS environment.
For example, Network Security uses the elastic load balancer that is already part of the AWS environment. If an issue is detected, rather than routing traffic on the inspection subnet to the protected private subnets, Network Security uses the AWS infrastructure to go directly to the enterprise’s protected public subnets. One or more instances of Network Security can be deployed in an availability zone, with both inbound and outbound traffic handled by the same instance—no need for dedicated inbound and outbound sets of appliances.

On top of these two configurations, enterprises also have the flexibility to pay for only what is used (in dynamic environments) or to purchase annual licenses (for more static network architectures).

A flow-based engine for transparent deployment

Network Security’s stateless, flow-based detection engine allows it to be seamlessly and transparently inserted into a company’s existing cloud architecture. Conventional firewalls are “stateful”, meaning they need to track every single connection and handshake, as well as where traffic begins and terminates—making them very disruptive to add or remove from the network. Network Security focuses on threat state, rather than network connections or policies, using the information it accumulates to determine or track the properties of potential and actual threats.

With Network Security, enterprises can begin inbound and outbound traffic inspection mid-flow, gaining immediate protection from the moment of deployment, without the need for any re-architecting or re-IPing. Network clients and servers will never even know Network Security has been added or removed, meaning there are zero disruptions to business applications, network connections, or DevOps processes. Attackers also have no idea the solution is there—until they find that previously successful attacks are now suddenly blocked.

Comprehensive, active threat protection

Network Security builds on the expertise and capabilities gained by Trend Micro™ TippingPoint™ over the past 15 years to effectively bring on-premises-type security to the cloud. Through virtual patching, vulnerability shielding, exploit blocking, advanced threat intelligence and protocol analysis, anomaly detection, machine learning and behavioral analysis, classic signature-based detection methods, and more, Network Security provides comprehensive protection against multiple evolving threat vectors and techniques—entire classes of attacks, as well as specific known threats. With its active blocking approach, it notifies security teams of detected breaches or attacks so they can take the most appropriate next steps.

Because of its flow-based engine, Network Security can even provide this level of deep protection in asymmetric environments, where both sides of the network connection (from the person who initiated the connection, to the server, and back) are not visible. This allows traffic to be inspected across a greater number of network scenarios without re-architecting the network to make it symmetrical, overcoming the limitations inherent in some other security solutions.
Because Network Security doesn’t need to track the whole connection, it also offers a fail open option: It can be removed from inspection without any risk of network outage or disruption to established connections. Flexible failover scenarios are also possible. For example, if a company’s strategy is to shift their workloads to another region if a particular cloud service region goes offline, Network Security eliminates the need to share and maintain the connection state (which risks workloads getting out of sync). Even when transitioning between regions, data and workloads stay highly available.

Centralized visibility across the cloud footprint

Network Security gives security teams centralized threat visibility, helping them avoid dashboard/console management overload. As part of the Trend Micro Cloud One platform, it goes beyond the traditional IPS by not being just another standalone point product. It works seamlessly with the other services of the platform to deliver unified security management across the entire cloud footprint of the enterprise. A single, consolidated management console gives the option of centralizing control over all of an enterprise’s cloud security solutions, improving the overall user experience and resulting in better security outcomes.

Simplifying compliance with data security regulations

The comprehensive protection available through Network Security helps organizations streamline compliance with various data privacy and security regulations.

For example, the Payment Card Industry Data Security Standard (PCI DSS) requires organizations that handle credit card data to put in place “compensating controls” for vulnerabilities that may exist in their network environments. A network-layer IPS meets the definition of a compensating control, which means Network Security gives enterprises an easy way to satisfy that requirement and maintain compliance with the standard. Network Security also incorporates a broad range of industry best practices that are aligned with other PCI DSS compliance requirements, such as minimizing access to outbound traffic.

POWERED BY RESEARCH EXCELLENCE

Network Security is built on the same engine and history of innovation as the next-generation Trend Micro™ TippingPoint™ IPS—the world’s first intrusion prevention system. Before it was introduced more than 15 years ago, there were only intrusion detection systems, which generated a lot of alerts, but did not actually block incoming threats.

For any IPS, data and research are essential to detecting and responding to threats and attacks quickly—and to keeping enterprises protected against the latest, most complex threats. The technology behind Network Security is informed by Trend Micro Research, which features a team of more than 500 researchers around the world and successful programs, such as the Trend Micro™ Zero Day Initiative™ (ZDI) and Trend Micro™ Smart Protection Network™.

Trend Micro Zero Day Initiative

The ZDI is the largest vendor-agnostic bug bounty program in the world, rewarding independent security researchers for identifying and reporting vulnerabilities in operating systems and software before they can be exploited.

Between the time an undisclosed threat is discovered and when the vendor releases a patch for it, enterprises are at risk. Trend Micro researchers take what has been learned by the ZDI to quickly develop and distribute security filters that cover an entire vulnerability, ensuring customers are protected well before the vendor’s patch is made available. In 2019, ZDI filters were distributed an average of 81 days ahead of the vendor patch.

The ZDI is the global leader in vulnerability research and discovery, and is a top provider of vulnerabilities to organizations, such as Adobe®, Microsoft®, and the U.S. Industrial Control Systems Cyber Emergency Response Team.

Trend Micro Smart Protection Network

The Smart Protection Network collects, identifies, and delivers the latest security intelligence to ensure Trend Micro products can adapt to and defend against current and emerging threats. Continuously mining data from known-good and known-bad files, applications, and URLs from around the world, the Smart Protection Network serves as a massive information source for driving innovation in Trend Micro technologies.
The Smart Protection Network consists of:

- A global network of more than 250 million sensors to collect more threat information in more places, including data on files, IPs, URLs, mobile applications, operating systems, and Internet of Things (IoT) transactions.
- Global threat intelligence that analyzes terabytes of data on a daily basis, drawing from a database of nearly one billion known-good files to identify more than five billion new threats each year.
- Proactive, cloud-based protection for half a million businesses around the world, blocking more than 48 billion threats yearly.

**A recognized leader in security**

Trend Micro is:

- Ranked #1 in IDC’s Worldwide Hybrid Cloud Workload Security Market Shares, 2019 report
- A leader with the highest score in the “current offering” and “strategy” categories in The Forrester Wave™: Cloud Workload Security, Q4 2019 report

**CONCLUSION**

As cloud security becomes increasingly complex, Trend Micro Cloud One aims to keep things as simple, scalable, and flexible as possible for enterprises. In addition to its Network Security service, the platform also includes services for securing containers, workloads, cloud file storage services, applications, and serverless functions, as well as services for compliance and cloud security posture management.

Trend Micro Cloud One is an all-in-one security services platform for organizations building in the cloud

With its all-in-one approach, Trend Micro Cloud One provides enterprises with the breadth, depth, and innovation they need to meet and manage their cloud security needs today and in the future.

Whether an enterprise is looking to overlay security across VPCs as they migrate to the cloud or want an extra layer of security for the cloud applications being built by their DevOps teams, Network Security delivers defense in depth quickly and at scale—without adding any friction into the network or disrupting the business. By simplifying the way they protect their assets in the cloud, Trend Micro is helping enterprises get the most value from their cloud investments.

---