A Trend Micro White Paper | **March 2017**

Servers, Servers, Everywhere

How the Hybrid Cloud Changes the Game for Security

>> Examining the dynamics of the hybrid cloud, and the challenges that organizations are facing as they adopt the latest technologies.

EXECUTIVE SUMMARY

Organizations today are facing significant challenges as they adopt the latest technologies to power business success. With major shifts from physical, to virtual, to cloud having occurred in the past 10 years, architectures have changed significantly and the rate of change is not slowing down. Technologies like containers and serverless functions are already on the horizon for broad enterprise adoption, adding a new set challenges for security teams.

At the same time, attacks are increasing in frequency and sophistication, highlighted by the over 81 billion threats blocked by the Trend Micro™ Smart Protection Network™ in 2016, a 56% increase over 2015. Specific to ransomware attacks, TrendLabs[1] reported that the number of discovered ransomware families jumped from 29 to 247 in 2016, a 752% increase over just 12 months. With over $1B in revenue attributable to ransomware in 2016[2], many new ransomware families are designed to target servers, including web servers, file servers, and virtual desktops, and even specific business critical file types. Good examples of these are the recent **WannaCry** and **Erebus** ransomware attacks that leveraged serious vulnerabilities and the **EternalRocks** tool to significantly impact many global organizations.

At the center of this technology shift are servers, the workhorse of the enterprise. Gartner, the leading IT research and advisory firm, explicitly points out that, "Servers often host the most critical data in the enterprise and have different functionality than client endpoints."[3] The challenge is that the architectural shifts have established server workloads in multiple locations and in different formats, which makes securing them more complex than ever before.

Designed to address the challenges of the hybrid cloud, Trend Micro™ Deep Security™ includes a broad set of security capabilities in a single product, enabling you to reduce the number of tools used and centralize visibility in a single management interface. Leveraging deep integration with VMware®, Amazon Web Services (AWS), and Microsoft® Azure™, Deep Security enables you to quickly and easily discover all workloads, protected and unprotected, giving a complete view of your security posture across physical, virtual, and cloud environments.

This paper examines the dynamics of the hybrid cloud and the challenges introduced at both the business and technical levels. It also outlines how Deep Security, powered by XGen™, helps to address many of these real-world problems in ways that can simplify operations and increase overall security of your data and applications across the hybrid cloud. You can find even more information about Deep Security at **www.trendmicro.com/hybridcloud**.

[1] TrendLabs 2016 Security Roundup: A Record Year for Enterprise Threats

[2] Maria Korolov. (5.Jan.2017). CSO Online. "Ransomware took in $1 billion in 2016–improved defenses may not be enough to stem the tide."

[3] Evaluation Criteria for Endpoint Protection Platforms, February 2017. Gartner ID G00317548

WHAT IS THE HYBRID CLOUD?

The speed of change in IT architectures over the past decade is unprecedented. The introduction of virtualization technologies from companies like VMware took the deployment of servers from weeks to days, changing the way data center operations and security teams worked, and resetting expectations of speed for business project delivery. Only a few years later, the public cloud market, driven by offerings like AWS and Azure, enabled the deployment of servers in minutes instead of days, empowering businesses to deliver new applications and projects at speeds that have never been seen before. With new technologies like containers, Docker and "serverless" offerings like AWS Lambda or Azure functions, the rate of change for IT is not showing any signs of slowing down.

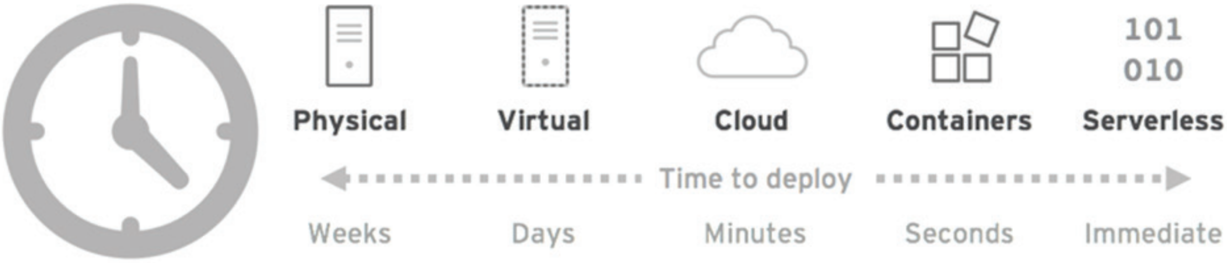


Figure 1: IT Architecture Evolution

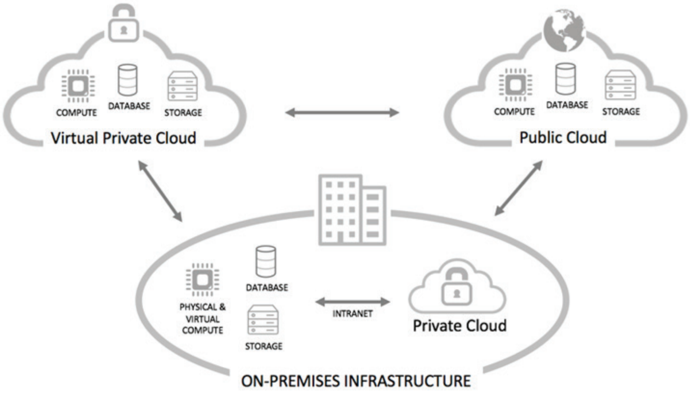


Figure 2: Hybrid Cloud Architecture

With such rapid change, the ability for an organization to simply abandon existing deployments in favor of the latest technology is severely limited. The result is that most organizations will have an IT architecture that spans multiple deployment environments, with new projects embracing the most modern approaches, but running projects that continue to operate within their existing environments. This concept is what underpins the use of "hybrid cloud" when describing modern IT. Hybrid cloud includes a mix of on-premises, private cloud and public cloud services with orchestration between the environments (see Figure 2). In this model, organizations can allow workloads to move between environments as computing needs and costs change, giving businesses greater flexibility, more deployment options, and increased opportunity for cost savings.

MODERN BUSINESS CHALLENGES

The reality of modern times is that every organization has become a technology organization. Businesses leverage new technologies, like virtualization and cloud, to improve the way they run IT, with the ultimate goal of speeding time-to-market, addressing capacity changes in economical ways, and dealing with ever-increasing compliance challenges.

THE NEED FOR SPEED

Today's global digital economy introduces both challenges and opportunities. Driven by the goal of speeding new projects to market, leveraging new technologies and approaches like DevOps can be especially attractive at both the corporate and the business-unit level. With compute, database, and storage easily accessible, the public cloud has enabled widespread use for rapid delivery of new projects, including at the business-unit level (often called 'shadow IT'). However, organizations can quickly be overwhelmed by the complexity created by constantly deploying the 'latest thing' without any central coordination, as well as introducing security risks based on a continually evolving threat landscape.

A SHIFTING IT LANDSCAPE

Significant investments have been made in data centers, including the relatively recent move from physical to virtual data centers. However, the attractiveness of the cloud and other new technologies are driving organizations to leverage more and more external capacity to manage changing IT needs. While this shift can deliver significant economic benefits, organizations are still faced with supporting existing on-premises deployments, which can introduce purchasing and support complexity, as well as operational and security challenges based on the diversity of environments.

MAINTAINING COMPLIANCE

According to the 2016 Verizon Data Breach report, there were 3,141 confirmed data breaches in 2015. With the Yahoo breach—the largest in history at 1 billion user accounts—and other examples like FriendFinder (412 million accounts) in 2016, it is clear that attackers continue their quest to penetrate corporations for financial gain. With threats on the rise, organizations are being mandated by external regulations to protect their IT infrastructure. Regulations like PCI DSS, HIPAA, FedRAMP, and the new European Global Data Protection Regulations (GDPR) are forcing organizations to implement specific security measures in order to be compliant. In order to help, frameworks for security, including the SANS/CIS Top 20, NIST 800-53, and ISO 27002, have been developed as a 'roadmap' to secure deployments. However, the shifting IT landscape has introduced new challenges for compliance. Organizations must now deal with deployments across multiple environments, ensuring that appropriate measures are in place for compliance while not overwhelming IT with tasks that are not central to the success of the business.

MODERN TECHNICAL CHALLENGES

New technologies like cloud bring tremendous potential gains through the promise of a flexible, on-demand and metered computing model. However, the rapid evolution of IT architectures and the reality of the hybrid cloud has introduced multiple challenges for technical teams supporting constantly shifting business needs. Inherent in these challenges is the fact that security needs to be looked at specifically for each environment, not generically.

MULTIPLE ENVIRONMENTS, TOO MANY TOOLS

While the benefits of new technologies like the cloud are obvious, including purchasing flexibility and deployment automation, most organizations will continue to have physical and/or virtual servers in the data center for the foreseeable future. This means that from both an operational and security perspective, organizations need to be able to deal with multiple environments at the same time, including ensuring connectivity between multi-tiered applications that leverage both data center and cloud for compute, data base, and storage services. The result often includes deploying multiple disparate security tools to address security, introducing significant complexity and operational cost, especially when tools work only in the data center and not the cloud.

STOP ADVANCED THREATS, SHIELD VULNERABILITIES

2016 could be labelled the year of ransomware, as millions of attacks were launched against users and enterprises with the goal of gaining a foothold and then executing a ransomware variant. 2017 is shaping up to follow suit, with the release of tools from **Shadow Brokers** and attacks like **WannaCry** and **Erebus** already impacting businesses. With multiple environments to deal with, the hybrid cloud introduces new complexity in dealing with advanced threats and vulnerabilities. As applications migrate from the data center to the cloud, the ability to protect these two environments from both existing and new vulnerabilities is a significant task, especially in the face of increasing compliance requirements. For example, an organization that continues to run Windows Server 2003 in the data center and also AWS Linux servers in the cloud will be subject to different vulnerabilities, but still require a unified and coordinated solution to protect from advanced attacks.

DEVOPS & THE SECURITY SKILLS SHORTAGE

According to IT market research firm Forrester, "Lack of skilled technical staff is a major challenge . . . 56% of security technology decision- makers rate lack of staff as a challenge, and 57% find unavailability of security employees with the right skills a challenge."[4] And with multiple environments that have different security requirements (ex: cloud service providers (CSP) are responsible for PART of the security story), security teams are being stretched thin. This is further exacerbated by the evolution of operations and the cloud, including the use of DevOps and introduction of the "DevSecOps" role. This role is all about getting things deployed quickly and efficiently in the cloud (including the use of containers such as Docker and serverless cloud functions), leveraging orchestration tools and automation to speed application delivery. This means that they are technology focused, not security experts—and using multiple, disconnected security tools that were not designed for automation, will quickly sabotage their success.

SECURING THE HYBRID CLOUD

Trend Micro is committed to helping our customers securely navigate their journey through these significant challenging times for IT . Integral to our XGen™ security strategy, for many years Trend Micro has been delivering new capabilities and security techniques to address threats across the hybrid cloud, while also enabling our customers to deploy them in ways that are optimized for each environment. Instead of using separate, siloed security solutions that don't share information, XGen™ security provides a cross-generational blend of threat defense techniques and a connected threat defense that protects our customers from advanced threats. Powering our Hybrid Cloud Security solution is Trend Micro Deep Security, a proven security product that helps thousands of our global customers secure millions of physical, virtual, and cloud servers. Leading analyst firms, including Gartner, Forrester, and IDC, consider servers a type of endpoint, and have included analysis in their reports on servers in the data center and cloud. **Ranked #1 in market share by IDC** in corporate server security for the past seven years[5], Trend Micro is also positioned furthest for completeness of vision and highest for ability to execute in the leaders quadrant of the **Gartner Magic Quadrant for Endpoint Protection Platforms**.[6]

[4] Report: The State of Network Security: 2016 To 2017, Forrester, January 2017

[5] IDC, Worldwide Endpoint Security Market Shares, 2015: Currency Volatility Headwind, #US41867116, November 2016

[6] Gartner Magic Quadrant for Endpoint Protection Platforms, # G00301183, January 2017.
Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

MULTIPLE CAPABILITIES, ONE PRODUCT

Deep Security is a host-based security control product that includes a broad range of cross-generational threat defense techniques for protecting servers, including:

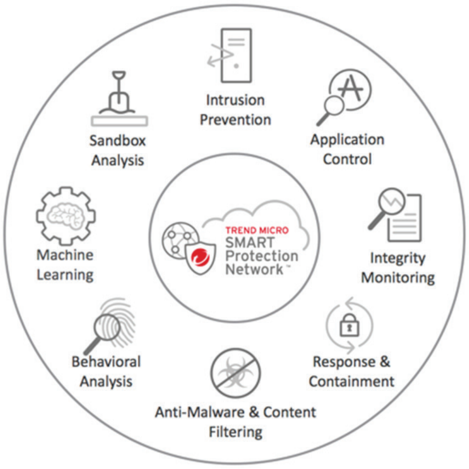
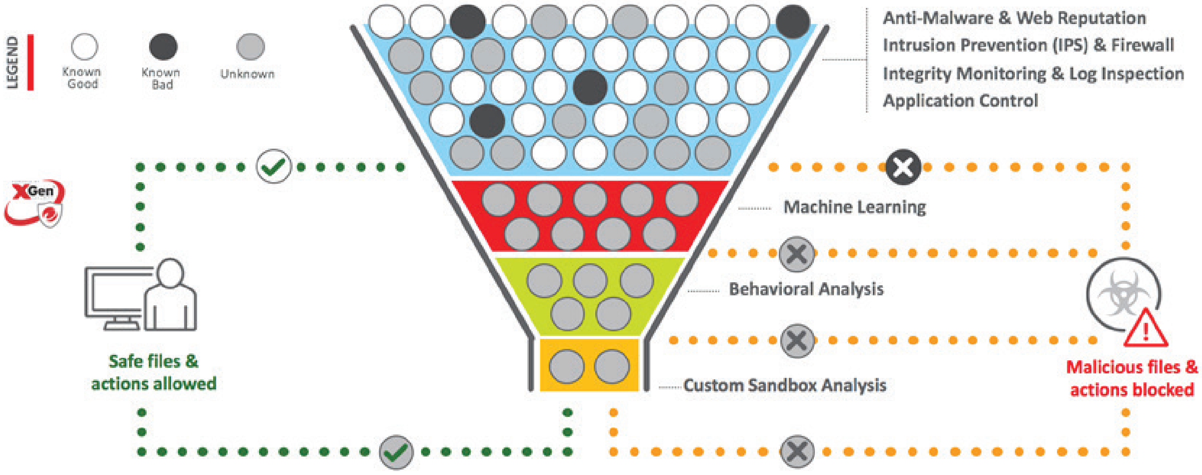


Figure 3: Multiple cross-generational security capabilities in a single product

- **Malware prevention**, including anti-malware, behavioral monitoring and network sandbox integration, for protecting against the latest in malware threats, including ransomware. It will also soon include machine learning to further enhance the detection of unknown threats.
- **Network security**, enabling protection from network attacks and the ability to virtually patch vulnerabilities with Intrusion Detection & Protection (IDS/IPS), as well as a host-based firewall to shield and help with reporting on network-based attacks.
- **System security** through application control and integrity monitoring, enabling the lock-down of servers and discovery of unplanned or malicious changes to registries, ports, and key system files. It can also help with response and containment, including leveraging log inspection for discovering anomalies in critical log files across the enterprise.

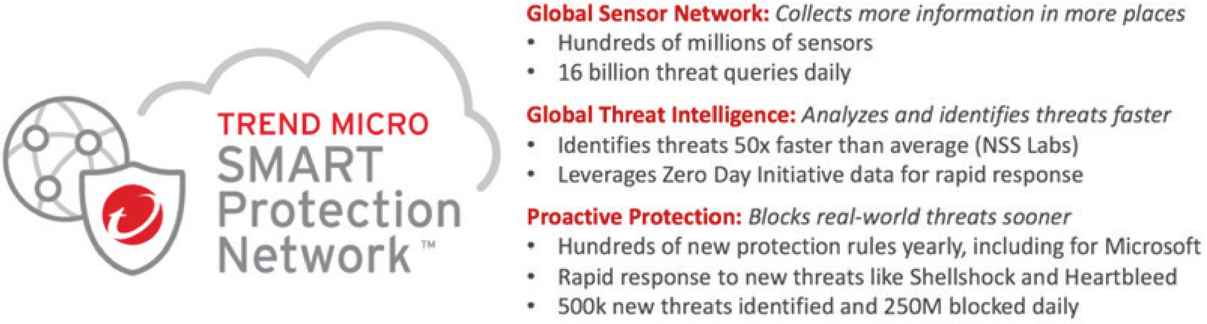
Despite the marketing efforts of new and unproven security providers, the challenges of securing workloads across the hybrid cloud preclude the concept of a security silver bullet. Protection from advanced threats while ensuring that performance is maximized requires the use of multiple techniques that can be applied to address known good, known bad, and unknown threats.

Taking security effectiveness one step further, Deep Security also has the ability to connect with other Trend Micro security products, sharing information and speeding response time to threats across the enterprise. This includes using information from the Trend Micro™ Smart Protection Network™, which has blocked over 170 million ransomware attacks in the past 12 months alone.


LEGEND
Known Good
Known Bad
Unknown
XGen
Anti-Malware & Web Reputation
Intrusion Prevention (IPS) & Firewall
Integrity Monitoring & Log Inspection
Application Control
Machine Learning
Behavioral Analysis
Custom Sandbox Analysis
Safe files & actions allowed
Malicious files & actions blocked

OPTIMIZED FOR THE HYBRID CLOUD

The challenge of the hybrid cloud is that each environment requires different approaches to the way that security is applied. The good news is that security strategies like defense in-depth remain relevant across all environments; it's how they are applied in ways that are both effective and operationally efficient that change. For example, for infrastructure-as-a-service (IaaS) deployments, there is a shared security responsibility, with the CSP responsible for everything up-to-and-including the hypervisor layer, and organizations responsible for everything they put in the cloud (See Figure 5).

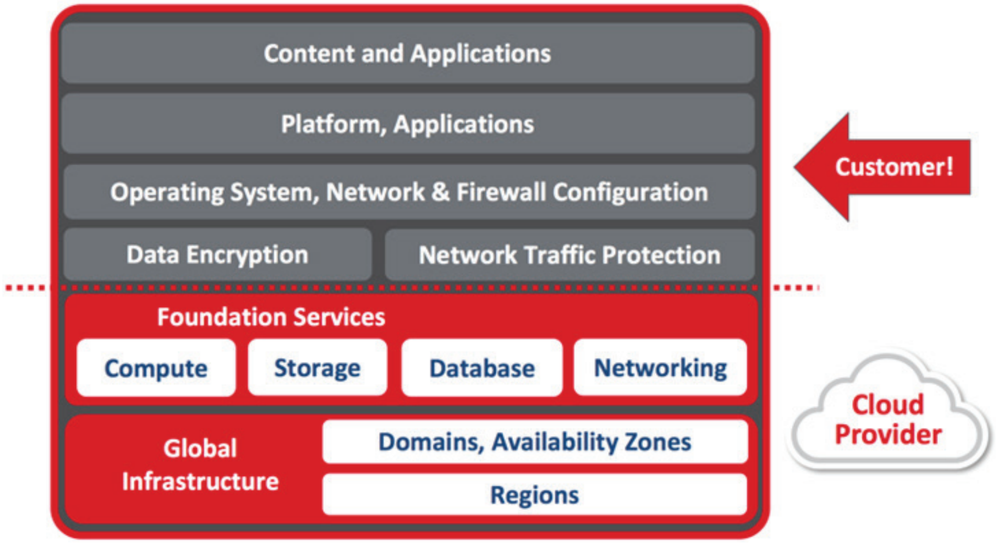


Global Sensor Network: *Collects more information in more places*
- Hundreds of millions of sensors
- 16 billion threat queries daily

Global Threat Intelligence: *Analyzes and identifies threats faster*
- Identifies threats 50x faster than average (NSS Labs)
- Leverages Zero Day Initiative data for rapid response

Proactive Protection: *Blocks real-world threats sooner*
- Hundreds of new protection rules yearly, including for Microsoft
- Rapid response to new threats like Shellshock and Heartbleed
- 500k new threats identified and 250M blocked daily

To help with this, Deep Security has been optimized to apply these security techniques across leading environments, including data center-focused technologies like VMware, as well as leading infrastructure-as-a-service (IaaS) providers like AWS and Azure. This enables organizations to deploy high performance security across the hybrid cloud without the need to purchase and manage multiple products in an already complex operating environment.



SOLVING REAL-WORLD SECURITY CHALLENGES

> *"No workload can be perfectly secured, nor do all workloads require equal protection. A risk-based approach to security control prioritization is needed. There is a shift in the importance of workload- centric protection with cloud computing, from a "secure network of workloads" to a "network of secure workloads."*
>
> "How to Make Cloud IaaS Workloads More Secure Than Your Own Data Center" ID# G00300337
> Gartner, June 2016
>
> Gartner®

It is important to remember that every workload in the data center, the cloud, or in a container, has a different level of risk, which means a wide range of capabilities need to be available to appropriately protect instead of a one-size fits all approach. While having many security capabilities in a single product will help with this risk-based approach, they are only applicable if those capabilities help organizations solve real-world security challenges. Let's take a look at a few examples of how Deep Security helps to address hybrid cloud security in multiple, meaningful ways.

PROTECT AGAINST ADVANCED THREATS: RANSOMWARE

Ransomware is malware that installs covertly on an endpoint and mounts an extortion attack by extracting and/or encrypting data, holding it inaccessible until a ransom is paid. While the majority of ransomware attacks leverage social engineering and email to gain access to an enterprise, servers are a prime target given the types of data and applications they hold. Figure 6 illustrates a typical attack sequence for ransomware.
Logically, the first step in the process is one of the most important points where security should be focused. Deep Security delivers multiple techniques that can help to stop ransomware as it attempts to move across the enterprise:

- *Shield servers from attack external attacks and lateral movement*: Once ransomware is in the enterprise, it will attempt to spread and achieve maximum damage. With host-based IPS and thousands of protection rules that can be automatically applied intelligently based on each specific machine context, the available attack surface is significantly reduced, both for external and internal attack vectors.

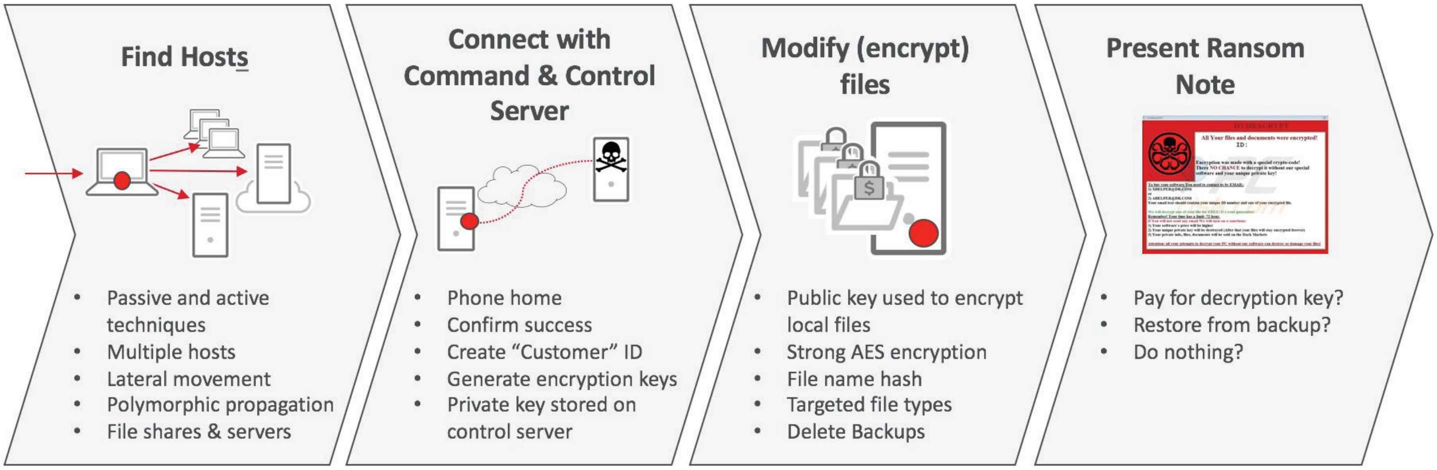
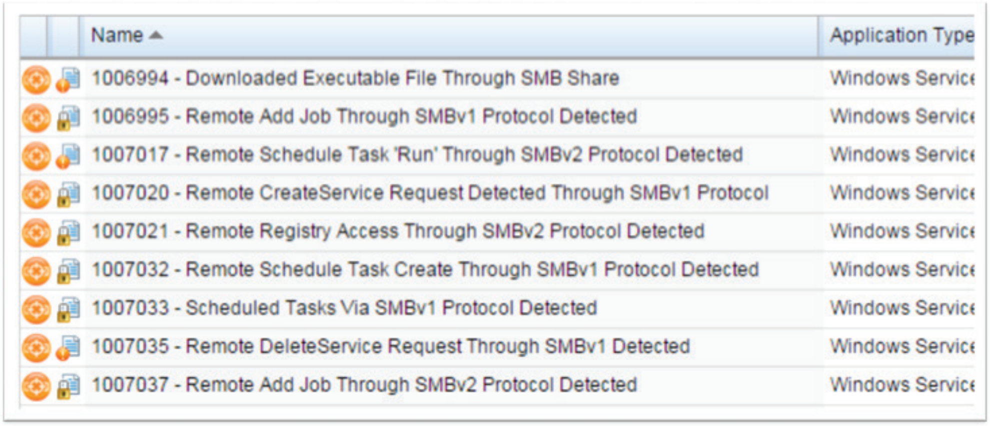


Figure 6: Ransomware attack sequence

Deep Security's smart rules are able to detect and prevent lateral movement as ransomware attempts to spread, including leveraging behavioral and heuristic data to catch unknown ransomware variants. Specific to situations where an end user machine has been compromised and has mapped drives to file servers, Deep Security can detect attacks over SMB, including encryption commands and file renaming thresholds, and be used to immediately shut down the connection and alert that ransomware is attempting to spread.



Name ▲	Application Type
1006994 - Downloaded Executable File Through SMB Share	Windows Service
1006995 - Remote Add Job Through SMBv1 Protocol Detected	Windows Service
1007017 - Remote Schedule Task 'Run' Through SMBv2 Protocol Detected	Windows Service
1007020 - Remote CreateService Request Detected Through SMBv1 Protocol	Windows Service
1007021 - Remote Registry Access Through SMBv2 Protocol Detected	Windows Service
1007032 - Remote Schedule Task Create Through SMBv1 Protocol Detected	Windows Service
1007033 - Scheduled Tasks Via SMBv1 Protocol Detected	Windows Service
1007035 - Remote DeleteService Request Through SMBv1 Detected	Windows Service
1007037 - Remote Add Job Through SMBv2 Protocol Detected	Windows Service

Figure 7: Smart rules detect and stop ransomware spread

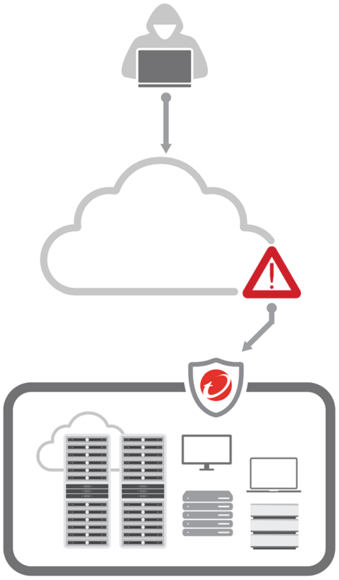
- *Block ransomware from running*: If ransomware somehow ends up on a server, it's first task is going to be to establish itself and start encrypting files. With application control, organizations can create a whitelist of authorized applications, ensuring that ransomware embedded in an unauthorized application simply cannot execute.

- *Stop command & control (C&C) traffic*: Without the ability to 'phone home', many ransomware variants are rendered harmless, as they have no means to receive the encryption key. Deep Security's smart rules detect both known and unknown C&C traffic on a server, stopping communication while alerting administrators of a potential attack.

- *Detect and block ransomware*: Attackers are innovative and determined, meaning that there is always a chance that a piece of malware will end up on a protected server. Deep Security's anti-malware capabilities include behavioral monitoring with real-time memory scanning that can detect suspicious activity and block it. This includes backing up files before they are encrypted and, once the malicious process has been stopped and quarantined, restoring them with minimal damage.

SHIELD SERVERS FROM VULNERABILITIES

Deep Security's network security controls can shield enterprise servers against known and unknown vulnerabilities—for example WannaCry (Windows SMB), Erebus (Linux) Shellshock and Heartbleed—from being exploited. Leveraging intrusion detection and prevention capabilities (IDS/IPS), Deep Security includes thousands of proven rules that apply to network traffic in layers 2-7. Using a recommendation scan to enable contextual security, these rules can be automatically applied based on a deployment environment to protect unpatched, network-facing system resources and enterprise applications. Protection applies to both the underlying operating system, as well as common enterprise applications deployed on those servers. Deep Security includes out-of-the-box vulnerability protection for hundreds of applications, including database, web, email, and FTP servers, defending against the most common web attacks, including SQL injection, cross-site scripting, and other web application vulnerabilities. In addition, it provides zero-day protection for known vulnerabilities that have not been issued a patch—typically in under 24 hours from disclosure—and unknown vulnerabilities using smart rules that apply behavioral analysis and self-learning to block new threats.



Attacks

Attacker attempts to exploit a vulnerability at the OS or application level over the network

Network Protection

Deep Security blocks malicious attacks at the network level, shielding servers from new and existing threats

Across the Hybrid Cloud

Deep Security protects applications and workloads from attacks across physical, virtual, cloud, and containers.

Figure 8: Network security shields servers from attack across the hybrid cloud

> *"Trend Micro's virtual patching capability in Deep Security lets us react quickly to a zero-day outbreak instead of working on a patching scheme that may take a week or a month to get in place."*
>
> **William Crank**, CISO,
> MEDHOST

To help with enforcement of IPS rules, Deep Security leverages its built-in, bi-directional and stateful firewall. The enterprise-grade firewall can also help to control communication over ports and protocols necessary for correct server operation, and blocks all other ports and protocols. This can further reduce the risk of unauthorized access to a deployment that includes EOS servers, like Windows Server 2003. The host firewall can also help with key compliance requirements from regulations like PCI DSS and HIPAA, particularly in cloud deployments where there is no access to the cloud provider firewall logs for network events.

ACCELERATE COMPLIANCE

More and more requirements are placed on businesses every day in the area of compliance. Regulations like PCI DSS, HIPAA, FedRAMP and GDPR are good examples that require organizations to implement multiple security controls and be able to report against them. Deep Security helps to accelerate the process of compliance, delivering:

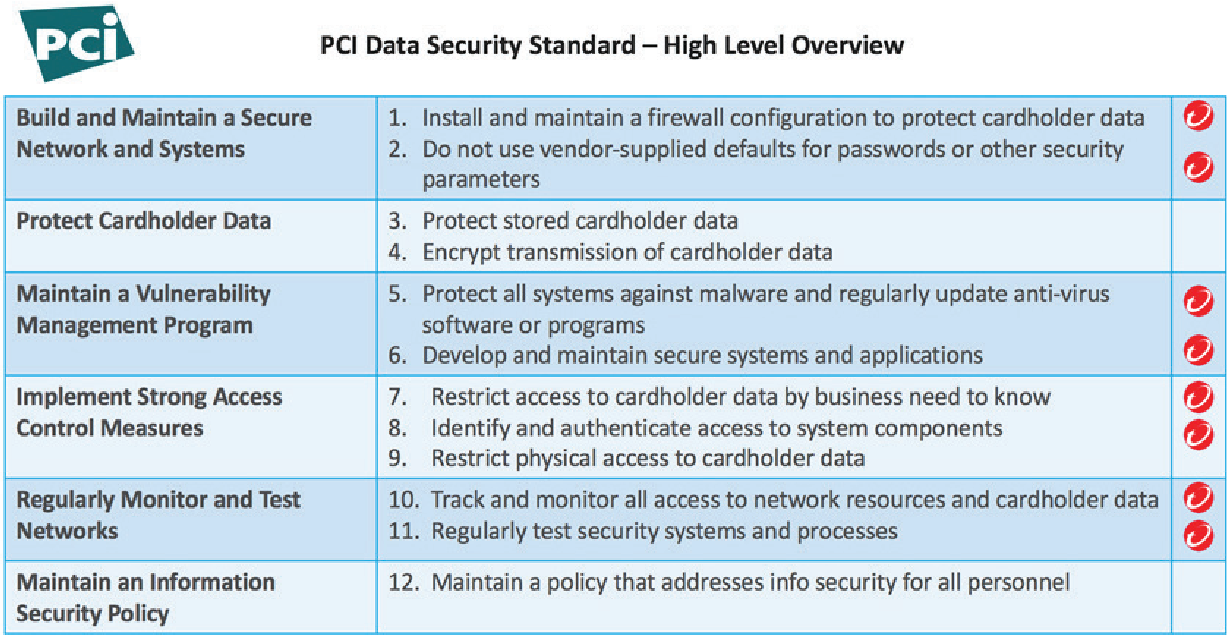
> *“The auditors were blown away by the information they could pull from Deep Security as a Service when certifying FedRAMP controls.”*
>
> **Justin Anderson**, CISO, iSite LLC
>
> iSite

- *A single product to address multiple security requirements*: From network shielding, to change detection, to mandated anti-malware protection, Deep Security includes the capabilities to address multiple compliance needs—through a single agent. For example, it helps to address 8 of 12 of the PCI DSS requirements. And the Deep Security as a Service offering is certified as a **PCI DSS Level 1 Service Provider**, enabling organizations rapidly deploy security from a service that will comply with audit requirements.

- *Single point of reporting*: Reporting is a big part of maintaining compliance, and Deep Security not only consolidates reporting across multiple security controls, it also includes templated and customizable reports for easier audits. Powerful options include the ability to report based on smart folders, which can easily give information on servers across the data center and cloud based on details that make sense for the compliance need, such as all in-scope servers running a particular application.

- *Built-in automation*: Compliance is not just about a point in time; it needs to be a continuous process. Deep Security enables continuous compliance with easy to understand automation features, including automated script generation for use with orchestration tools like Chef, Puppet, and Ansible, as well as the ability to deal with dynamic cloud activities like auto-scaling in AWS without creating security or compliance gaps.

- *Broad platform support, including end of support (EOS) systems*: With IT environments continually evolving, you need the ability to protect systems that are in-scope for audit without unreasonable cost or complexity. Deep Security includes built-in protection for EOS systems like Windows Server 2003, Windows XP, and more without the need to purchase expensive extended support contracts or upgrade faster than is right for the business.



PCI Data Security Standard – High Level Overview

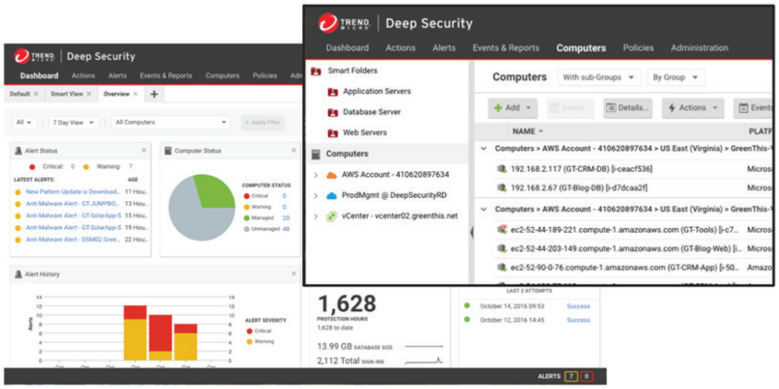
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data	✓
	2. Do not use vendor-supplied defaults for passwords or other security parameters	✓
Protect Cardholder Data	3. Protect stored cardholder data	
	4. Encrypt transmission of cardholder data	
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs	✓
	6. Develop and maintain secure systems and applications	✓
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know	✓
	8. Identify and authenticate access to system components	✓
	9. Restrict physical access to cardholder data	
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data	✓
	11. Regularly test security systems and processes	✓
Maintain an Information Security Policy	12. Maintain a policy that addresses info security for all personnel	

Figure 9: Address **8 of 12** PCI DSS requirements with one product: Deep Security

STREAMLINE SECURITY OPERATIONS AND MANAGEMENT

With multiple environments to deal with and a steady stream of new applications being developed to help the business, it is critical that security can be addressed in a scalable way, especially in light of a global security skills shortage. Deep Security includes a broad set of security capabilities that enable you to reduce the number of security tools used while giving full hybrid cloud visibility in a single interface. Built on deep integration with VMware, AWS, and Azure, Deep Security lets you discover all workloads across physical, virtual, and cloud environments, and apply protection based on server context.

Smart folders also enable you to easily view servers in ways that make sense to your operational processes, providing visibility across multiple environments based on criteria set by you (ex: show web servers across the data center, AWS, and Azure). And with automated recommendation scans for new and deployed workloads, new vulnerabilities can be highlighted and protected immediately.



Deep Security

Dashboard | Actions | Alerts | Events & Reports | Computers | Policies | Administration

Smart Folders
- Application Servers
- Database Server
- Web Servers

Computers
- AWS Account - 410620897634
- ProdMgmt @ DeepSecurityRD
- vCenter - vcenter02.greenthis.net

Computers | With sub-Groups | By Group

Add | Delete... | Details... | Actions | Events

NAME	PLATF
Computers > AWS Account - 410620897634 > US East (Virginia) > GreenThis-	
192.168.2.117 (GT-CRM-DB) [i-ceacf536]	Micros
192.168.2.67 (GT-Blog-DB) [i-d7dcaa2f]	Micros
Computers > AWS Account - 410620897634 > US East (Virginia) > GreenThis-	
ec2-52-44-189-221.compute-1.amazonaws.com (GT-Tools) [i-c7...	Micros
ec2-52-44-203-149.compute-1.amazonaws.com (GT-Blog-Web) [i...	Micros
ec2-52-90-0-76.compute-1.amazonaws.com (GT-CRM-App) [i-50...	Amazo

Dashboard: Default | Smart View | Overview

All | 7 Day View | All Computers | Apply Filter

Alert Status: Critical: 0 Warning: 7

LATEST ALERTS:	AGE
New Pattern Update is Download...	11 Hou...
Anti-Malware Alert - GT-JUMPBO...	13 Hou...
Anti-Malware Alert - GT-SolarApp-S	15 Hou...
Anti-Malware Alert - GT-SolarApp-S	19 Hou...
Anti-Malware Alert - DSM02 Gree...	22 Hou...

Computer Status — COMPUTER STATUS: Critical 0, Warning 0, Managed 20, Unmanaged 48

Alert History — ALERT SEVERITY: Critical, Warning

1,628 PROTECTION HOURS, 1,628 to date

13.99 GB DATABASE SIZE

2,112 Total SIGN-INS

LAST 2 ATTEMPTS

October 14, 2016 09:53	Success
October 12, 2016 14:45	Success

ALERTS 7 0

Figure 9: Single dashboard with visibility across the hybrid cloud

> *“Deep Security fits the DevSecOps model, giving us full visibility of all cloud workloads and automated provisioning of a broad range of security controls, enabling us to easily support an ever-expanding pipeline of new applications with a small, nimble team.”*
>
> **Jason Cradit**, Sr. Director Technology,
> TRC Solutions

Even with multiple security capabilities, there is only ever a single security agent to be deployed, simplifying deployment and management. The agent can be automatically deployed via scripting or orchestration tools like Chef, Puppet, Ansible, and SaltStack, and only deploys security components dictated by policy, streamlining the size of the agent and maximizing workload performance. The Deep Security agent can also automatically update to the latest version to deal with any kernel incompatibility that may arise due to a new OS version. This allows organizations to leverage the OS version needed for the business, without adding additional work to the taxed IT team.

Embracing the continuous integration/continuous deployment (CI/CD) model, Deep Security also includes the ability to integrate the application control update process into the development pipeline. This enables organizations to not only leverage application control for traditional whitelisting processes, but to also integrate security into the application update process with tools like Jenkins and GitHub. Literally, this means that the development teams are able to move at the speed required by the business without overloading the Ops team.

SIMPLIFY SECURITY ACQUISITION

With multiple security controls that can be deployed across the hybrid cloud, Deep Security enables organizations to reduce the number of security vendors they need to manage. Recognizing that the way you buy IT infrastructure changes depending on where it is, Deep Security is priced and sold in ways that further simplify security acquisition.

> *"Deep Security replaces four or five different tools that Infor used to use to provide security services. The best part is we get one portal to look at. ... The visibility keeps Infor compliant and makes audits three to four times faster than they used to be."*
>
> **Jim Hoover**, VP & CISO,
> Infor

In the data center, per server or per CPU pricing makes sense; however, in the cloud, you are paying based on what you use and by the hour. Working closely with leaders like AWS and Azure, Deep Security can be purchased in both traditional data center approaches, as well as by the hour, which is aligned to the cloud. Finally, Deep Security can be deployed in 3 different ways, giving maximum flexibility while also offering further simplification through options like purchasing through AWS or Azure marketplaces for a single-invoice cloud billing experience.

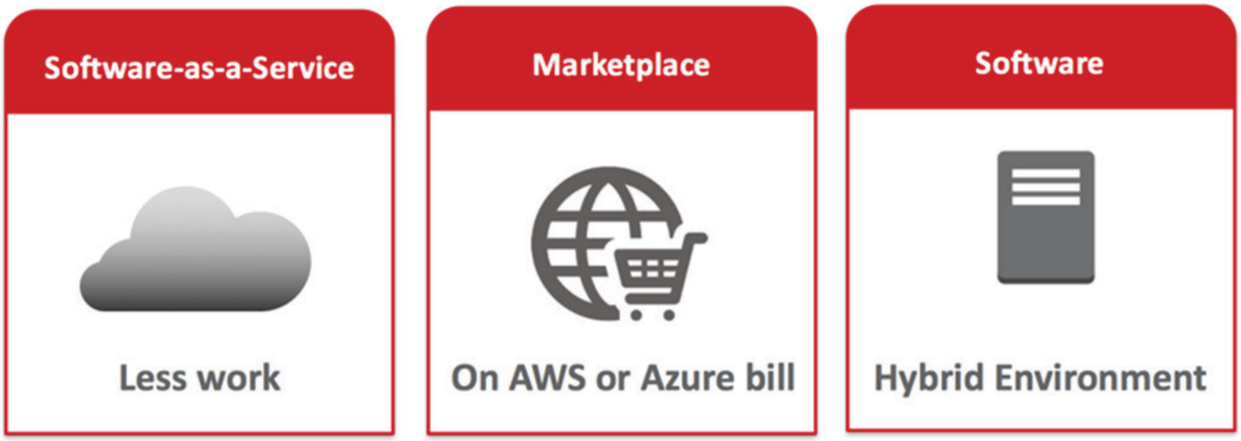


Figure 11: Multiple purchase options for securing hybrid cloud deployments

SUMMARY: SECURING THE HYBRID CLOUD

The hybrid cloud includes physical, virtual, cloud and container workloads, with new technologies like serverless functions introducing new complexity in the way that your organization operates. While embracing new technologies to gain benefits like increased agility and rapid application delivery make good business sense, the reality is that existing architectures also need to be maintained and secured at the same time. With increasingly sophisticated threats like WannaCry, Erebus, and others combined with ever-growing attack volumes, protecting the critically important data residing on server workloads across the hybrid cloud has never been more challenging or important.

With thousands of customers and millions of servers protected, Trend Micro Deep Security is designed for the hybrid cloud, delivering a cross-generational blend of threat defense techniques in a single product that has been optimized for securing physical, virtual, cloud, and container workloads. Delivering protection from advanced attacks like ransomware and multiple capabilities in a single product that allows for vendor consolidation, Deep Security solves real-world problems, simplifying operations without compromising security. Ranked **#1 in market share by IDC** and positioned furthest for completeness of vision and highest for ability to execute in the leaders quadrant of the **Gartner Magic Quadrant for Endpoint Protection Platforms**, you can feel confident in choosing Deep Security to protect your hybrid cloud deployments.

Find out more and start a trial today at **www.trendmicro.com/hybridcloud**.

Trend Micro Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our Web site at www.trendmicro.com.

TREND MICRO INC.
U.S. toll free: +1 800.228.5651
phone: +1 408.257.1500
fax: +1 408.257.2003