Trend Micro™ Deep Security™

# Optimized Security for the Modern Data Center

## Executive Pitch

Remove obstacles preventing you from realizing the power of the fully software-defined data center by using the most adaptive, aware, and comprehensive security solution. Deep Security is designed for the modern data center.

**Security optimized for virtual environments** with both file-based and network security controls; better VM visibility with hypervisor-level integration; efficient provisioning with automated workflow and tagging.

**Comprehensive security capabilities**
Intrusion Prevention (IPS), Firewall, Anti-malware with Web Reputation, Application Control, Integrity Monitoring, and Log Inspection, all built as part of the market-leading Deep Security solution.

**Fits enterprise standards – today and tomorrow**
Support for leading virtualization environments (VMware, Microsoft HyperV, Citrix) and cloud providers (AWS, Microsoft Azure). First to be certified for converged infrastructures like Cisco UCS, VCE vBlock, EMC.

## How to Win

- Align security with the data center operations strategy
- Go beyond antivirus to differentiate
- Leverage VMware partner ecosystem

## Identifying Ideal Customers

**Company size:** Amount of computing resources is more important than the number of employees.

**Key Buyers to know:**

- Data Center Operations
- CIO, CISO, Security manager

In many cases, security team can be a barrier. Get to know the data center operations team – they have budget and traditional security is painful for them.

## Customer Issues

Many customers have virtualized part or all of their data centers, but are unhappy with the negative impacts legacy security approaches have on performance and scalability. The evolution to hybrid cloud deployments further highlights these issues.

**Minutes to deploy a new server, weeks to secure it**
Customers can provision new virtual machines (VM) in minutes but it can take weeks to apply the appropriate security with traditional solutions (think change tickets, approvals, maintenance windows).

**Compliance and patch management headaches**
Virtualization & cloud makes it easier to adopt multiple platforms and applications – but it also creates a challenge to keep up with updates and patches and create a consolidated auditable report for compliance.

**Security impact on resources**
Are your customers using virtualization or cloud technology to speed deployments, increase usage/uptime and respond faster to business needs? Are they concerned that security will impact performance or storage size?

## How Trend Micro Helps

**PROVISION SECURITY AUTOMATICALLY**

- Tight integration with VMware, AWS and Microsoft Azure APIs to see what is running and recommend rules
- Seamless integration with leading configuration management tools (Chef, Puppet, Salt, Rightscale, OpsWorks) to secure as soon as it is provisioned

**MANAGE SECURITY EFFICIENTLY AS YOU SCALE**

- Virtual patching to ease patch management process
- Range of agentless and agent-based deployment options for integration with VMware
- Continuous VM monitoring enables consistent policy application and quick issue response

**OPTIMIZE DATA CENTER RESOURCES**

- Optimized for modern data centers to improve overall performance and VM densities (VDI)
- Comprehensive security options to reduce system load
- Avoid duplication of efforts with scan caching; resulting in 20X faster full scans

**SIMPLE, CENTRALIZED SOLUTION FOR SECURITY**

- Single console for physical, virtual, cloud, and hybrid environments
- Only product with both file and network based security controls for NSX
- Support for AWS, Microsoft Hyper-V and Azure, XenServer, and VMware vCloud Air
- Tight integration with Trend Micro Control Manager and VMware vCenter Operations Manager
- Detailed, auditable reports for compliance (PCI), easy integration with leading SIEM and log management servers (e.g., ArcSight, QRadar)

CONFIDENTIAL – NOT FOR GENERAL DISTRIBUTION
This document is intended to provide general guidance to and for the exclusive use of Trend Micro field sales and marketing personnel and authorized partners. The contents represent the best information available to Trend Micro at the time of publication and is provided "AS IS," without warranty of any kind as to its accuracy, currency or completeness, express or implied. The contents may not be applicable in all situations, may not reflect the most current situation, and are subject to change without notice and at the sole discretion of Trend Micro. It is not intended and should not be construed to constitute legal advice and should not be relied upon as such. Neither Trend Micro nor any party involved in creating, producing, preparing or delivering the contents shall be liable for any consequences, losses, or damages, including direct, indirect, special, consequential, loss of business profits or special damages, whatsoever arising out of access to, use of or inability to use, or reliance upon, the contents of this document, or any errors or omissions in

# Discovery Questions & What to Listen For

- **What are the current projects in the data center?**
  Are they virtualizing servers and/or desktops (VDI)? Are they deploying projects in the cloud? Do they have a mix of physical, virtual, and hybrid environments? Are they considering moving to VMware NSX? Trend Micro is the only solution that covers all environments in a central console.
- **How are you currently securing your environment?**
  If they have just shifted their existing security, there are performance and operational improvements that can be realized with Deep Security, especially with VDI.
  If they are using a perimeter solution (IPS, Firewall), talk about why it's important to move security closer to the host to enable scalability and reduce gaps in coverage.
  If they only have AV, ask about local regulations or compliance requirements (PCI DSS, EU data protection act) that require more than anti-malware.
- **Is security impacting your time to provision?**
  Does it take minutes to provision a new VM and weeks to ensure it's secured correctly? Trend Micro can automate deployment across virtual and cloud environments.
- **Is security impacting CPU, network, storage?**
  Is security counteracting all the benefits that virtualization and cloud environments provide with a clunky legacy security solutions designed for only physical environments?
- **How do you ensure the right policies are on the right VMs when one hypervisor may support multiple guests, OS's and applications? How are you tackling patch management? How does the cloud impact your security strategy? How did you respond to the Heartbleed vulnerability?**
  Were they able to virtually patch in minutes and schedule the update for a more convenient time?
- **How do you demonstrate compliance with PCI DSS or local regulatory requirements?**
  Want to reduce the number of tools and simplify process for reporting. Need detailed, auditable reports that document prevented vulnerabilities and policy compliance status. Would they like a single view of all security across environments. Dynamic cloud (bursting up /down) makes compliance more difficult without automation.
- **Are you customizing security policies based on workloads?**
  Can you automate the application of policies based on metadata? Can their solution automatically detect what is on a new VM and recommend the appropriate controls and virtual patches to protect it?
- **How do you determine what rules or policies to apply to a new VM that you are introducing to the environment?**
  Is it a manual process? What about VMs that may support multiple guests, OS's and applications? How do they manage patching in a complex environment?

# Objection Handling

Trend Micro can help customers with security across hybrid environments and is tightly integrated with leading virtualization and cloud providers so security can be automated.

- ***I am going to shift my existing legacy data center security to my virtual or hybrid cloud environment***
  Using traditional security approaches means you will likely face scalability and performance issues, and you are limited to statically defined security policies. Deep Security's architecture ensures optimization of: management, network usage, scan speed, host-wide CPU and Memory usage, IOPS, and the overall storage.

- ***All security solutions offer the same integration and protection with VMware environments***
  Only Trend Micro Deep Security was built from the ground up to efficiently secure virtualized data centers built on VMware technologies. It was designed to provide full visibility into VMware deployments and automated security to help streamline your data center ops while speeding up compliance.

- ***I have basic security in place. Why would I switch?***
  Are you encountering security issues causing headaches with provisioning, managing, or resources, there is a better option – optimized for virtual and hybrid environments with automation, central management, and trusted security. If considering hybrid cloud as well, traditional security approaches just don't scale—Trend Micro's deep integration and automation with cloud providers like AWS, Microsoft Azure, and VMware make it easy to address shared security responsibility.

- ***We patch all our systems on time… we don't need IPS/firewall, just anti-malware***
  There will always be challenges with timing and patches, including times when there are no patches (Microsoft, Java examples) available and that AV alone will not protect. What about legacy or custom applications? A good example of a need for rapid patching was the Heartbleed vulnerability…Trend Micro customers were protected the same day.

# Deep Security Competitive Summary

★★★ Full capabilities ★★ Partial capabilities ★ Limited capabilities

| | Capabilities | | Legacy Security | | AV Niche Players | | Network | |
|---|---|---|---|---|---|---|---|---|
| | | | Symantec | McAfee | Sophos | Kaspersky | Palo Alto | Juniper |
| Security Capabilities | Anti-Malware | ★★★ | ★★★ | ★★★ | ★★★ | ★★★ | ★★ | ★★ |
| | Application Visibility and Control | ★ | ★★ | ★★ | | | | |
| | IDS/IPS | ★★★ | ★ | ★ | | ★ | ★★★ | ★ |
| | Firewall | ★★ | ★★ | ★★ | | ★ | ★★★ | ★★★ |
| | File Integrity Monitoring | ★★ | ★★ | ★★ | | | | |
| | Event Monitoring | ★★ | ★★ | ★★ | | | | |
| | Vulnerability Assessment | ★ | | ★★ | | | | |
| Management & Deployment | Programmability & Automation | ★★★ | ★★ | ★★ | | | ★★★ | |
| | Hybrid Environment Support | ★★★ | ★ | ★ | | | | |
| | Multi-tenant (Service Provider) | ★★★ | | | | | | |
| | Agent Protection Architecture | ★★★ | ★★★ | ★★★ | ★★★ | ★★★ | | |
| | Security Management API | ★★★ | | | | ★★★ | | ★★★ |
| | Agentless (Virtual Appliance) Option | ★★★ | ★★ | ★★ | | | | |
| | VMware vRealize Operations Integration | ★★★ | | | | | | |
| Virtual Platform Support | VMsafe – Network | ★★★ | | | | ★★★ | | ★★ |
| | Vshield – Host | ★★★ | | ★★ | | ★★★ | | |
| | NSX | ★★★ | ★★ | | | ★ | ★★ | ★★ |
| | Hyper-V (Agent-based) | ★★★ | ★★ | ★★ | ★★ | ★★ | | |

# Primary Competitor Weaknesses

## McAfee

### Higher Resource Consumption

- Anti-malware only for agentless protection even with NSX; with more than one security control, multiple agents (including ePO) occupy a significant amount of memory in each virtual machine
- More agents translate into reduced consolidation ratios and increased capital (CapEx) and operational expenditures (OpEx)

### Increased Operational Overhead

- Higher admin costs for provisioning new security controls beyond anti-malware (separate products)
- Higher ongoing operational costs from continually reconfiguring these agents as the virtual machines move around or change state
- Management processes can be extremely time consuming (expensive) and result in security gaps

### No Vulnerability Monitoring

- Lack of vulnerability assessment means security controls may not be configured to protect against serious vulnerabilities
- Increased operational costs to configure and maintain secure systems

### Security Gaps for the Business

- Difficult to consistently provision and keep security up-to-date for VMs that are constantly activated/deactivated
- Without automated vulnerability monitoring, dormant virtual machines can deviate from baseline and introduce security vulnerabilities
- Lack of platform support (especially for Linux and kernels) and inconsistencies across product introduces security gaps and issues for the business (critical for IPS and the cloud)

## Symantec

### Business Exposed to Vulnerabilities

- Symantec SEP is a legacy endpoint product that has been stretched into virtual and hybrid cloud environments and created security gaps because it was not designed for virtual and cloud environments.
- Symantec has no vulnerability assessment capabilities. Lack of Recommendation Scanning that identifies vulnerabilities on servers and applies the appropriate Intrusion Prevention (Virtual Patching) rules.
- Symantec has limited agentless AM and IPS capabilities (Antimalware and IPS) with NSX.

### Higher Operations Costs

- Symantec SEP is deployed broadly as an endpoint solution and has been used a stop-gap in virtual and cloud environments. This has led to system performance challenges because it was not architected specifically for these environments.
- Symantec does not have AWS or Azure connectors. This creates serious limitations with respect to auto scaling security to fit the size of deployment.
- Symantec lacks Linux automation and requires an update to the installed agent package, as there is no automatic kernel update support. Deep Security has an extensive automated kernel support process.

### Limited User Flexibility

- Symantec does not have a SaaS offering or the ability to purchase through the AWS/Azure marketplaces.
- Symantec does not have multi-tenant capabilities.
- Symantec has limited Operating System coverage and it is not consistent across their security offerings.

## The Competition Can't Match:

Gartner analysts say Deep Security's differentiation in the marketplace remains strong. This is due to our optimizations for AWS and VMware and the broader platform support we offer for servers than competitors (Gartner Endpoint Protection MQ 2016)

- Seamless transition from physical to virtual to hybrid cloud
- Only vendor to provide file and network-based security for NSX
- Lower operational cost through security automation in virtual and cloud environments
- Agentless model option for key security controls in VMware NSX, not just anti-malware
- Scale easily with a single management console – highly available and scalable

# Deep Security Capabilities

Deep Security automatically recognizes VMs and cloud instances at launch. Initiates security at start to dramatically reduce the risk of servers going unprotected.

- ✓ **Anti-malware with Web Reputation:** Timely protection against new malware being created and used to attack systems and steal data, detect/prevent command-and-control traffic supported by information from the Trend Micro Smart Protection Network (SPN).
- ✓ **Intrusion Prevention:** Shield vulnerabilities from attack (virtual patching) with auto-updating security policies to ensure the right protection is applied to the right servers.
- ✓ **Host-based Firewall:** For cloud and non-NSX environments, creates a firewall perimeter around each server to block attacks and limit communication to only the ports and protocols necessary. Also provides reporting at the host level, which is not possible with cloud service provider firewalls.
- ✓ **Application Control:** Detects and blocks unauthorized software automatically. Scans a machine and determines which applications are currently on it and locks down the system once the inventory is created, preventing new applications from running without being whitelisted.
- ✓ **Integrity Monitoring:** Meet your compliance file and system monitoring requirements and ensure unauthorized system changes are detected and reported.
- ✓ **Log Inspection:** Identify important security events in system logs to quickly identify suspicious behavior, as well as meet compliance requirements. Easily send information to a SIEM.

# Key New Features in Deep Security 10

- **Application Control**
  Automatically detects and blocks unauthorized software preventing new applications from running without being whitelisted.
- **Sandbox Analysis**
  Advanced threat detection and remediation of suspicious objects through Sandbox Analysis
- **Container Protection**
  Protects Docker containers on a host across all of their environments by applying pre-defined policies to the host in order to secure these containers

# What to Sell

Trend Micro's modern data center security capabilities are delivered by:

**Deep Security** to protect servers: Anti-malware with Web Reputation, Intrusion Detection and Prevention, Firewall, Application Control, Integrity Monitoring, and Log Inspection

# Why Choose Trend Micro?

- Comprehensive security capabilities (agentless and agent-based options)
- Reduced cost and complexity with security automation
- Single platform for management across multiple environments and capabilities
- API integration with VMware and AWS
- Seamlessly extends security from physical servers to virtualized, cloud and hybrid environments

# Customer Call to Action

Visit TrendMicro.com/VMware

## More Information

- www.trendmicro.com/datacenter
- www.trendmicro.com/cloud
- www.trendmicro.com/deepsecurity

## Market Success

- #1 provider of server security for physical, virtual, cloud and hybrid environments since 2009 (IDC, 2017)
- Trend Micro is a leader in Gartner's Endpoint Protection Platform MQ and is a good shortlist candidate for buyers looking for server protection platform capabilities
- Chosen by thousands of customers to protect millions of instances

## Order Information

**Deep Security**

Deployment options: Software; as a service

Deep Security Packages:

- Anti-malware: Anti-malware with Web Reputation,
- Network: Intrusion Detection and Prevention (IPS), Firewall,
- System: Application Control, Integrity Monitoring and Log Inspection
- Enterprise: All Capabilities listed in other packages

## Sales Tools

The following assets are available on Sales Library:

- Customer presentation
- Sales training presentation
- Data sheets: Deep Security, Deep Security Packages
- VMware Focused Materials: NSX vRealize Operations, Horizon VDI, vCloud Air
- Sales Library Chatter Relevant Market Information
- Solution brief: Optimized Security for the Modern Data Center
- Channel Sell Sheet: Modern Data Center
- Much more…

## Contacts

Global Product Manager: Rick Abbott

Global Product Marketing: Steve Neville