Next Generation Data Security for Software Defined Data Centre

Veli-Pekka Kusmin
Senior Sales Engineer
6.11.2014

A world safe for exchanging digital information

CEO	Eva Chen
Founded	1988, United States
Headquarters	Tokyo, Japan
Employees	5,217
Offices	36
2013 Sales	$1.1B USD

New malware every ½ second

Global Threat Intelligence

- 1,200+ experts worldwide

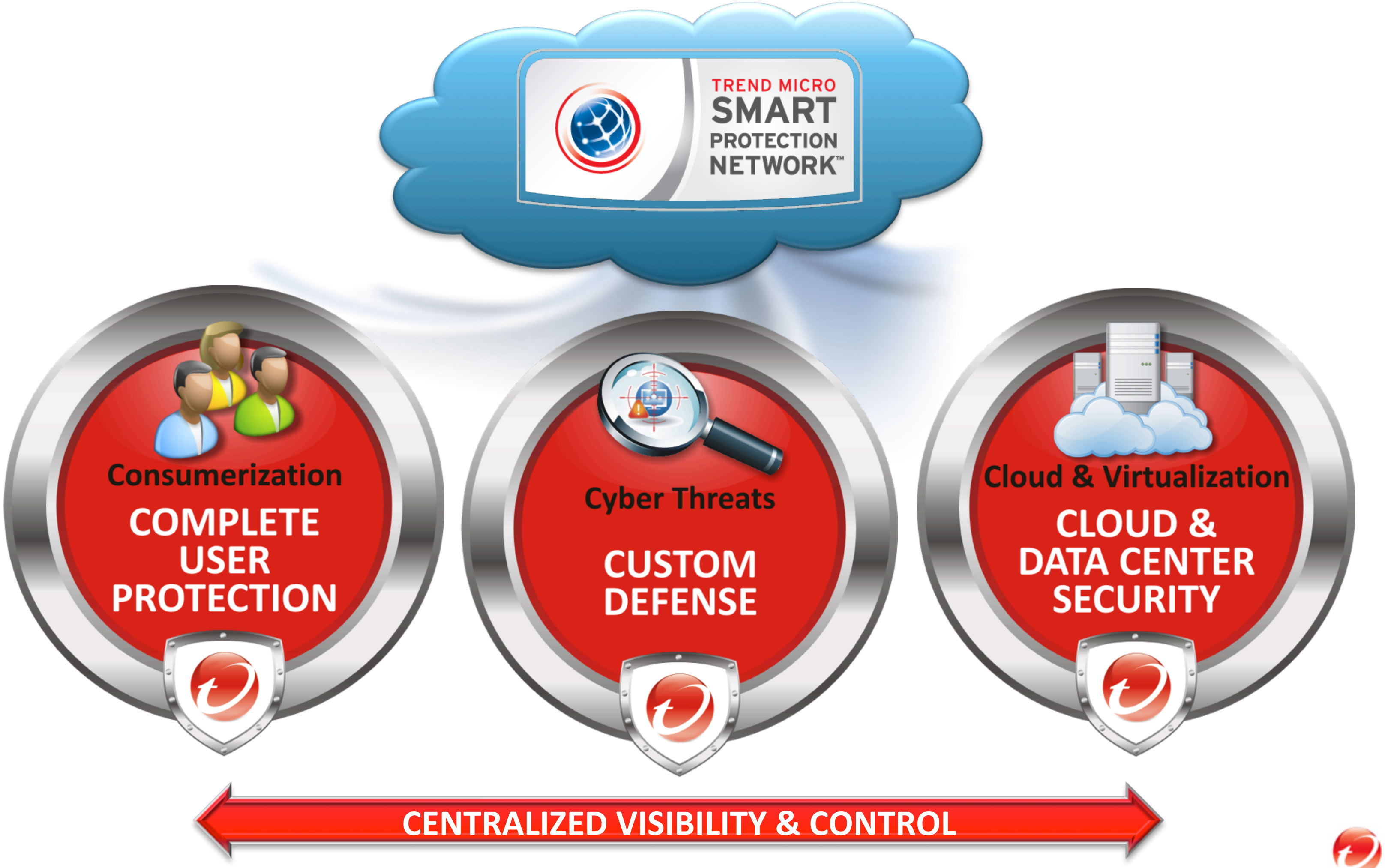
96% of the top 50 global corporations.

100% of the top 10 automotive companies.

100% of the top 10 telecom companies.

80% of the top 10 banks.

90% of the top 10 oil companies.



TREND MICRO SMART PROTECTION NETWORK™

Consumerization

COMPLETE USER PROTECTION

Cyber Threats

CUSTOM DEFENSE

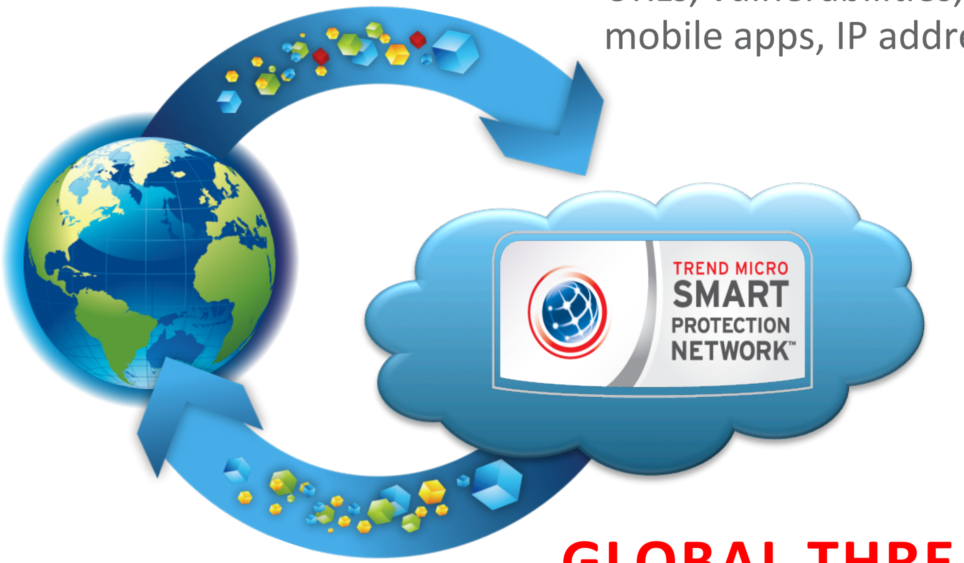
Cloud & Virtualization

CLOUD & DATA CENTER SECURITY

CENTRALIZED VISIBILITY & CONTROL

COLLECTS VIA GLOBAL SENSORNET

- Honeypots, customers, threat researchers, community…
- Over 300M nodes; 8.6B threat events daily
- URLs, vulnerabilities, files, domains, network traffic, threat actors, mobile apps, IP addresses, exploit kits



BIG DATA ANALYTICS

- Identifies using data mining, machine learning, modeling and correlation
- 100 TB data; 500K unique threats identified daily

GLOBAL THREAT INTELLIGENCE

- 250M threats blocked daily
- Email reputation, file reputation, web reputation, network traffic rules, mobile app reputation, known vulnerabilities/exploits, threat actor research, C&C…

The enterprise boundary is gone

By 2016, 71% of server workloads will be virtualized[1]

461 cloud apps in enterprises, 10X IT's estimate[2]

731M records lost due to hacking & Web compromises[3]

[1] Gartner, Forecast Analysis: Data Center, May 2012;

[2] Forrester Study, 2013;

[3] Netscope Cloud Report, April 2014

By virtualization are you dealing with…

… Servers that share resources… but security that consumes it?

… Minutes to deploy a server… weeks to secure it?

… Virtual scale beyond physical limits … and hitting a wall on security?

Security principles remain the same…

…but the APPROACH to security must change.

ADAPTIVE

Intelligent, dynamic provisioning & policy enforcement

CONTEXT

Workload & application-aware

SOFTWARE

Optimized for virtualization & cloud infrastructure

PLATFORM

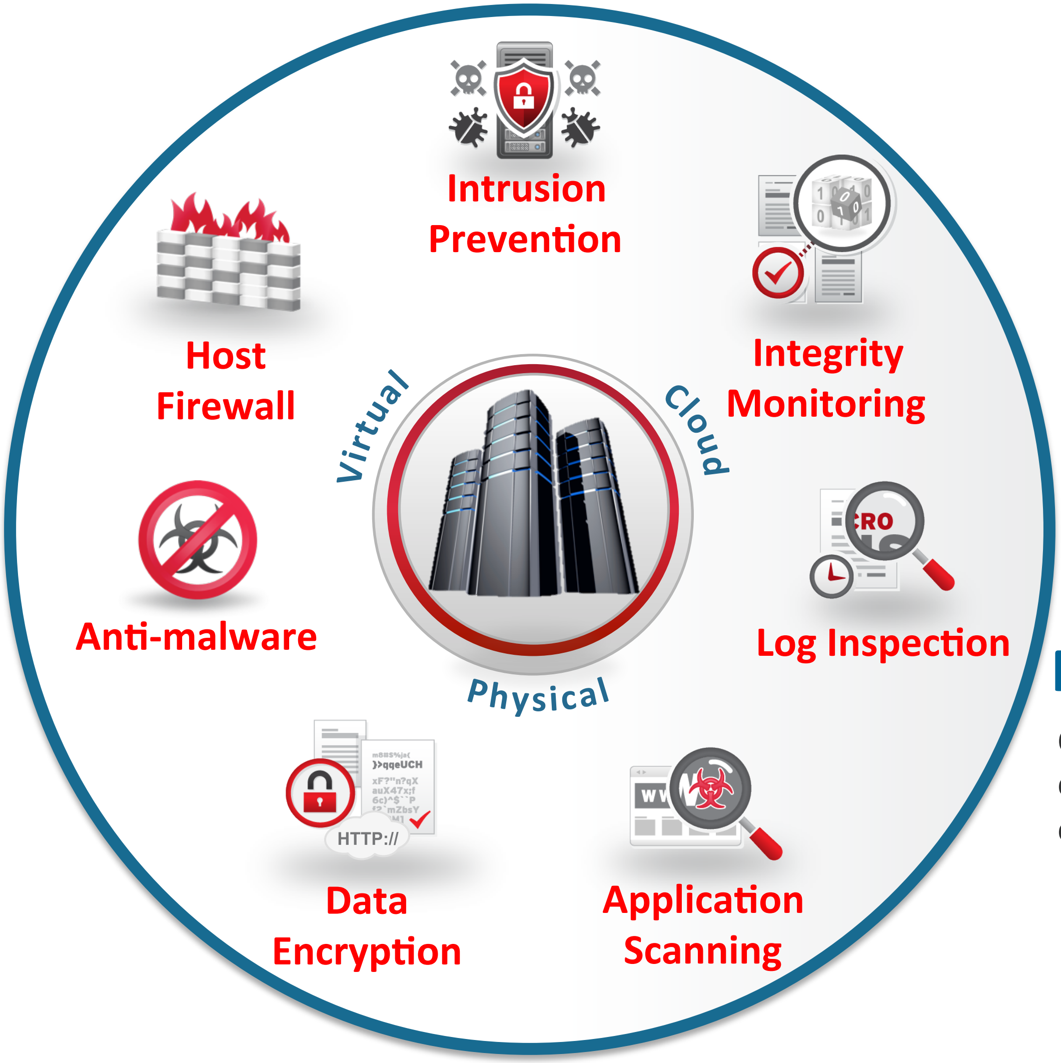
Comprehensive capabilities across data center & cloud

ADAPTIVE

Intelligent, dynamic provisioning & policy enforcement

CONTEXT

Workload & application-aware



Intrusion Prevention

Host Firewall

Integrity Monitoring

Anti-malware

Log Inspection

Data Encryption

Application Scanning

Virtual

Cloud

Physical

SOFTWARE

Optimized for virtualization & cloud infrastructure

PLATFORM

Comprehensive capabilities across data center & cloud vmware

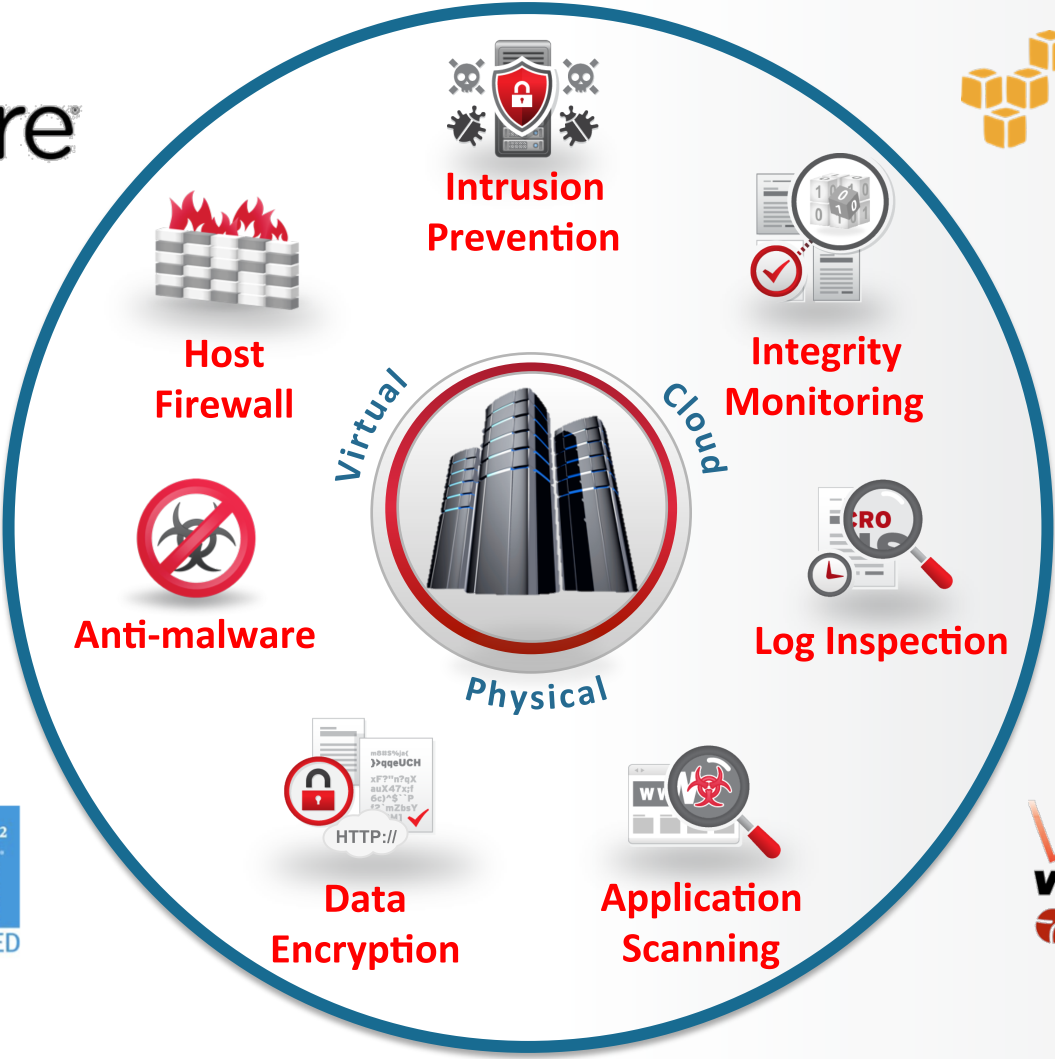
Hyper-V™

CISCO PARTNER Technology Developer

CiTRIX ready

VCE

EMC² VSPEX LABS VALIDATED



Intrusion Prevention

Host Firewall

Integrity Monitoring

Virtual

Cloud

Physical

Anti-malware

Log Inspection

Data Encryption

Application Scanning

amazon webservices™

Microsoft Azure

IBM

rackspace HOSTING

verizon terremark

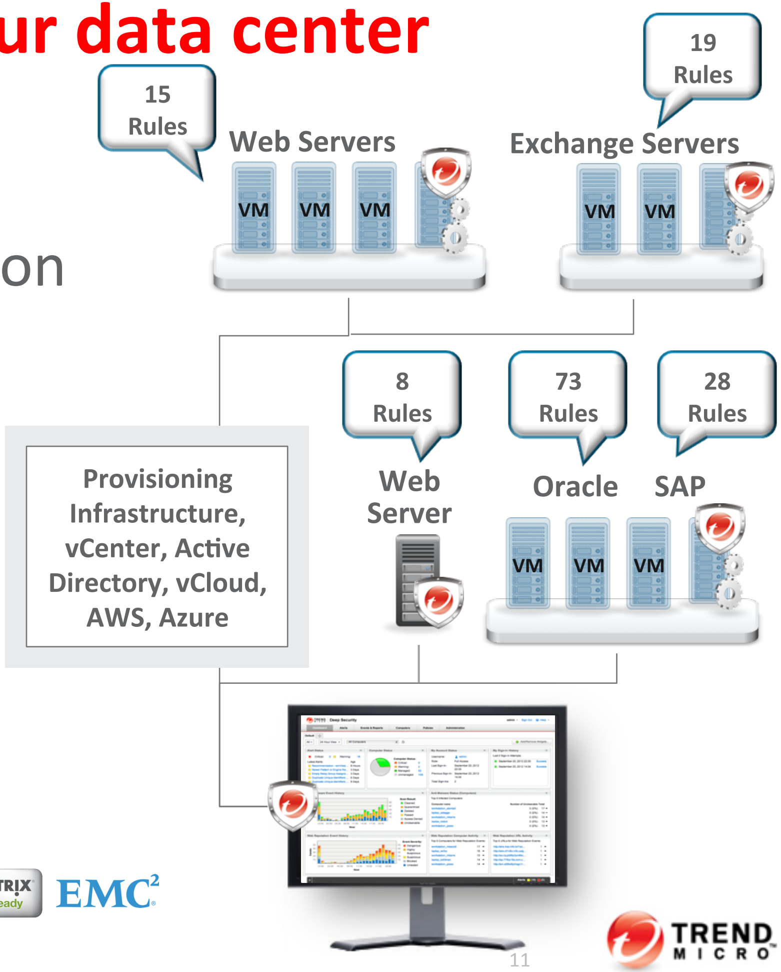
TREND MICRO

New approach can deliver optimized security for the modern virtualized data center

- Provision security automatically across environments
- Manage security efficiently as you scale
- Security optimized for the modern data center

Automate security specific to your data center

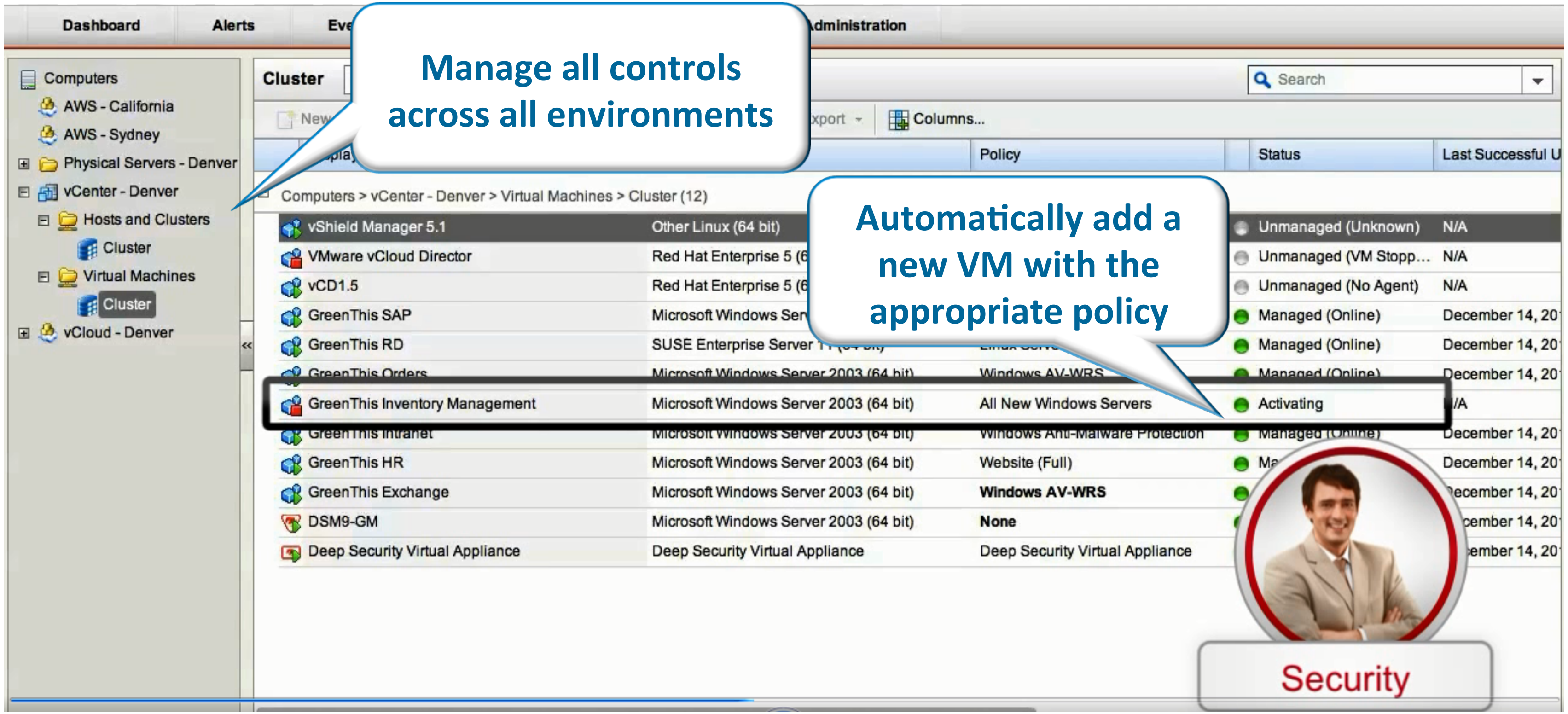
- Gain visibility vCenter Operations Manager and vCloud Director integration
- Recommend and apply policies automatically - specific to your data center environment
- Automatically scale up and down across data center *and* cloud as required—with no security gaps



Provisioning Infrastructure, vCenter, Active Directory, vCloud, AWS, Azure

vmware · amazon webservices · Microsoft Azure · Windows Hyper-V · CISCO PARTNER Technology Developer · VCE · NetApp · CITRIX ready · EMC²

Automatically protect new VMs



Manage all controls across all environments

Automatically add a new VM with the appropriate policy

Computers > vCenter - Denver > Virtual Machines > Cluster (12)

play		Policy	Status	Last Successful U
vShield Manager 5.1	Other Linux (64 bit)		Unmanaged (Unknown)	N/A
VMware vCloud Director	Red Hat Enterprise 5 (6		Unmanaged (VM Stopp…	N/A
vCD1.5	Red Hat Enterprise 5 (6		Unmanaged (No Agent)	N/A
GreenThis SAP	Microsoft Windows Ser		Managed (Online)	December 14, 20
GreenThis RD	SUSE Enterprise Server 11 (64 bit)	Linux Serve	Managed (Online)	December 14, 20
GreenThis Orders	Microsoft Windows Server 2003 (64 bit)	Windows AV-WRS	Managed (Online)	December 14, 20
GreenThis Inventory Management	Microsoft Windows Server 2003 (64 bit)	All New Windows Servers	Activating	/A
GreenThis Intranet	Microsoft Windows Server 2003 (64 bit)	Windows Anti-Malware Protection	Managed (Online)	December 14, 20
GreenThis HR	Microsoft Windows Server 2003 (64 bit)	Website (Full)	Ma	December 14, 20
GreenThis Exchange	Microsoft Windows Server 2003 (64 bit)	**Windows AV-WRS**		ecember 14, 20
DSM9-GM	Microsoft Windows Server 2003 (64 bit)	**None**		cember 14, 20
Deep Security Virtual Appliance	Deep Security Virtual Appliance	Deep Security Virtual Appliance		ember 14, 20

Optimized for your VMware investments

- Secures using agentless innovation for file & network controls, not just anti-malware
- Automate provisioning, workflow and tagging
- Integrates with management layer for complete real-time visibility
- Manage security consistently across physical, virtual, & cloud

✓ **VMware vSphere™**

✓ **VMware vShield**

✓ **VMware NSX™**

✓ **VMware vCenter™**

✓ **VMware vCenter Operations™**

✓ **VMware Horizon Desktop™**

✓ **VMware vCloud & vCloud Air™**

Continued Innovation with VMware

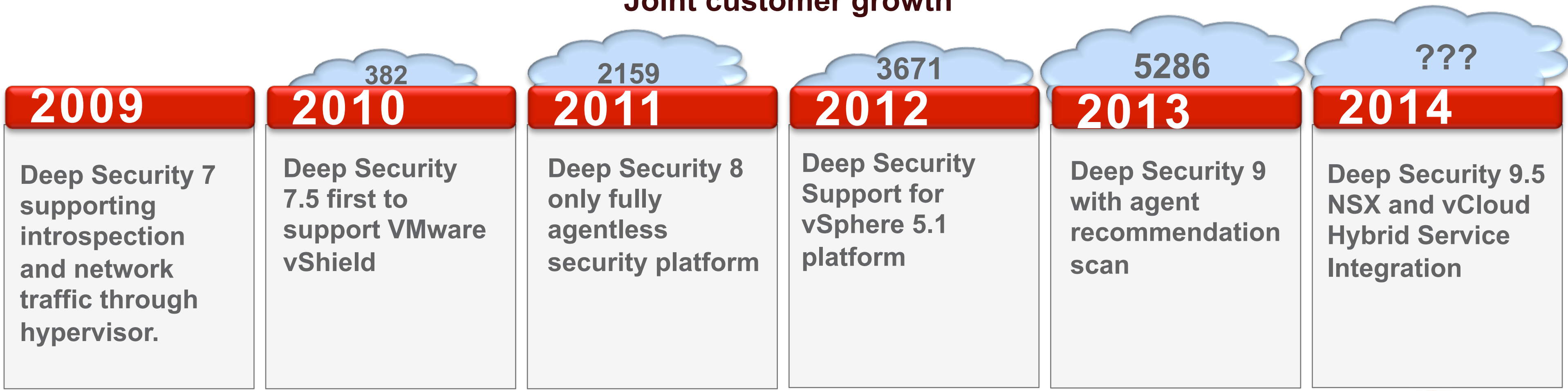
vmware

the most secure virtualization infrastructure, with APIs, & certification programs

TREND MICRO

security solutions architected to fully enhance the VMware platform

Joint customer growth



2009

Deep Security 7 supporting introspection and network traffic through hypervisor.

382

2010

Deep Security 7.5 first to support VMware vShield

2159

2011

Deep Security 8 only fully agentless security platform

3671

2012

Deep Security Support for vSphere 5.1 platform

5286

2013

Deep Security 9 with agent recommendation scan

???

2014

Deep Security 9.5 NSX and vCloud Hybrid Service Integration

Strengthening Alignment with VMware

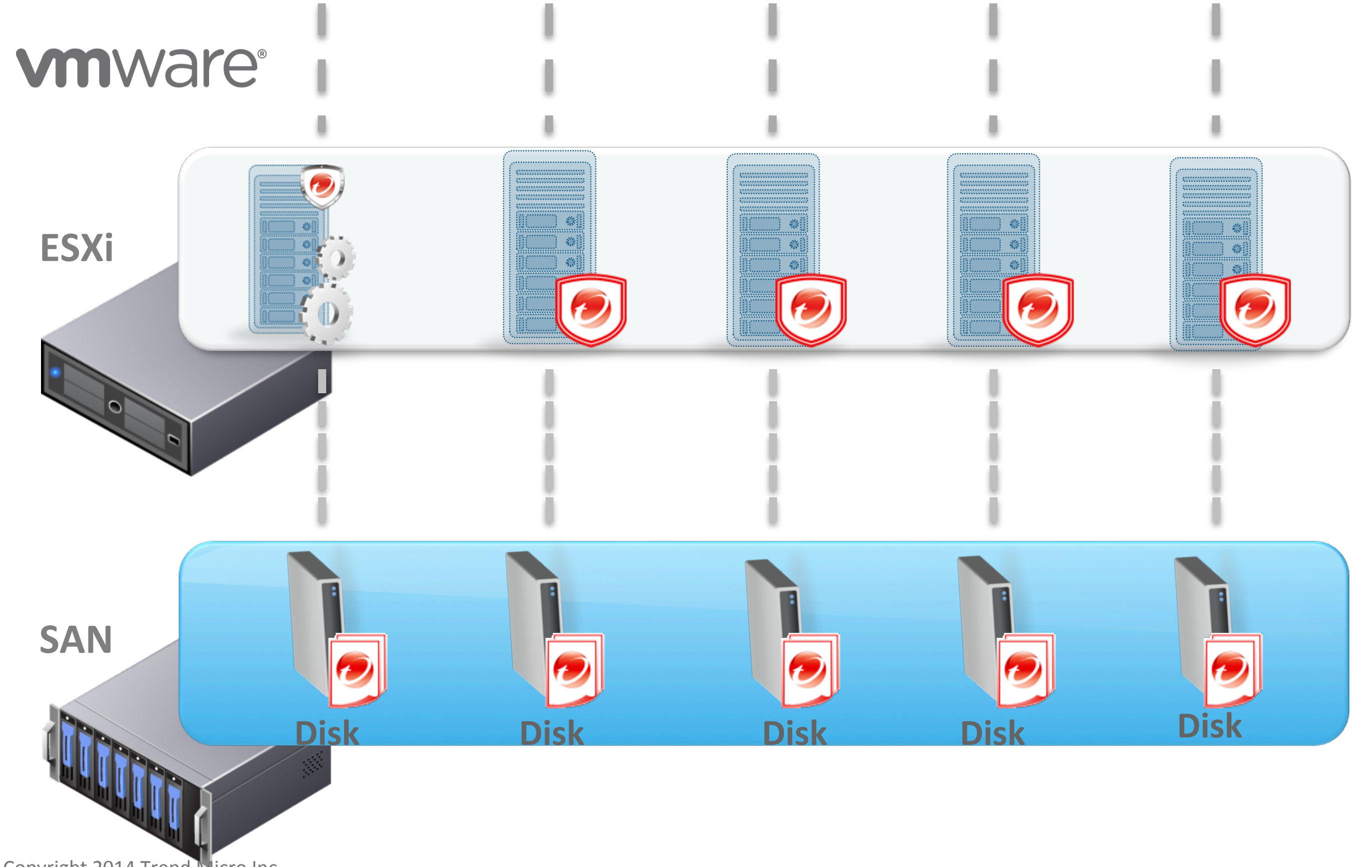
- **vCloud Air (formerly vCloud Hybrid Service)**
  - Seamlessly move on-premise deployment to the public cloud (announced in June, 2014)
- **vCenter Operations Plug-in**
  - Allows the operations team to see the security status, security related events and overall health from a single view (VMworld announcement)
- **Horizon Desktop as a Service (DaaS)**
  - New Deep Security reference architecture validated by VMware for Horizon DaaS
  - Integrate agentless security and deliver fully-managed or co-managed security as part of a desktop as a service offering
  - VMworld announcement

vmware® vCloud
Hybrid Service

vCenter Operations Manager

VMware
Horizon DaaS

Use agentless security to reduce system load



Network Usage

Scan Speed

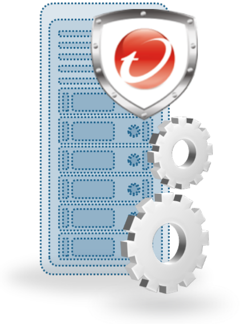
CPU/Memory Usage

IOPS

Storage

Avoid duplication of effort to impact performance

Scan Cache



Up to **20X** Faster*

Full Scans

Up to **5X** Faster

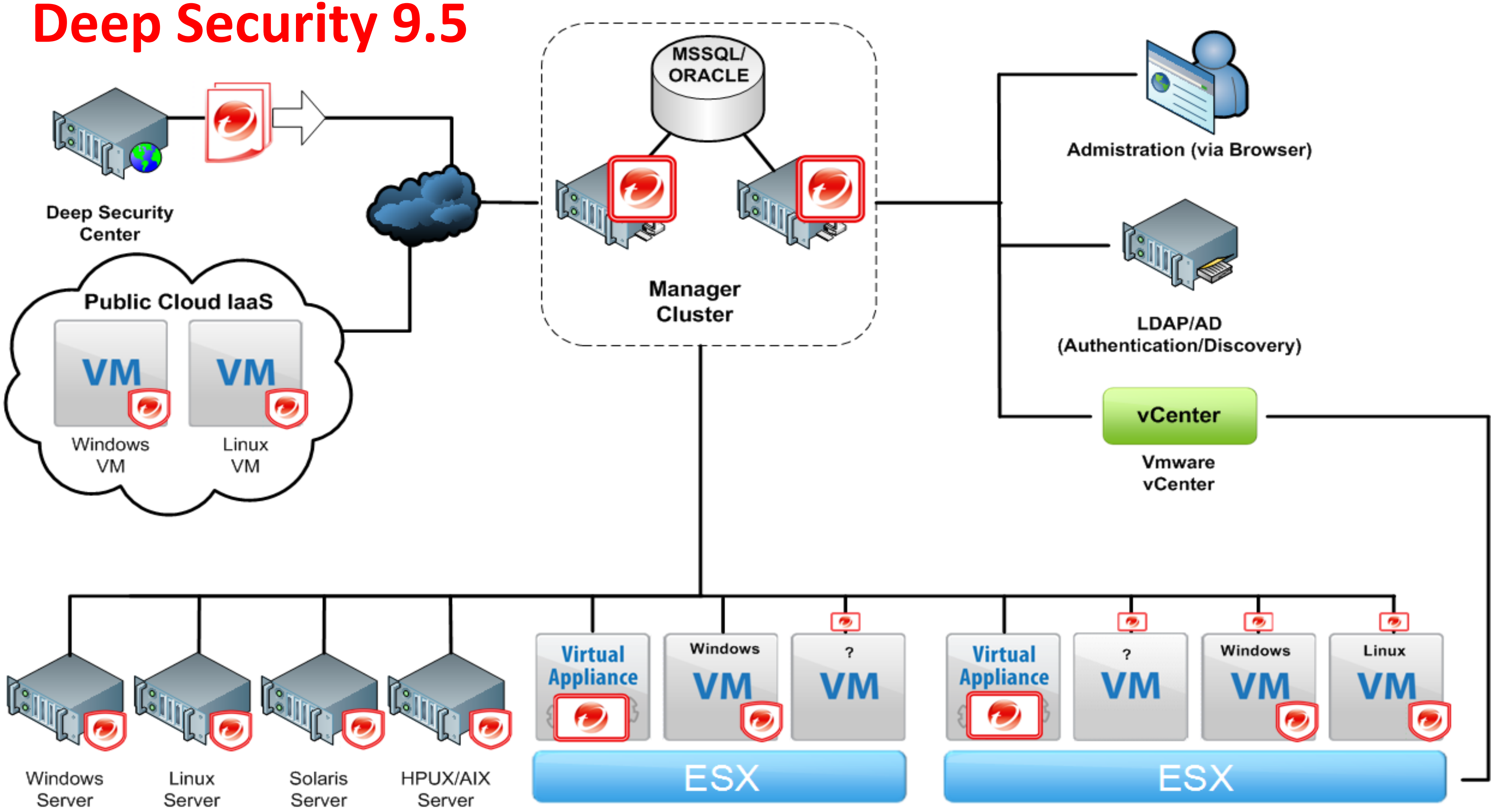
Realtime Scans

Up to **2X** Faster

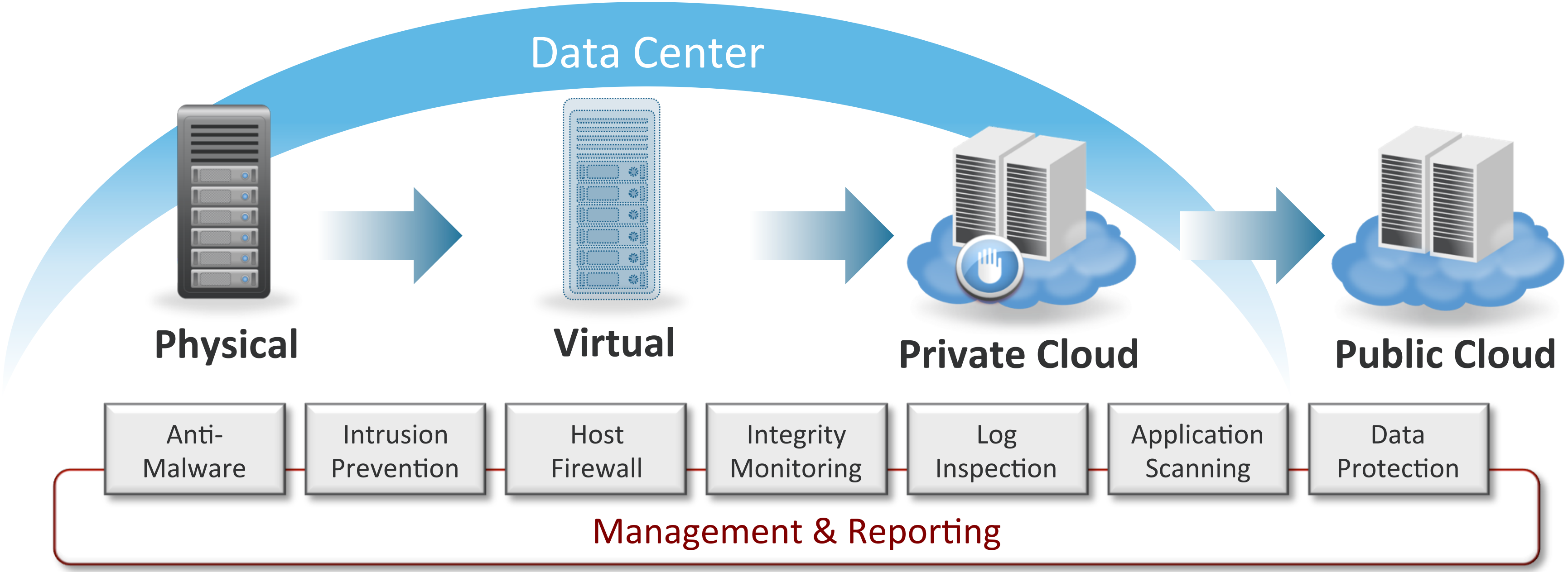
VDI Login

*All results based on internal testing using VMware View simulators

Deep Security 9.5



Single platform for the modern data center & cloud



Data Center

Physical

Virtual

Private Cloud

Public Cloud

Anti-Malware

Intrusion Prevention

Host Firewall

Integrity Monitoring

Log Inspection

Application Scanning

Data Protection

Management & Reporting

- Address security across **ALL** your environments
- Comprehensive security to address varying risk

Trend Micro Cloud & Data Center Security Capabilities

Anti-malware with Web Reputation:
Detect malware on servers

Firewall:
Perimeter around each server to block attacks and limit communication

Intrusion Prevention:
Intrusion detection, recommendation scan and virtual patching

Integrity Monitoring:
Detect & report unauthorized or out-of-policy changes

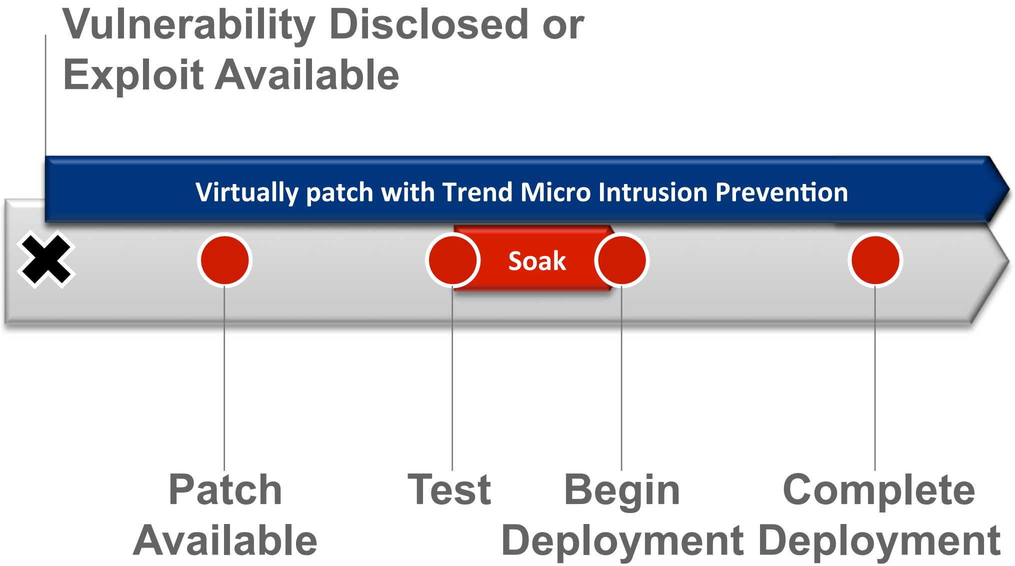
Log Inspection:
Identify security-relevant events & suspicious behavior in system logs

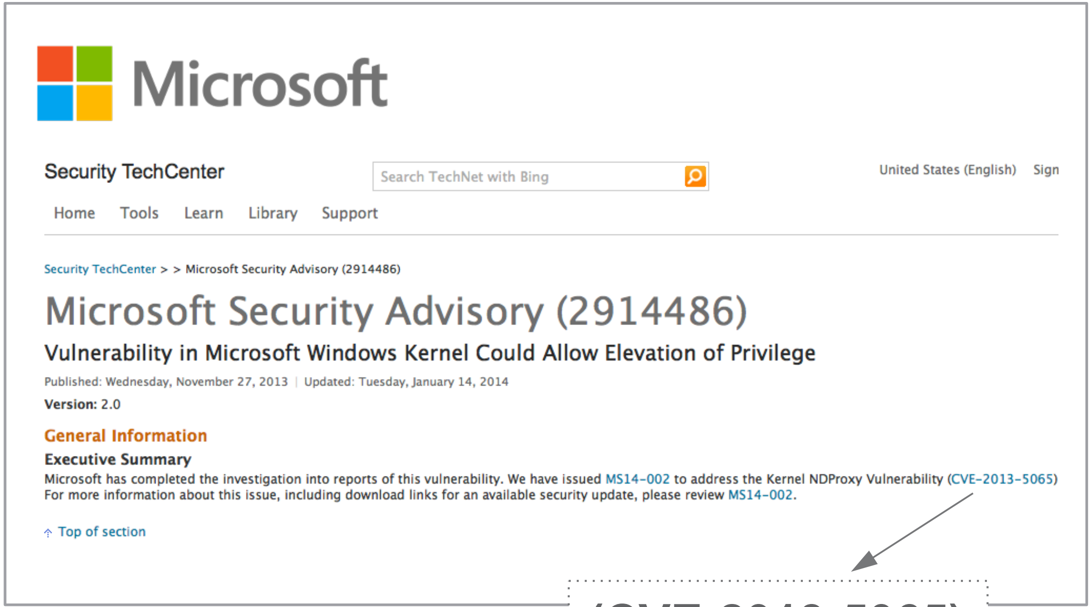
Application Scanning (DS for Web Apps):
Vulnerability detection and protection for Web apps

Data Protection (SecureCloud):
Encrypt data at rest and protect data in motion (SSL)

Protect against vulnerabilities - before you patch

- Reduce risk of exposure to vulnerability exploits – especially as you scale
- Save money avoiding costly emergency patching
- Patch at ***your convenience***


Vulnerability Disclosed or Exploit Available
Virtually patch with Trend Micro Intrusion Prevention
Soak
Patch Available
Test
Begin Deployment
Complete Deployment



Security TechCenter > > Microsoft Security Advisory (2914486)

Microsoft Security Advisory (2914486)

Vulnerability in Microsoft Windows Kernel Could Allow Elevation of Privilege

Published: Wednesday, November 27, 2013 | Updated: Tuesday, January 14, 2014

Version: 2.0

General Information

Executive Summary

Microsoft has completed the investigation into reports of this vulnerability. We have issued MS14-002 to address the Kernel NDProxy Vulnerability (CVE-2013-5065) For more information about this issue, including download links for an available security update, please review MS14-002.

↑ Top of section

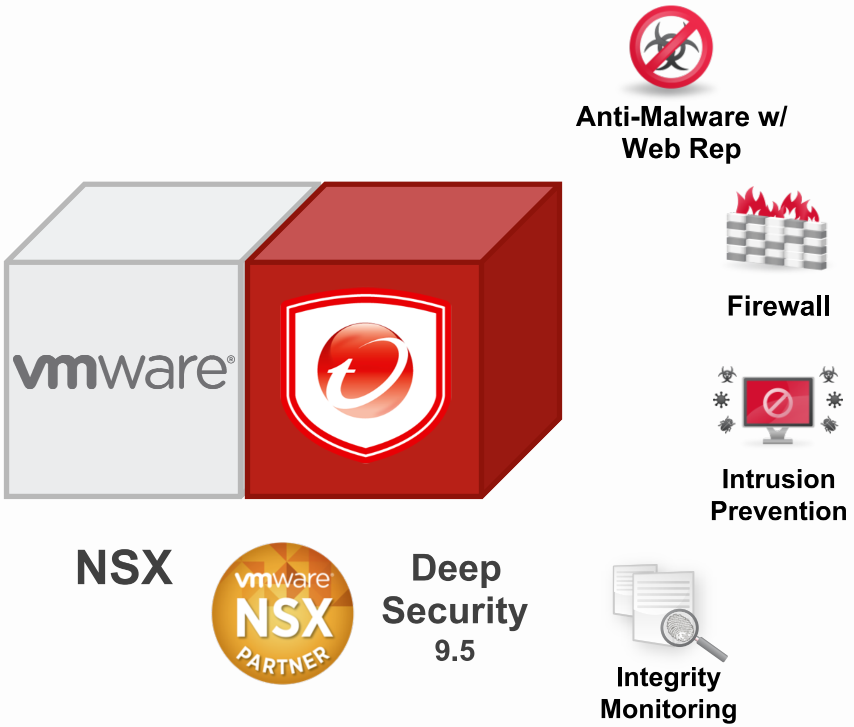
(CVE-2013-5065)

Trend Micro's Intrusion Prevention rules were released **more than a month** before this vulnerability was addressed!

What’s new in Deep Security 9.5

Enhanced Security for the Software Defined Data Center

- Extend VMware NSX's core networking and security services
  - Extend the benefits of micro-segmentation with security policies and capabilities that automatically follow VMs
  - Agentless security across network and file-based security controls for NSX
  - Automate real-time remediation and incident response during attacks



Deep Security for VMware® NSX

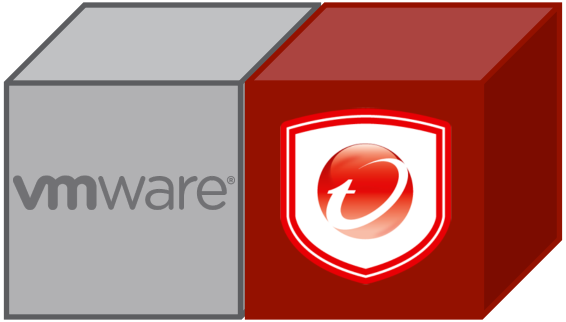
Logical
Switching

Logical
Routing

Logical
Load Balancer

Logical
VPN

Logical
Firewall



NSX

Deep
Security
9.5

Au

Deployment

Anti-Malware
with Web Reputation

No Hyp or Install

No Reboot

Firewall

Fine Grained

Control

Intrusion
Prevention

Autom Through

Tagging

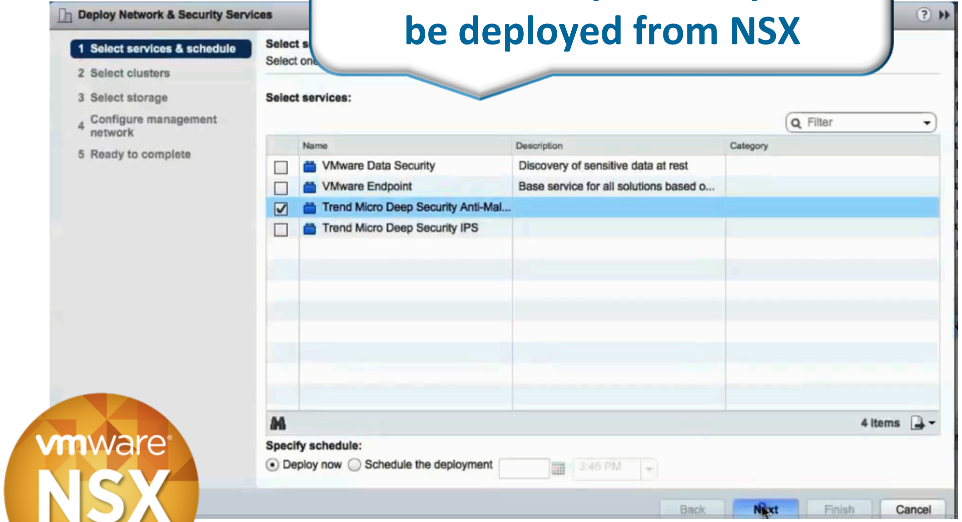
Integrity
Monitoring

Vulnerability
& Software Inventory
Scan

Leverage VMware NSX for automating security

- Automatically deploy agentless file-based & network security that works seamlessly with NSX
- No maintenance mode or re-boot required…just deploy

Security is an available service…Deep Security can be deployed from NSX



1 Select services & schedule
2 Select clusters
3 Select storage
4 Configure management network
5 Ready to complete

Select s
Select one

Select services:

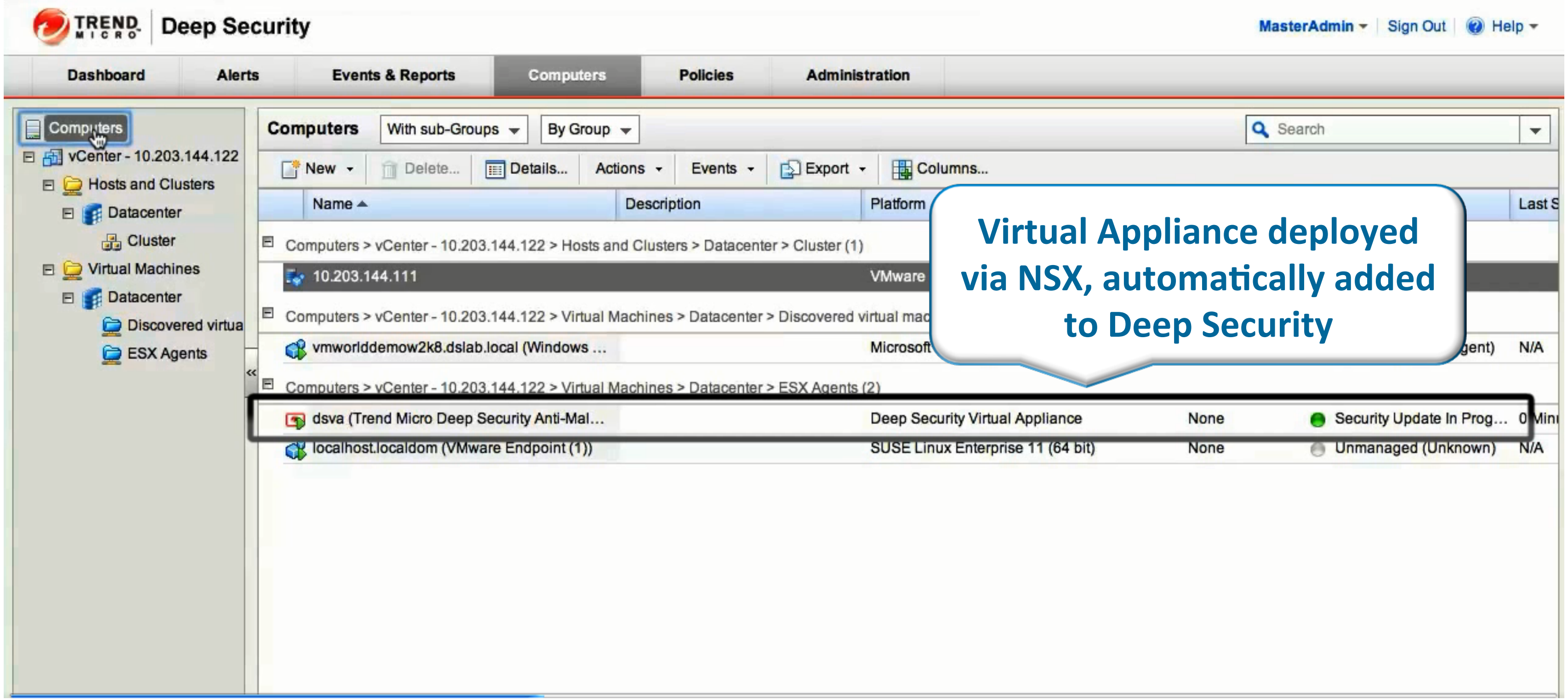
	Name	Description	Category
□	VMware Data Security	Discovery of sensitive data at rest	
□	VMware Endpoint	Base service for all solutions based o...	
☑	Trend Micro Deep Security Anti-Mal...		
□	Trend Micro Deep Security IPS		

4 items

Specify schedule:

● Deploy now ○ Schedule the deployment 3:46 PM

Virtual Appliances added automatically to DSM



Name ▲	Description	Platform			Last S
Computers > vCenter - 10.203.144.122 > Hosts and Clusters > Datacenter > Cluster (1)					
10.203.144.111		VMware			
Computers > vCenter - 10.203.144.122 > Virtual Machines > Datacenter > Discovered virtual mac					
vmworlddemow2k8.dslab.local (Windows ...		Microsoft		gent)	N/A
Computers > vCenter - 10.203.144.122 > Virtual Machines > Datacenter > ESX Agents (2)					
dsva (Trend Micro Deep Security Anti-Mal...		Deep Security Virtual Appliance	None	● Security Update In Prog...	0 Min
localhost.localdom (VMware Endpoint (1))		SUSE Linux Enterprise 11 (64 bit)	None	● Unmanaged (Unknown)	N/A

Virtual Appliance deployed via NSX, automatically added to Deep Security

NSX Summary

Benefits of NSX

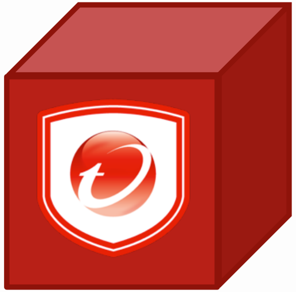
- **No Trend Micro Hypervisor component**
- **Automatic Deployment of DSVA on ESXi 5.5+**
- **No maintenance mode/reboot**
- **Automated policy management in vSphere Web Client**
- **Multi-product interoperability and automation through tagging**

NSX Alternatives:

- **Deep Security 9.5 support all modules (using vShield with VMsafe-NET) on:**
  - **ESXi 5.5**
  - **ESXi 5.1**

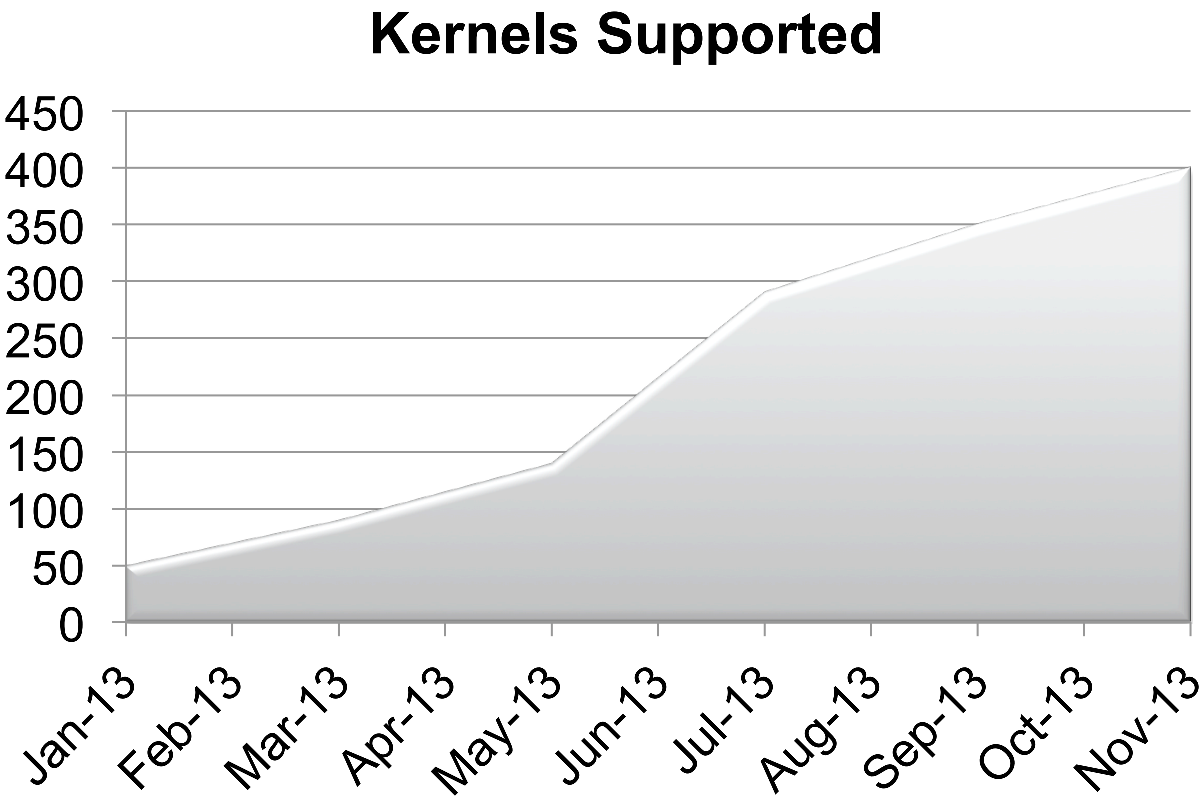
Improved Operational Efficiency

- Smart Agent: Lighter and more dynamic deployment
  - Quicker installation and ease of deployment
  - Policy-based module install and support



- Improved Linux support
  - Now supporting CloudLinux, Oracle Unbreakable and Ubuntu
  - Realtime malware scan (Redhat & SUSE)
  - On demand malware scan (all distros)

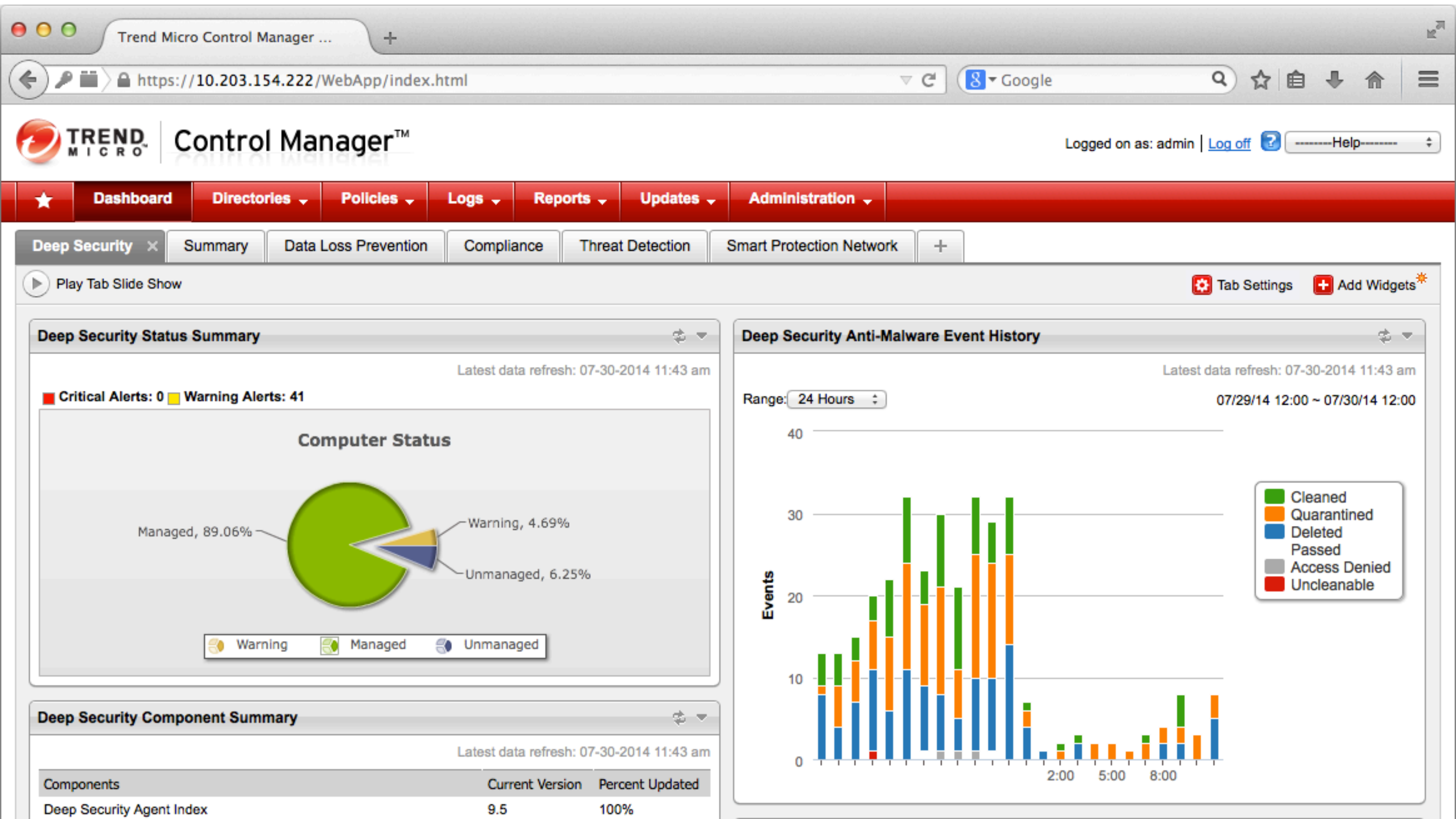
Linux



4-9 Day SLA For New Kernels
Over 500 kernels today!

Simplified Administration

- Enhanced Central Management Console
  - Visibility to multiple products from Control Manager
  - Enhanced centralized reporting through cross product views of multiple security controls
  - Expanded visibility to customize their view
    - Including both Top ”X” and Historical



Deep Security Status Summary

Latest data refresh: 07-30-2014 11:43 am

🟥 Critical Alerts: 0 🟨 Warning Alerts: 41

Deep Security Component Summary

Latest data refresh: 07-30-2014 11:43 am

Components	Current Version	Percent Updated
Deep Security Agent Index	9.5	100%

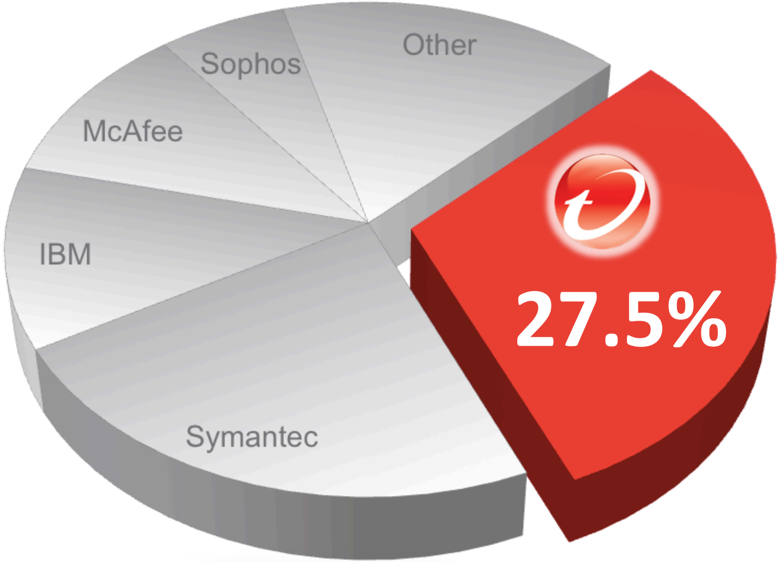
Deep Security Anti-Malware Event History

Latest data refresh: 07-30-2014 11:43 am

Range: 24 Hours

07/29/14 12:00 ~ 07/30/14 12:00

#1 Corporate Server Security Market Share[1]



CLOUD LEADER 2013

Cloud Leader 2014

experton GROUP

citrix ready

VCE

vmware PARTNER TECHNOLOGY ALLIANCE

amazon web services Partner Network ADVANCED TECHNOLOGY PARTNER

Microsoft Partner
Gold Application Development

EMC² VSPEX LABS VALIDATED

cisco PARTNER Technology Developer

Source: IDC Worldwide Endpoint Security 2014-2018 Forecast and 2013 Vendor Shares, Figure 2, doc #250210, August 2014

Thousands of customers….millions of servers protected

Reduced impact on performance

Automated security

Addressed compliance

Centralized security

Deployed multiple controls to protect data

Secured > 3,000 virtual desktops

Deployed virtual patching

Thank you!

Veli-Pekka Kusmin
✉ veli-pekka_kusmin@trendmicro.com
☎ +358 50 67181