



Securing Your Web World



PCI DSS Compliance

A Better Way with Trend Micro Enterprise Security

David Gubiani • Trend Micro Italy.

Trend Micro

A global cloud security leader that creates a world safe for businesses and consumers exchanging digital information, through content security and threat management

EVA CHEN

CEO and Co-Founder



VISION

A world safe for exchanging digital information

MISSION

Innovate to provide the best content security that fits into the IT infrastructure

Founded
United States
in 1988

Headquarters
Tokyo, Japan

Employees
4,846

Market
Content Security and
Threat Management

Locations
28 Offices Worldwide

**\$1 Billion Annual Revenue /
\$1.7 Billion Total Assets**

**#1 in Corporate Server
Security**

**Top 3 in Messaging, Web
and Endpoint Security**

**A Leader in Virtualization
and Cloud Computing
Security**

The PCI DSS Standard

Too Little?

Too Much?

Too Costly?

Verizon 2010 PCI & Data Breach Reports...

- Only 20% of audited companies were 100% compliant at time of Initial Report On Compliance
- 79% of breached companies were not PCI compliant at the time of breach
- The top breach causes are covered by PCI

Category	Threat Actions	% of Breaches
Malware	Backdoor	25%
Hacking	SQL Injection	24%
Hacking	Exploitation of backdoor or command/control channel	21%
Hacking	Exploitation of default or guessable credentials	21%
Misuse	Abuse of system access/privileges	17%
Hacking	Use of stolen login credentials	14%
Malware	RAM scraper	13%
Hacking	Exploitation of insufficient authorization	13%
Malware	Packet sniffer	13%
Malware	Keylogger / Spyware	13%



PCI DSS 2.0

Clarifications, Guidance, Evolving Requirements But still much leeway left to the QSA and Card Processor

Clarifications

- ASV Scan Requirements
- Testing Procedures
- Alignment with PA-DSS, PTS
- Terminology
- ...

Guidance

- Discovery
- Scoping
- Risk Assessment
- ...

Evolving Requirements

- Logging
- Passwords
- Vulnerability Management
- Emerging Technologies
 - Wireless
 - Tokenization
 - Encryption
 - **Virtualization**

Information Supplements on emerging technologies may have the greatest impact...

PCI Compliance

A Better Way with Trend Micro

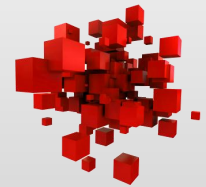
Implement Core Security Controls

- Vulnerability Management
- Patch Management
- IT Policy Compliance
- Intrusion / Incident Response
- Sensitive Data Protection
- Firewall; IDS/IPS
- Antivirus / Anti-malware
- Anti-spam / Anti-phishing
- Logging & Reporting



Solve Tough Compliance Challenges

- Server/Desktop Virtualization
- Public Cloud Computing
- Websites and Portals
- Non-Standard Systems
- Distributed Locations
- Risk Visibility & Control
- Effective Data Protection
- Worker Mobility



Trend Micro Enterprise Security...

- Reduces the cost and complexity of regulatory compliance
- Solves the toughest compliance challenges
- Maximizes the real security value of your investments

PCI Compliance with Trend Micro Focus Products

Deep Security & OfficeScan

Firewall, IPS, File Integrity, AV,
Log Inspection, Virtual Patching

Server & Endpoint Security
Physical, Virtual, Cloud

Vulnerability Mgt Services

Vulnerability Scan, Web App Scan,
PCI Scan/ASV, Policy Compliance

Network-Wide Audit
SaaS Convenience

Data Protection Solutions

Network & Endpoint DLP,
Email , Endpoint, Cloud Encryption

Complete Data Protection
From Endpoint to Cloud

Threat Management Services

Threat Detection, Remediation, Logging
Device Protection, Data Loss Reporting

Risk Visibility & Control
Device Compliance

Trend Micro Core PCI Solutions



Deep Security

Vulnerability Management Services

Data Protection Solutions

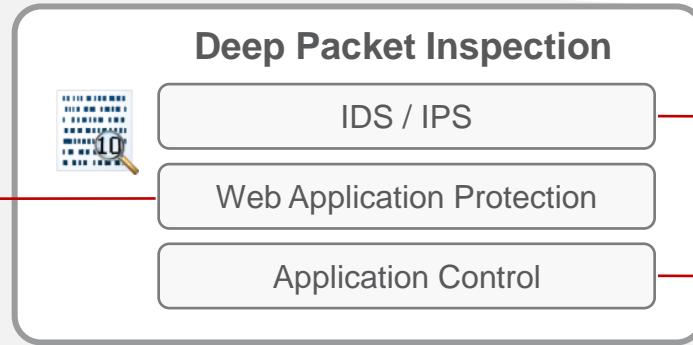
Threat Management Services

Trend Micro Deep Security

Comprehensive self-defense for servers and endpoints



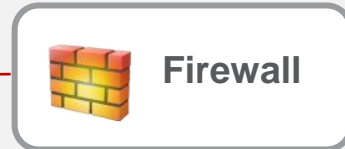
Shields web application vulnerabilities



Detects and blocks known and zero-day attacks that target vulnerabilities

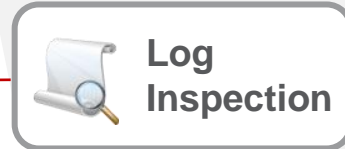
Provides increased visibility into, or control over, applications accessing the network

Reduces attack surface. Prevents DoS & detects reconnaissance scans



Detects malicious and unauthorized changes to directories, files, registry keys...

Optimizes identification of important security events across multiple log files



Detects and blocks malware (viruses & worms, Trojans)



Physical Servers



Virtual Servers



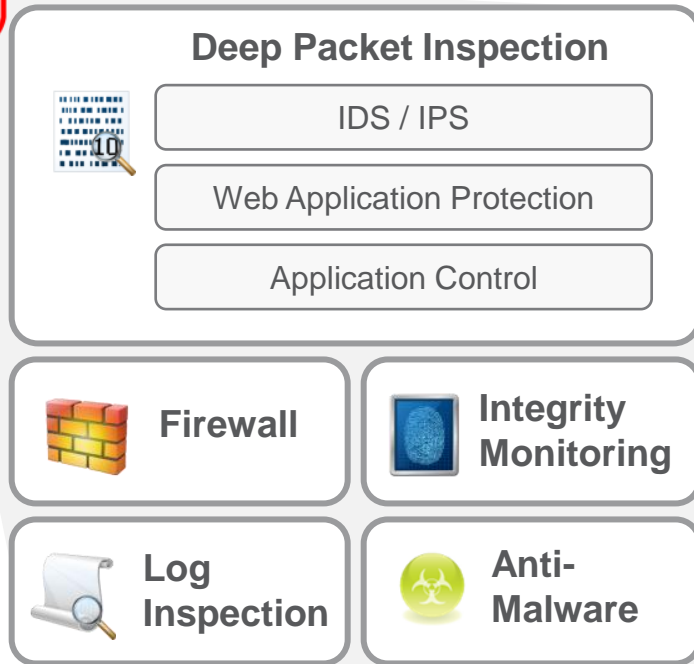
Cloud Computing



Endpoints & Devices

Protection Is Delivered Via Agent and/or Virtual Appliance

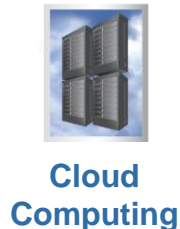
Deep Security for PCI compliance



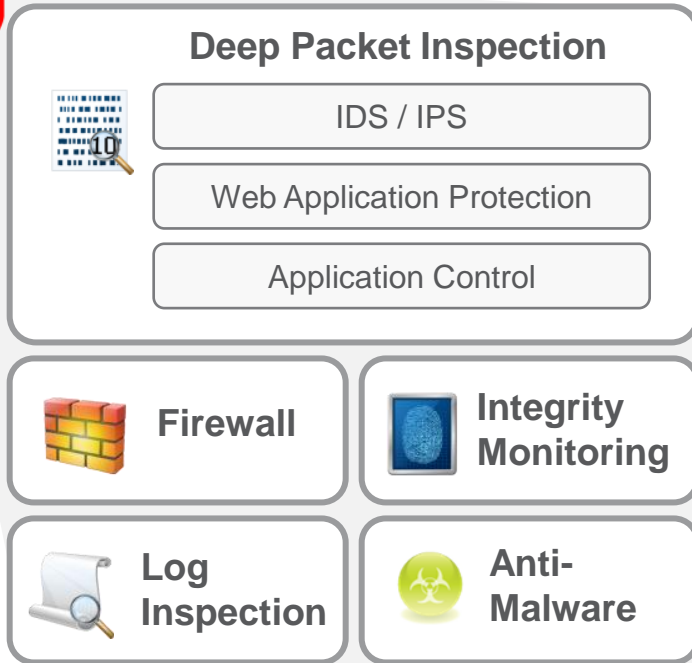
Addressing 7 PCI Regulations and 20+ Sub-Controls Including:

- (1.) Network Segmentation
- (1.x) Firewall
- (5.x) Anti-virus*
- (6.1) Virtual Patching**
- (6.6) Web App. Protection
- (10.6) Daily Log Review
- (11.4) IDS / IPS
- (11.5) File Integrity Monitoring

* Available for VMware only until Q2 2011
 ** Compensating Control

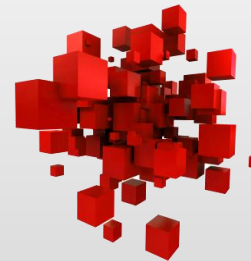


Deep Security for PCI compliance



PCI Compliance Challenges

- Server/Desktop Virtualization
- Cloud Computing
- Public Websites
- Timely System Patching
- Remote/Distributed Locations
- Risk Visibility & Control



Physical Servers



Virtual Servers



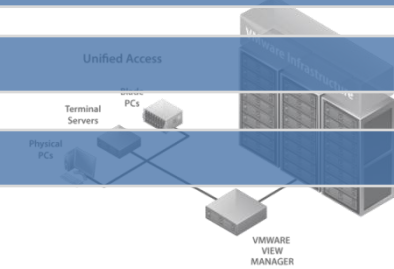
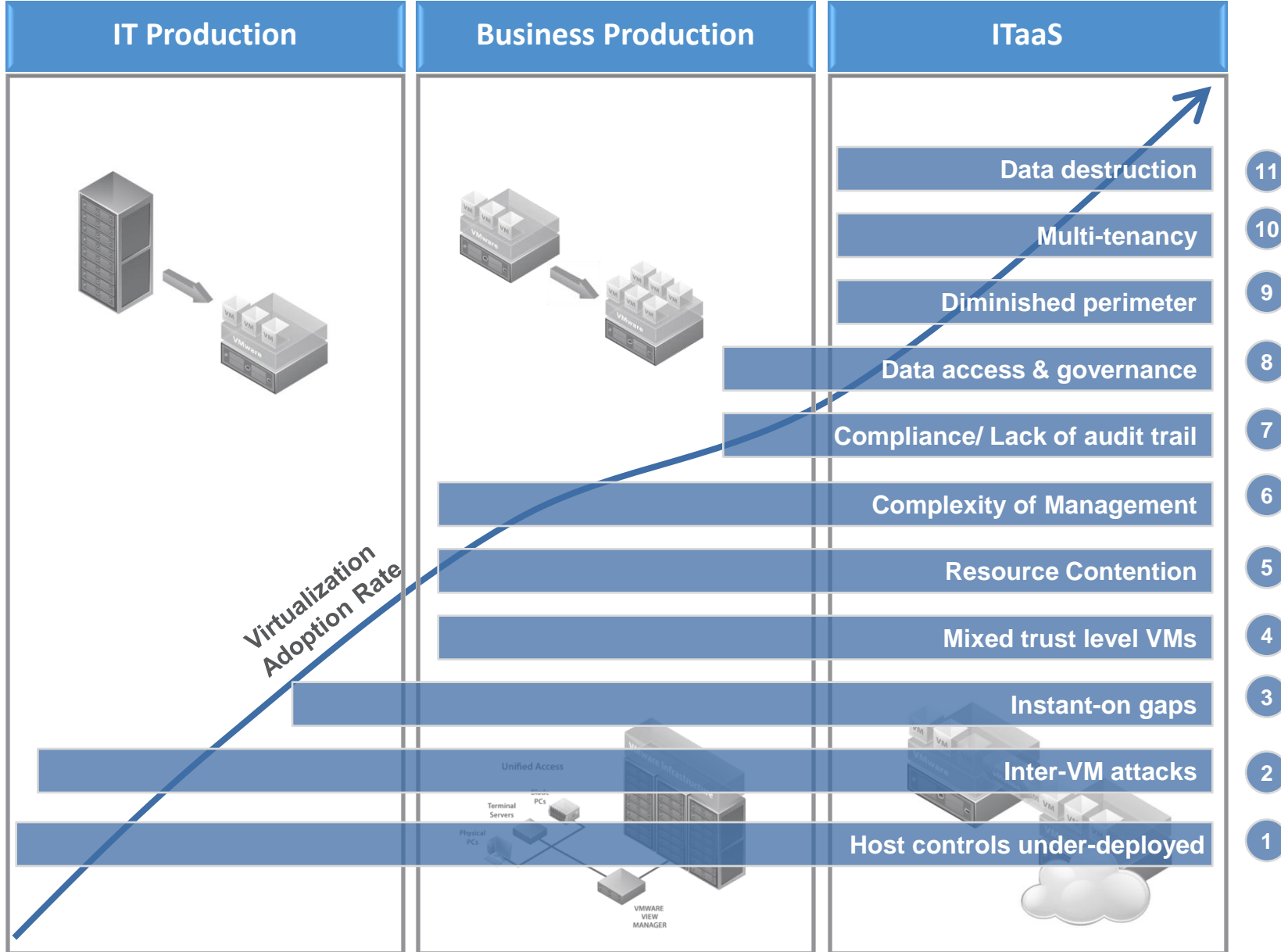
Cloud Computing



Endpoints & Devices

Security Challenges Along the Virtualization Journey

VMware and Trend Micro help customers address these issues, and accelerate the journey



Virtualization and PCI Guidance

Anticipated guidance to be published in early 2011

- Lack of physical isolation (Req. 1)
 - Hypervisor represents new attack surface
 - Logical vs. Physical Segmentation
- Hypervisor vulnerabilities (Req. 6)
- Multiple “primary functions” per host (Req. 2.2.1)
- Enforcement of Least Privilege (Req.7)
- Configurations are more complex (Reqs. 2 & 6)
 - More variables to consider
 - More layers of compliance to manage
- Virtual machine state and migration (Req. 10)
- Immaturity of monitoring solutions (Reqs. 10 & 11)

Deep Security - 3 ways to protect VMs

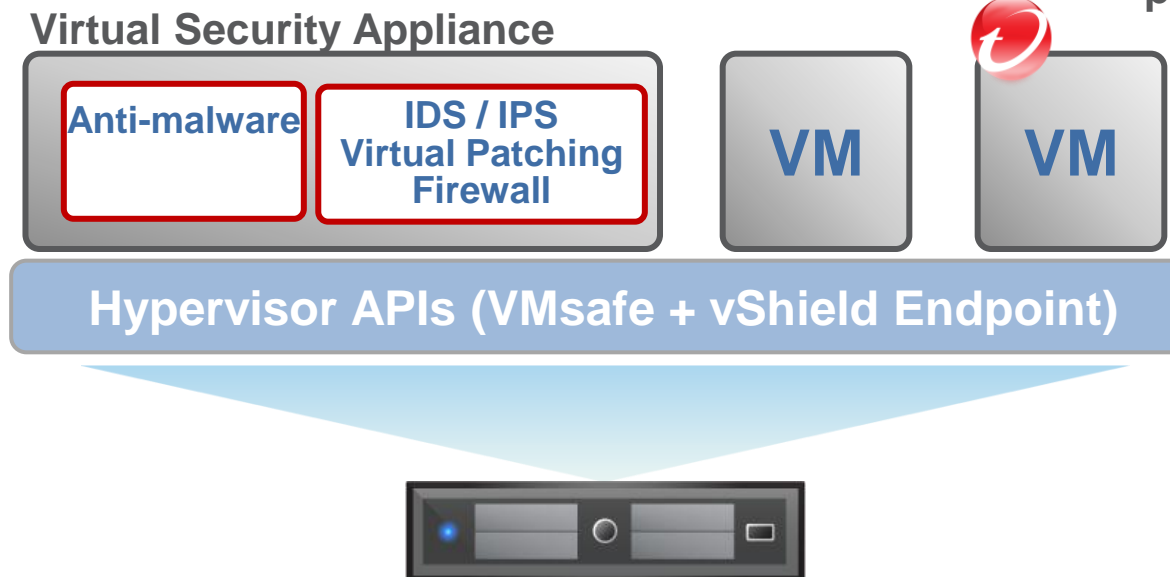
Agent-less

- 1**
- **Agent-less AV**
 - **Eliminates resource contention**

- 2**
- **IDS/IPS**
 - **Virtual Patching**
 - **Web App Protection**
 - **Firewall**
 - **VMsafe-based Virtual Appliance**

Agent-based

- 3**
- **Integrity Monitoring**
 - **Log Inspection**
 - **IDS/IPS**
 - **Virtual Patching**
 - **Web App Protection**
 - **Firewall**
 - **1 universal agent for protection modules**



Vulnerabilities: Risk & Compliance Impacts

Enterprise Applications

2,723 Critical “Software Flaw” Vulnerabilities in 2009



ORACLE®



How often / easily do you patch these vulnerabilities?

Unsupported OSs & Apps



2009/
2010



ORACLE®
10.1



Next?

Untouchable Applications



Medical
ATM, POS
Other

Reason for not patching:

Cost of refresh

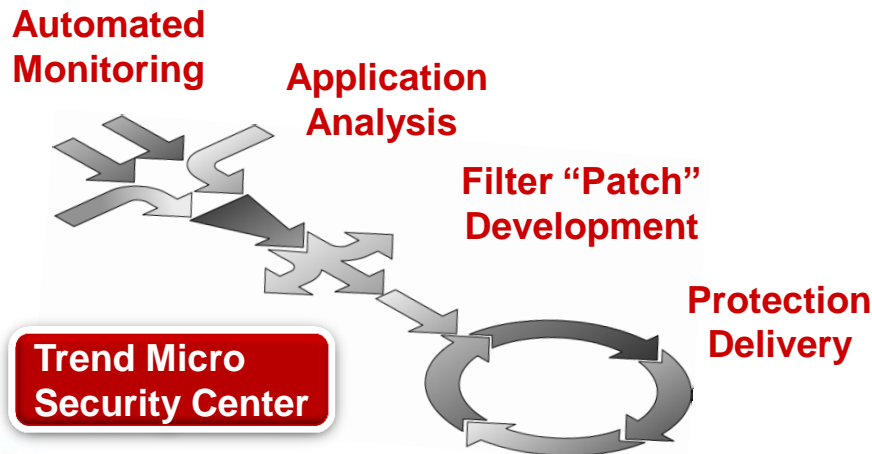
Compliance restrictions

Service Level Agreements

The Virtual Patching Solution

Trend Micro Security Center provides Virtual Patches within hours of vulnerability disclosure

- Automated centralized distribution
- Protection available:
 - Deep Security product module
 - With OfficeScan IDF plugin



Risk Mgt & Compliance

- Close window of vulnerability for critical systems and applications
- Protect "unpatchable" systems
- Meet 30-day PCI patch requirement

Operational Impact

- Reduce patch cycle frequency
- Avoid ad-hoc patching
- Minimize system downtime



Physical / Virtual / Cloud Servers



Endpoints & Devices

Security & compliance challenges for distributed environments

- Flat, mixed-use networks create scope challenges
- Point Of Sale device compliance
- No local IT staff, limited central staffing
- Lack of visibility into suspicious remote activity
- Security log/event data overload
- Multiplied costs of appliances & standalone products



Meeting PCI requirements across 100's – 1000's of locations requires a laser focus on controlling cost and complexity

Addressing Distributed Environment Challenges



Firewall

Full function centrally managed network and application firewall

Reduces PCI scope without the cost and complexity of network firewalls



Deep Packet Inspection

Provides IDS / IPS, Web App Protection, Application Control

In-depth system self-defense

Protects “un-patchable” systems and applications



Integrity Monitoring

Full System Monitoring in real-time; Scheduled & on-demand scanning

Detects remote malicious activities

Provides audit trail of system changes



Log Inspection

Collects & analyzes OS and application logs for security events

Automates event collection & analysis

Prioritized alerting focuses management and minimizes overhead



Anti-Malware

Malware protection for virtual servers

Optimized virtualization performance

Trend Micro Core PCI Solutions



Deep Security

Vulnerability Management Services

Data Protection Solutions

Threat Management Services

Vulnerability Management Services



Trend Micro
**Vulnerability
Management**



Trend Micro
**Policy
Compliance**



Trend Micro
**Web Application
Scanning**



Trend Micro
PCI Compliance



Trend Micro
**PCI Scanning
Service**

Available as a suite
or individual services

Available as a
standalone service

Addressing PCI Regulations and Compliance Procedures:

- (2.2) Configuration Standards
- (6.2) Vulnerability Identification
- (6.6) Web App. Protection
- (11.2) Vulnerability Scanning
- ASV Scanning Services
- SAQ Filing



Copyright 2010 Trend Micro Inc.



Vulnerability Management Services



Trend Micro
**Vulnerability
Management**



Trend Micro
**Policy
Compliance**



Trend Micro
**Web Application
Scanning**



Trend Micro
PCI Compliance



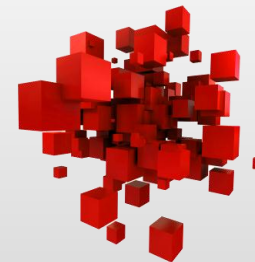
Trend Micro
**PCI Scanning
Service**

Available as a suite
or individual services

Available as a
standalone service

PCI Compliance Challenges

- Risk Visibility & Control
- Public Website Protection
- Timely System Patching



Trend Micro Core PCI Solutions



Deep Security

Vulnerability Management Services

Data Protection Solutions

Threat Management Services

Effective Data Protection Challenges

- Full-disk encryption benefits are limited and insufficient
- PKI-based encryption schemes are notoriously complex and burdensome to administer and use
- DLP should be a key component but varying needs can't be met by a “one-size-fits-all” approach
- Cloud data protection and key management is complex and subject to compromise

How can you incorporate an efficient and effective data protection into your compliance and overall risk management programs?

Effective Data Protection

Trend Micro Enterprise Security



Full-Suite Enterprise DLP

- Endpoint & Network Deployment
- Pre-Built Compliance Templates
- Sophisticated Fingerprinting for IP



Integrated *DLP-Lite*

- Messaging Gateway
- Comm. & Collaboration Products
- Threat Management Services



Email Encryption

- Identity-Based Universal Reach
- Cloud-Based Key Management
- User and Policy-Based Options



Endpoint Encryption

- Full-Disk Encryption
- File/Folder & Removable Media Encryption

Trend Micro data protection solutions emphasize flexibility, ease of management and usability

Trend Micro Endpoint Encryption Modules

PolicyServer

- Central Management Server and Console for Policy Management, Authentication, Reporting, and Auditing across the Mobile Armor Suite.

FileArmor

- File, Folder & Removable Media Encryption (USB & CD/DVD)

DataArmor

- Full Disk Encryption for Laptops, Desktops, Tablet PCs, PDAs, and Smartphones

DriveArmor

- A centrally managed trusted hard drive featuring full disk encryption and central management

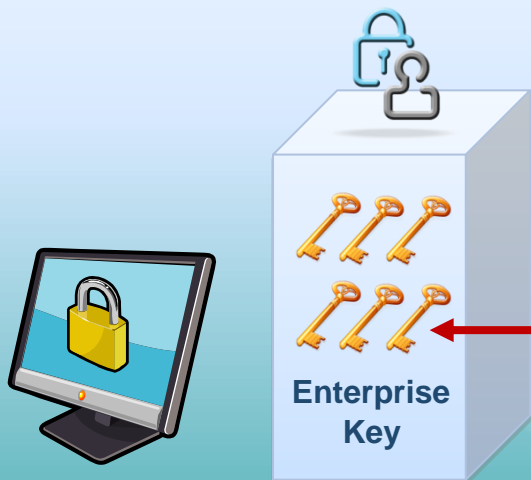
KeyArmor

- Fully Encrypted & Hardened USB Flash Drive with embedded anti-malware/virus

SecureCloud: Data Governance and Protection

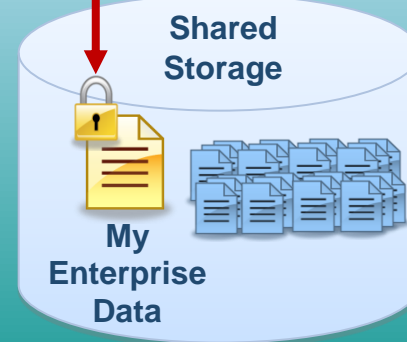
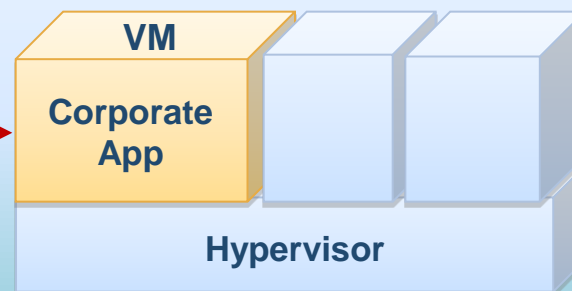
Patent pending Trend Micro technology enables enterprises to encrypt, secure and control data in the cloud

Enterprise Datacenter Or SaaS Offering



Trend Micro
SecureCloud
Console

Enterprise Cloud Deployment



Trend Micro Core PCI Solutions



Deep Security

Vulnerability Management Services

Data Protection Solutions

Threat Management Services

PCI Compliance with Threat Mgt Services

- AV compensating control for any networked system/device
 - Legacy , non-standard, hard/impossible to directly secure
 - POS, medical devices, manufacturing systems, SCADA systems, servers & endpoints
- TMS helps support compliance controls:
 - Passive Scanning
 - Controls against malicious code
 - Vulnerability Protection Program
 - Monitor and Test Networks
- Compliance Reporting Module
 - Examines network traffic and reports exit of possible protected information
 - Preloaded DLP compliance templates for PCI-DSS, SB-1386, HIPAA, GLBA, US PII



Compliance – A Better Way

Master Core Compliance Controls

- Deploy converged cross-regulation solutions

Solve Key Compliance Challenges

- Support evolving business & IT initiatives

Achieve Compliance Without Compromise

- Best-in-class security that provides maximum protection



**Trend Micro
Enterprise Security**

Thank You

END