Trend Micro
The Evolution of the Cloud and Securing Your Data

How to survive in a world of Virtualization and Cloud Computing, where you even can't trust your own environment anymore.

Raimund Genes, CTO

JOIN THE JOURNEY

TEN. TECH EXEC NETWORKS

Data everywhere – but protection?

Unprotected Data Needing Protection

Exabytes

18,000											
16,000											
14,000											
12,000											
10,000											
8,000											
6,000											
4,000											
2,000											
0											
	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020

■ Data Needing Protection
Data Actually Protected

Unprotected in 2020= Size of Entire Digital Universe in 2018

Source: IDC Digital Universe Study, sponsored by EMC, May 2010
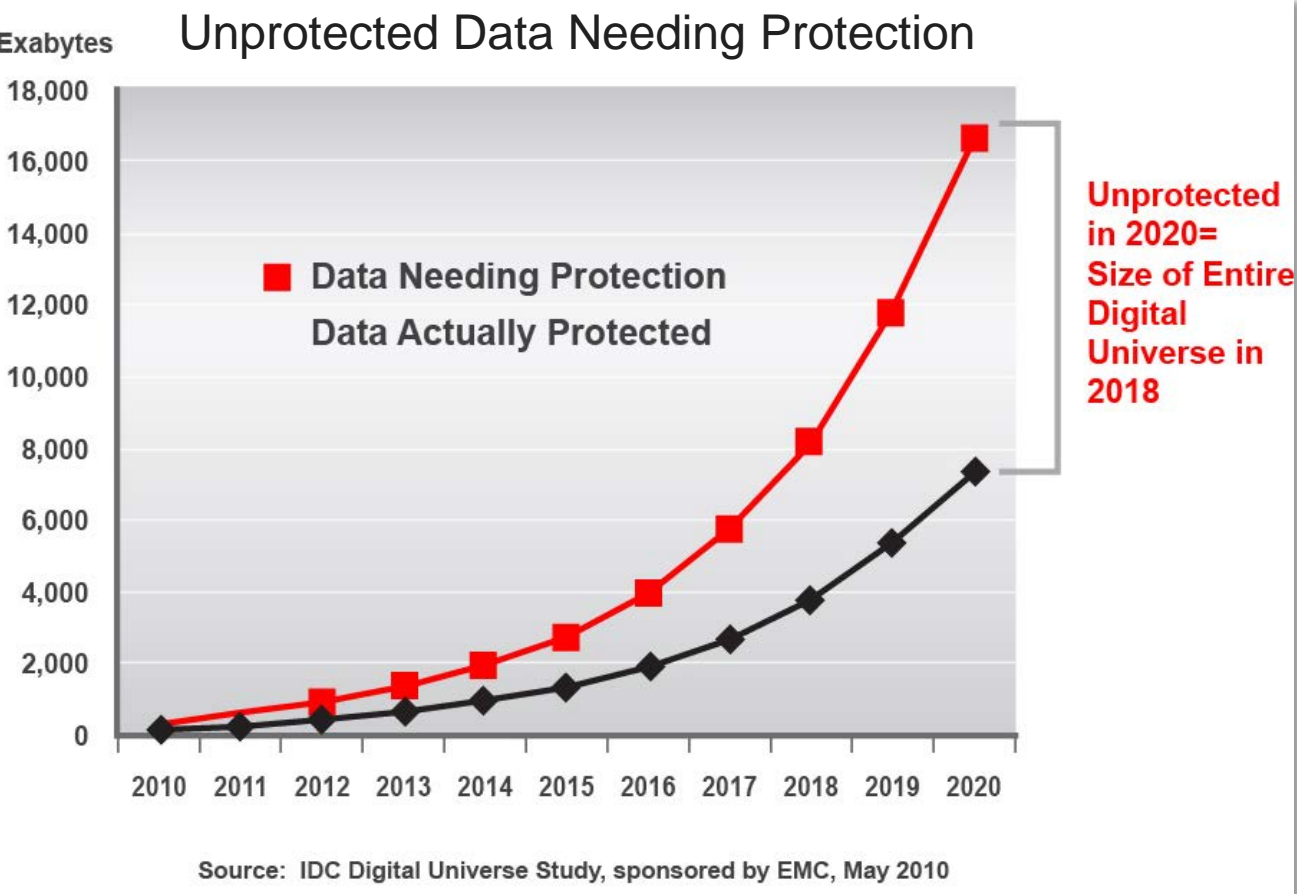
Amount of data needing protection will grow by a factor of 90 by 2020

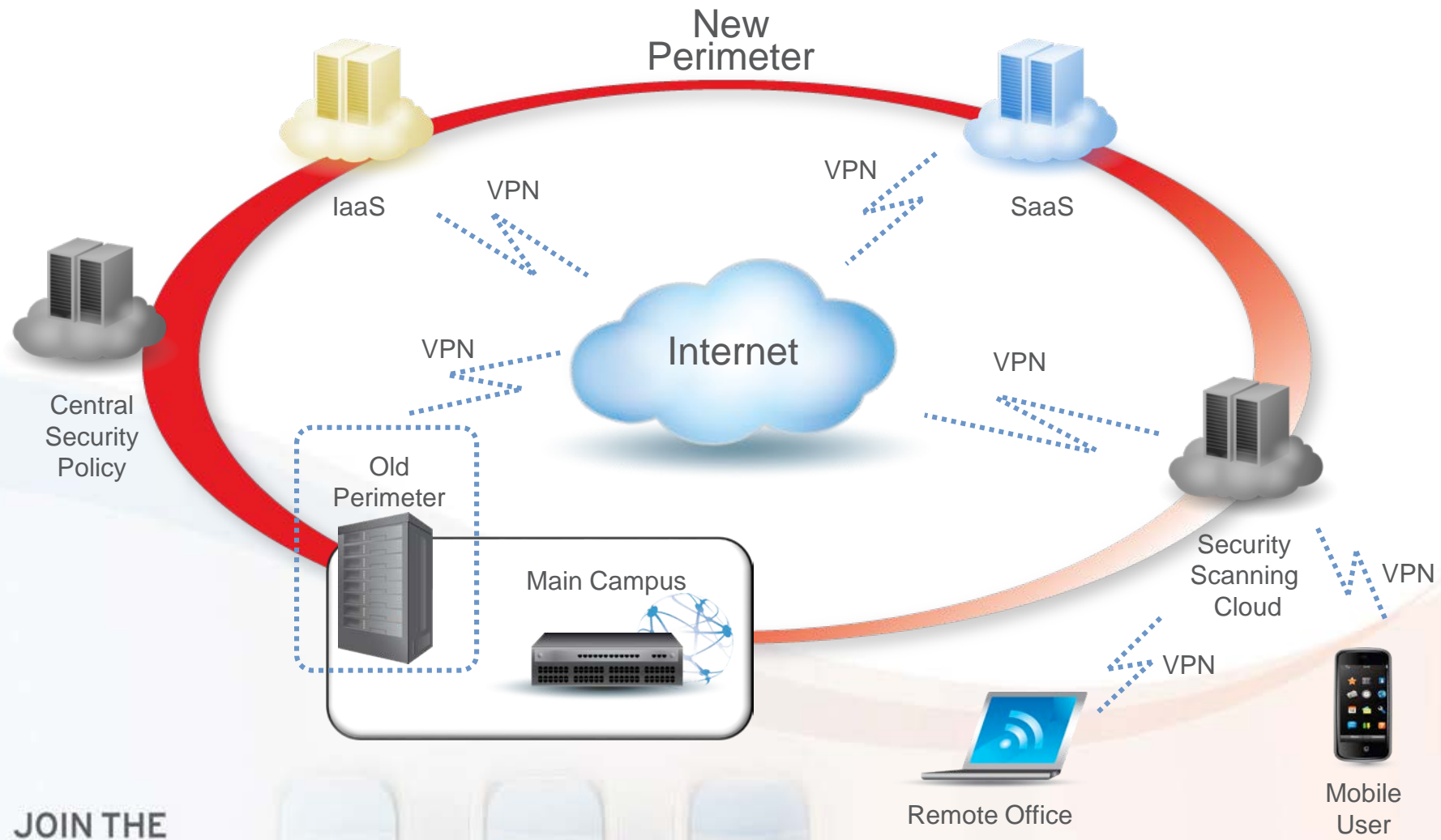*-IDC*

JOIN THE JOURNEY

Because the Network Perimeter is Expanding

You Need an Elastic Network Security Architecture

New Perimeter

IaaS

SaaS

VPN

VPN

Internet

Central Security Policy

VPN

VPN

Old Perimeter

Main Campus

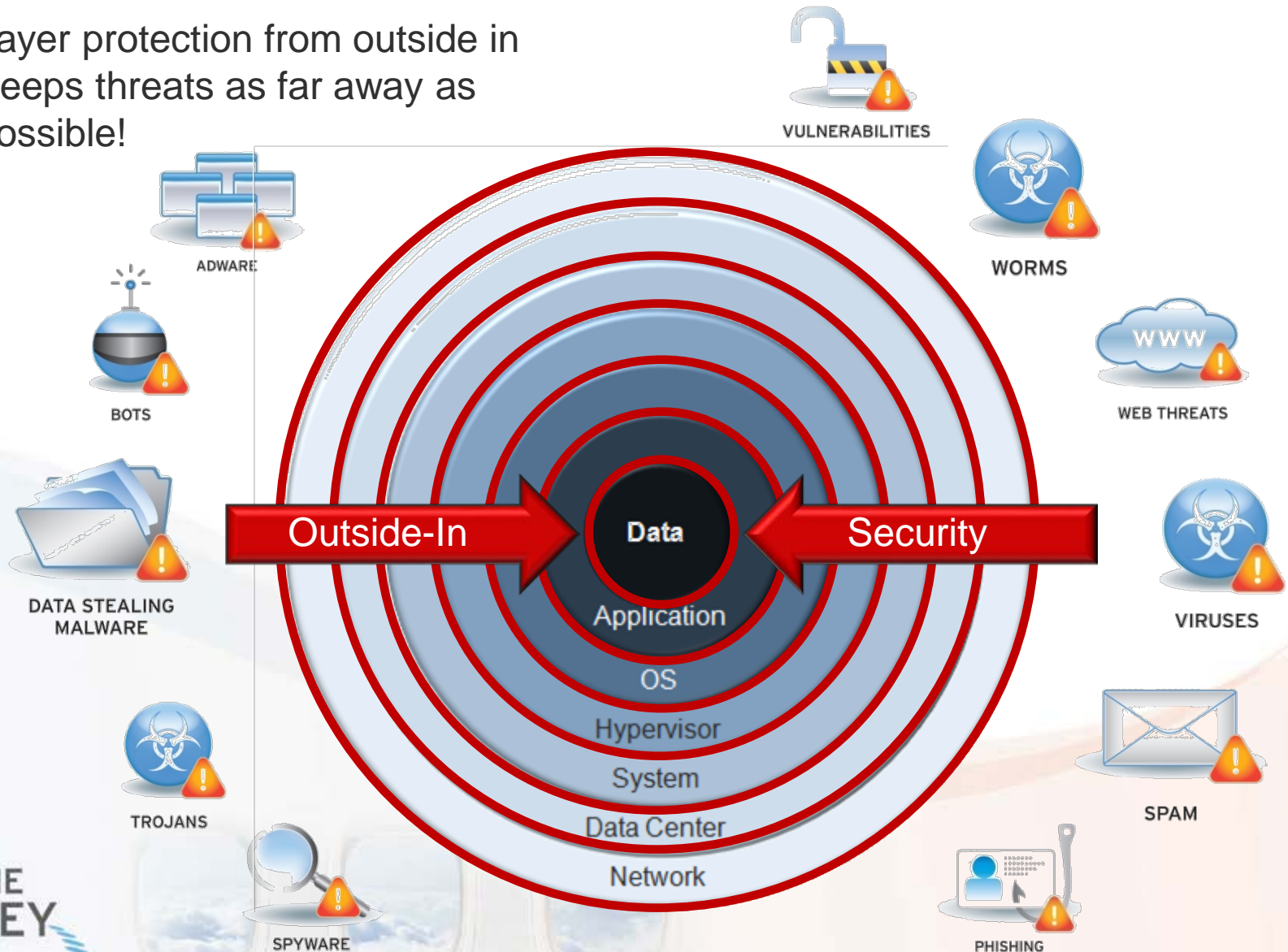Security Scanning Cloud

VPN

VPN

Remote Office

Mobile User

JOIN THE JOURNEY

Integrated Security Across Platforms
Outside-in Model of Perimeter Defense

Layer protection from outside in
Keeps threats as far away as
possible!

Integrated Security Across Platforms
Inside-out Security

Endpoints   Datacenters

Devices   Cloud

Branch office Server   Virtual

Inside-Out   **Data**   Security

Application
OS
Hypervisor
System
Data Center
Network

Desktop   Physical
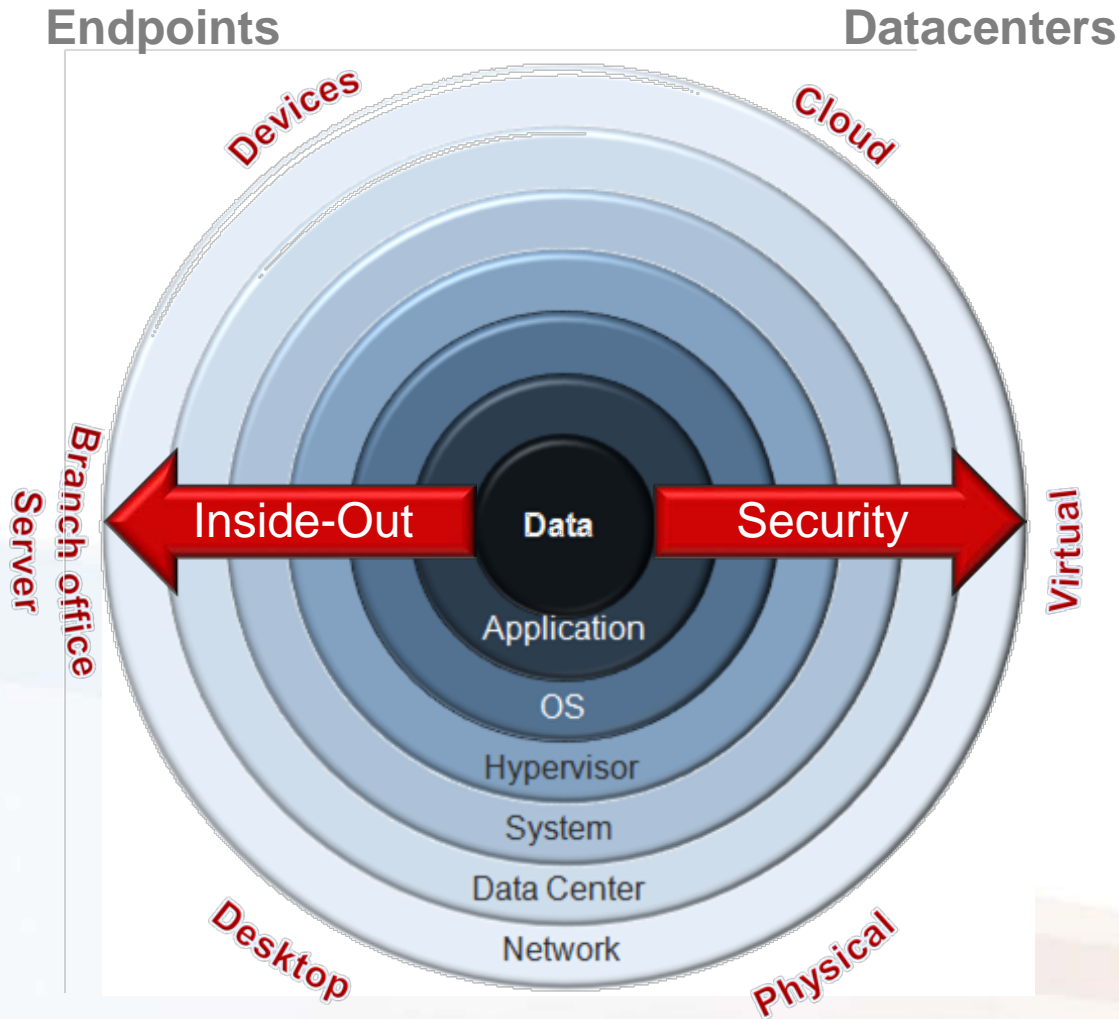
- Self-Secured Workload
- Local Threat Intelligence
  - When-Timeline Aware
  - Who-Identity Aware
  - Where-Location Aware
  - What-Content Aware
- User-defined Access Policies
- Encryption

All network-connected data must be able to defend itself from attacks

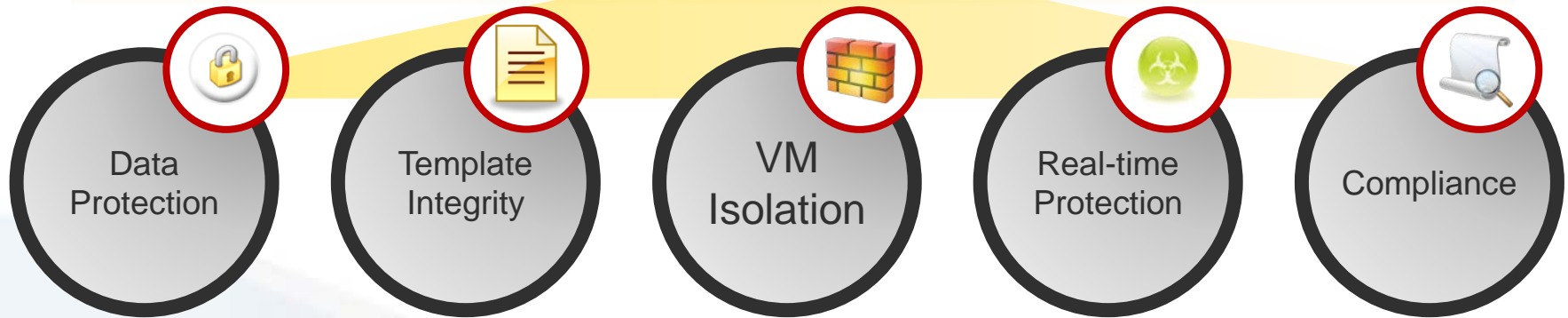JOIN THE JOURNEY

What is the Solution?
Security that Travels with the VM

Cloud Security – Modular Protection

Data Protection

Template Integrity

VM Isolation
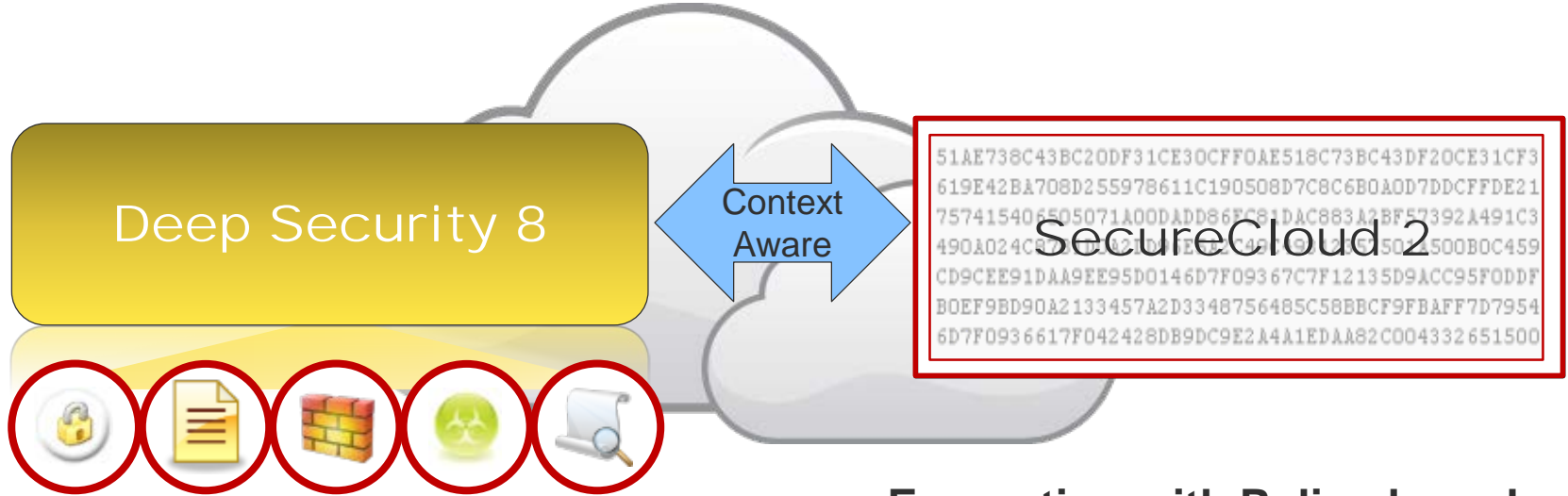
Real-time Protection

Compliance

Self-Defending VM Security in the Cloud

- Agent on VM - can travel between cloud solutions
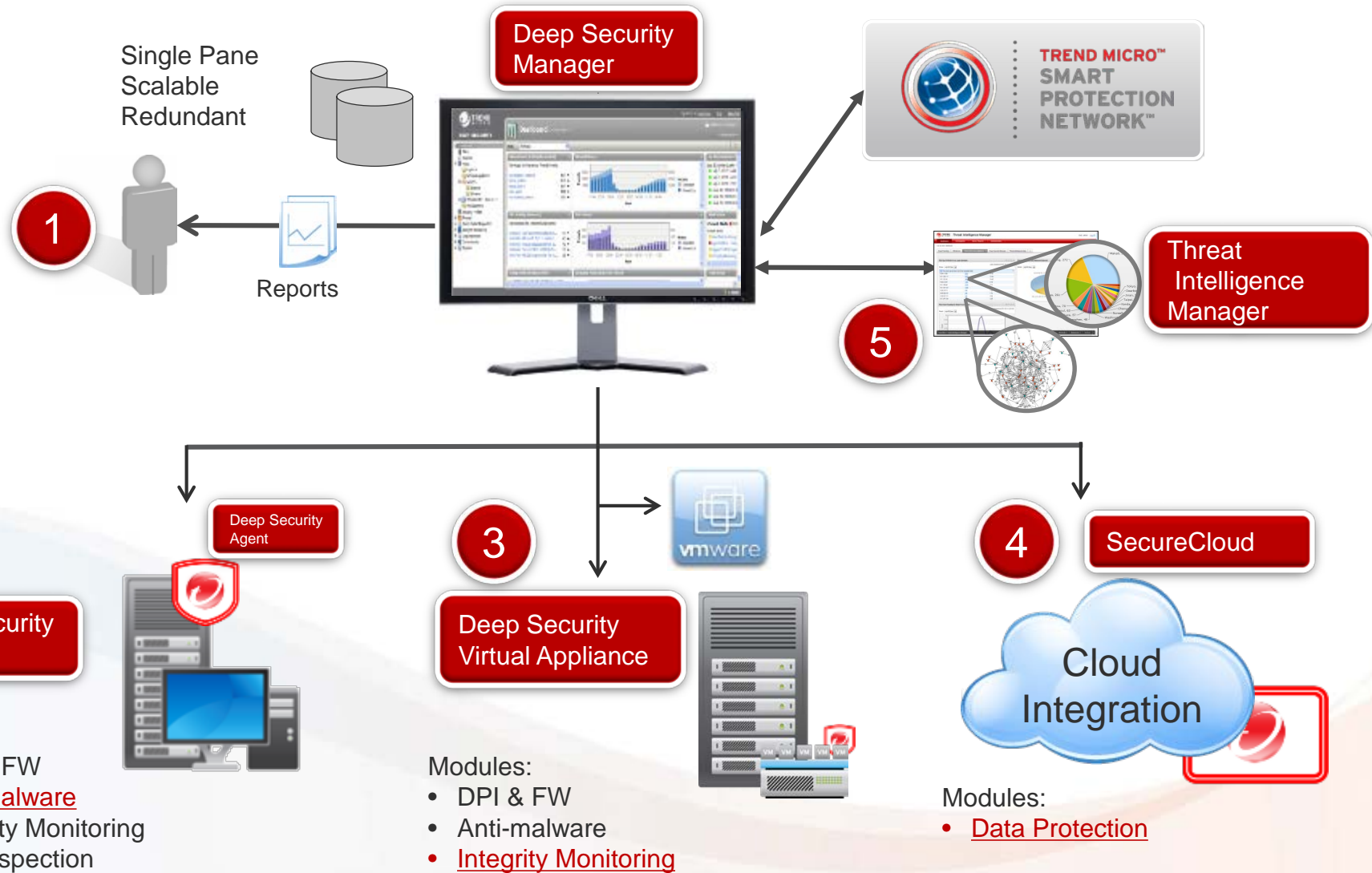- One management portal for all modules
- SaaS security deployment option

amazon web services™   vmware®

Total Cloud Protection

System, application and data security in the cloud

Deep Security 8

Context Aware

SecureCloud 2

51AE738C43BC20DF31CE30CFF0AE518C73BC43DF20CE31CF3
619E42BA708D255978611C190508D7C8C6B0A0D7DDCFFDE21
757415406505071A00DADD86FC81DAC883A2BF57392A491C3
490A024C5... ...5... ...500B0C459
CD9CEE91DAA9EE95D0146D7F09367C7F12135D9ACC95F0DDF
B0EF9BD90A2133457A2D3348756485C58BBCF9FBAFF7D7954
6D7F0936617F042428DB9DC9E2A4A1EDAA82C004332651500

Modular protection for servers and applications

- Self-Defending VM Security in the Cloud

- Agent on VM allows travel between cloud solutions

- One management portal for all modules

Encryption with Policy-based Key Management

- Data is unreadable to unauthorized users

- Policy-based key management controls and automates key delivery

- Server validation authenticates servers requesting keys

JOIN THE
JOURNEY

Deep Security Architecture

Single Pane
Scalable
Redundant

Deep Security Manager

TREND MICRO™
SMART PROTECTION NETWORK™

1

Reports

5

Threat Intelligence Manager

2

Deep Security Agent

Deep Security Agent

Modules:
- DPI & FW
- Anti-malware
- Integrity Monitoring
- Log Inspection

3

Deep Security Virtual Appliance

vmware

Modules:
- DPI & FW
- Anti-malware
- Integrity Monitoring

4

SecureCloud

Cloud Integration

Modules:
- Data Protection

JOIN THE JOURNEY

APT in comparison

	APT	The old stuff
Infiltration	• Combination of multiple attack methologies • Long Preparation time. • Social engineering on a few selected victims	• One or 2 attack methods • Not selective • Tries to infect many users
Infection/Attack	• Silent and hidden • Low and slow approach • Targeted	• Noisy and aggressive • Infects multiple users • Higher visibility
Data Leakage/Exfiltration	• Happens slow and over several weeks • Only accesses certain data • Coordinated human involvement – they know what they are looking for	• Generic information stealer – credit card info or login credentials • Mindless and automated piece of code, not aware of the environment

Microsoft: Remote Desktop Protocol Vulnerability Should be Patched Immediately

By Brian Prince on March 13, 2012

Microsoft is urging organizations to apply the sole critical update in this month's Patch Tuesday release as soon as possible.

The critical bulletin – one of six security **bulletins** issued as part of today's release – addresses two vulnerabilities in the Remote Desktop Protocol (RDP).
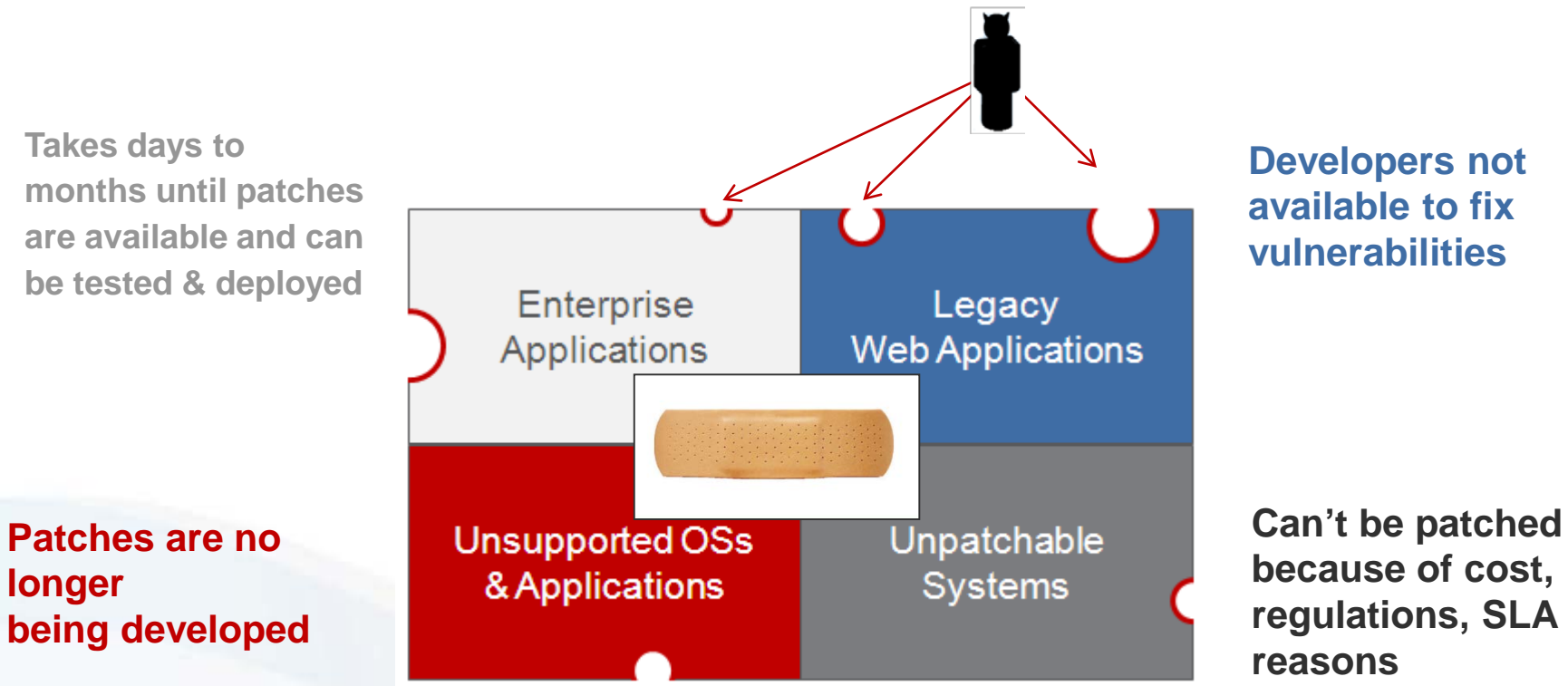
"A little about MS12-020...this bulletin addresses one Critical-class issue and one Moderate-class issue in Remote Desktop Protocol (RDP)," **Angela Gunn**, security response communications manager for Microsoft's Trustworthy Computing Group, explained in a blog post. "Both issues were cooperatively disclosed to Microsoft and we know of no active exploitation in the wild. The Critical-class issue applies to a fairly specific subset of systems – those running RDP – and is less problematic for those systems with Network Level Authentication (NLA) enabled."

Microsoft®

"That said, we strongly recommend that customers examine and prepare to apply this bulletin as soon as possible," she added. "The Critical-class issue could allow a would-be attacker to achieve remote code execution on a machine running RDP (a non-default configuration); if the machine does not have NLA enabled, the attacker would not require authentication for RCE access."

JOIN THE
JOURNEY

Vulnerability Shielding solves the Patching Nightmare

Takes days to months until patches are available and can be tested & deployed

Developers not available to fix vulnerabilities

Enterprise Applications

Legacy Web Applications

Patches are no longer being developed

Unsupported OSs & Applications

Unpatchable Systems

Can't be patched because of cost, regulations, SLA reasons

- Enterprises spend a third of their time on patching
- But ¾ of enterprises say their patching is not effective

Source: InformationWeek, Analytics Report: 2010 Strategy Security Survey

JOIN THE JOURNEY

Deep Security 8 Integrity Monitoring
Agentless Integrity Monitoring

The Old Way
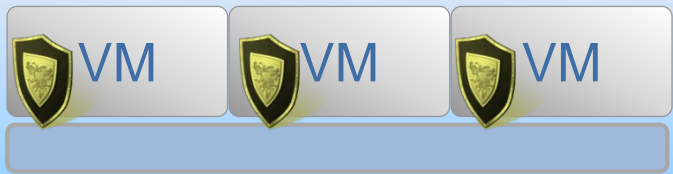
With Agent-less Integrity Monitoring

VM VM VM

Security Virtual Appliance VM VM VM VM
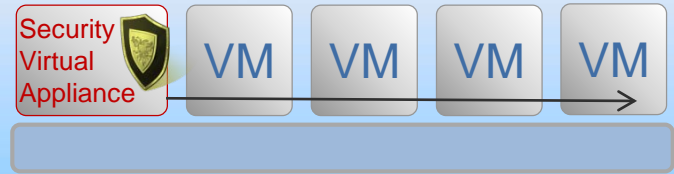
| Zero Added Footprint | Faster Performance | Better Manageability | Stronger Security |

JOIN THE JOURNEY

So now we could trust our own systems – but what about systems outside our control?
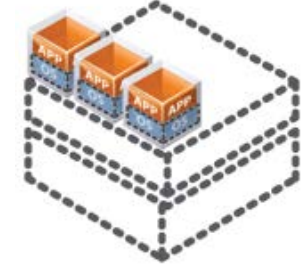
Who Has Control?

Servers

Virtualization &
Private Cloud
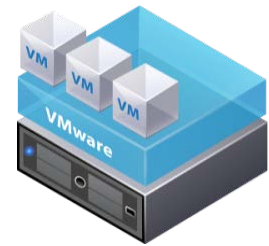
Public Cloud
IaaS
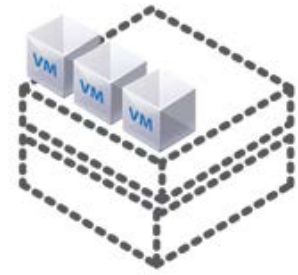
Public Cloud
PaaS
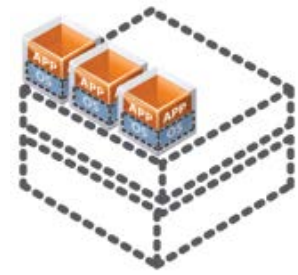
Public Cloud
SaaS

End-User (Enterprise)

Service Provider

Amazon Web Services™ Customer Agreement

4.2 Other Security and Backup. <u>You are responsible</u> for properly configuring and using the Service Offerings and <u>taking your own steps to maintain appropriate security</u>, protection and backup of Your Content, which may include the use of encryption technology to protect Your Content from unauthorized access and routine archiving Your Content.
http://aws.amazon.com/agreement/#4 (30 March 2011)

The cloud customer has responsibility for security and needs to plan for protection.

What is there to worry about?

Use of encryption is rare:
• Who can see your information?

Virtual volumes and servers are mobile:
• Your data is mobile — has it moved?

Rogue servers might access data:
• Who is attaching to your volumes?

Rich audit and alerting modules lacking:
• What happened when you weren't looking?

Encryption keys remain with vendor:
• Are you locked into a single security solution? Who has access to your keys?

Virtual volumes contain residual data:
• Are your storage devices recycled securely?

Name: John Doe
SSN: 425-79-0053
Visa #: 4456-8732…

Name: John Doe
SSN: 425-79-0053
Visa #: 4456-8732…
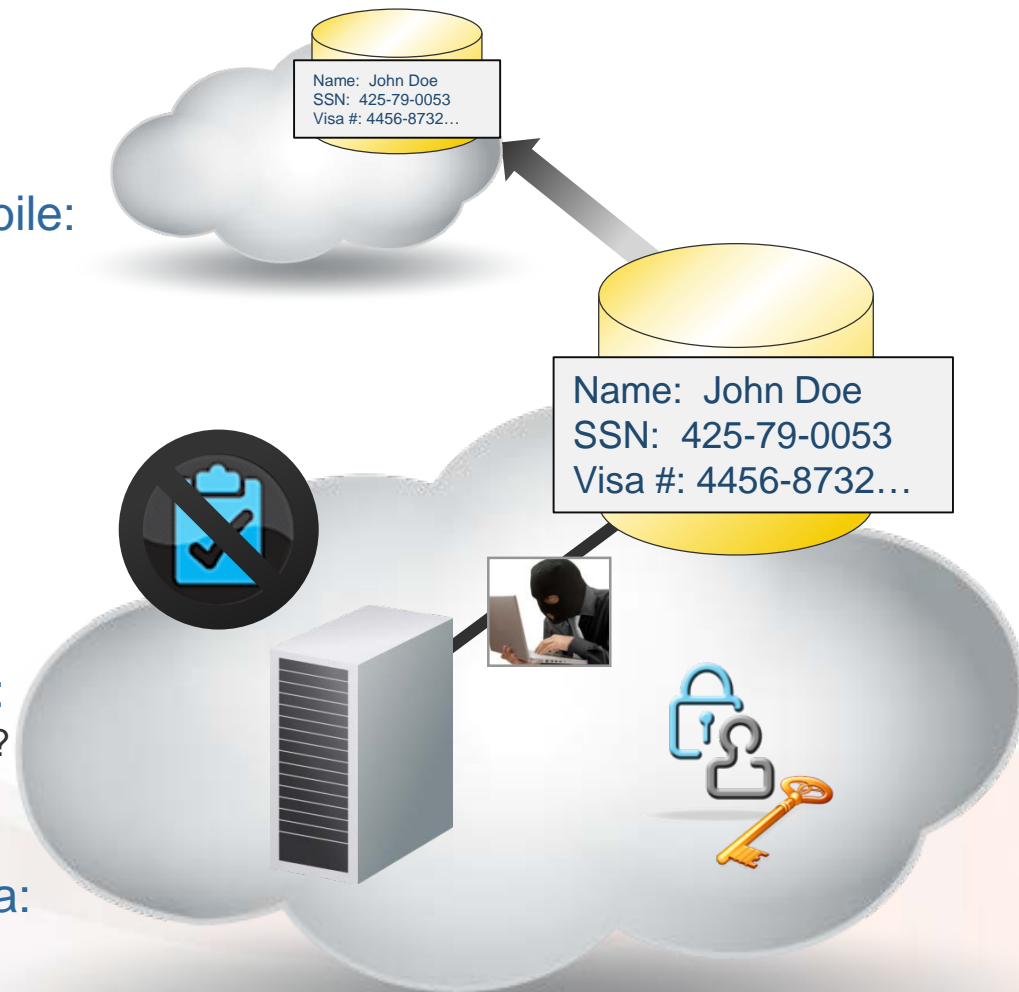
JOIN THE
JOURNEY

What we offer: SecureCloud

- **<u>Encrypts</u>** data in public or private cloud environments
  - Military grade, FIPS 140-2 compliant encryption to 256-bits
- **<u>Manages</u>** encryption keys
  - Typically a very tedious, detailed and expensive process
  - Application upkeep offloaded to trusted partner
- **<u>Authenticates</u>** servers requesting access to data
  - Policy-based system gives wide range of factors on which key deployment decisions are made
  - Delivers keys securely over encrypted SSL channels
- **<u>Audits</u>**, alerts, and reports on key delivery activities
  - Multiple reports and alerting mechanisms available

JOIN THE
JOURNEY

Trend Micro SecureCloud
How It Works

Cloud Service Provider

VM Corporate App

VM

VM

VM

Hypervisor

Trend Micro SecureCloud Console

Enterprise Key

Shared Storage

My Data
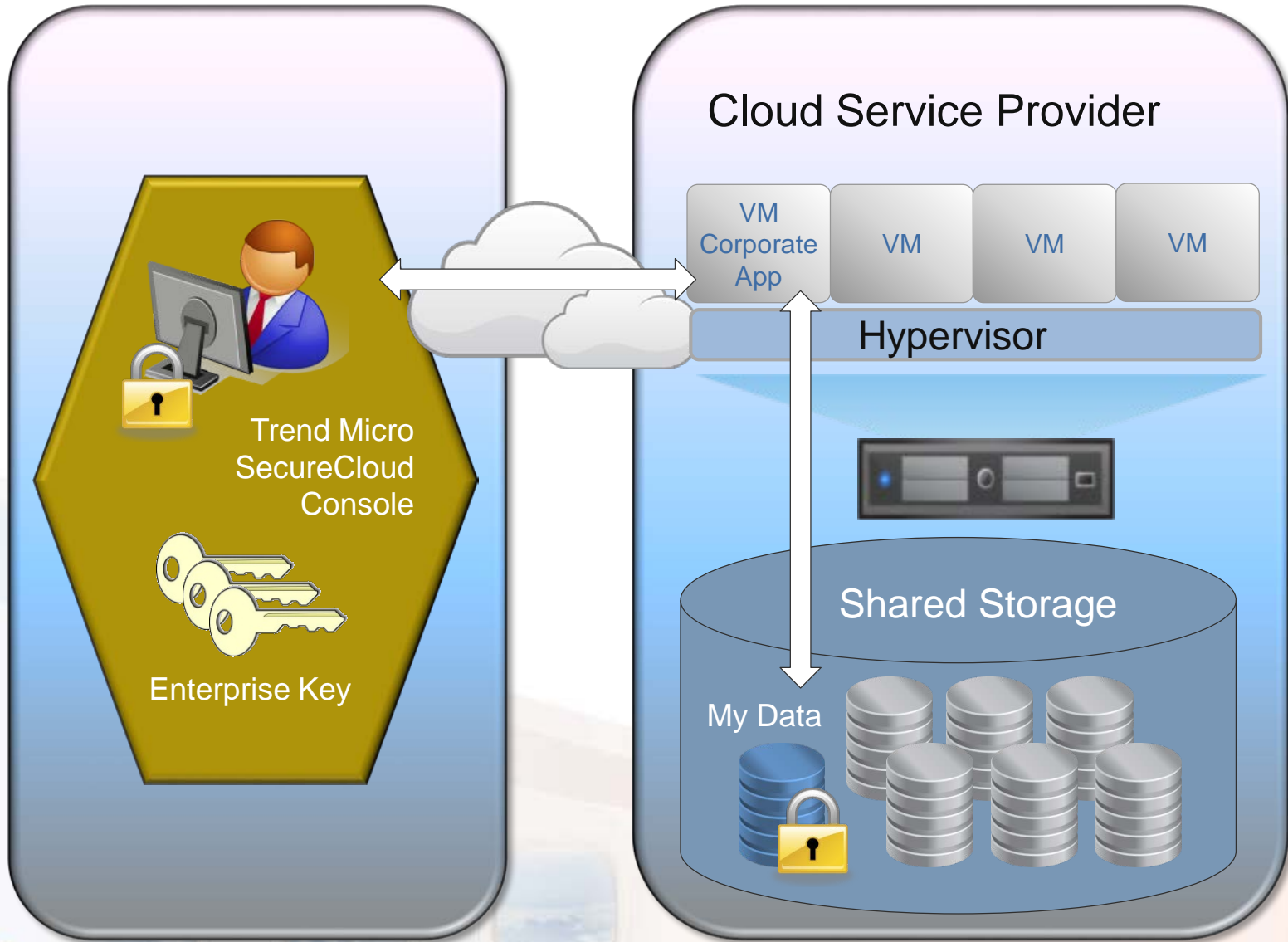
JOIN THE JOURNEY

Policy-based Key Management in the Cloud

Identity	*Integrity*
"Is it mine?"	"Is it okay?"
• Embedded keys • Location • Start-up time • etc	• Firewall • Antimalware • Self integrity check • etc

Auto or Manual rules based key approval

What Does a Policy Look Like?

trendmicro.com/JoinTheJourney