TREND MICRO

Securing Your Journey to the Cloud

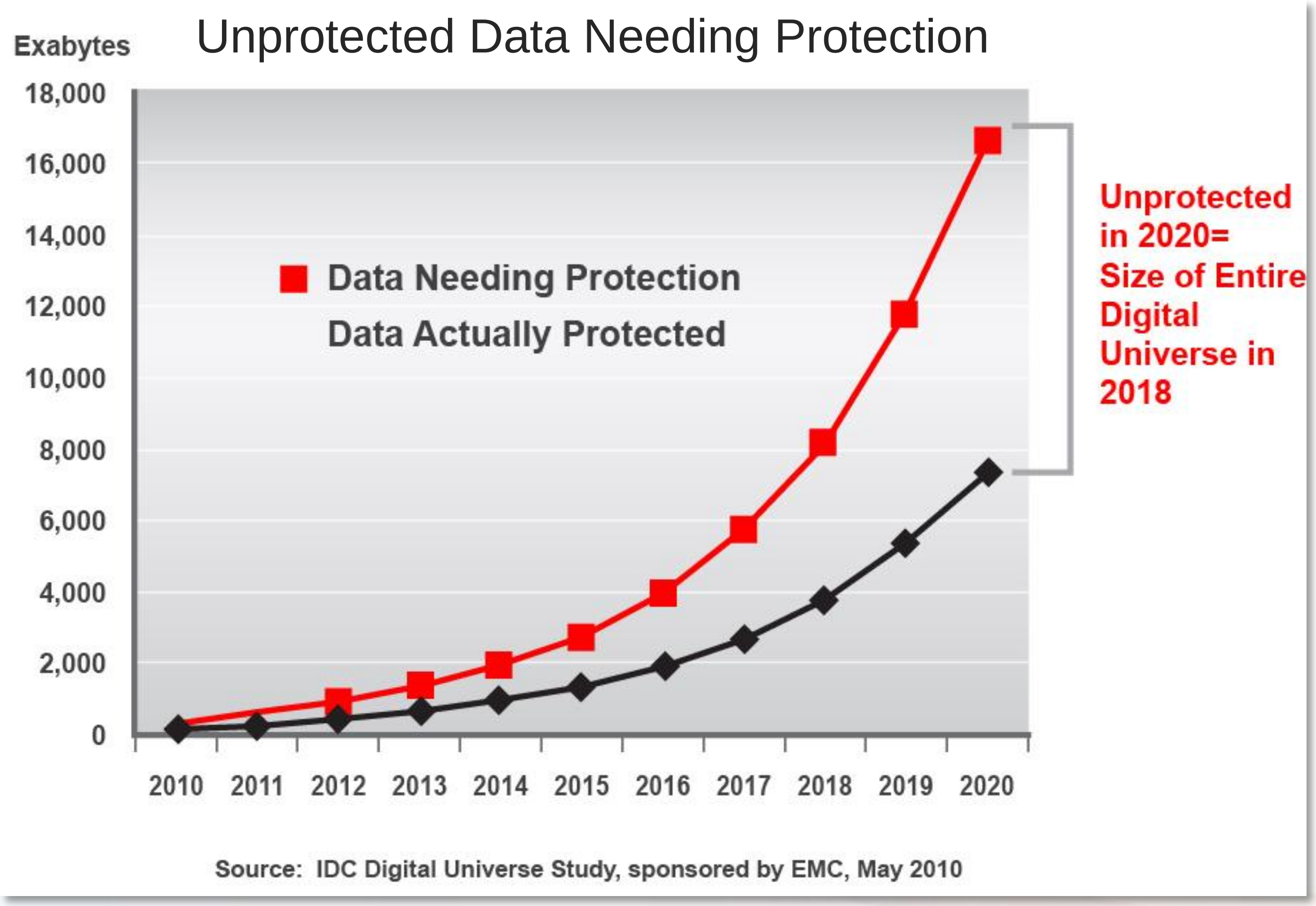
How to survive in a Virtualized and Cloud Computing World

JOIN THE JOURNEY

Dan Reis
Director Product Marketing

EXXON
Mobil
MARATHON
bp
HBGary
BAKER HUGHES
C·O·M·O·D·O
Creating Trust Online™
ConocoPhillips
BARRACUDA
NETWORKS
epsilon
SONY
RSA®
The Security Division of EMC
globalpayments
trapster.com

Data everywhere – but protection?



Source: IDC Digital Universe Study, sponsored by EMC, May 2010

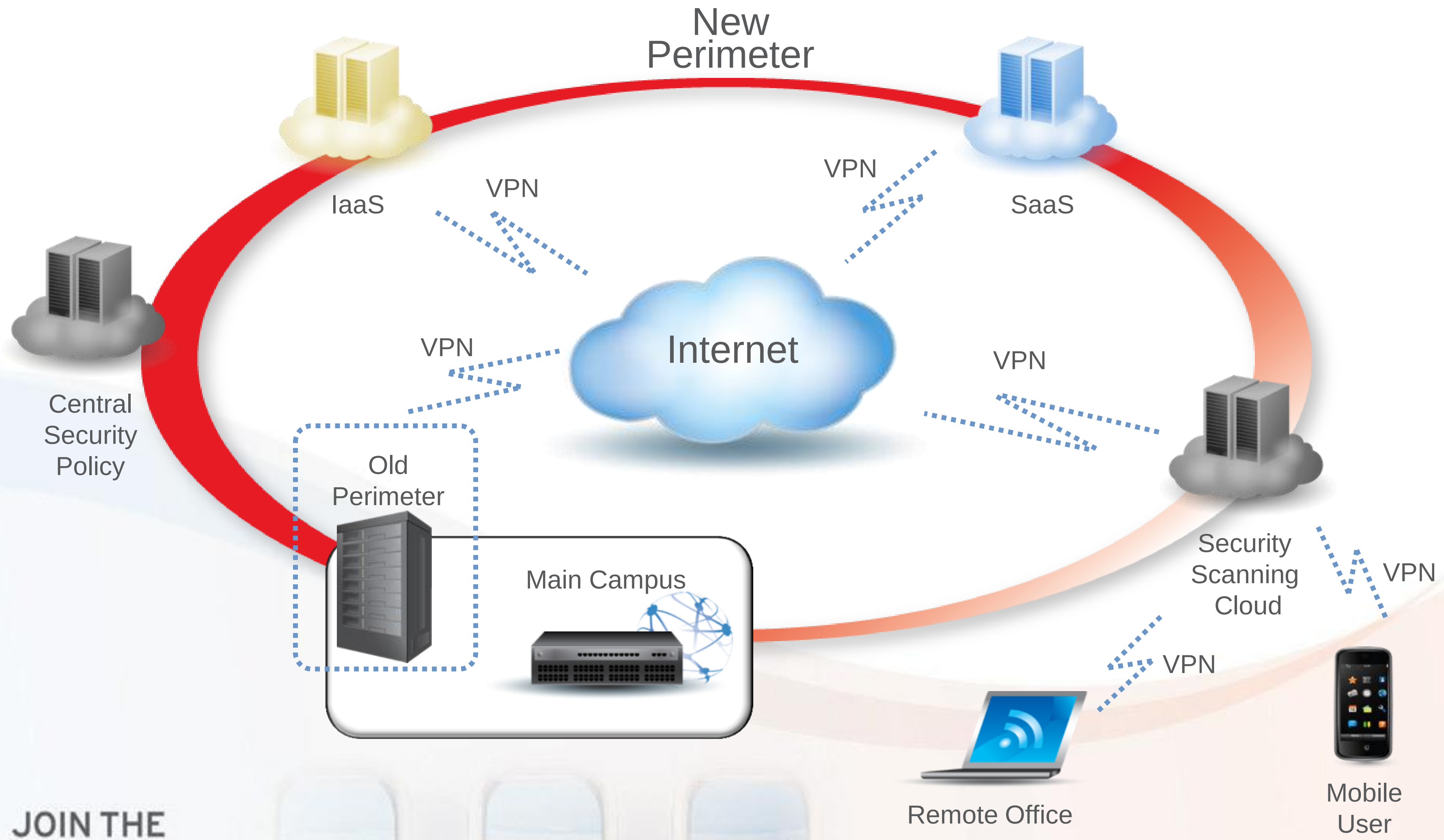
Amount of data needing protection will grow by a factor of 90 by 2020

-IDC

JOIN THE JOURNEY

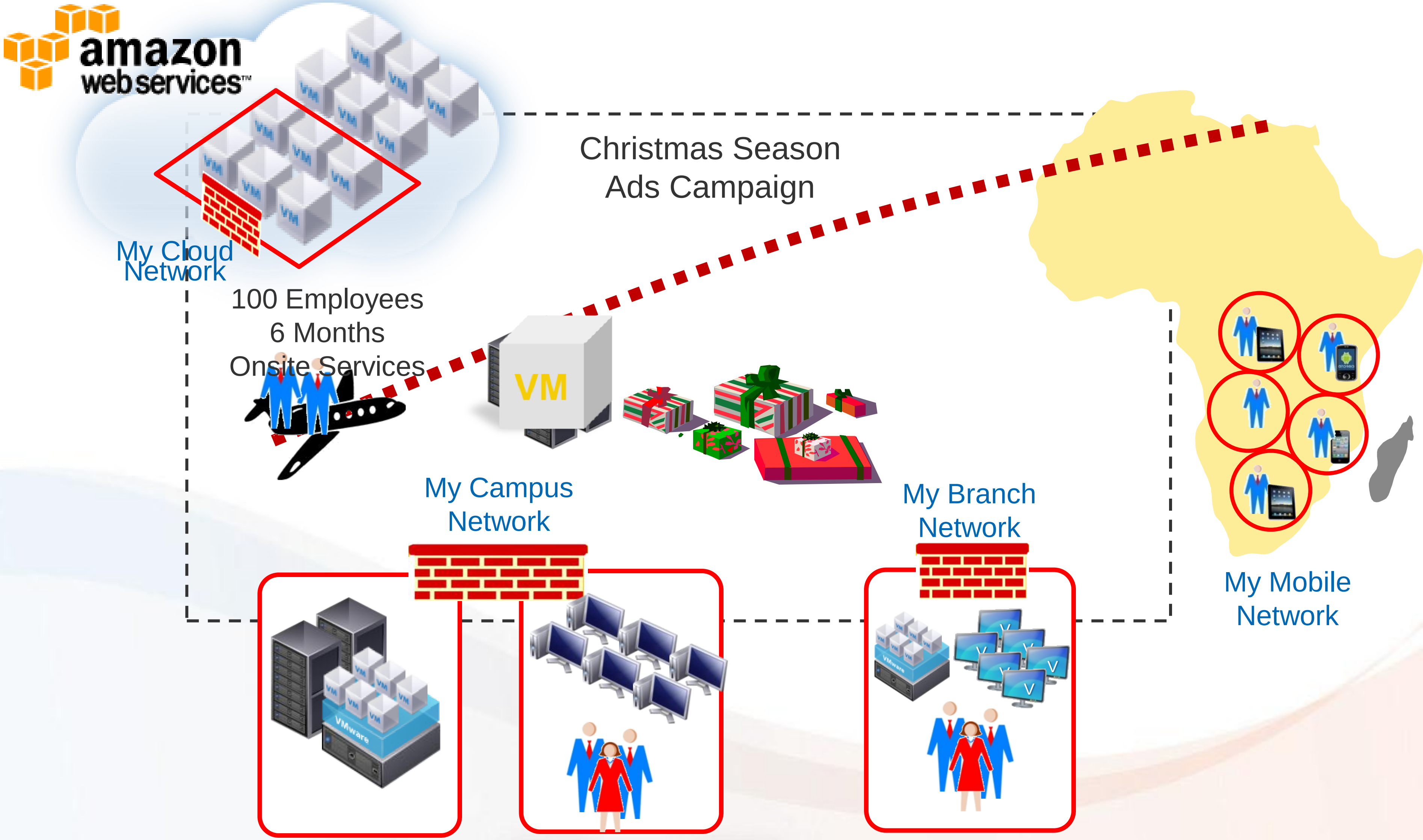
Because the Network Perimeter is Expanding

You Need an Elastic Network Security Architecture



JOIN THE JOURNEY

Your Network is Expanding and is Elastic



Christmas Season
Ads Campaign

My Cloud
Network

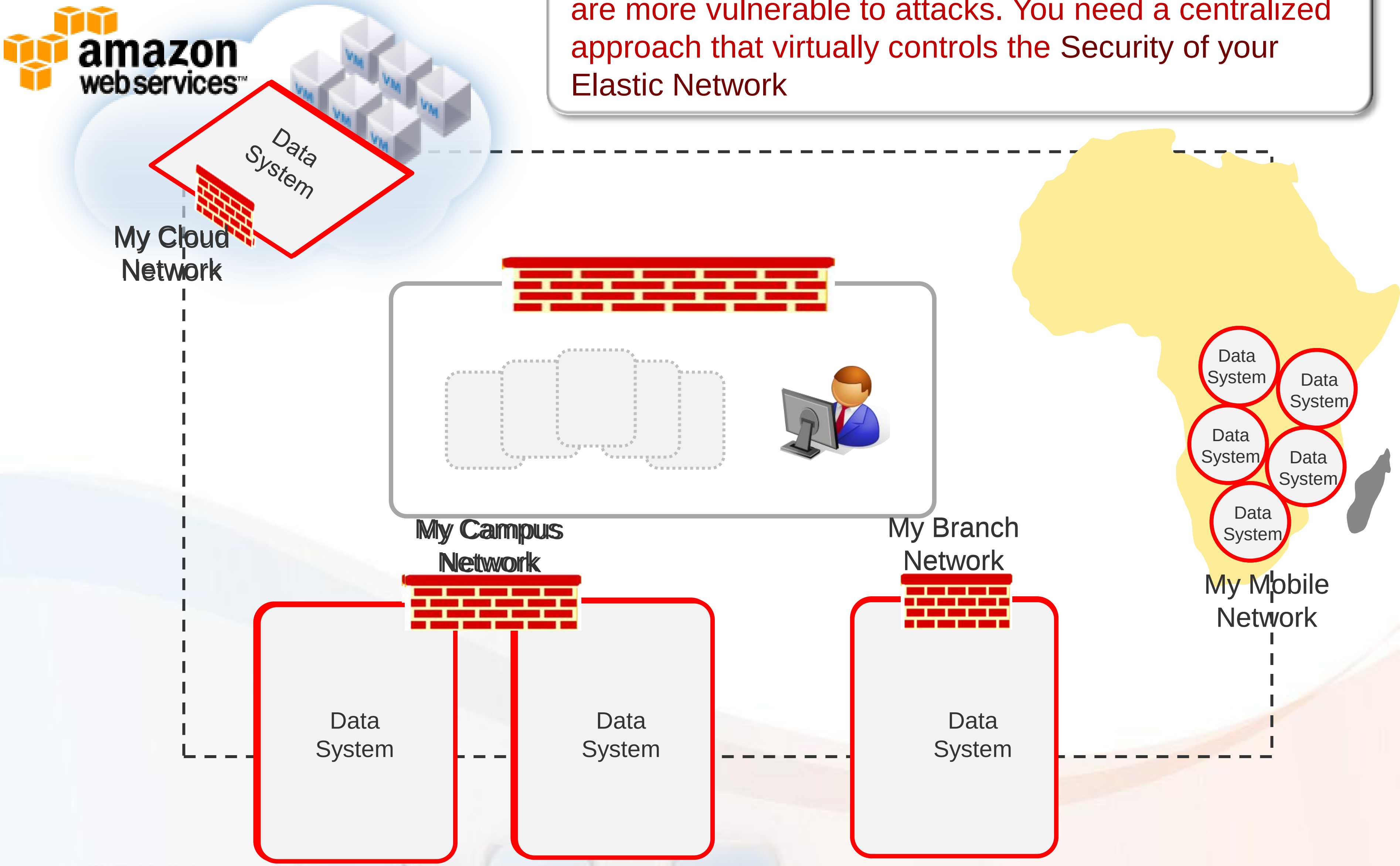
100 Employees
6 Months
Onsite Services

My Campus
Network

My Branch
Network

My Mobile
Network

Because now your perimeter is elastic, Data and system are more vulnerable to attacks. You need a centralized approach that virtually controls the Security of your Elastic Network

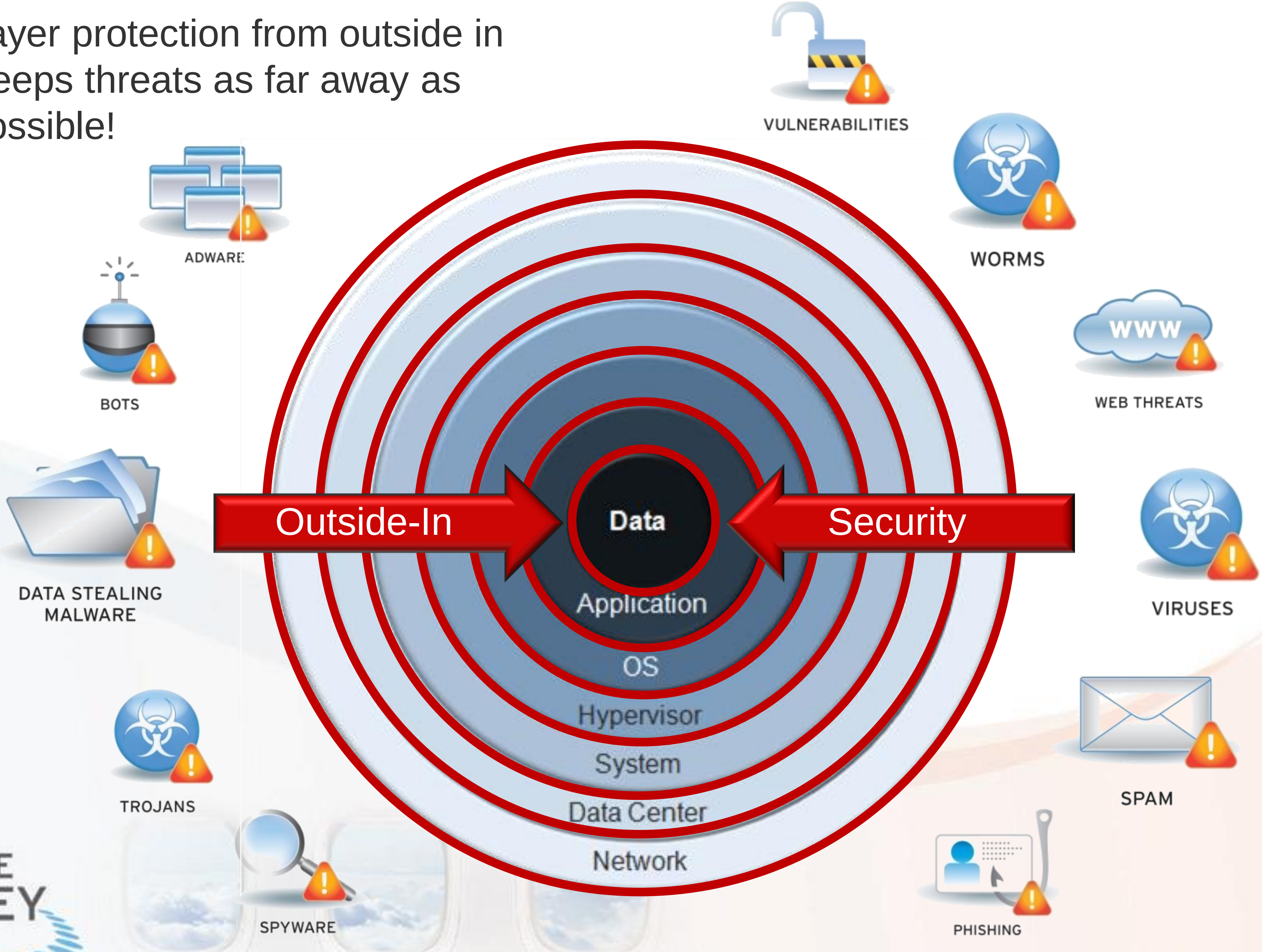


JOIN THE JOURNEY

Integrated Security Across Platforms

Outside-in Model of Perimeter Defense

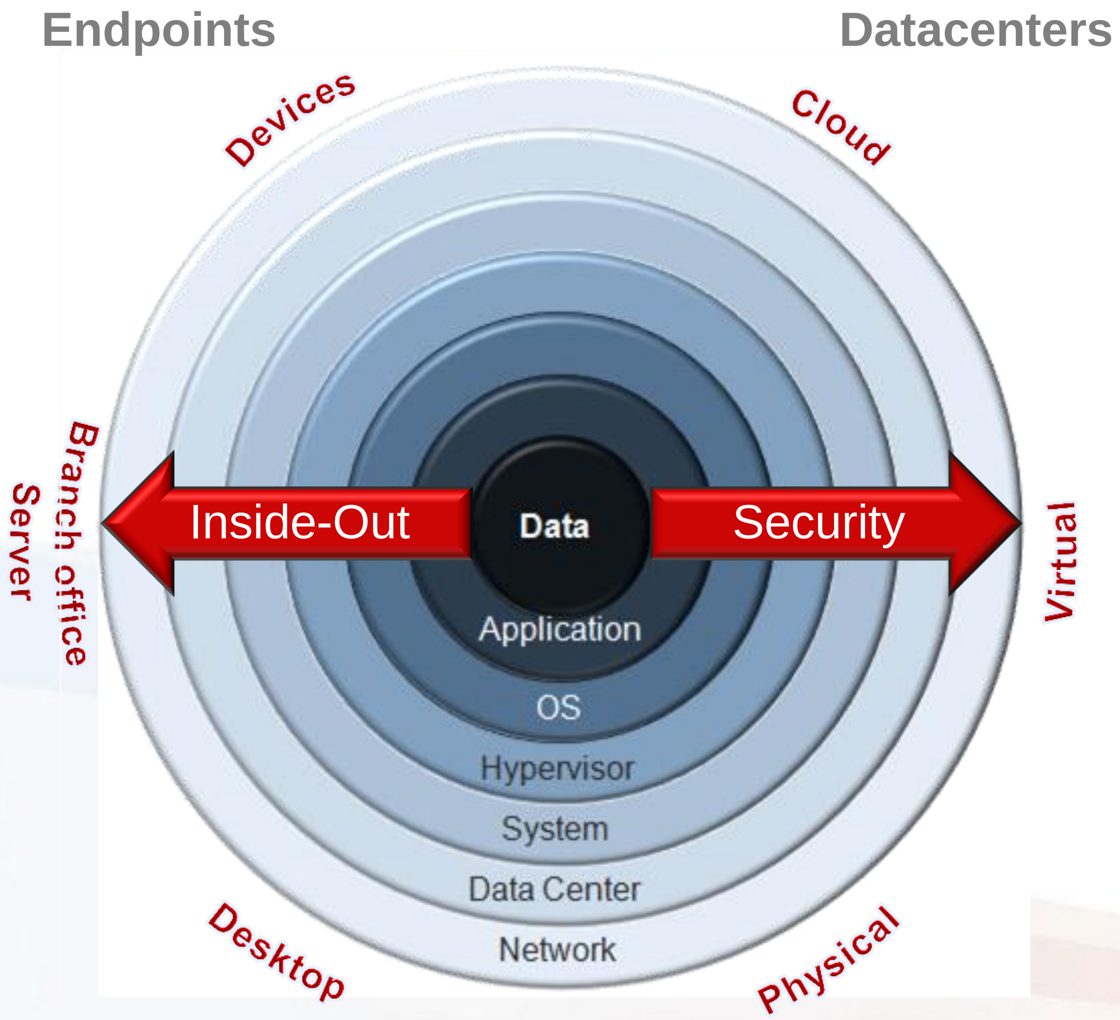
Layer protection from outside in
Keeps threats as far away as possible!



JOIN THE JOURNEY

Integrated Security Across Platforms

Inside-out Security



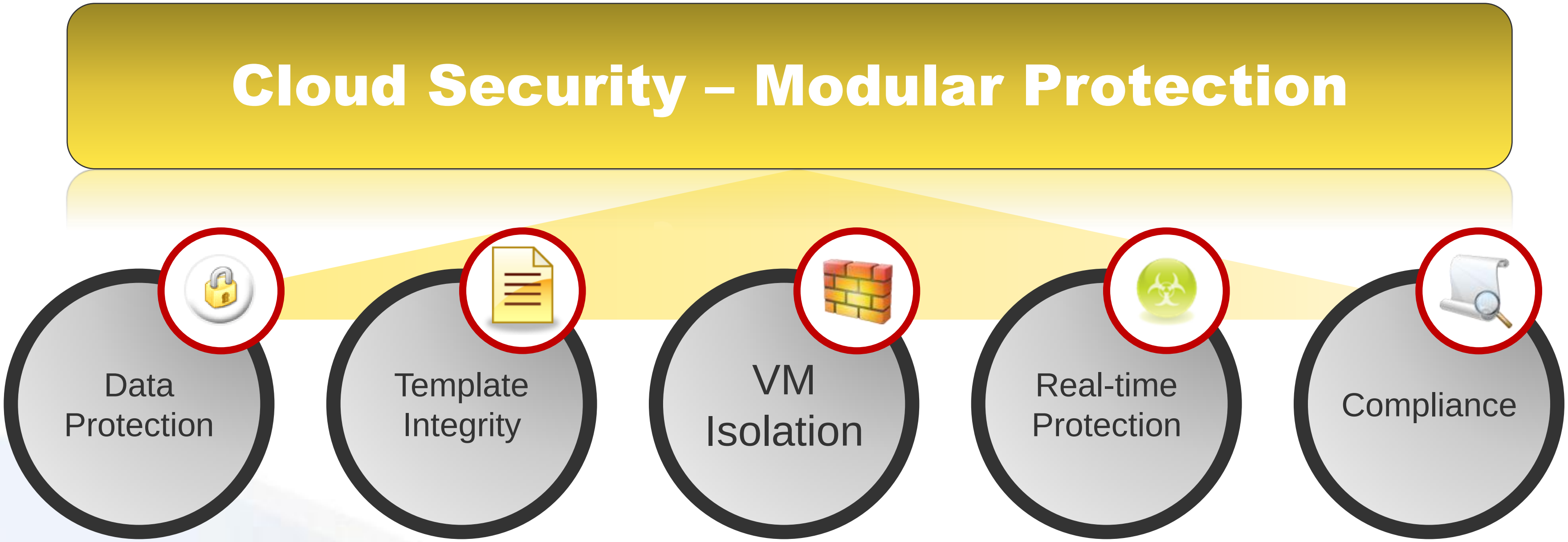
- Self-Secured Workload
- Local Threat Intelligence
  - When-Timeline Aware
  - Who-Identity Aware
  - Where-Location Aware
  - What-Content Aware
- User-defined Access Policies
- Encryption

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

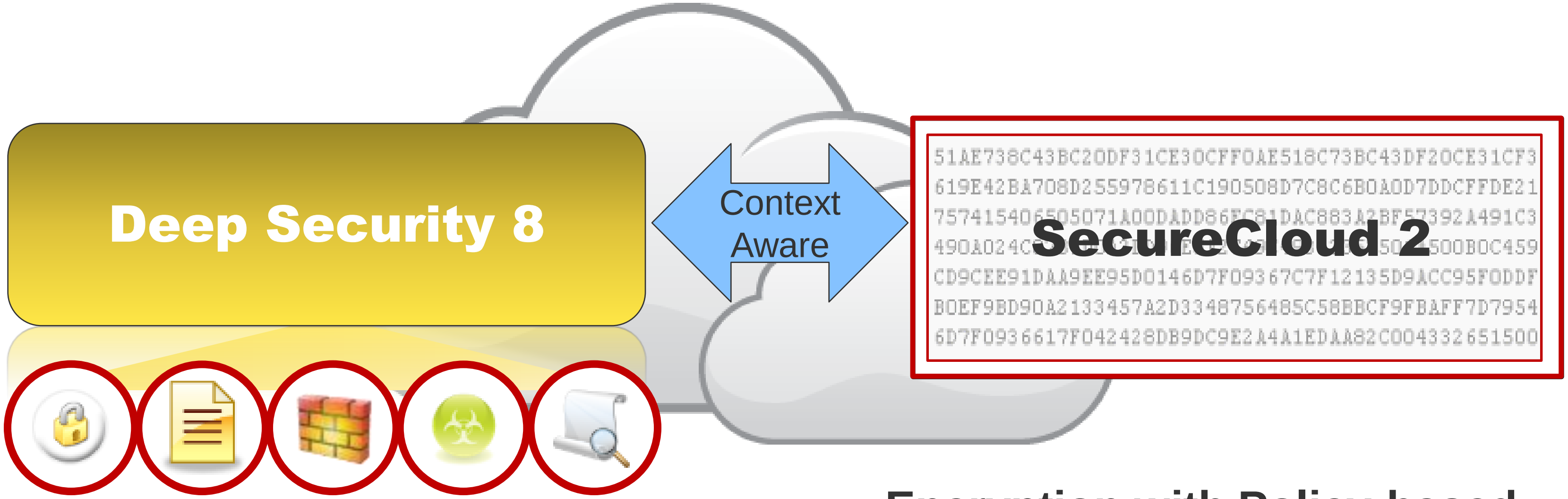
Self-Defending VM Security in the Cloud

- 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



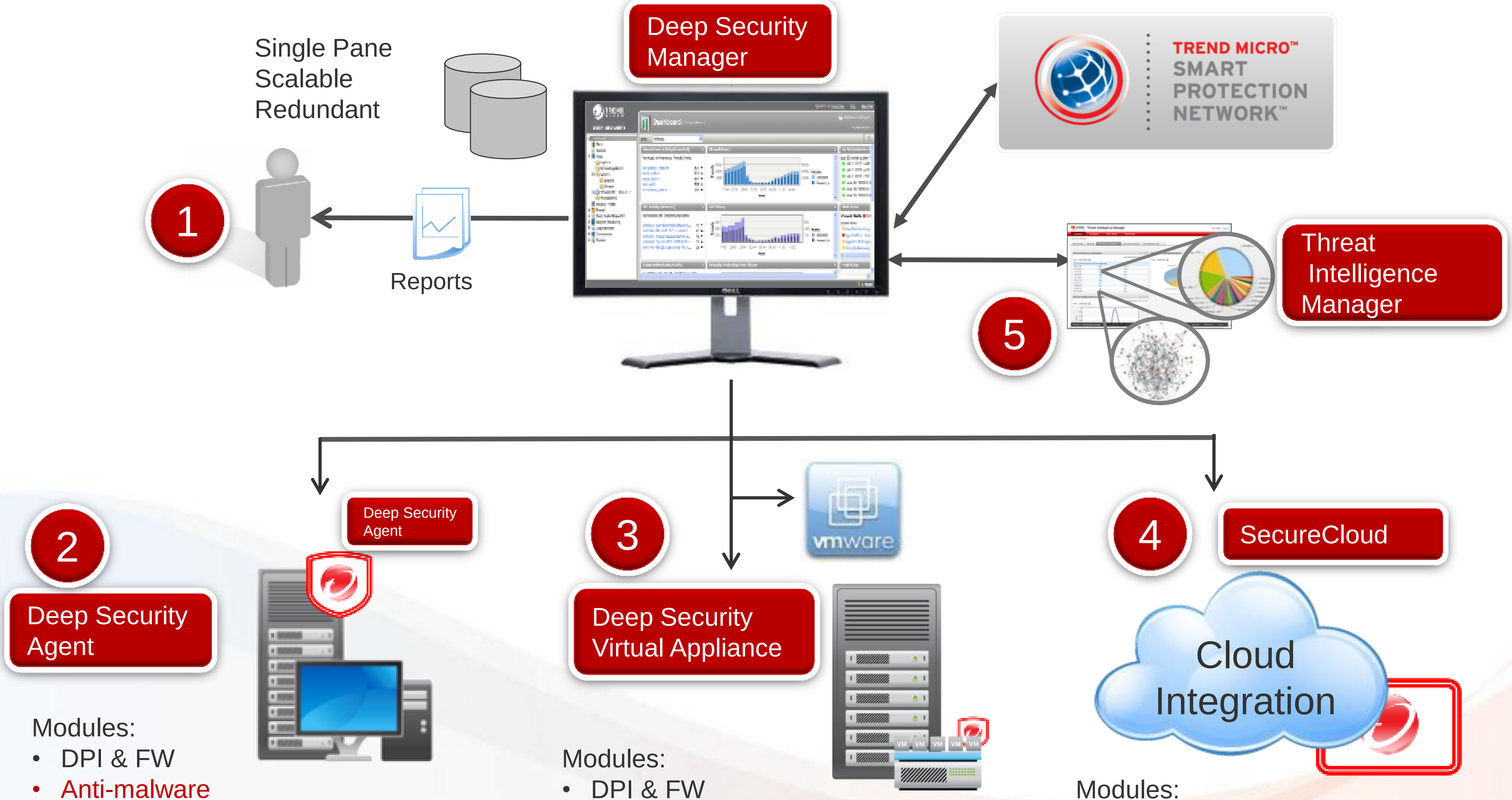
Modular protection for servers and applications

- 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

Deep Security Architecture



1

Single Pane
Scalable
Redundant

Reports

Deep Security Manager

5

Threat Intelligence Manager

2

Deep Security Agent

Modules:

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

3

Deep Security Virtual Appliance

Modules:

- DPI & FW
- Anti-malware
- Integrity Monitoring

4

SecureCloud

Cloud Integration

Modules:

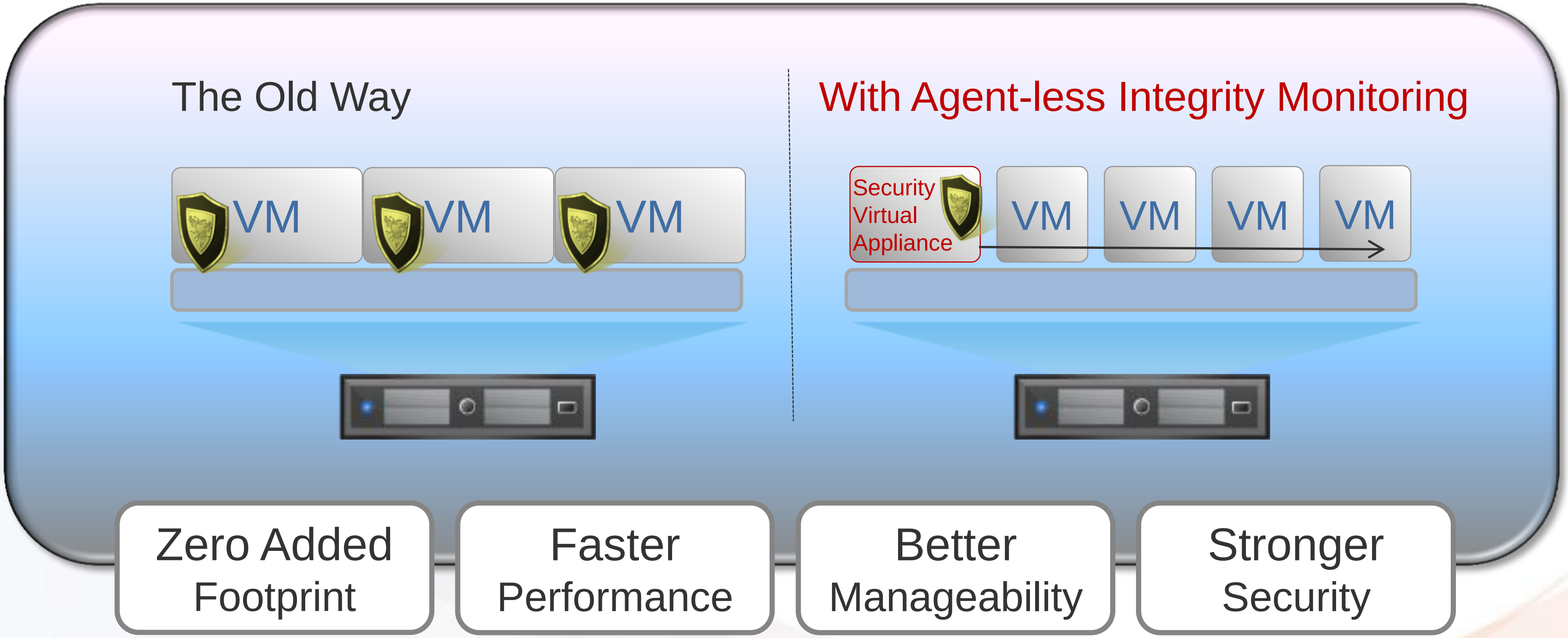
- Data Protection

JOIN THE JOURNEY

APT (Targeted Attacks) 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 or more • 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

Deep Security 8 Integrity Monitoring
Agentless Integrity Monitoring



The Old Way

With Agent-less Integrity Monitoring

Zero Added Footprint

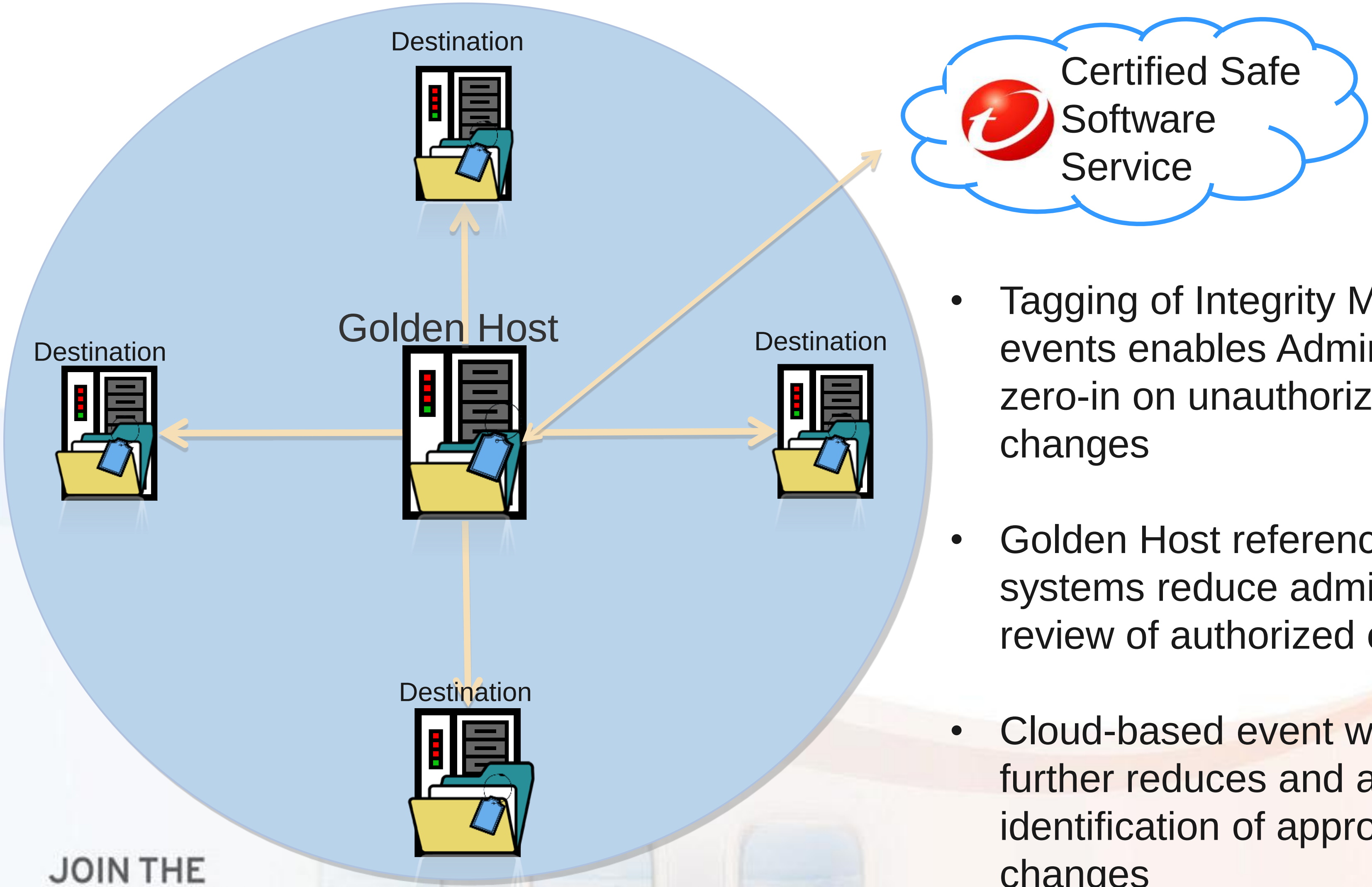
Faster Performance

Better Manageability

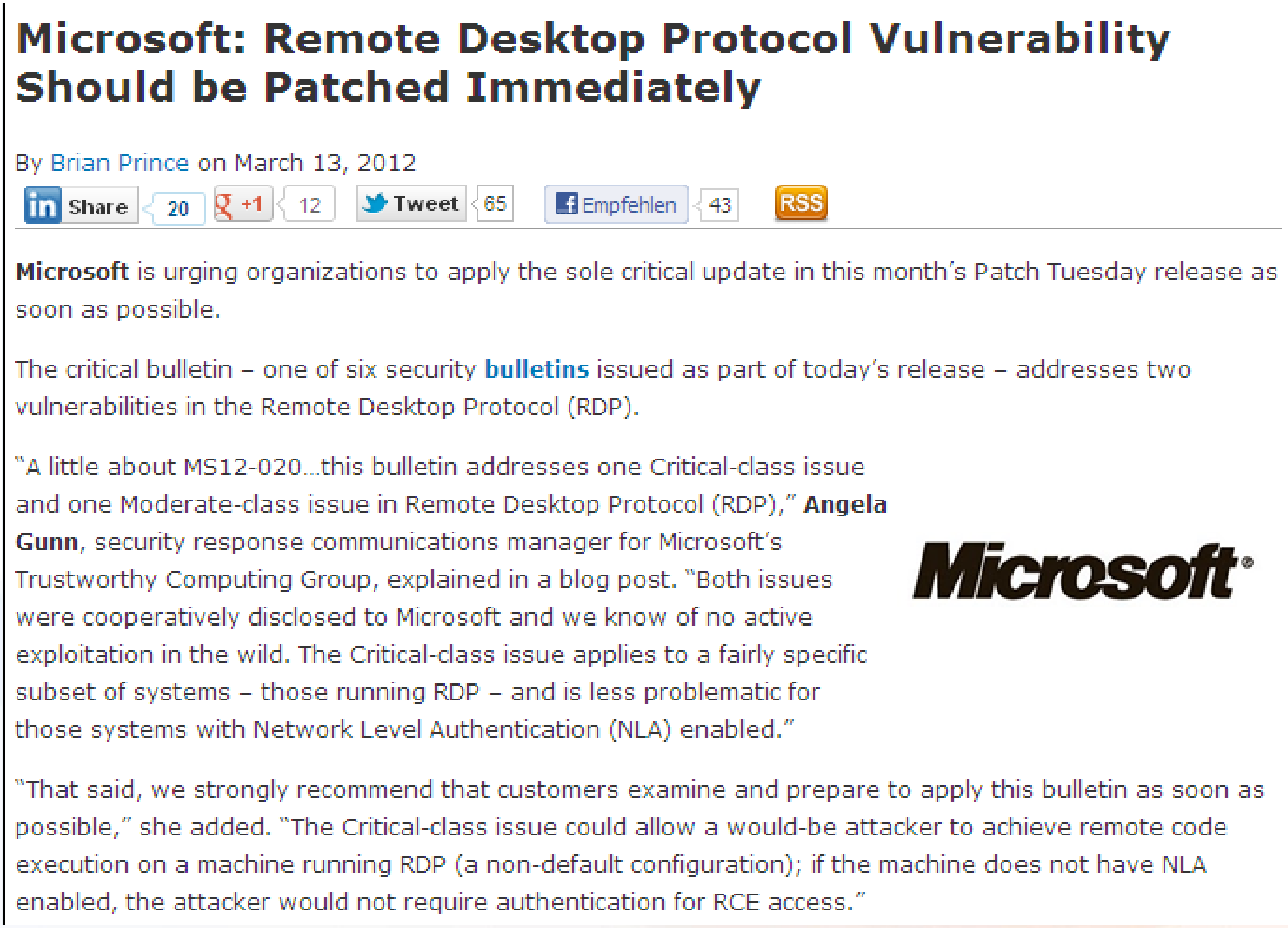
Stronger Security

Deep Security 8

Integrity Monitoring Ease of Use Enhancements



- Tagging of Integrity Monitoring events enables Admins to zero-in on unauthorized changes
- Golden Host reference systems reduce administrative review of authorized changes
- Cloud-based event whitelisting further reduces and automates identification of approved changes



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).

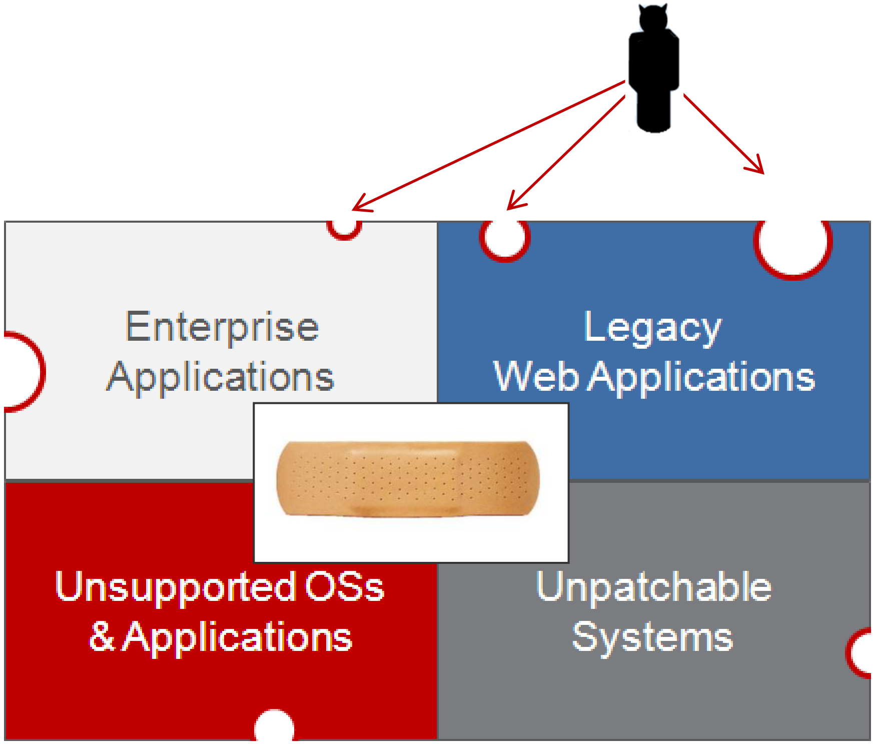
"A little about MS12-020…this bulletin addresses one Critical-class issue and one Moderate-class issue in Remote Desktop Protocol (RDP)," **Angela Gunn**, security response communications manager for Microsoft's Trustworthy Computing Group, explained in a blog post. "Both issues were cooperatively disclosed 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."

"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



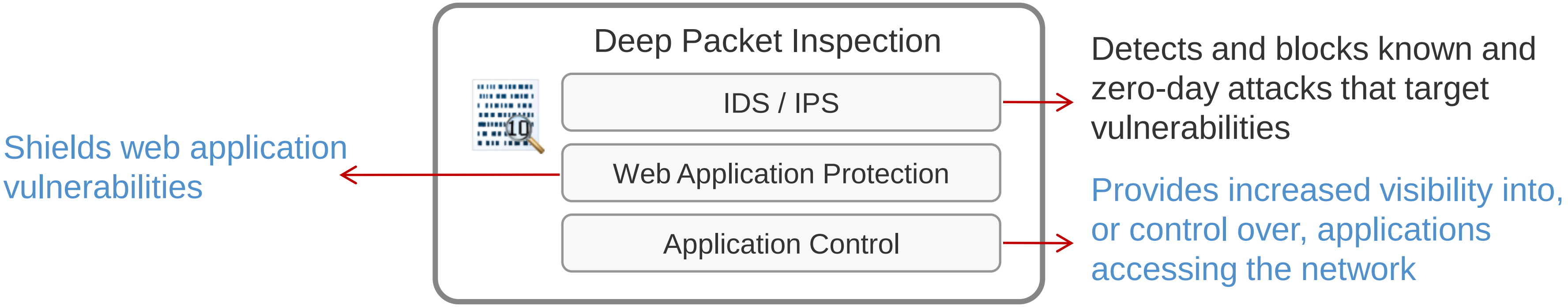
Developers not available to fix vulnerabilities

Patches are no longer being developed

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



Deep Packet Inspection

IDS / IPS

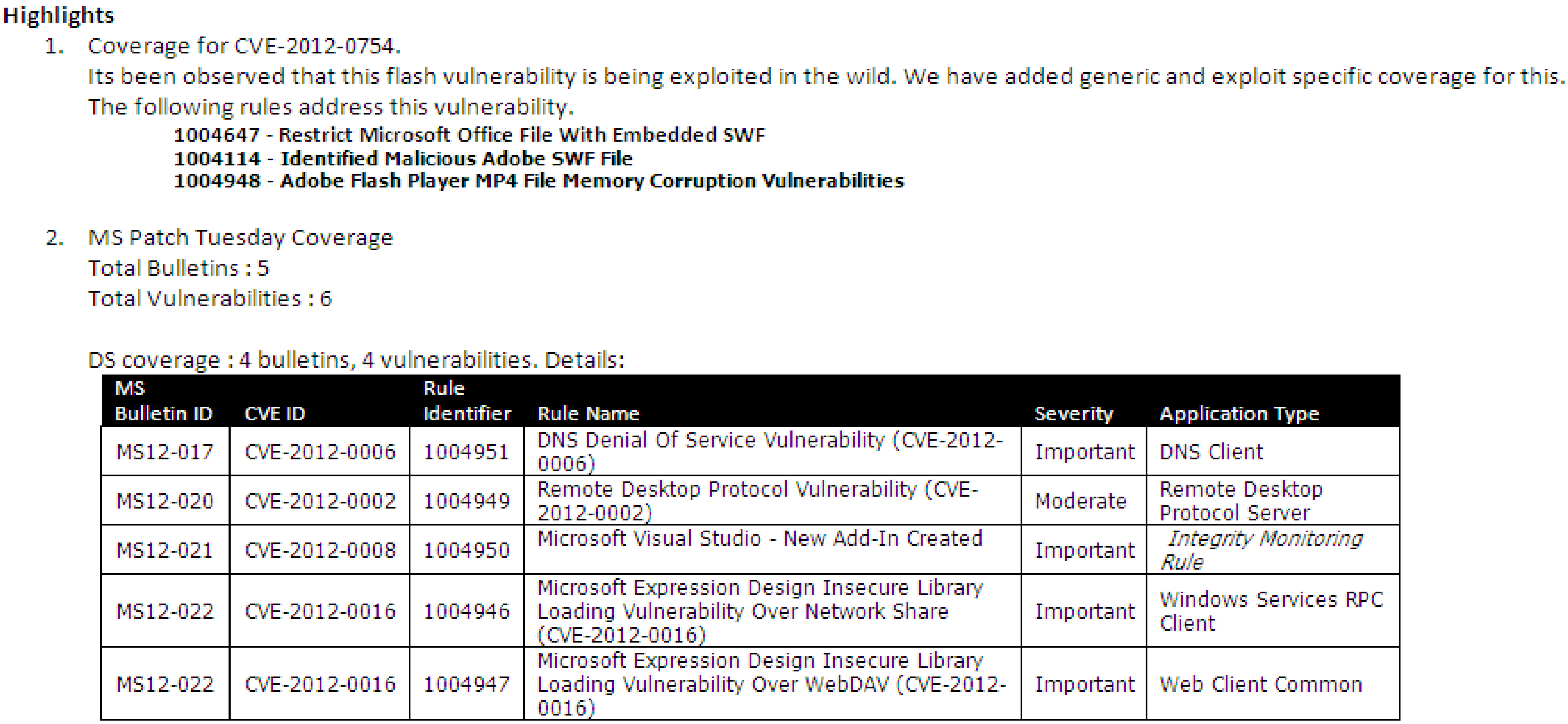
Web Application Protection

Application Control

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



Highlights

1. Coverage for CVE-2012-0754.
   Its been observed that this flash vulnerability is being exploited in the wild. We have added generic and exploit specific coverage for this.
   The following rules address this vulnerability.
   1004647 - Restrict Microsoft Office File With Embedded SWF
   1004114 - Identified Malicious Adobe SWF File
   1004948 - Adobe Flash Player MP4 File Memory Corruption Vulnerabilities

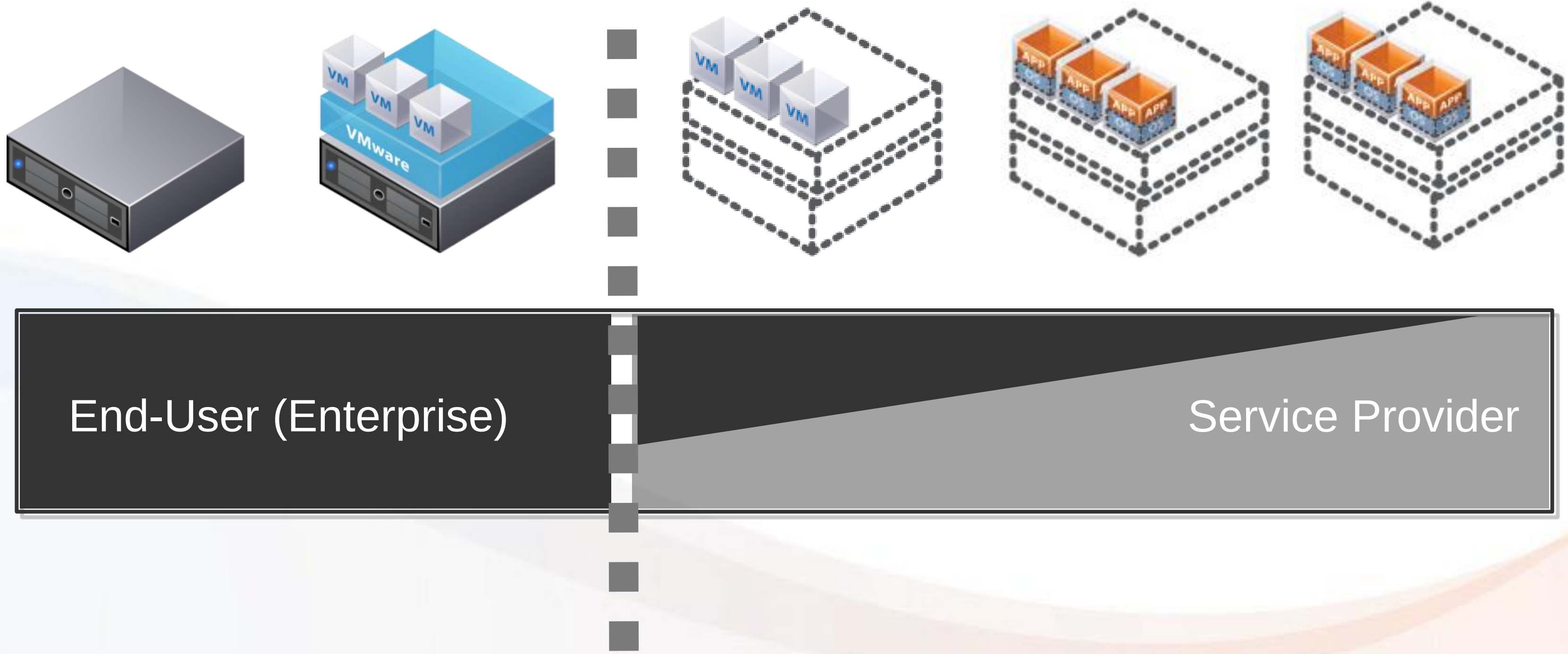
2. MS Patch Tuesday Coverage
   Total Bulletins : 5
   Total Vulnerabilities : 6

   DS coverage : 4 bulletins, 4 vulnerabilities. Details:

MS Bulletin ID	CVE ID	Rule Identifier	Rule Name	Severity	Application Type
MS12-017	CVE-2012-0006	1004951	DNS Denial Of Service Vulnerability (CVE-2012-0006)	Important	DNS Client
MS12-020	CVE-2012-0002	1004949	Remote Desktop Protocol Vulnerability (CVE-2012-0002)	Moderate	Remote Desktop Protocol Server
MS12-021	CVE-2012-0008	1004950	Microsoft Visual Studio - New Add-In Created	Important	*Integrity Monitoring Rule*
MS12-022	CVE-2012-0016	1004946	Microsoft Expression Design Insecure Library Loading Vulnerability Over Network Share (CVE-2012-0016)	Important	Windows Services RPC Client
MS12-022	CVE-2012-0016	1004947	Microsoft Expression Design Insecure Library Loading Vulnerability Over WebDAV (CVE-2012-0016)	Important	Web Client Common

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. You are responsible for properly configuring and using the Service Offerings and taking your own steps to maintain appropriate security, 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:

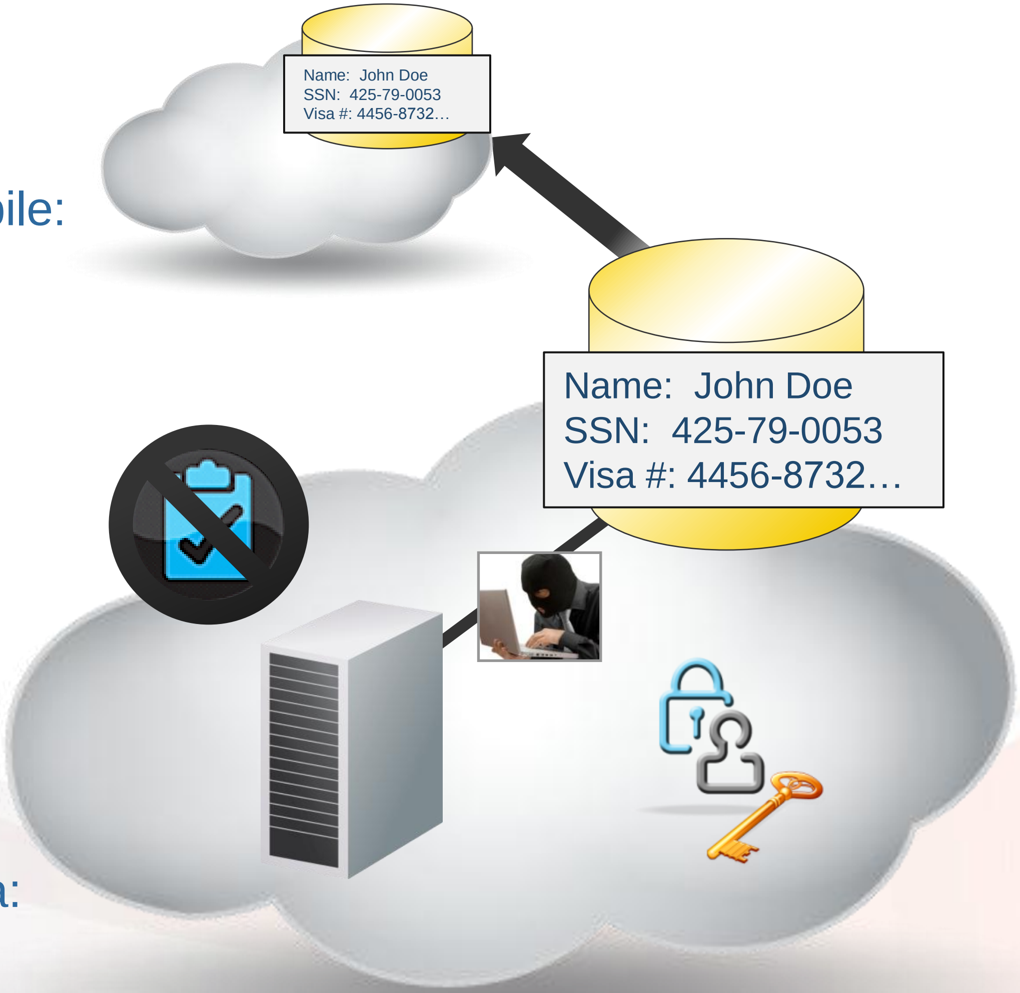
- What happened when you weren't looking?

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?

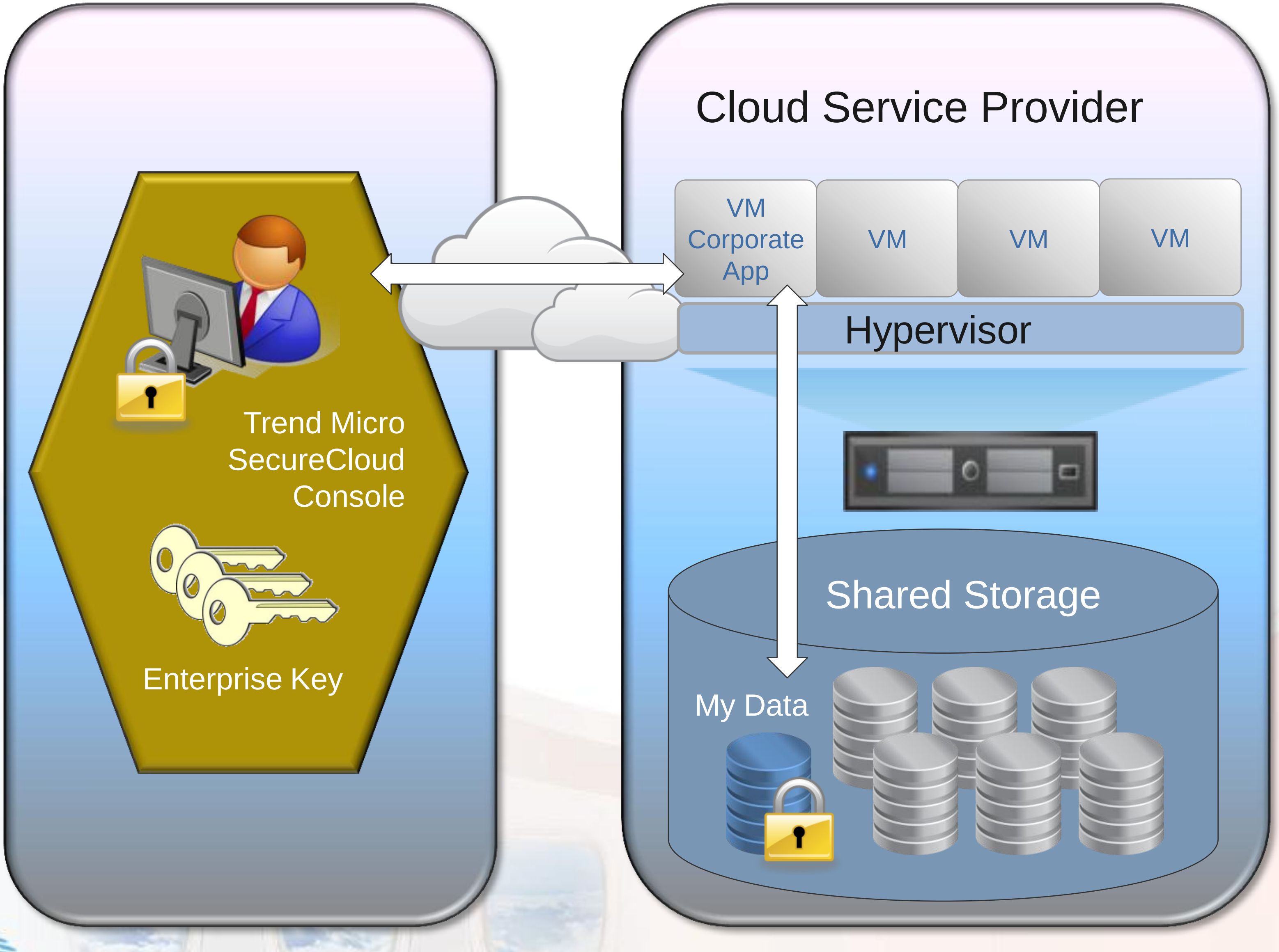


JOIN THE JOURNEY

What we offer: SecureCloud

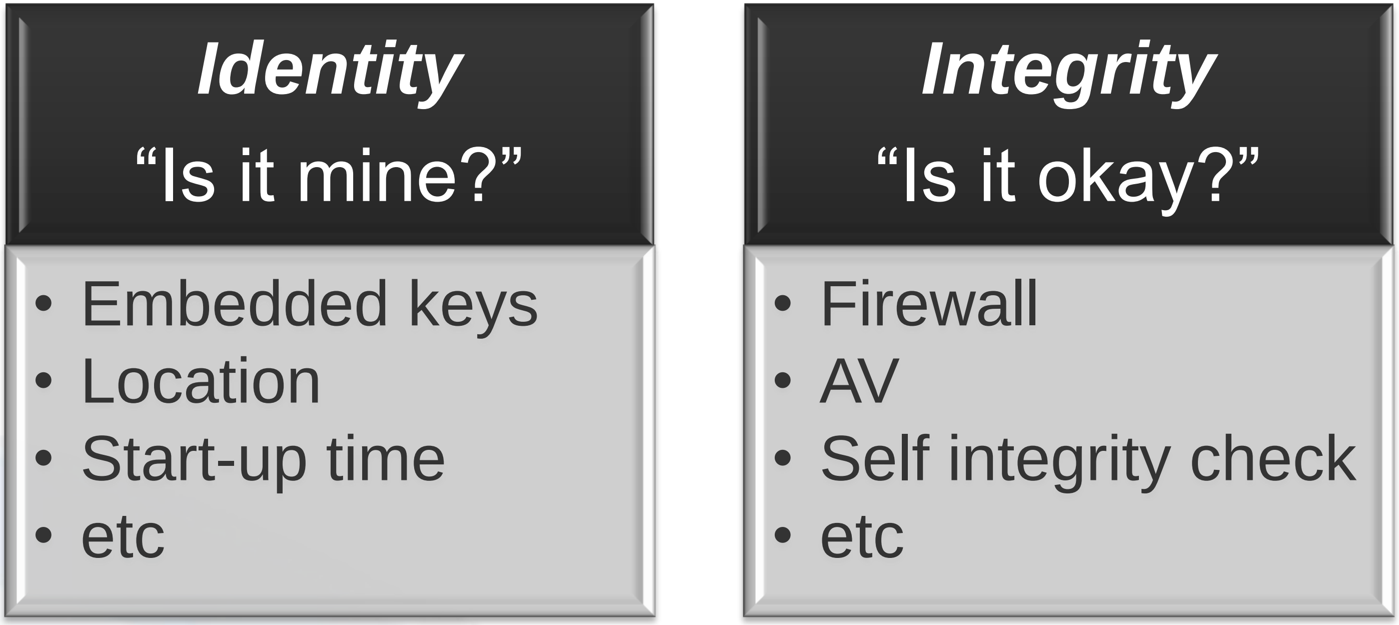
- **Encrypts** data in public or private cloud environments
  - Military grade, FIPS 140-2 compliant encryption to 256-bits
- **Manages** encryption keys
  - Typically a very tedious, detailed and expensive process
  - Application upkeep offloaded to trusted partner
- **Authenticates** servers requesting 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
- **Audits**, alerts, and reports on key delivery activities
  - Multiple reports and alerting mechanisms available

Trend Micro SecureCloud
How It Works



JOIN THE
JOURNEY

Policy-based Key Management in the Cloud



Identity

“Is it mine?”

- Embedded keys
- Location
- Start-up time
- etc

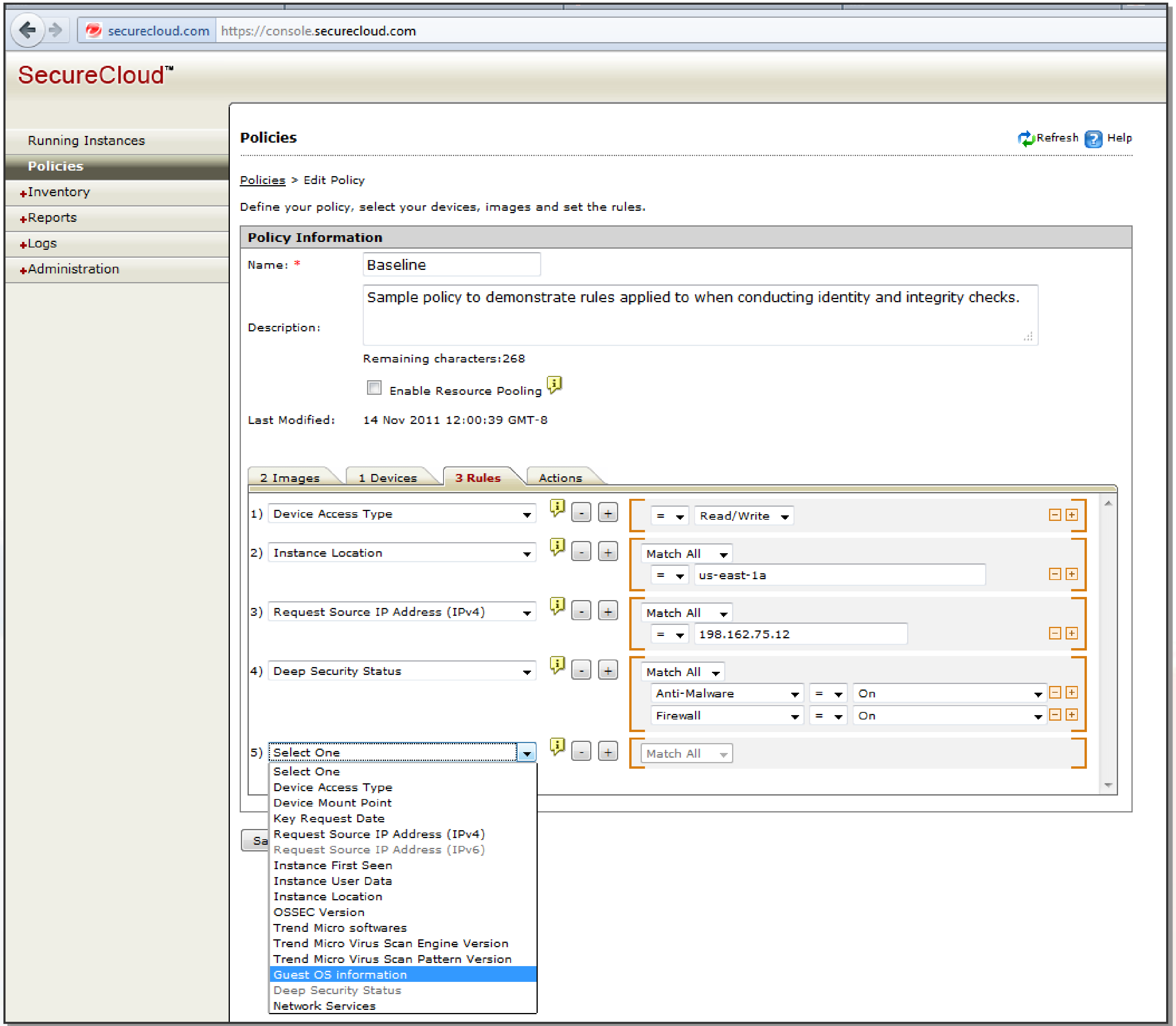
Integrity

“Is it okay?”

- Firewall
- AV
- Self integrity check
- etc

Auto or Manual rules based key approval

What Does a Policy Look Like?



Policies

Policies > Edit Policy

Define your policy, select your devices, images and set the rules.

Policy Information

Name: * Baseline

Description: Sample policy to demonstrate rules applied to when conducting identity and integrity checks.

Remaining characters:268

□ Enable Resource Pooling

Last Modified: 14 Nov 2011 12:00:39 GMT-8

2 Images | 1 Devices | **3 Rules** | Actions

1) Device Access Type — = Read/Write

2) Instance Location — Match All — = us-east-1a

3) Request Source IP Address (IPv4) — Match All — = 198.162.75.12

4) Deep Security Status — Match All
   - Anti-Malware = On
   - Firewall = On

5) Select One — Match All

JOIN THE JOURNEY

TREND MICRO

Securing Your Journey to the Cloud

JOIN THE JOURNEY

trendmicro.com/JoinTheJourney