TREND MICRO | Securing Your Web World

SecureCloud: Controlling Private Data in the Public Cloud

Harri Kaikkonen

Country Sales Manager, Finland and Baltics

A working definition of Cloud Computing

Cloud computing is a pay-per-use model for enabling available, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

National Institute of Standards & Technology (NIST), USA

5 Key Cloud Characteristics

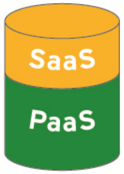
- On-demand self-service
- Ubiquitous network access
- Location independent resource pooling
- Rapid elasticity
- Pay per use

Cloud Computing Service Models

Software as a Service (SaaS)

- Use provider's application over the Internet
- Proprietary infrastructure

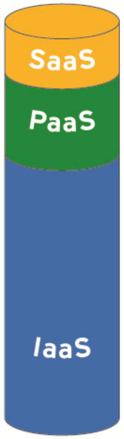
salesforce.com Success On Demand
NETSUITE
Google apps
webex
Microsoft Dynamics CRM
Kenexa
SuccessFactors People Performance



Platform as a Service (PaaS)

- Deploy enterprise-created applications to a cloud
- Proprietary infrastructure

force.com platform as a service
webex connect
Google App Engine
Windows Azure
intuit Intuit Partner Platform



Infrastructure as a Service (IaaS)

- Rent processing, storage, network capacity, and other fundamental computing resources
- Full access to infrastructure stack with basic security services (Firewall, Load Balancers etc.)

amazon webservices
IBM
verizon
at&t
nirvanix
flexiscale
Sun microsystems
GOGRID beta

Based on National Institutes of Standards & Technology (NIST) definitions - http://csrc.nist.gov/groups/SNS/cloud-computing/

TREND MICRO

Agenda

▶ **Cloud Computing Evolution**

Security Challenges

Overall high-level architecture

The Creative Security Solution

Deployment models & licensing

Value proposition

Roadmap

The Evolving Datacenter

Lowering Costs, Increasing Flexibility

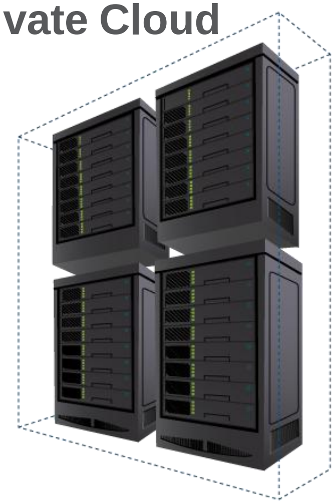
Physical

Traditional datacenter

Virtual

Servers virtualized with minimal changes to datacenter processes

Private Cloud



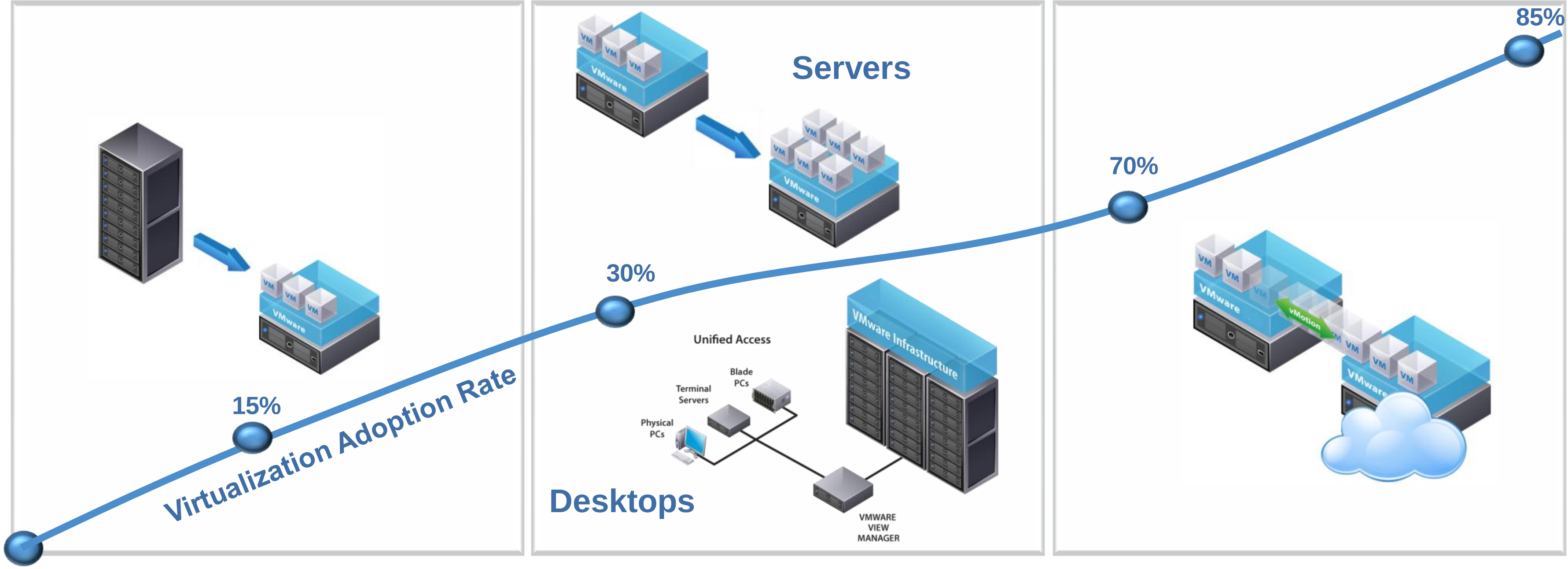
Servers virtualized in scalable, shared, automated & elastic environment

Public Cloud

Select enterprise applications in public cloud

The Evolving Datacenter

Stage 1 Consolidation	Stage 2 Expansion & Desktop	Stage 3 Private > Public Cloud
Cost-efficiency ✓	+ Quality of Service ✓	+ Business Agility ✓

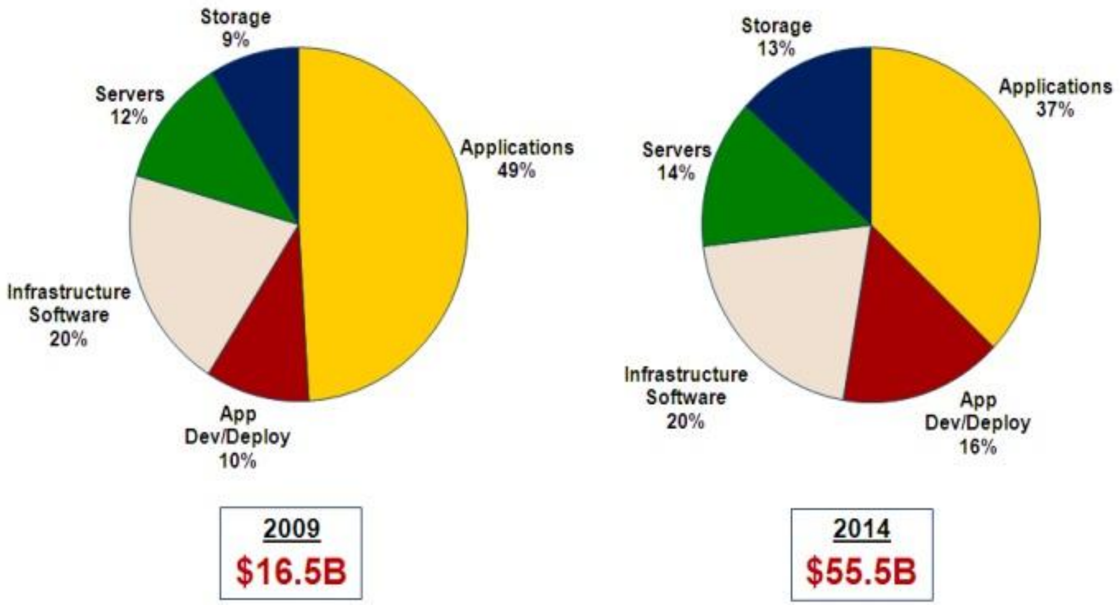


Datacenters are evolving to drive down costs and increase business flexibility

Adoption of cloud computing

- IDC Predicts: IT spending on cloud to reach 10% by 2013

- Information Week Cloud survey:
  - 17% in public cloud
  - 30% planning for private cloud
    - 25% spending at 20% of total budget



Worldwide Public IT Cloud Services* Spending ($B) by Offering Category
2009, 2014

Source: IDC, June 2010

*Includes spending on Applications, Application Development & Deployment Software, Systems Infrastructure Software, Server capacity and Storage capacity provided via the public Cloud Services delivery model.

Agenda

Cloud Computing Evolution

▶ **Security Challenges**

Overall high-level architecture

The Creative Security Solution

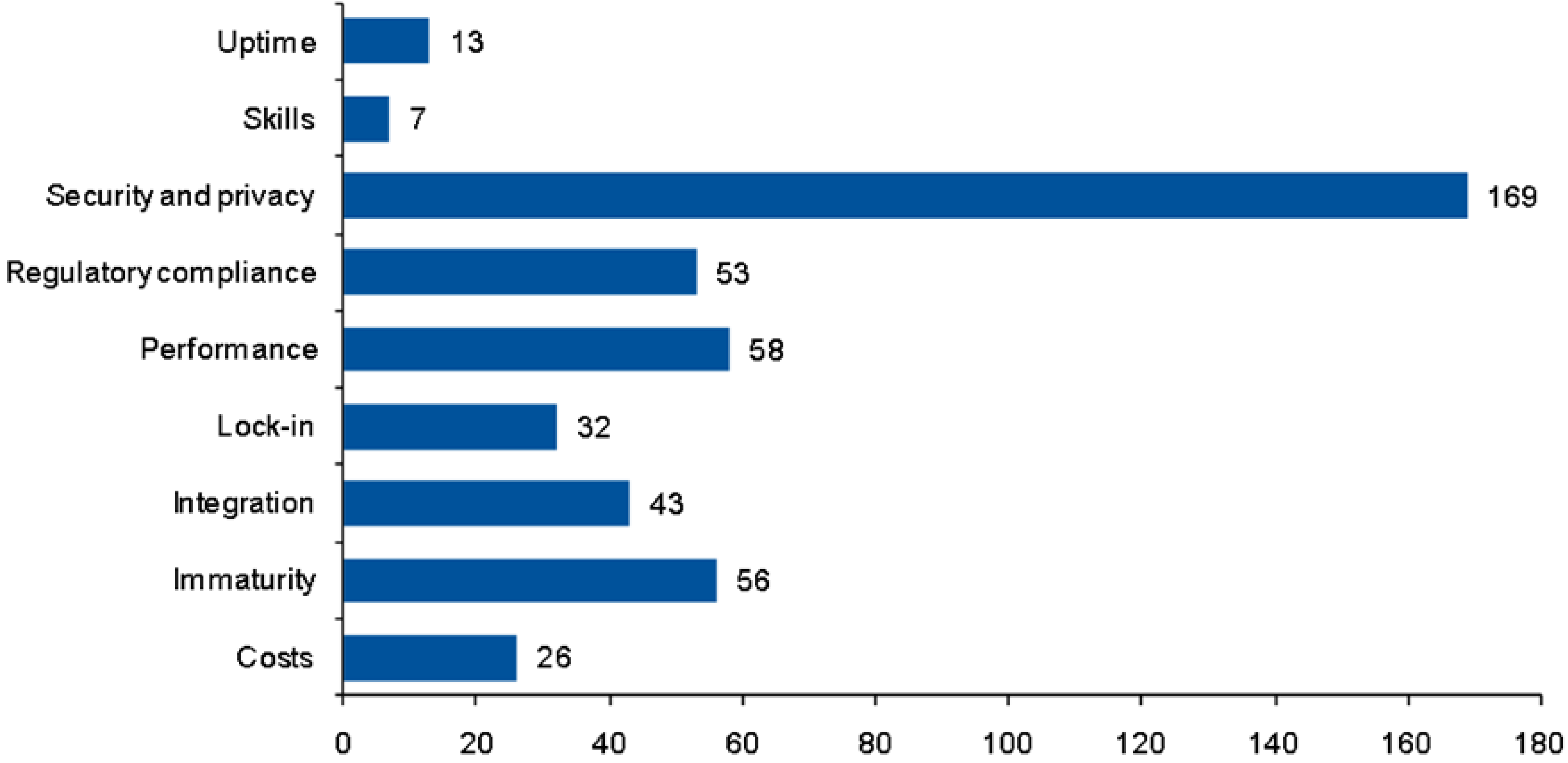
Deployment models & licensing

Value proposition

Roadmap

Security: the #1 Cloud Challenge

Security and privacy were the foremost concerns by far, with a weighted score higher than the next three (performance, immaturity and regulatory compliance) combined.

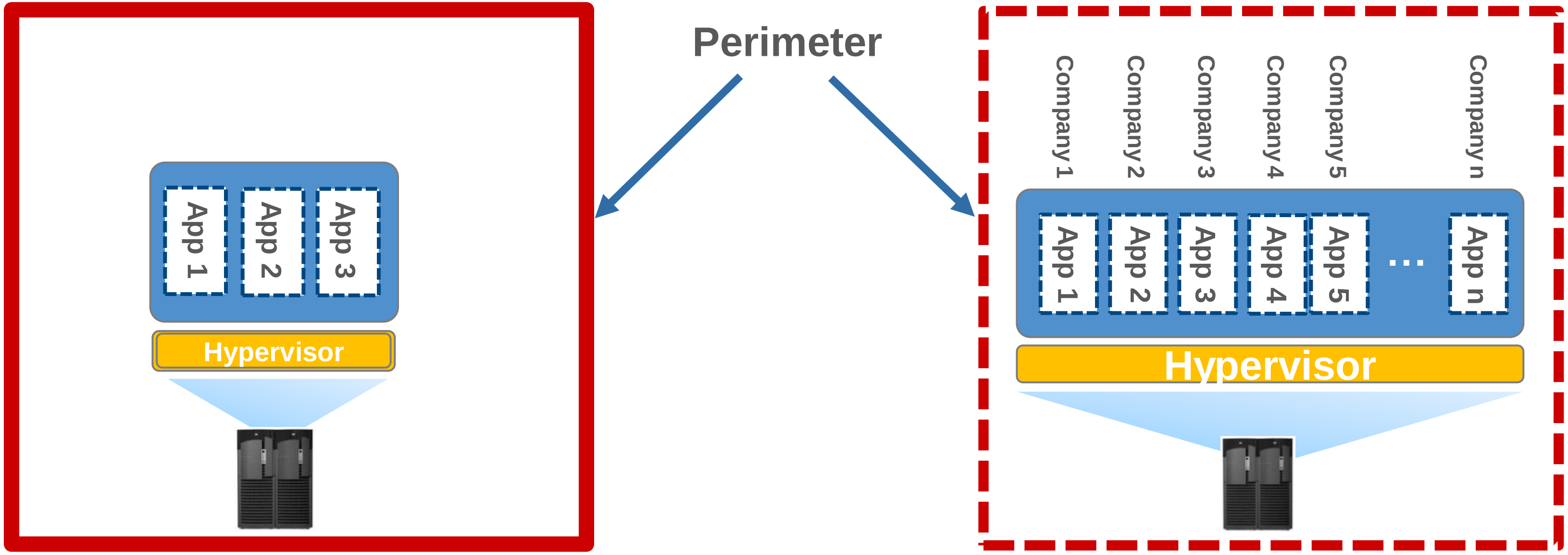


Gartner (April 2010)

Challenge of Securing Data

Datacenter

Public Cloud



Perimeter

App 1

App 2

App 3

Hypervisor

Company 1

Company 2

Company 3

Company 4

Company 5

Company n

App 1

App 2

App 3

App 4

App 5

…

App n

Hypervisor

Strong perimeter security

No shared CPU

No shared network

No shared storage

Weak perimeter security

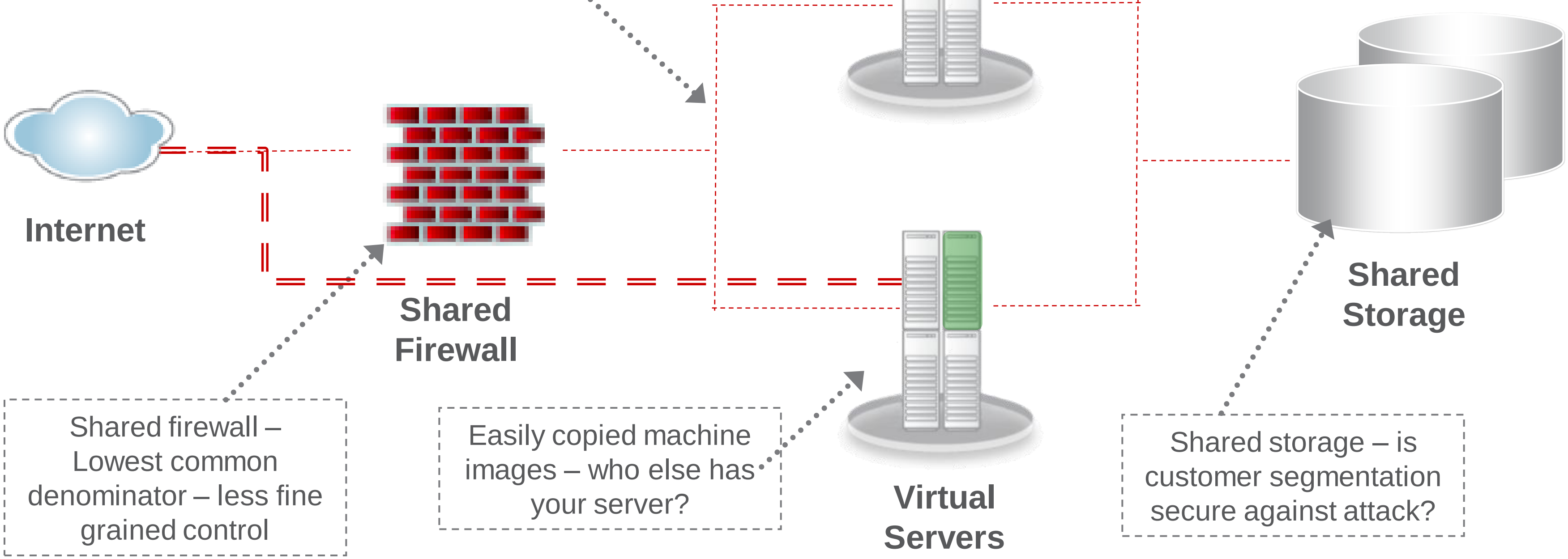
Shared CPU

Shared network

Shared storage

Traditional “outside-in” approach is inadequate in an “inside-out” cloud world full of strangers

Challenges for Public Cloud



Multiple customers on one physical server – potential for attacks via the hypervisor

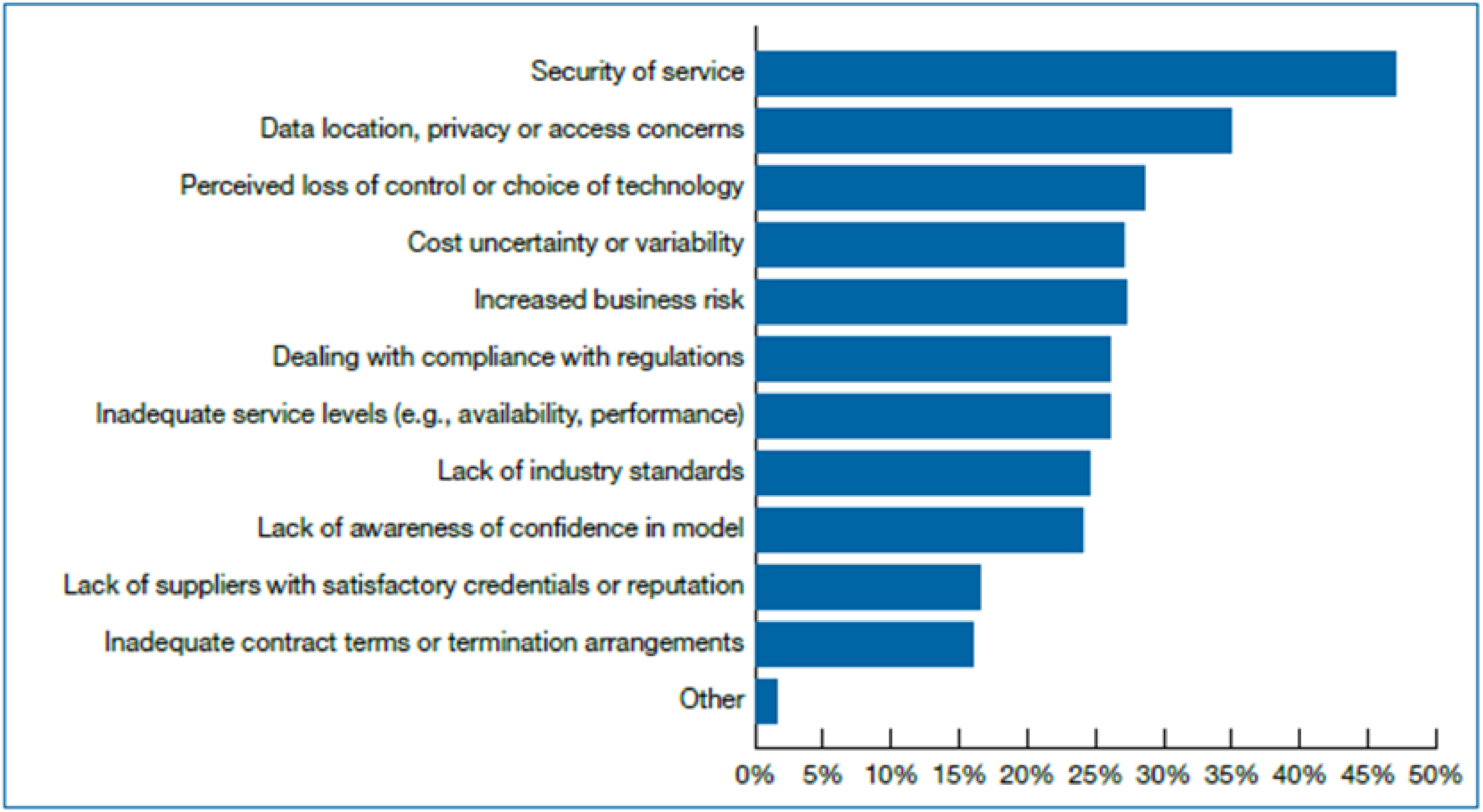
Shared network inside the firewall

Shared firewall – Lowest common denominator – less fine grained control

Easily copied machine images – who else has your server?

Shared storage – is customer segmentation secure against attack?

Top concerns in cloud computing adoption



Source: Gartner Field Survey, January – February 2010 (n=332, top 3 choices)

Who Has Control?

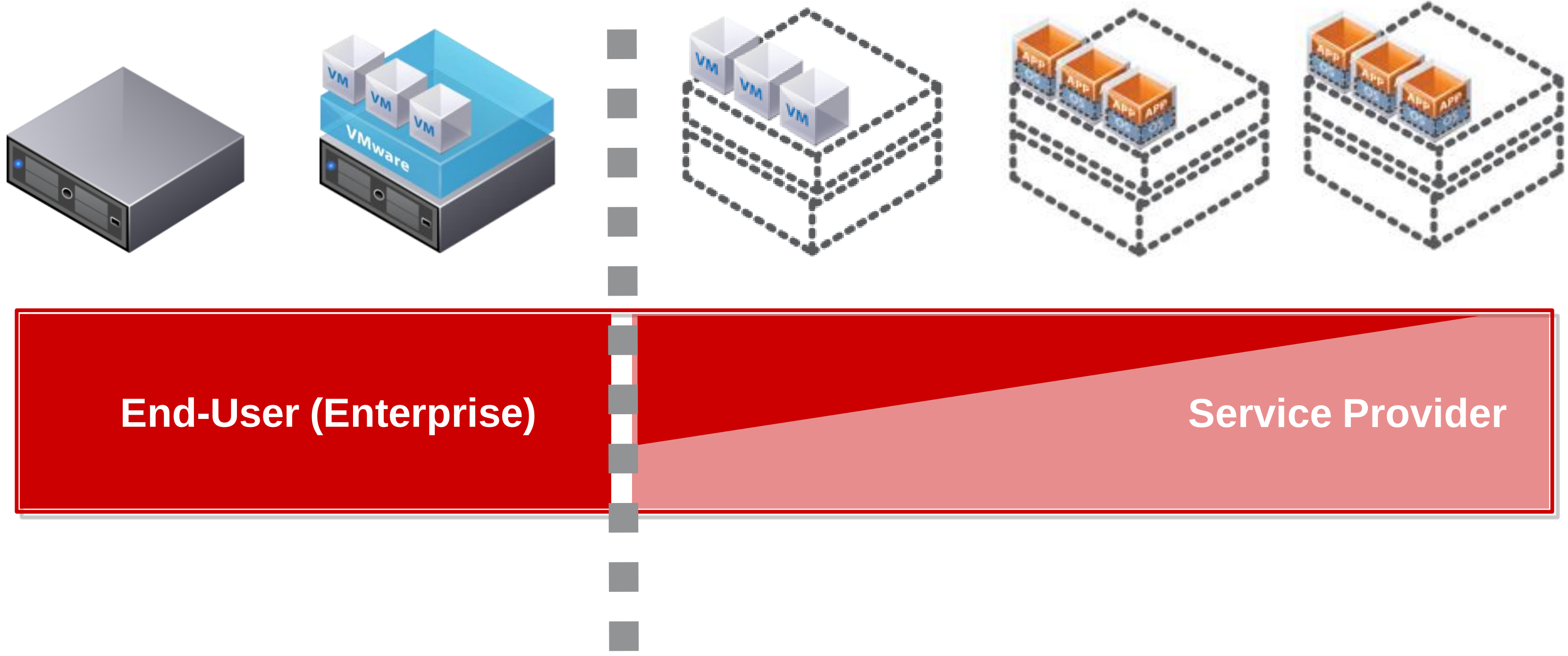
Servers

Virtualization & Private Cloud

Public Cloud IaaS

Public Cloud PaaS

Public Cloud SaaS



End-User (Enterprise)

Service Provider

Amazon Web Services™ Customer Agreement

7.2. Security. We strive to keep Your Content secure, but cannot guarantee that we will be successful at doing so, given the nature of the Internet. Accordingly, without limitation to Section 4.3 above and Section 11.5 below, you acknowledge that **you bear sole responsibility for adequate security, protection and backup of Your Content and Applications**. We strongly encourage you, where available and appropriate, to (a) **use encryption technology to protect Your Content from unauthorized access**, (b) routinely archive Your Content, and (c) keep your Applications or any software that you use or run with our Services current with the latest security patches or updates. We will have no liability to you for any unauthorized access or use, corruption, deletion, destruction or loss of any of Your Content or Applications.

http://aws.amazon.com/agreement/#7 (3 March 2010)

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:

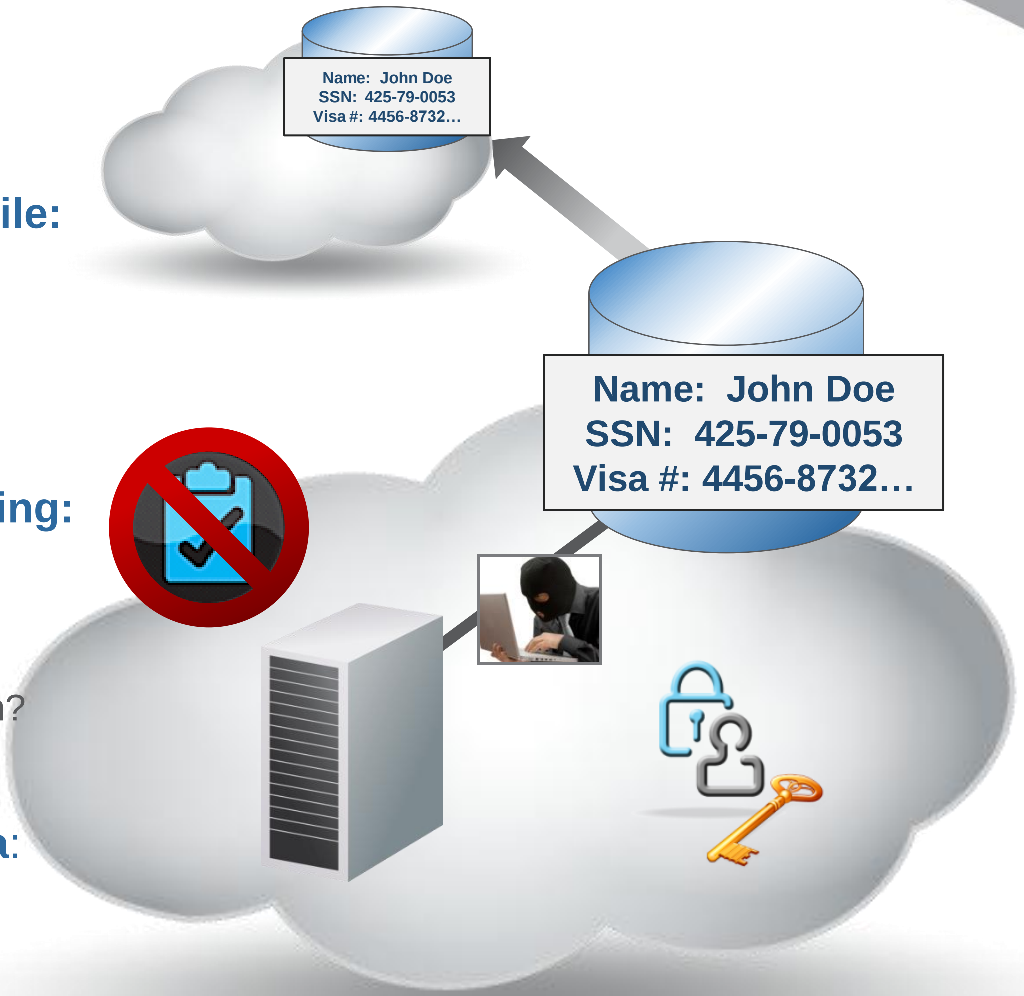
- What happened when you weren’t looking?

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…

Agenda

Cloud Computing Evolution

Security Challenges

▶ **Overall high-level architecture**

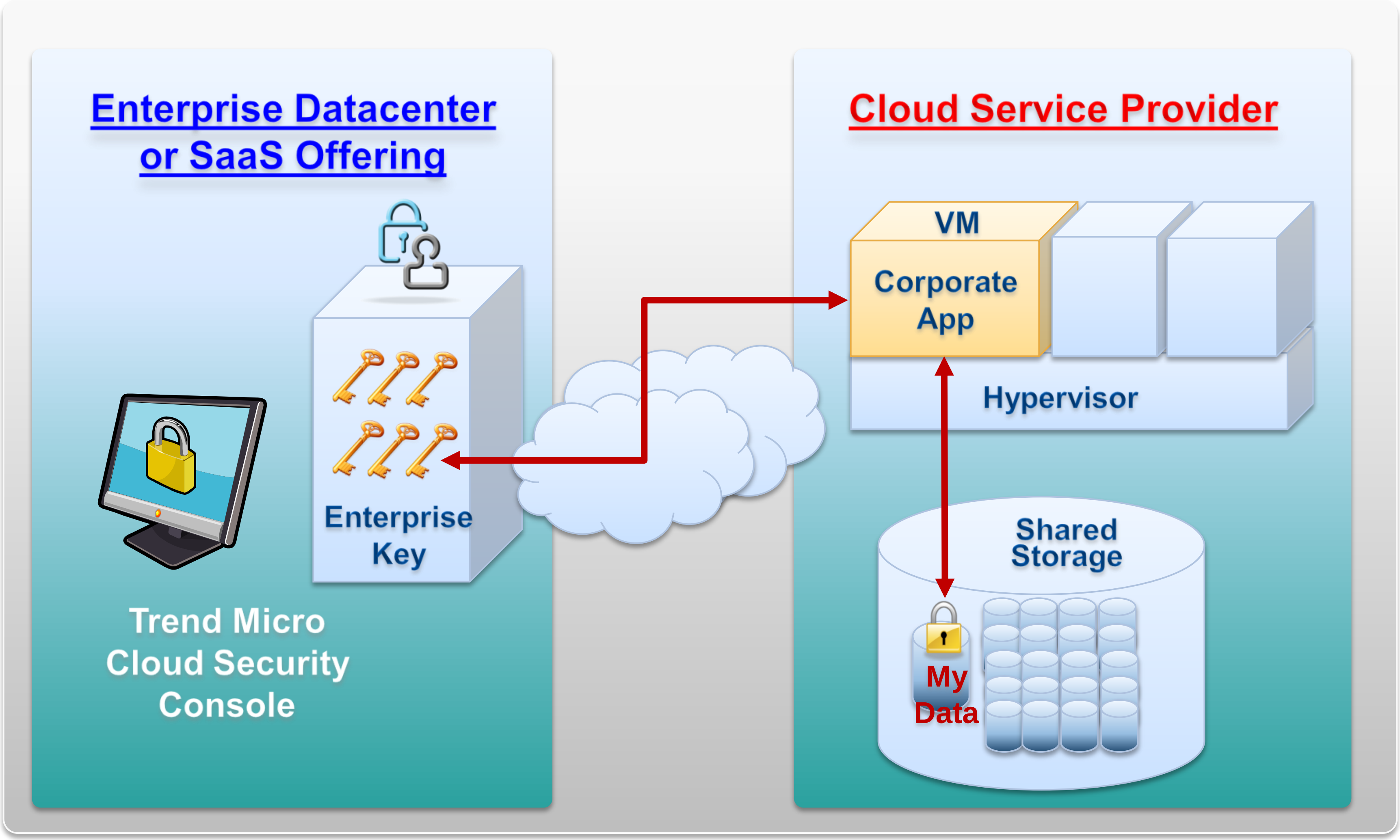
The Creative Security Solution

Deployment models & licensing

Value proposition

Roadmap

SecureCloud: Enterprise Controlled Data Protection for the Cloud



Policy-based Key Management in the Cloud

Identity

“Is it mine?”

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

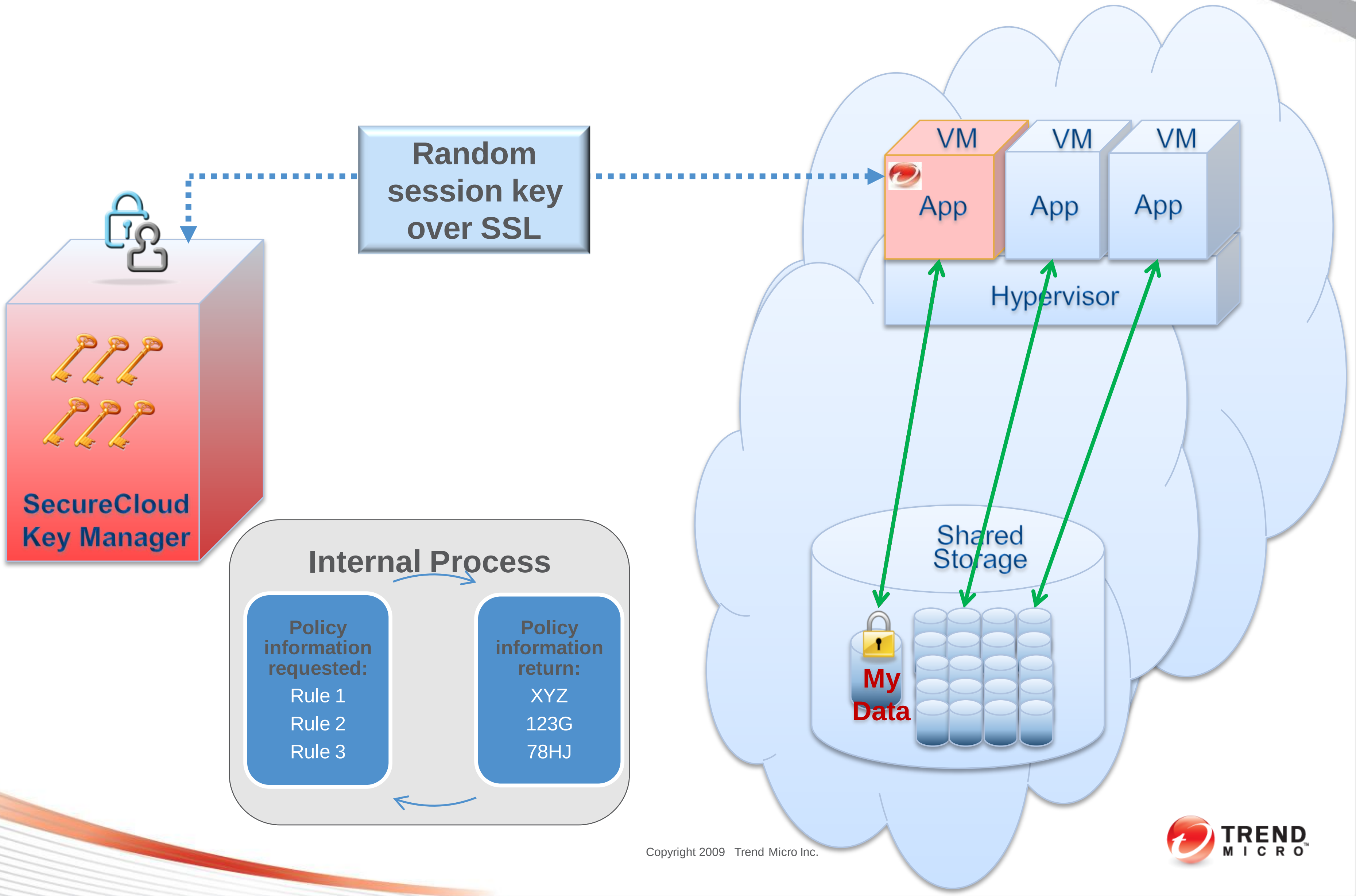
Integrity

“Is it okay?”

- Firewall
- AV
- Self integrity check
- etc

Auto or Manual rules based key approval

SecureCloud: Key exchange



Random session key over SSL

SecureCloud Key Manager

Internal Process

Policy information requested:
Rule 1
Rule 2
Rule 3

Policy information return:
XYZ
123G
78HJ

SecureCloud Protection Coverage

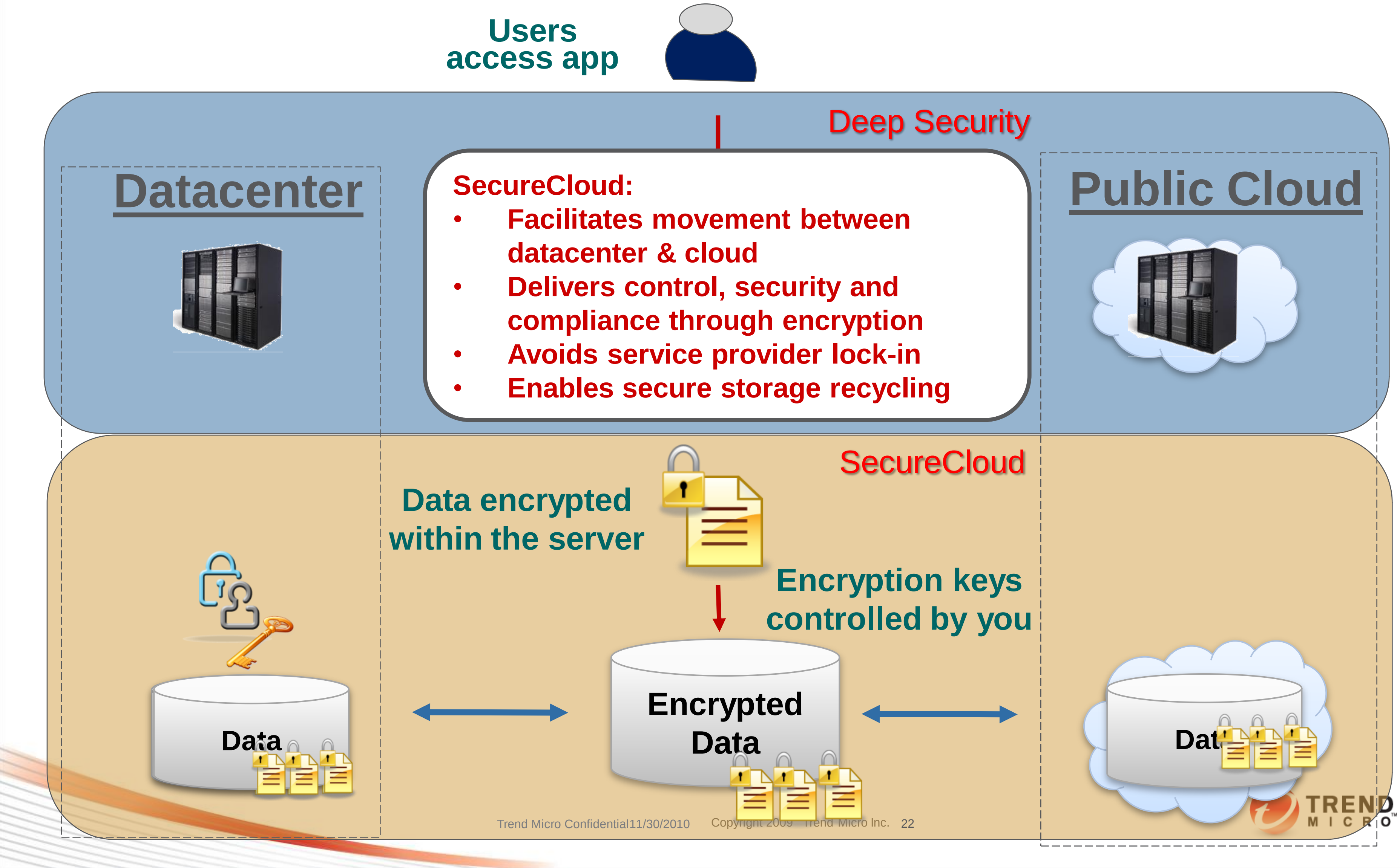
- Data at rest
  - Encrypted while stored
- Data in motion
  - Encrypted on internal network
  - Encrypted while passing through hypervisor
- Data in use
  - Data must ultimately be decrypted at the point of use
  - SecureCloud ensures that happens in a secure way… Identity & Integrity

Managing SecureCloud Data Protection (or “Where are my keys?”)

- Do It Yourself
  - Enterprise maintains control of IaaS data via on-premise enterprise console
- SaaS Alongside My IaaS
  - Enterprise obtains service via SaaS console
- Cloud Broker
  - Enterprise uses broker to manage data in multiple IaaS vendors

A New Security Architecture For A New Era

All environments should be considered un-trusted



Users access app

Deep Security

Datacenter

SecureCloud:

- Facilitates movement between datacenter & cloud
- Delivers control, security and compliance through encryption
- Avoids service provider lock-in
- Enables secure storage recycling

Public Cloud

SecureCloud

Data encrypted within the server

Encryption keys controlled by you

Data

Encrypted Data

Data

Agenda

Cloud Computing Evolution

Security Challenges

Overall high-level architecture

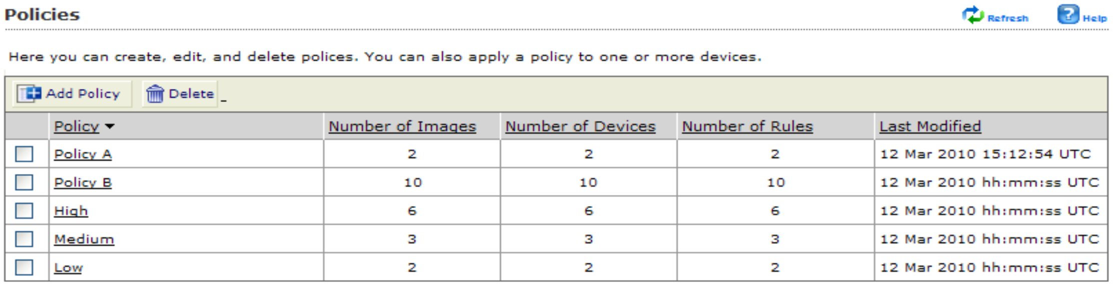
▶ **The Creative Security Solution**

Deployment models & licensing

Value proposition

Roadmap

Policy configuration

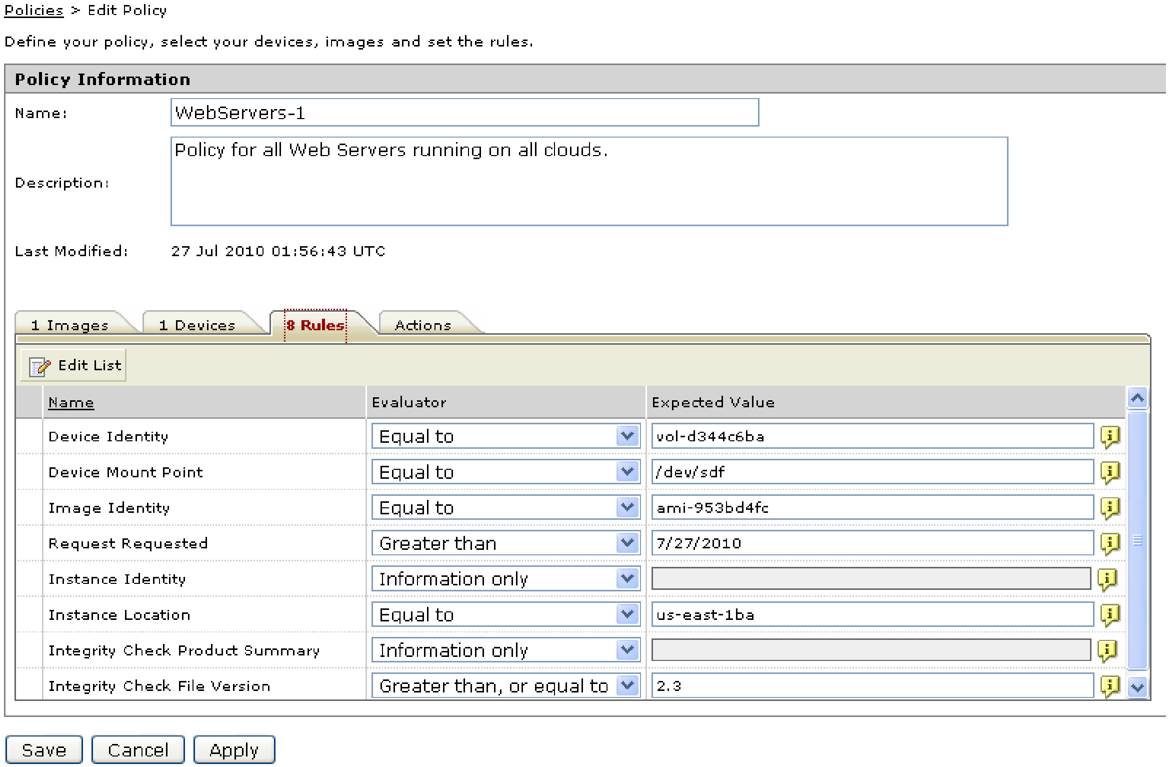


Policies

Here you can create, edit, and delete polices. You can also apply a policy to one or more devices.

	Policy ▾	Number of Images	Number of Devices	Number of Rules	Last Modified
□	Policy A	2	2	2	12 Mar 2010 15:12:54 UTC
□	Policy B	10	10	10	12 Mar 2010 hh:mm:ss UTC
□	High	6	6	6	12 Mar 2010 hh:mm:ss UTC
□	Medium	3	3	3	12 Mar 2010 hh:mm:ss UTC
□	Low	2	2	2	12 Mar 2010 hh:mm:ss UTC

- Can group multiple Images & Devices to one policy.
- Granular policies allow 1-1 mapping with devices.
  - Rules are configured based on evaluator operators.



Policies > Edit Policy

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

Policy Information

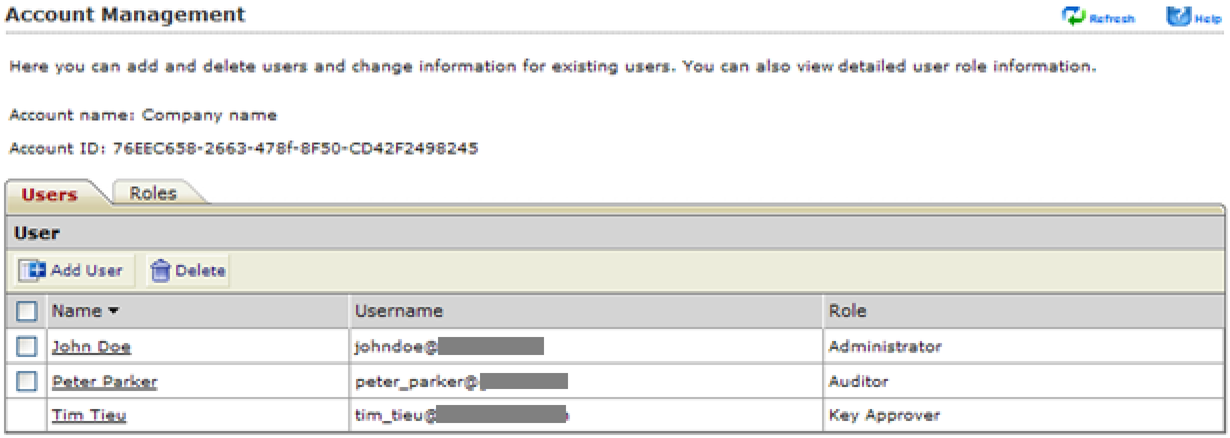
Name: WebServers-1

Description: Policy for all Web Servers running on all clouds.

Last Modified: 27 Jul 2010 01:56:43 UTC

Name	Evaluator	Expected Value
Device Identity	Equal to	vol-d344c6ba
Device Mount Point	Equal to	/dev/sdf
Image Identity	Equal to	ami-953bd4fc
Request Requested	Greater than	7/27/2010
Instance Identity	Information only	
Instance Location	Equal to	us-east-1ba
Integrity Check Product Summary	Information only	
Integrity Check File Version	Greater than, or equal to	2.3

Account management



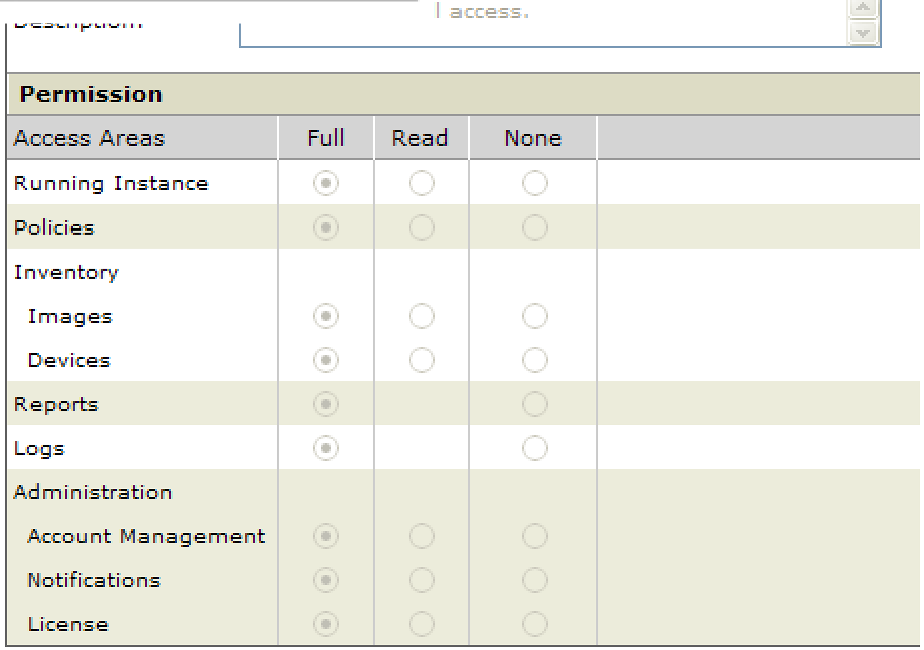
Account Management

Here you can add and delete users and change information for existing users. You can also view detailed user role information.

Account name: Company name

Account ID: 76EEC658-2663-478f-8F50-CD42F2498245

□	Name ▾	Username	Role
□	John Doe	johndoe@[redacted]	Administrator
□	Peter Parker	peter_parker@[redacted]	Auditor
	Tim Tieu	tim_tieu@[redacted]	Key Approver



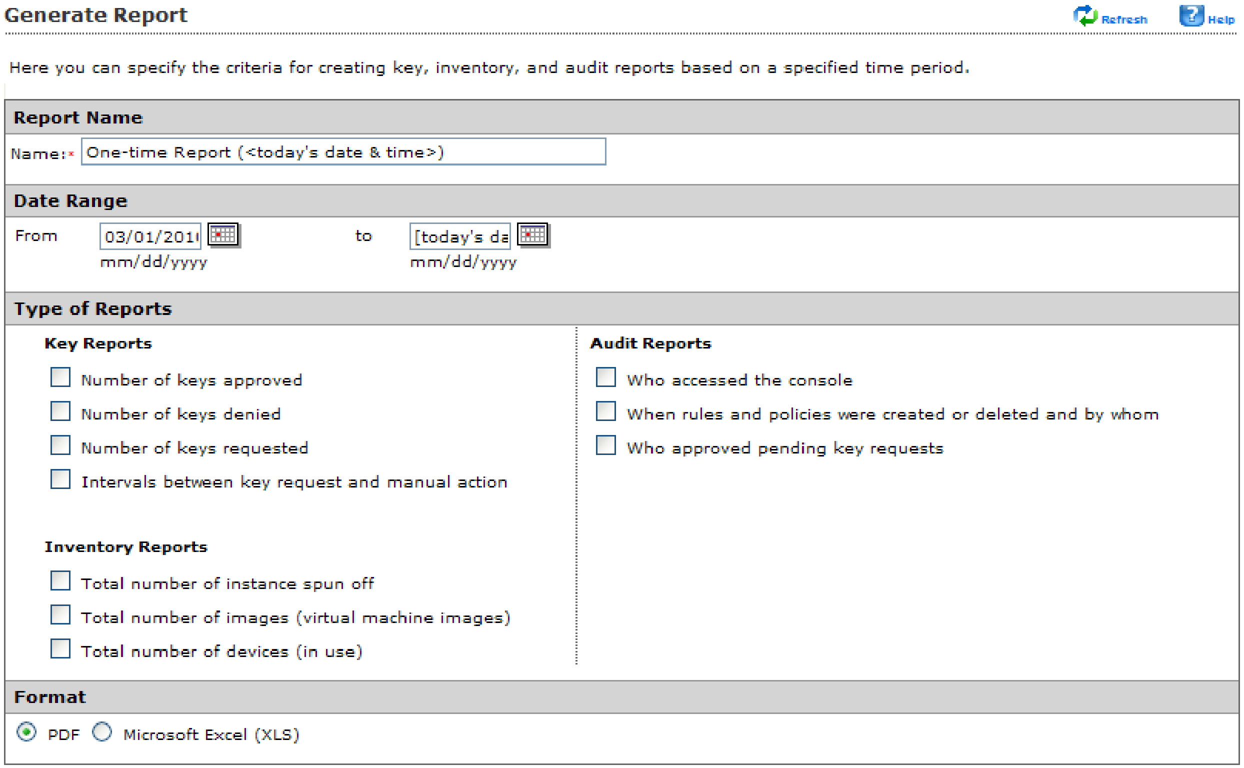
Permission

Access Areas	Full	Read	None
Running Instance	●	○	○
Policies	●	○	○
Inventory			
Images	●	○	○
Devices	●	○	○
Reports	●		○
Logs	●		○
Administration			
Account Management	●	○	○
Notifications	●	○	○
License	●	○	○

- Multi-tenancy support.
  - Role-based access.
- Built in security to avoid one account with full access.

Reporting and Auditing

- Full audit logging for: Agent, key, policy and user events.
  - Auto log archiving for rolling 12 months (SaaS).



Generate Report

Here you can specify the criteria for creating key, inventory, and audit reports based on a specified time period.

Report Name

Name:* One-time Report (<today's date & time>)

Date Range

From 03/01/201(mm/dd/yyyy to [today's da mm/dd/yyyy

Type of Reports

Key Reports

□ Number of keys approved
□ Number of keys denied
□ Number of keys requested
□ Intervals between key request and manual action

Inventory Reports

□ Total number of instance spun off
□ Total number of images (virtual machine images)
□ Total number of devices (in use)

Audit Reports

□ Who accessed the console
□ When rules and policies were created or deleted and by whom
□ Who approved pending key requests

Format

● PDF ○ Microsoft Excel (XLS)

Agenda

Cloud Computing Evolution

Security Challenges

Overall high-level architecture

The Creative Security Solution

▶ **Deployment models & licensing**

Value proposition

Roadmap

Deployment models & licensing

- v1.0
  - Software-as-a-Service
  - Hosted in TM datacenter
  - Priced by key
  - GA date: October 25, 2010

Free Trial

- v1.1 (ENT)
  - Software installer
  - Maintained in customer’s datacenter
  - Priced by perpetual license
  - Planned GA date: Feb, 2011

- v1.1 (xSP)
  - Software installer
  - Maintained in cloud service provider’s datacenter
  - Priced by key
  - Planned GA date: Feb, 2011

Agenda

Cloud Computing Evolution

Security Challenges

Overall high-level architecture

The Creative Security Solution

Deployment models & licensing

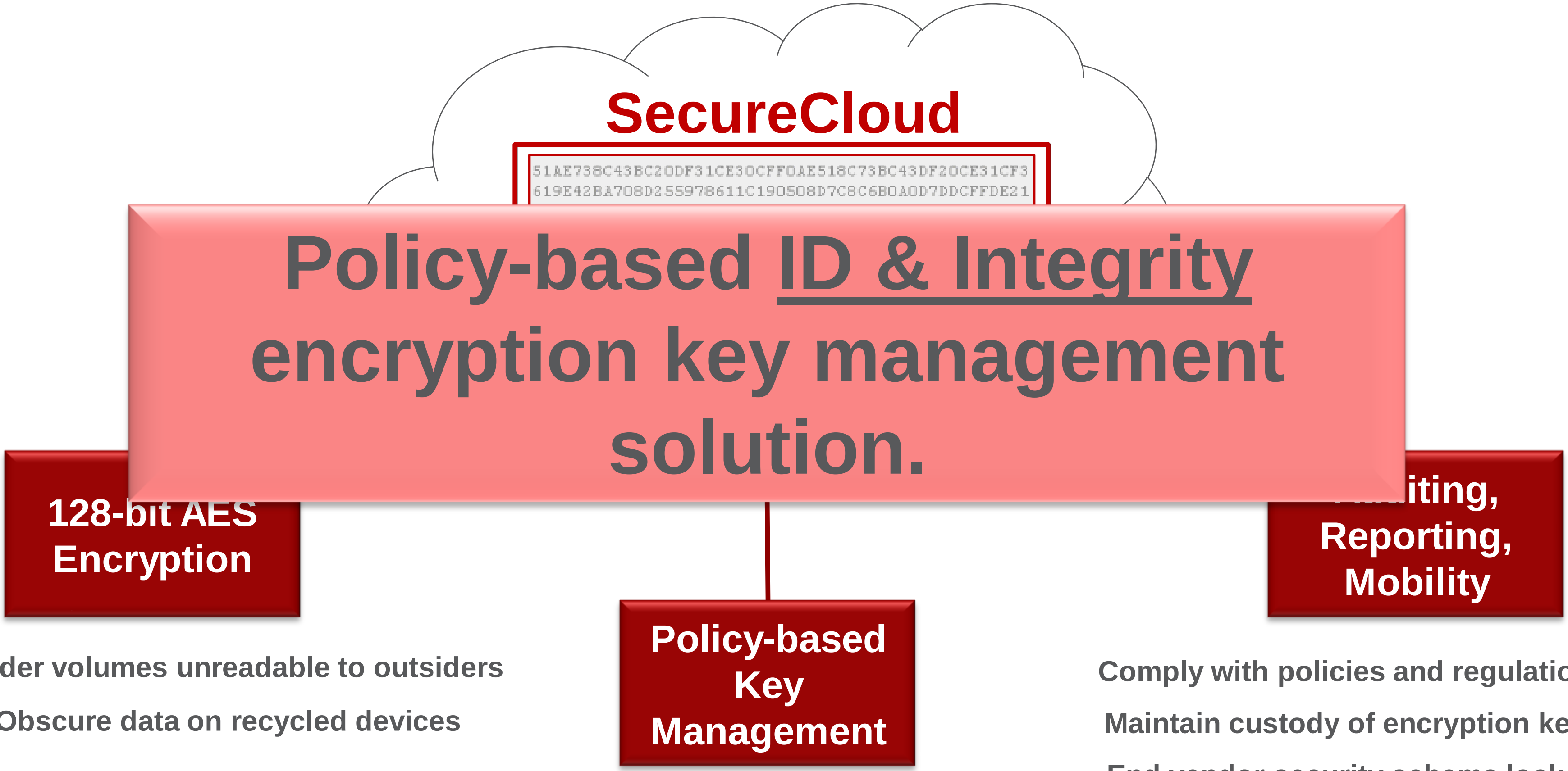
▶ **Value proposition**

Roadmap

SecureCloud Protects Enterprise Data in the Cloud

Benefit	Business Impact
Enablement	•Enables business to leverage cloud economics while protecting data
Compliance	•Enables compliance with security best practices, internal governance & external regulations for encryption of sensitive data
Control	•Control of data resides with enterprise no matter where data is located in the cloud
Business Power	•Obviates need to rely on proprietary cloud vendor security because security is controlled by the enterprise •Avoids reliance on cloud provider to “destroy” data when required by the enterprise •Minimizes legal risk for cloud provider if data is subpoenaed
Flexibility	•Enables bursting or deploying applications to cloud while maintaining adequate security

Trend Micro Protects Your Data in the Cloud


SecureCloud
51AE738C43BC20DF31CE30CFF0AE518C73BC43DF20CE31CF3
619E42BA708D255978611C190508D7C8C6B0A0D7DDCFFDE21
128-bit AES Encryption
iting, Reporting, Mobility
Policy-based Key Management

Policy-based <u>ID & Integrity</u> encryption key management solution.

Render volumes unreadable to outsiders

Obscure data on recycled devices

Ensure access given only to trusted servers

Control when and where data is accessed

Set manual or automatic key release

Comply with policies and regulations

Maintain custody of encryption keys

End vendor security schema lock-in

SecureCloud Value Proposition

Public Cloud:

- Customers:
  - Controlled data access.
  - Ensure integrity of accessing machine.
  - High value in being able to adhere to regulatory compliance (PCI).

Private Cloud:

- Customers:
  - Control of access to sensitive data through segregation.
  - Regulatory compliance (PCI) and governance controls.
  - Data protection in hosted

- Providers
  - Use SecureCloud as a differentiator & MSP opportunity.
  - Provides customer control over security & governance policies in the cloud.
  - Reduces CSP risk of litigation.
  - Allow customers to implement fine grained internal governance policies.

Agenda

Cloud Computing Evolution

Security Challenges

Overall high-level architecture

The Creative Security Solution

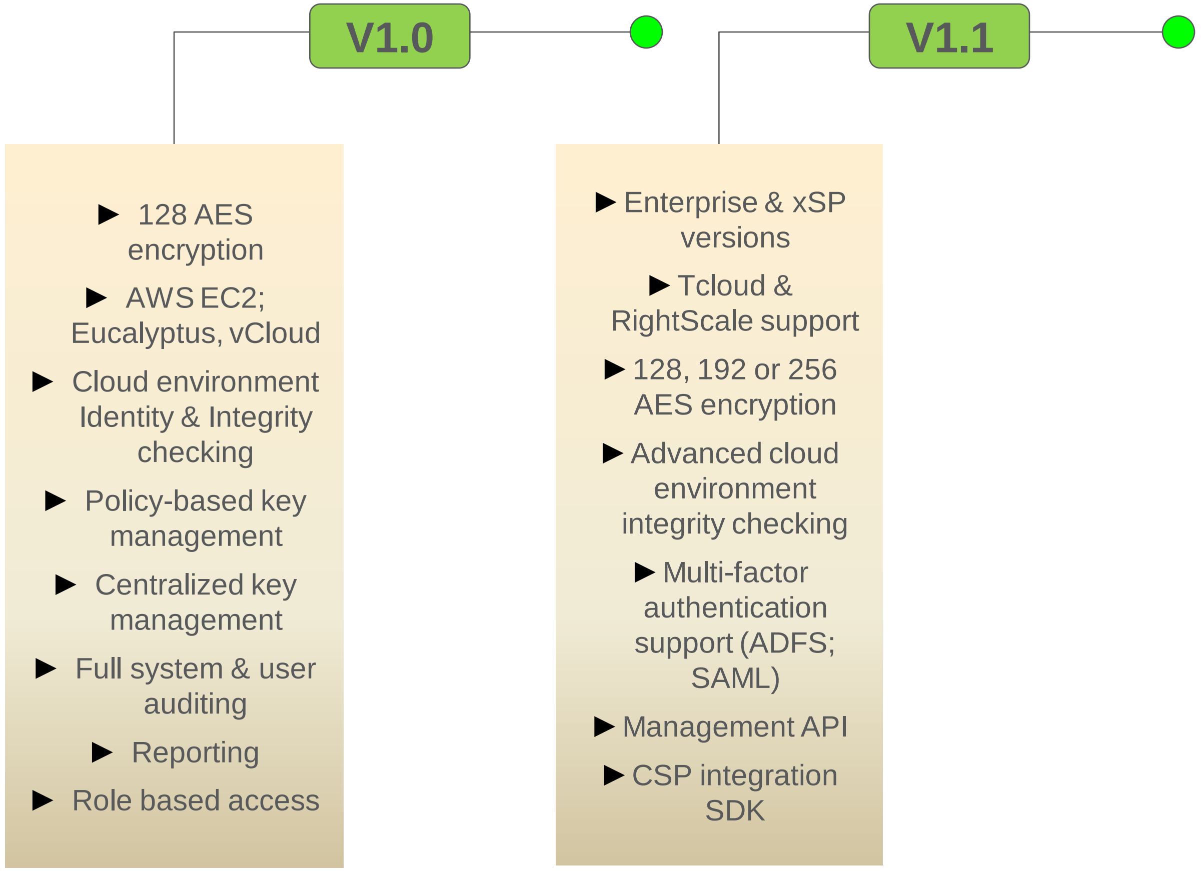
Deployment models & licensing

Value proposition

▶ **Roadmap**

SecureCloud Roadmap

Q2 10			Q3 10			Q4 10			Q1 11		
Apr	May	June	July	Aug	Sept	Oct	Nov	Dec	Jan	Feb	Mar



V1.0

- ▶ 128 AES encryption
- ▶ AWS EC2; Eucalyptus, vCloud
- ▶ Cloud environment Identity & Integrity checking
- ▶ Policy-based key management
- ▶ Centralized key management
- ▶ Full system & user auditing
- ▶ Reporting
- ▶ Role based access

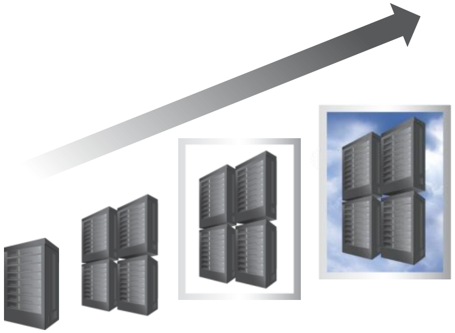
V1.1

- ▶ Enterprise & xSP versions
- ▶ Tcloud & RightScale support
- ▶ 128, 192 or 256 AES encryption
- ▶ Advanced cloud environment integrity checking
- ▶ Multi-factor authentication support (ADFS; SAML)
- ▶ Management API
- ▶ CSP integration SDK

Why Trend Micro for Cloud Security?

Future Proof

Facilitates evolution from datacenter to the cloud



Business Power

Avoids lock-in & enables portability between cloud providers

Freedom and Control

Govern your data and operate securely in the cloud

?