TREND MICRO™ | Securing Your Web World

Securing the Cloud – Technology Designed for Cloud Utilization

Dan Reis

Director Product Marketing

Agenda

- Cloud Adoption – based on the Numbers
- So, what is “The Cloud”
- The Cloud Landscape and its Data Security Challenges
- The SecureCloud Solution
  - Addressing a primary concern in Cloud Adoption

Use of "The Cloud"

- Primary customer concerns for cloud adoption: Security, Availability, Vendor Viability, Maturity
- 2010 Global Cloud Services Revenue to reach $68.3bil – 16.6% growth from 2009
- 2014 projected growth to $148.8bil
- Over the course of the next 5 years, enterprises will cumulatively spend $112bil on SaaS, PaaS and IaaS
- Economic downturn has made cloud computing more attractive
- US percentage of 2010 Global Cloud Services utilization at 60%, 50% by 2014 - translating into $74.4bil cloud revenue

Gartner – June 2010

So, What is 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.

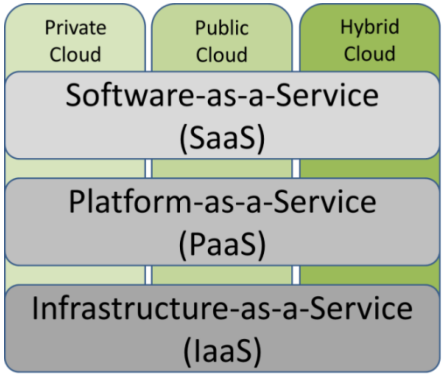
National Institute of Standards & Technology (NIST), USA

5 Key Cloud Characteristics

- Multi-tenancy
- Massively scalability
- Elasticity
- On-demand, pay per use access
- Location independence

Cloud Layers

- Three basic cloud layers: IaaS, PaaS, SaaS
  - **IaaS:** is the cloud layer in which cloud consumers have the ability to provision virtual servers, storage, networks, and other fundamental computing resources
  - **PaaS:** provides a development platform, sandbox and management system to develop, and in some cases, sell the applications that will be operated in the cloud.
  - **SaaS:** capability for a consumer to use the provider's applications running on a cloud infrastructure.


Private Cloud
Public Cloud
Hybrid Cloud
Software-as-a-Service (SaaS)
Platform-as-a-Service (PaaS)
Infrastructure-as-a-Service (IaaS)

Cloud – Where is It?

- This depends where the cloud abstraction layer is relative to the user's data center
- Three different deployments models:
  - Public Cloud: cloud service provider hosts cloud environment and rents resources to the general public
    - Think Amazon Amazon EC2, GoGrid, Rackspace, Savvis
  - Private Cloud: either internal to the customer's data center or hosted by another provider – but resources are dedicated to a single, defined entity
    - Think Vmware vCloud, Rackspace,
  - Hybrid Cloud: joining public and private clouds to take advantage the near infinite, instant-on resources offered by the public cloud without long procurement and provisioning cycles
    - Think Eucalyptus, RightScale

Why the Cloud Matters

Speed and Business Impact

Expertise and Performance

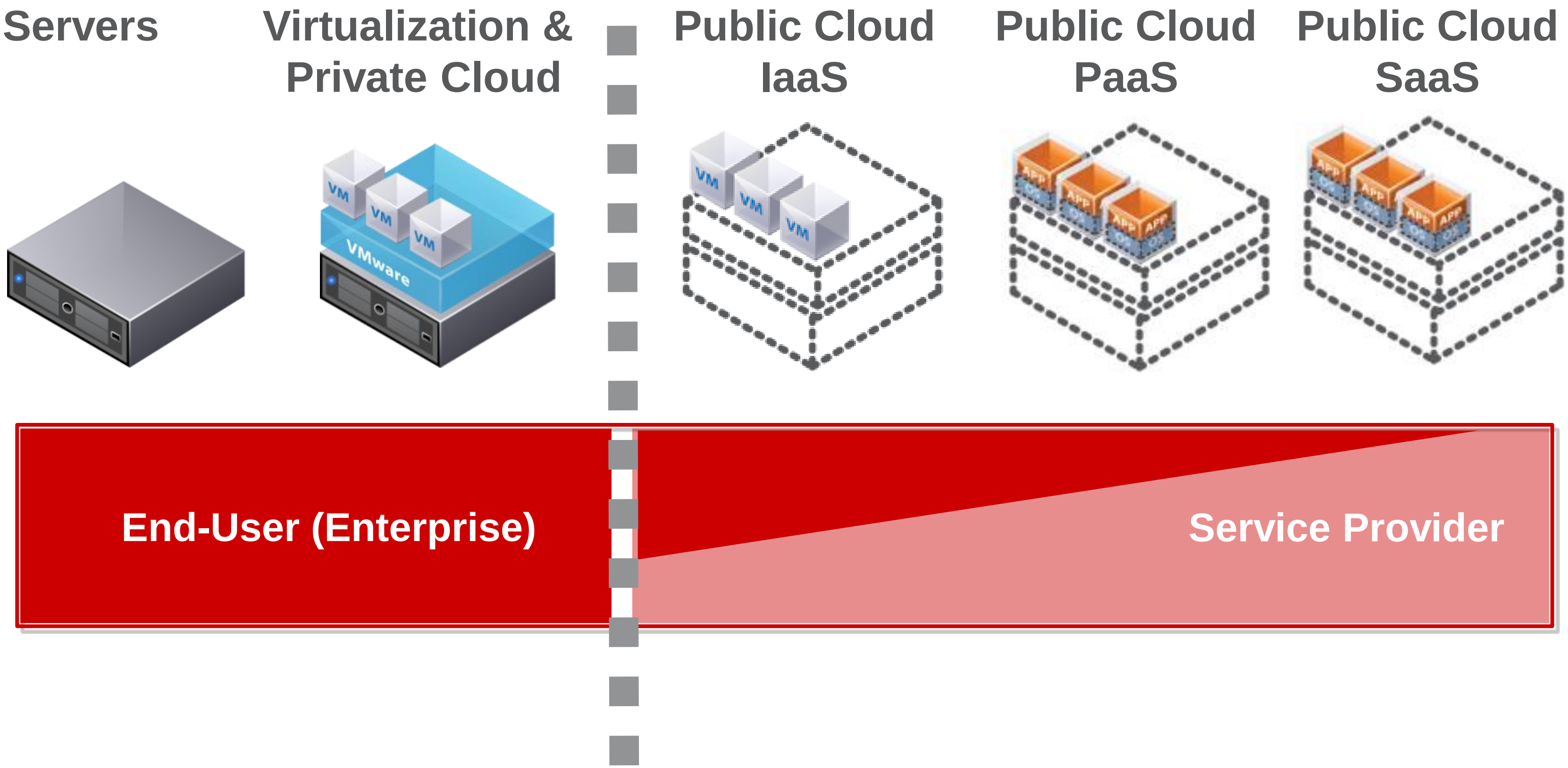
Significant Cost Reduction

1) The Cloud Imperative… If by mid-year you have not developed and begun to execute upon an ambitious and enterprise-wide cloud strategy, then by year-end the odds are good you'll no longer be a CIO.

“Global CIO: The Top 10 CIO Issues For 2010” *InformationWeek, 21 December 2009*

The Clouds Challenge for Data Security

Who Has Control?



Servers

Virtualization & Private Cloud

Public Cloud IaaS

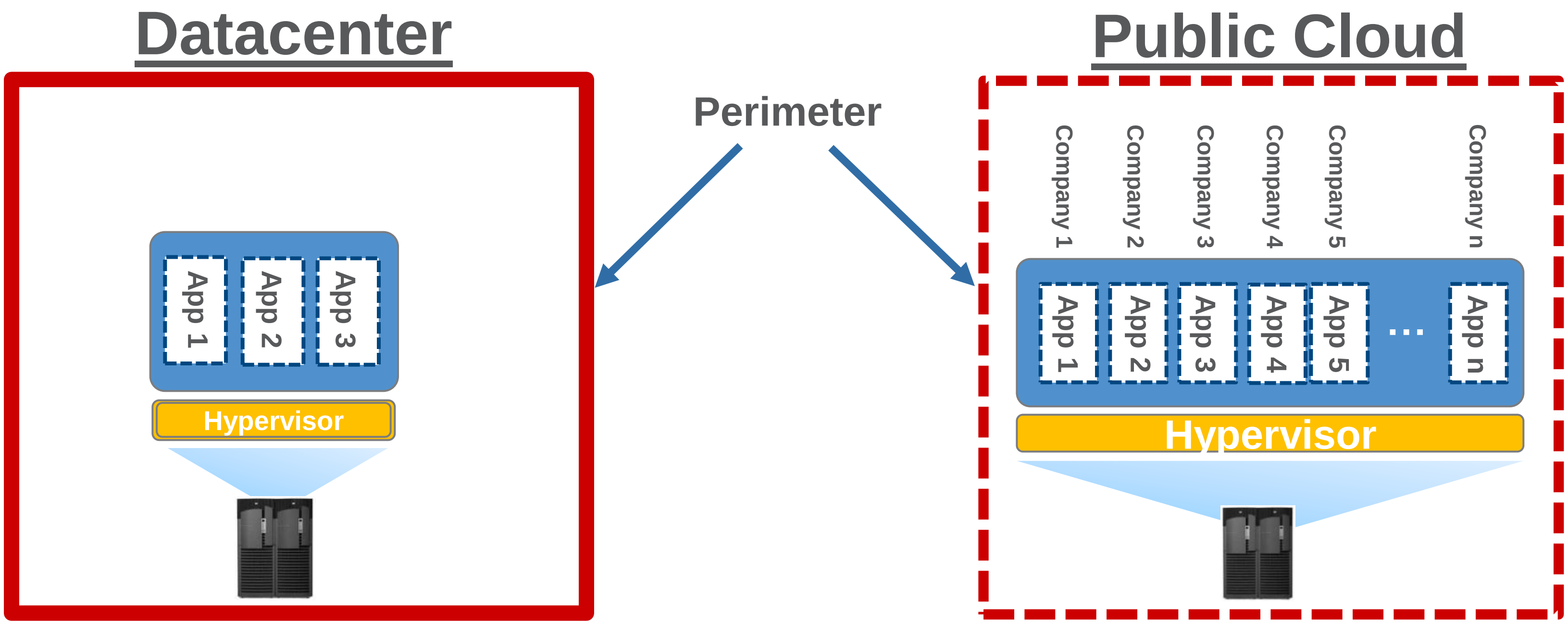
Public Cloud PaaS

Public Cloud SaaS

End-User (Enterprise)

Service Provider

The Challenge of Securing Data



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

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:

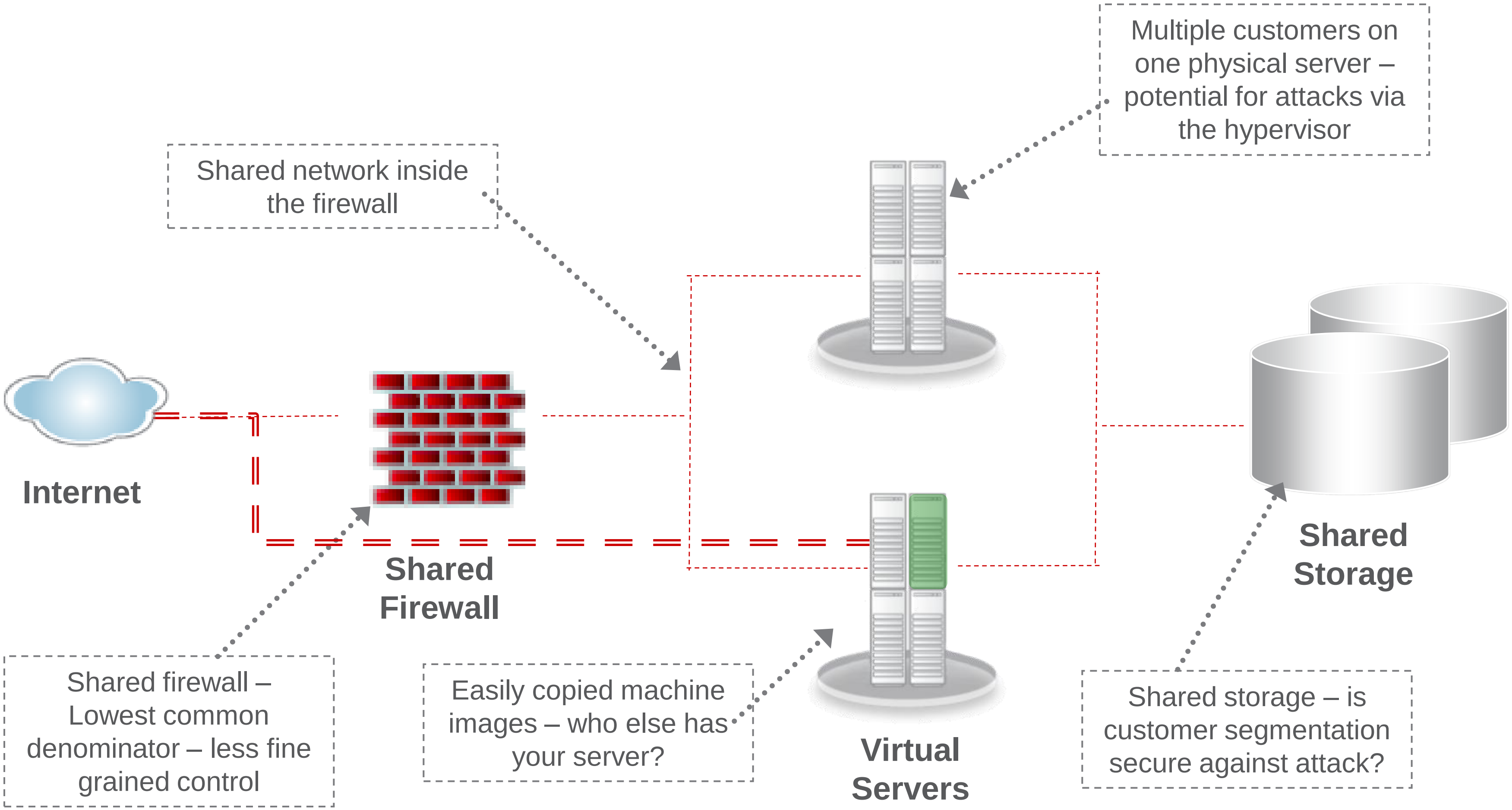
- Are you locked into a single security solution? Who has access to your keys?

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…

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?

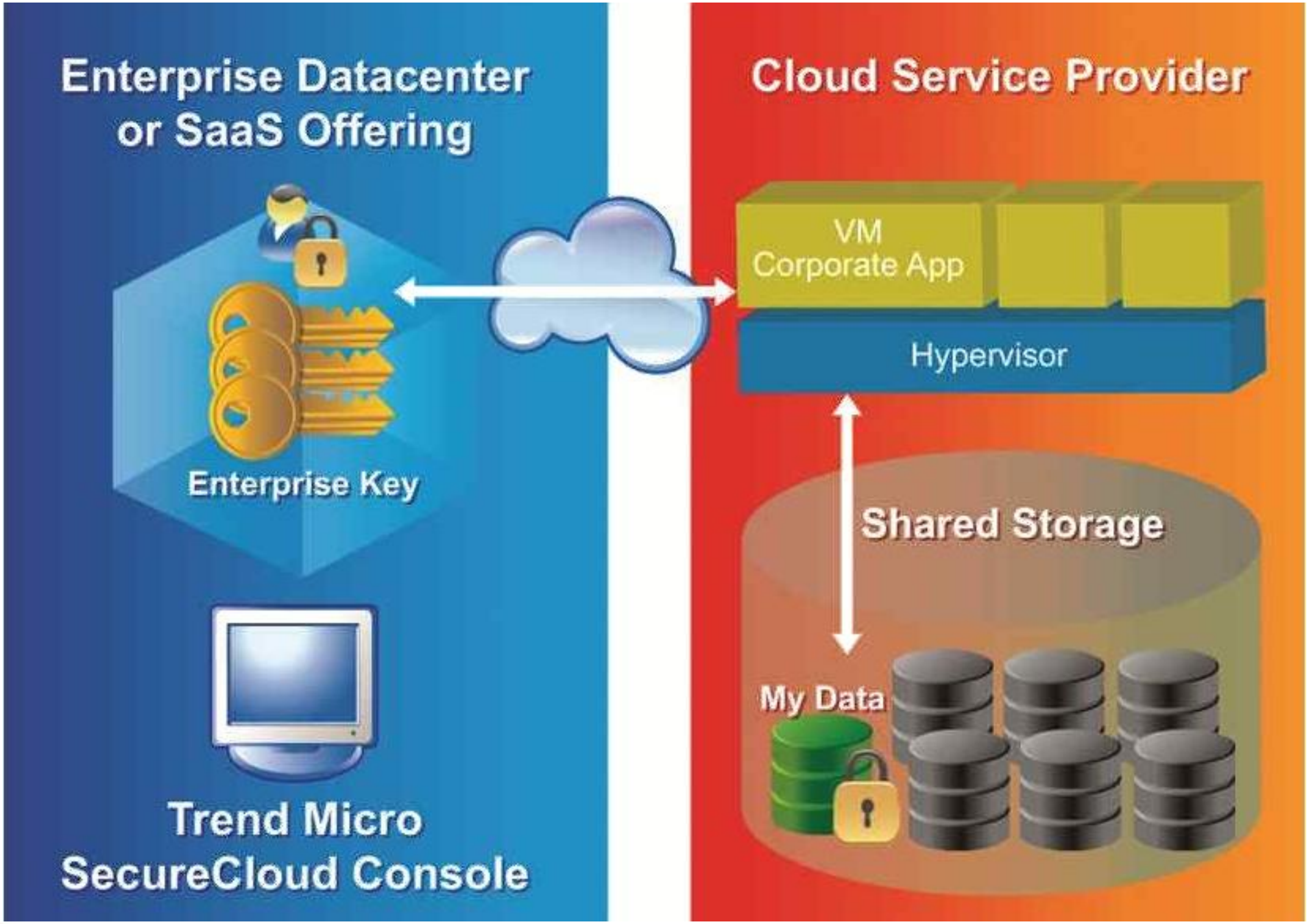
Shared storage – is customer segmentation secure against attack?

Addressing the Security Challenges of the Cloud

What Should a Cloud Solution Do?

- **Control -** Allow businesses to encrypt and control data in public and private cloud environments via simple policy-based key management, to give businesses power over how and where data is accessed and greatly reduces the complexity inherent in traditional key management solutions.
- **For the Public Cloud:** *(Amazon.com or Terremark)*
  - Safely leverage operational and cost efficiencies of cloud computing
  - Control access to data in shared public cloud environments
  - Additional safety by authenticating virtual servers
- **For the Private Cloud:** *(vCloud in customer's data center)*
  - Segregation of sensitive data stored in internal shared storage
  - Greater ability to achieve compliance with regulations and best practices

How it Works


Enterprise Datacenter or SaaS Offering
Enterprise Key
Trend Micro SecureCloud Console
Cloud Service Provider
VM Corporate App
Hypervisor
Shared Storage
My Data

The Basics: What Should Cloud Security Do?

- **Encrypt** data in public or private cloud environments
  - Industry standard AES encryption (128, 192 or 256-bit keys)
- **Manage** encryption keys
  - Typically a very tedious, detailed and expensive activity
  - Management happens either in Trend's data center or in customer's
- **Authenticate** 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
- **Audit**, alerts, and reports on key delivery activities
  - Multiple reports and alerting mechanisms available

Data Encryption

- **Protect** customer from data breaches because info is now unreadable to anyone without access to encryption keys
  - Includes external storage administrators employed by cloud vendors or internal customer employees
- **Segregate** sensitive information from less important data
  - Important in private cloud environments – mitigates insider threat
- **Virtually destroy** information in the cloud
  - Unruly, nomadic information no longer a concern
- **Enable compliance** with various data regulations
  - HIPAA, HITECH, SOX, PCI – DSS, EU Data Privacy Directive…

Encryption Key Management

- **Simplify** key management by providing a simple, easy to use – easy to deploy - key delivery system
- **Reduce** costs complexity with hosted system
- **Security** enhanced by controlling and keeping keys within customer’s physical data center
- **Separation of duties** is established through different user roles set by key administrator

Server Authentication

- **Verifie** the identity of virtual machines requesting encryption keys through a series of user defined policies
  - Know when and from where your requests are coming
- **Dictate** when and where VMs receive keys and access data
  - Important to ensure geographic or chronologic rules mandates are followed
- **Protect** by adding an additional layer of security before keys are released and data unlocked

Auditing, Reporting and Alerting

- **Accountability** is set for all key request and release activities
  - Know when and from where your requests are coming
- **Audit trail** is established to comply with external regulations and security best practices
- **Notification** of key deployment activities and requests speeds time-to-resolution when problems occur

So, Now what is there to worry about?

Use of encryption is rare:

- Now only authorized servers can read data!

Virtual volumes and servers are mobile:

- Policies only allow access in authorized areas!

Rogue servers might access data:

- Yes – but the information is unreadable and safe!

Rich audit and alerting modules lacking:

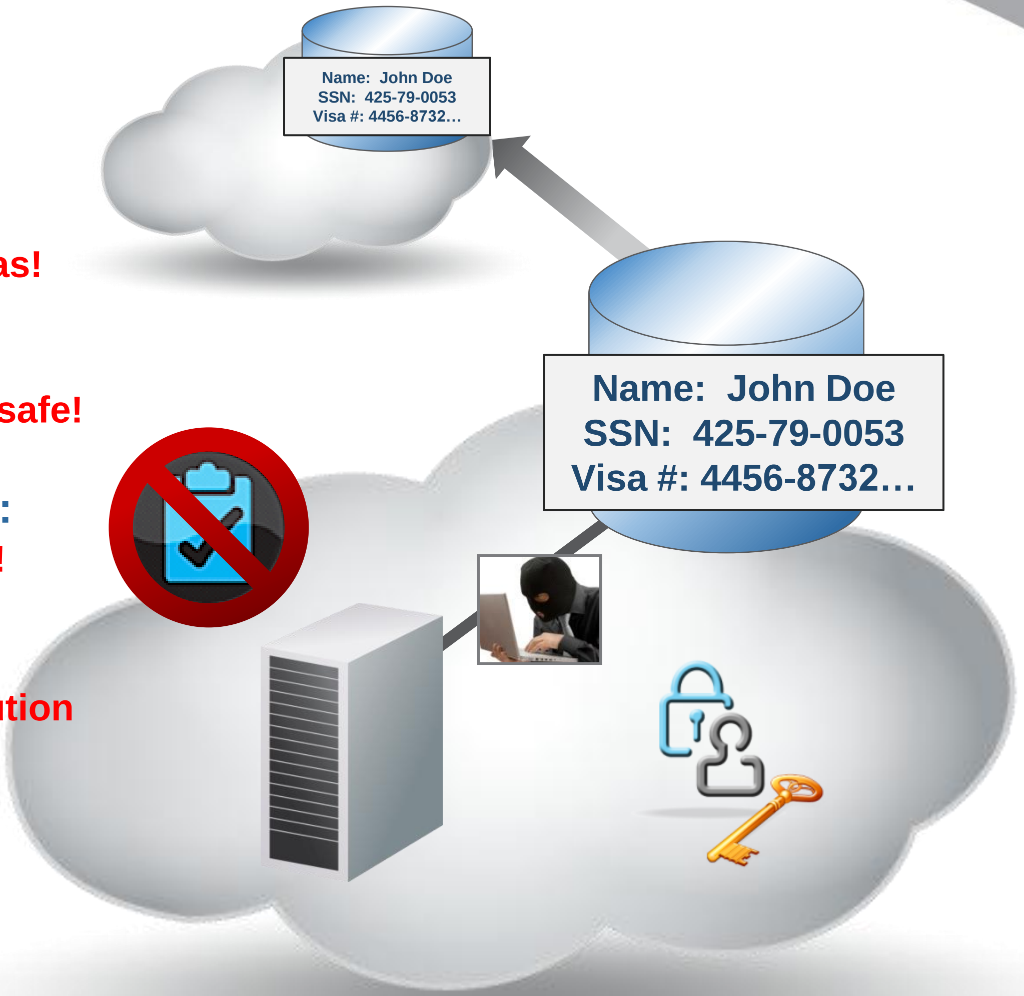
- Now we have reports, alerts and audit trails!

Encryption keys remain with vendor:

- No vendor lock-in since customer owns solution
- Customer decides where keys are stored!

Virtual volumes contain residual data:

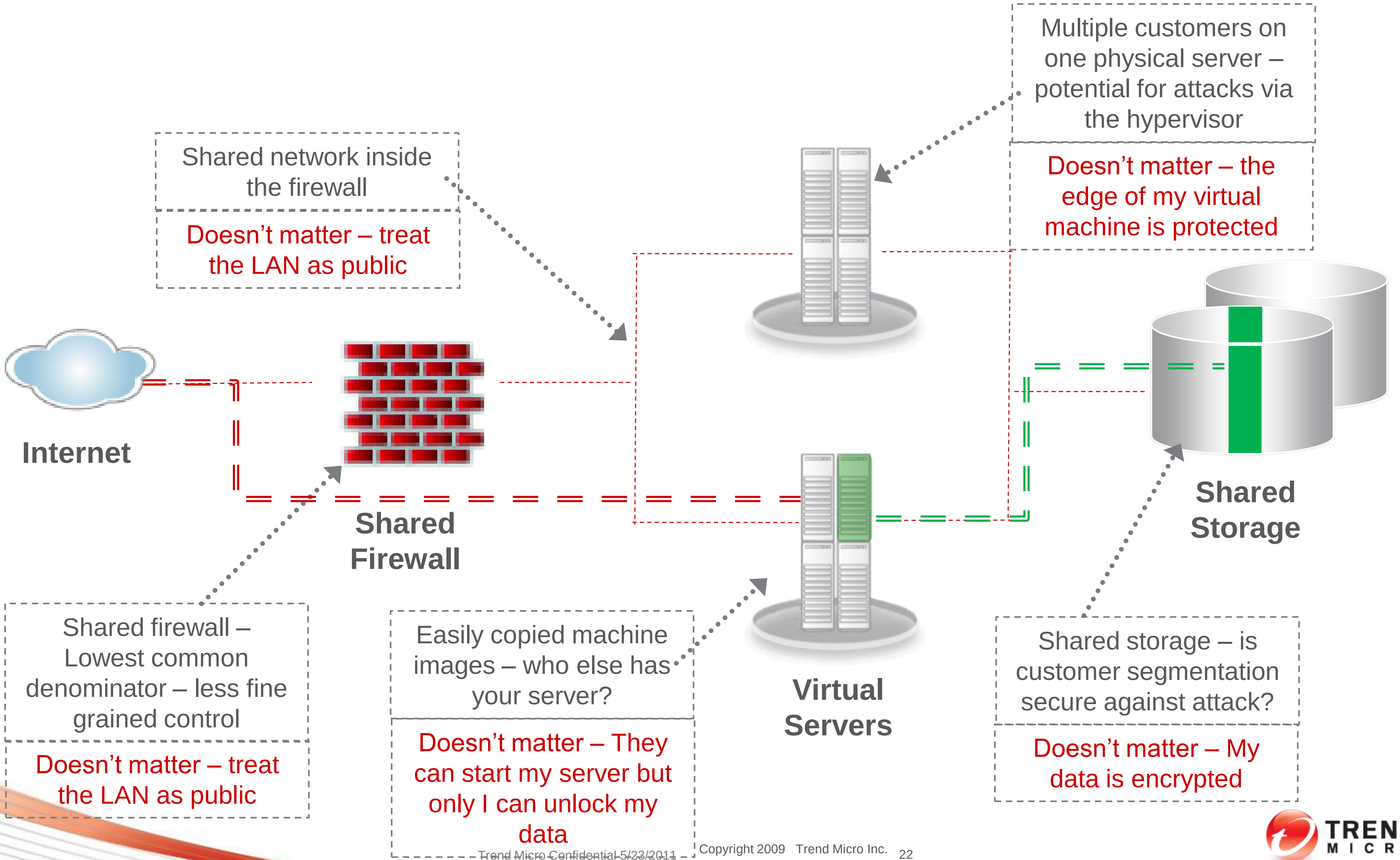
- Doesn't matter – disks are unreadable!



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

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

Challenges for Public Cloud: The Private Security Answer



Shared network inside the firewall

Doesn't matter – treat the LAN as public

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

Doesn't matter – the edge of my virtual machine is protected

Shared firewall – Lowest common denominator – less fine grained control

Doesn't matter – treat the LAN as public

Easily copied machine images – who else has your server?

Doesn't matter – They can start my server but only I can unlock my data

Shared storage – is customer segmentation secure against attack?

Doesn't matter – My data is encrypted

Protecting 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
Flexibility	•Enables bursting or deploying applications to cloud while maintaining adequate security

In the Cloud Data Security

- 128 or 256-bit AES encryption
- Policy-based key delivery
  - Automated for fast operations or manual when extra control is needed
  - Controls how and where data can be accessed by authenticating virtual servers to storage volumes
- Centralized key management
  - SaaS or on-premise delivery models (on-premise in later version)
  - SaaS (hosted) reduces administrative and maintenance costs.
  - On-premise increases control and ensures custody of encryption keys
- Audit, alerting and reporting functionalities
  - Records user activity, key use and requests, virtual machine operations, encryption information and more

In the Cloud Data Security

- Key Management
  - Not just encryption: unique in the way it manages keys and its environment
  - Excellent compliment to Deep Security
- Industry standard encryption
  - Makes data unreadable without encryption keys
  - Greatly reduces the risks of data theft, unauthorized data disclosure or data modification
- Control of encryption keys
  - Know exactly where your keys are at all times
  - Vendor administrators with powerful rights unable to see information
  - Not subjected to lock-in with cloud vendor’s encryption system
  - Governments can no longer seize data without your knowledge

In the Cloud Data Security

- Secure Storage recycling
  - Residual data left on storage devices is unreadable after volumes are terminated
- Auditing and logging functions
  - Helps ensure compliance with regulations, policies and best practices
  - Reduces work required for external or internal investigations
  - Creates accountability and helps manage system resources
- Automated policy-based key management
  - Determines which virtual servers access data
  - Imposes security requirements and location constraints on VMs
  - Reduces the likelihood of malware infection, system cloning and server modifications

TREND MICRO | Securing Your Web World

Thank You!

Dan Reis dan_reis@trendmicro.com

Director Regional Product Marketing