AWS re:Invent

How to Meet Strict Security Compliance Requirements in the Cloud

JD Sherry, VP Technology & Solutions, Trend Micro

Mark Nunnikhoven, Principal Engineer, Cloud & Emerging Technologies, Trend Micro

November 13, 2013

Enterprises & the Cloud

- Security & compliance are top priorities for enterprises, regardless of where things are deployed

- Many organizations recognize the benefits of the cloud – and need to understand security requirements

Enterprises & the Cloud

- Data sovereignty

- Multi-tenancy

- Compliance

76% indicated they had compliance or data confidentiality requirements

Source: Trend Micro survey, May 2013

PCI Requirements as a Reference …

February, 2013

NEW

PCI Security Standards Council

Standard: PCI Data Security Standard (PCI DSS)
Version: 2.0
Date: February 2013
Author: Cloud Special Interest Group
PCI Security Standards Council

Information Supplement:
PCI DSS Cloud Computing Guidelines

	Client
	CSP

Cloud Layer	Service Models		
	IaaS	PaaS	SaaS
Data			
Interfaces (APIs, GUIs)			
Applications	You!		
Solution Stack (Programming languages)			
Operating Systems (OS)			
Virtual Machines			
Virtual network infrastructure			
Hypervisors			
Processing and Memory			
Data Storage (hard drives, removable disks, backups, etc.)	amazon web services		
Network (interfaces and devices, communications infrastructure)			
Physical facilities / data centers			

Shared responsibility

- Facilities
- Physical Security
- Physical Infrastructure
- Network Infrastructure
- Virtualization Infrastructure

- Operating System
- Application
- Account Management
- Security Groups
- Network Configuration

Deep Security

Deep Security Manager

Amazon EC2 instances

Centralized security control management

Technical details

Unified management interface for multiple regions/credentials
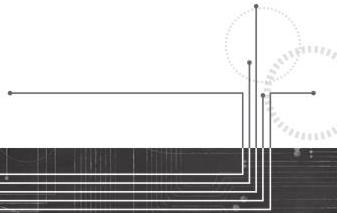
Simplified policy management across the organization

Broad platform support

Agent provides protection on the Amazon EC2 instance

Your needs

Helps address compliance challenges

Enforces security policy within your organization

Managing another binary

Flexible deployment to fit any situation

Deploy via user-data, Chef, Puppet, SSH/PowerShell, etc.

Install the agent in an AMI and activate on demand

Keeping up to date

Agent updates via Deep Security, no extra tools needed

Demo – User-data deployment

Demo – Manager-initiated activation

Being aware of assets in AWS

Deep AWS integration

AWS cloud connector automatically polls region

Automate security actions for new instances

Full visibility of unprotected instances

Keeping up to date

Connector syncs regularly for constant awareness

Demo – Automated decision making

Deep Security + SecureCloud

Deep Security Manager

SecureCloud

Amazon EC2 instances

Full disk encryption

Technical details

Intelligent block level encrypted

Used AES-256 cipher from FIPS 140-2 certified library
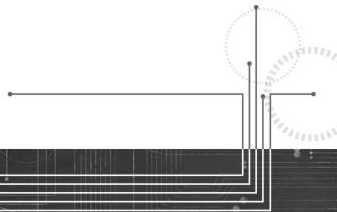
Broad platform support

Agent provides protection on the Amazon EC2 instance

Your needs

Helps address compliance challenges

Enforces security policy within your organization

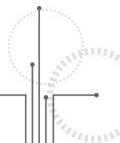# Preventing unauthorized access to data

Deep AWS integration

Leverage AWS metadata for key management policies

Boot-volume encryption for Windows & Linux

Keeping up to date

Integrity check regularly validates encryption policy

Demo – Advanced key release policy

Session Summary

Meet strict security and compliance requirements with a security solution that is:

- **Smart:** Automatically apply security controls

- **Simple:** Manage through a single console with reporting and alerting

- **Security that fits:** Embed security into your cloud architecture

Learn about Trend Micro at AWS re:Invent

- **Join us at our booth to meet R&D experts and see in-depth product demo**

- **SEC 309: Learn How Trend Micro Used AWS to Build their Enterprise Security Offering (Deep Security as a Service)**
  - **Thursday 11 am - noon**

Try out Trend Micro today!

- **Test Drive: aws.amazon.com/testdrive**
- **Free Trials:**
  - **DeepSecurity.TrendMicro.com**
  - **Webappsecurity.trendmicro.com**
  - **securecloud.com**