

Improving Systems Security, Virtualization and Applications

Dave Vijzelman

CA Technologies

Principal Solution Strategist Security



why control privileged users?

IT Worker Indicted For Setting Malware Bomb At Fannie Mae

IT contractor deployed highly malicious script before his administrative rights were terminated

48% of internal breaches are from privileged user misuse; a 26% increase from the prior year

Source: Verizon 2010 Data Breach Report

Ex-TSA Employee Indicted For Tampering With Database Of Terrorist Suspects

Case serves as a wake-up call about the potential dangers of malicious insider access to sensitive data

Google fired engineer for privacy breach

by Tom Kraatz

Font size Print E-mail Share

Google confirmed on Tuesday that it fired an employee earlier this year for violating its policies on accessing the accounts of its users.

Former Gucci Employee Indicted for IT Rampage

A network engineer at Gucci America was indicted on charges of illegally accessing the company's network and deleting documents shortly after he was fired. His IT rampage cost Gucci an estimated \$200,000 in lost sales, diminished productivity, restoration and remediation expenses.

Sam Chihlung Yin was charged on April 4 with 50 counts, including computer tampering, identity theft, falsifying business records, computer trespass, criminal possession of computer-related material, unlawful duplication of computer-related material and unauthorized use of a computer. The charges carry penalties of up to 15 years in prison.



challenges

membership has its privileges and consequences

Privileged Users

- All **POWERFUL ACCESS** to resources
- Typically a **SHARED ACCOUNT** – lack **ACCOUNTABILITY**
- **NO SEGREGATION** of duties
- Poor **LOG INTEGRITY**
- **Lack of TRANSPARENCY** on access
- **VIRTUALIZATION and CLOUD** amplify the challenges by introducing virtualization admins

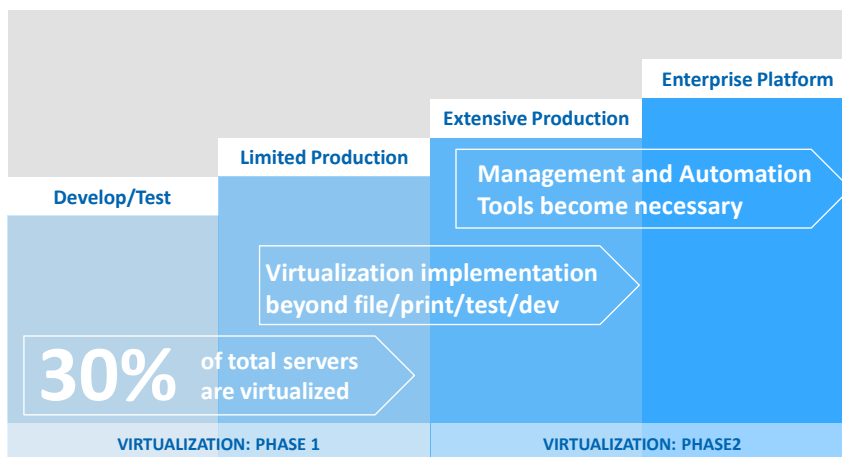


3 Copyright (c) 2011 CA. All rights reserved. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. CA confidential and proprietary. No unauthorized copying or distribution permitted.



virtualization today

management “tipping points”



The 451 Group; “Virtualization Survey Results”; January 2010

4 Copyright © 2011 CA. All rights reserved. CA confidential and proprietary information for CA internal use only. No unauthorized copying or distribution permitted.



situation

“By 2015, 40% of the security controls used within enterprise data centers will be virtualized, up from less than 5% in 2010.”¹

“There will be more virtual machines deployed on servers during 2011 than in 2001 through 2009 combined”²

¹Gartner; “From Secure Virtualization to Secure Private Clouds”; Neil MacDonald & Thomas J. Bittman; 13 October 2010

²Gartner; “Q&A: Six Misconceptions About Server Virtualization”, Thomas J. Bittman; 29 July 2010

5

Copyright © 2011 CA. All rights reserved. CA confidential and proprietary information for CA internal use only. No unauthorized copying or distribution permitted.



virtualization platform effects on security



Abstraction and Consolidation

- ↑ Capital and Operational Cost Savings
- ↓ New infrastructure layer to be secured and subject to compliance
- ↓ Greater impact of attack or misconfiguration



Faster Deployment in Shared Environment

- ↑ IT responsiveness
- ↓ Inconsistencies in configuration
- ↓ Physical change processes ineffective
- ↓ Inadequate tenant segmentation



Collapse of Switches and Servers into One Device

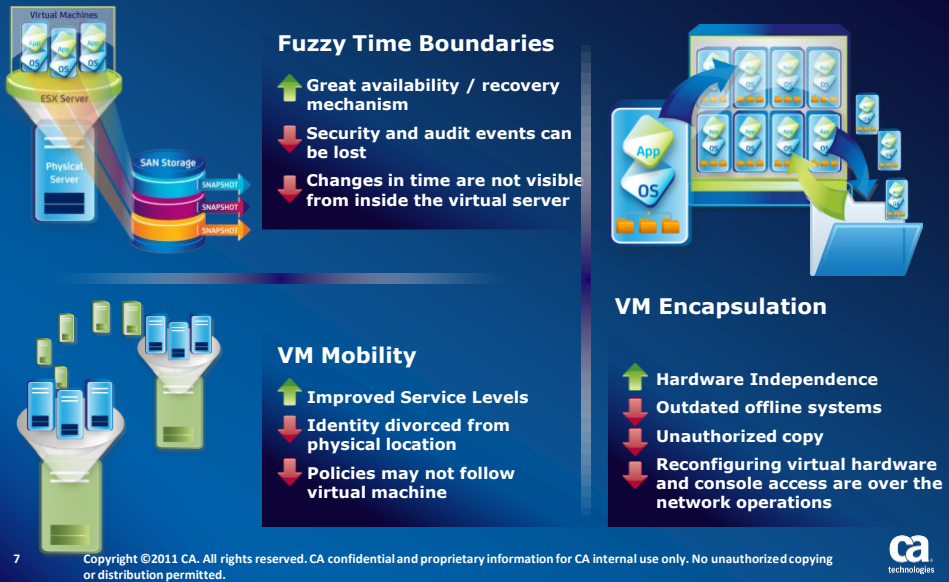
- ↑ Flexibility
- ↑ Cost-savings
- ↓ Lack of visibility and control for virtual network and storage
- ↓ No separation of church and state (network, security, storage administration)

6

Copyright © 2011 CA. All rights reserved. CA confidential and proprietary information for CA internal use only. No unauthorized copying or distribution permitted.



virtualization containers effects on security



CA Technologies Approach







CA Virtual Privilege Manager 2.0

A simple solution for managing access to virtual environments. integrated, agentless and channel friendly

- Regains *Visibility* into The Virtual Environment
- Control The *Dynamic* Nature of The Virtual Environment
- *Enforce* Security Policies and Network Policies From a Single Management Console
- Easy to *Deploy* and to Manage with vCenter Integration



Main Features

 Privileged Users Password Management	<i>Automatic</i> privileged account management for each and every component of the virtual environment
 User Activity Monitoring	<i>Automatic</i> log collection and reporting for each and every component in the virtual environment
 Hypervisor Hardening	Best practice hypervisor hardening
 Business Aware Network Isolation	Business, rather network, oriented approach towards achieving network segmentation
 Advance Policy Management	Flexible policy engine, including asset tagging, provides the ability to control the privileges of the virtualization admin
 Seamless Deployment	Easy deployment provided by a Virtual Appliance

9 Copyright (c) 2011 CA. All rights reserved. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. CA confidential and proprietary. No unauthorized copying or distribution permitted.



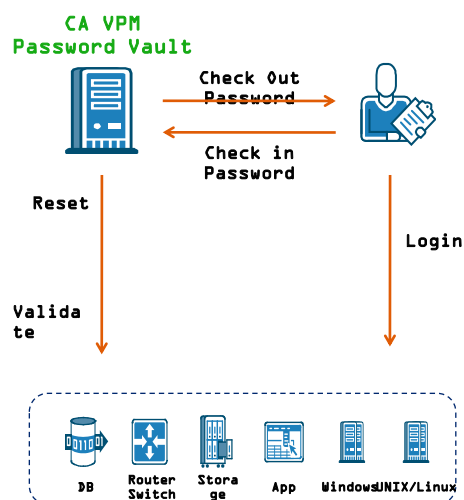
Privileged User Password Manager (PUPM) manage all shared accounts automatically!

Challenge

- Privileged/Shared accounts
- Accountability for shared accounts
- Control Hypervisor shared accounts
- Administrative ID's beyond OS
- Regulatory compliance

Solution

- Automatic VM discovery
- Manage access to shared passwords
- Manage emergency access passwords
- Automatic login for password security
- Correlate privileged activity to the user
- Agent-less architecture
- Session recording
- vCenter Integration



10 Copyright (c) 2011 CA. All rights reserved. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. CA confidential and proprietary. No unauthorized copying or distribution permitted.



User Activity Monitoring ensure proper audit and control

Challenge

- Ensure proper audit controls while taking into account the dynamic nature of the virtual environment
- Regain visibility and control on actions being performed
- Comply with regulatory requirements

Solution

- Automatic discovery and configuration for both Guest and Hypervisors
- Agent-less architecture
- Reporting and Alerting capabilities

Time	Event	Source	Destination	Amount
2011-03-08 10:10:00	Power On	VMware ESX	VMware ESX	100%
2011-03-08 10:10:00	Power Off	VMware ESX	VMware ESX	100%
2011-03-08 10:10:00	Power On	VMware ESX	VMware ESX	100%
2011-03-08 10:10:00	Power Off	VMware ESX	VMware ESX	100%
2011-03-08 10:10:00	Power On	VMware ESX	VMware ESX	100%
2011-03-08 10:10:00	Power Off	VMware ESX	VMware ESX	100%
2011-03-08 10:10:00	Power On	VMware ESX	VMware ESX	100%
2011-03-08 10:10:00	Power Off	VMware ESX	VMware ESX	100%
2011-03-08 10:10:00	Power On	VMware ESX	VMware ESX	100%
2011-03-08 10:10:00	Power Off	VMware ESX	VMware ESX	100%

11 Copyright (c) 2011 CA. All rights reserved. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. CA confidential and proprietary. No unauthorized copying or distribution permitted.



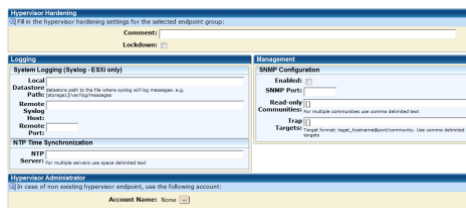
Hypervisor Service Console Hardening

Challenge

- Protect key system resources
- Protect VM images and VM Configuration
- Detect and alert on configuration changes
- Comply with regulatory requirements

Solution

- Automatic discovery hypervisors
- Agent-less architecture
- Enforce VMware security best practices
- Compatible with ESX and ESXi



12 Copyright (c) 2011 CA. All rights reserved. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. CA confidential and proprietary. No unauthorized copying or distribution permitted.



DEMO

13



Business Aware Network Isolation

Challenge

- Have control on who access which VMs based on business attributes
- Isolate sensitive VMs without changing network topology
- Reduce scope of regulatory checks

Solution

- Granular policy based network isolation
- Definition of business rules rather than network rules



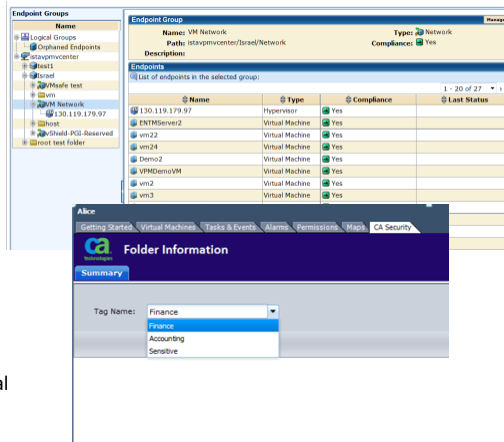
Advance Policy Management

Challenge

- Define and enforce security policies without being limited by hypervisor management constrains
- Allow SoD between VM owners, Security Teams and Virtualization Administrators

Solution

- Automatic Criteria-Based Tagging (Network, OS, VM properties, etc.)
- Cross-vCenters ,Data Centers and Containers
- Controlled separately from the virtual environment management

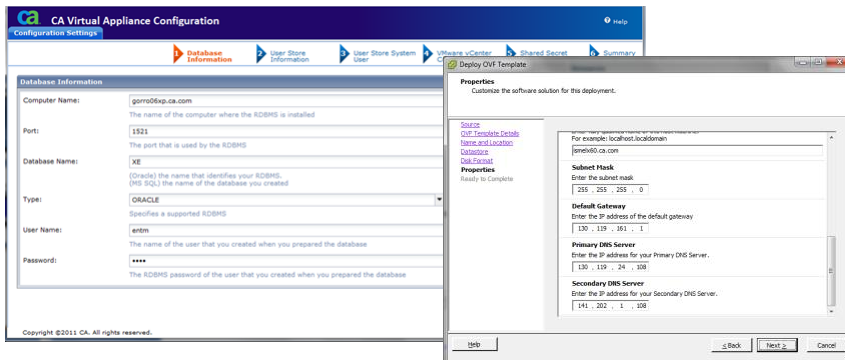


15 Copyright (c) 2011 CA. All rights reserved. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. CA confidential and proprietary. No unauthorized copying or distribution permitted.



Seamless Deployment

- Small footprint Virtual Appliances
- Fast and Easily deployed



16 Copyright (c) 2011 CA. All rights reserved. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. CA confidential and proprietary. No unauthorized copying or distribution permitted.

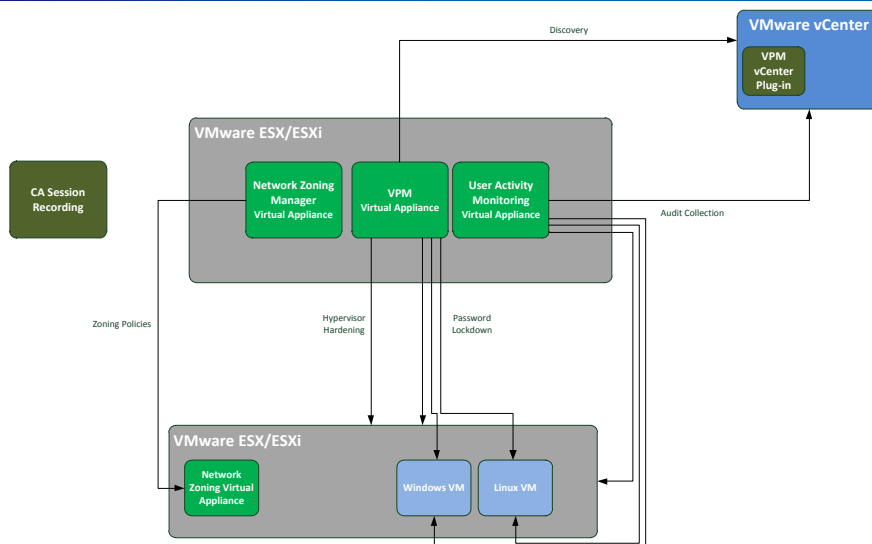


Solution Use Cases

- Privileged User Management
 - Separation of duties
 - PUPM
 - Least privilege access
- User Activity Auditing and Reporting
- Secure Multi Tenancy
- Operational Transparency to vCenter users
- Compliance
 - PCI / SOX / FISMA / SAS70 / HIPAA control mapping



Solution Architect



18

10/7/2011 Copyright (c) 2009 CA. All rights reserved. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies.



Questions



19 Copyright (c) 2011 CA. All rights reserved. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. CA confidential and proprietary. No unauthorized copying or distribution permitted.



20

Copyright © 2010 CA. All rights reserved. CA confidential and proprietary information for CA internal use only. No unauthorized copying or distribution permitted.

