Advanced Persistent Threats & Cyber Attacks: Defending from the inside out

Shirief Nosseir

Security Business Lead, Eastern & Africa

17 June 2014

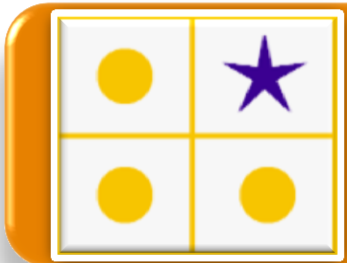
agility
made possible™

ca technologies

Agenda

The new breed of attacks

Traditional infrastructure security is no longer enough



Detecting breaches early & reducing their impact

What is an “Advanced Persistent Threat”?

Sophisticated capabilities

APTs and cyber attacks are a real risk

PCWorld

RSA SecurID Hack Shows Danger of APTs
Mar 18, 2011

WIRED

Second Defense Contractor L-3 ‘Actively Targeted’ With RSA SecurID Hacks
May 31, 2011

infosecurity

Insiders exploiting privileged accounts likely behind Saudi Aramco attack
24 October 2012

The Register®
Biting the hand that feeds IT

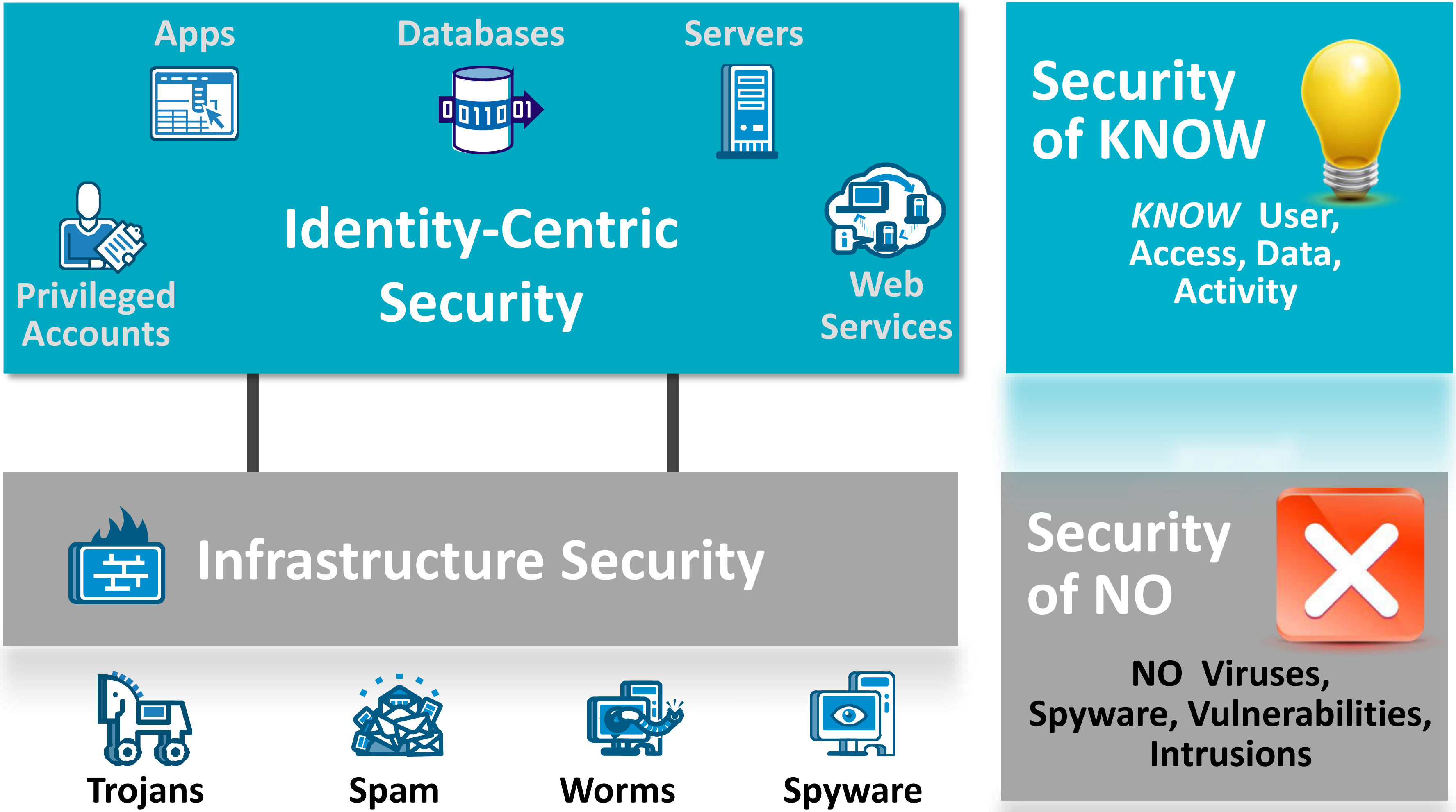
China fingered for Coca Cola hack - report
5th November 2012

Bucharest Herald

SRI: “Red October,” most powerful cyber-attack targeting Romania in the last 20 years
20 January 2013

http://www.pcworld.com/article/222555/rsa_securid_hack_shows_danger_of_apts.html
http://www.wired.com/threatlevel/2011/05/l-3/
http://www.infosecurity-magazine.com/view/28973/insiders-exploiting-privileged-accounts-likely-behind-saudi-aramco-attack-/
http://www.theregister.co.uk/2012/11/05/coca_cola_breach_china_hackers/
http://www.bucharestherald.ro/dailyevents/41-dailyevents/39733--sri-red-october-most-powerful-cyber-attack-targeting-romania-in-the-last-20-years

Moving from "No" to "Know"
Traditional infrastructure security is no longer enough



Apps

Databases

Servers

Privileged Accounts

Identity-Centric Security

Web Services

Infrastructure Security

Trojans

Spam

Worms

Spyware

Security of KNOW

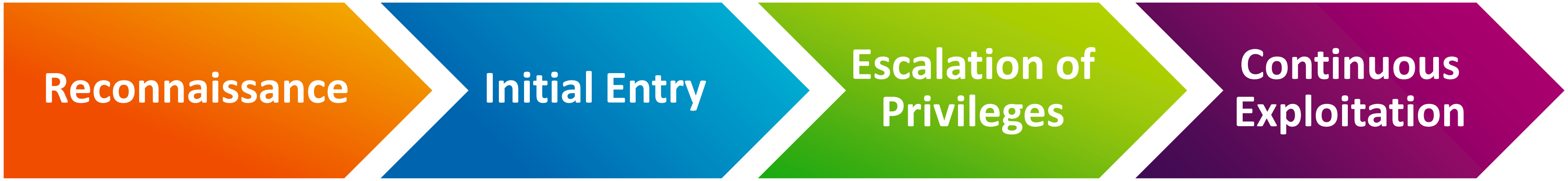
KNOW User, Access, Data, Activity

Security of NO

NO Viruses, Spyware, Vulnerabilities, Intrusions

The stages of an APT attack

Stages of an Advanced Persistent Threat



Reconnaissance

Initial Entry

Escalation of Privileges

Continuous Exploitation

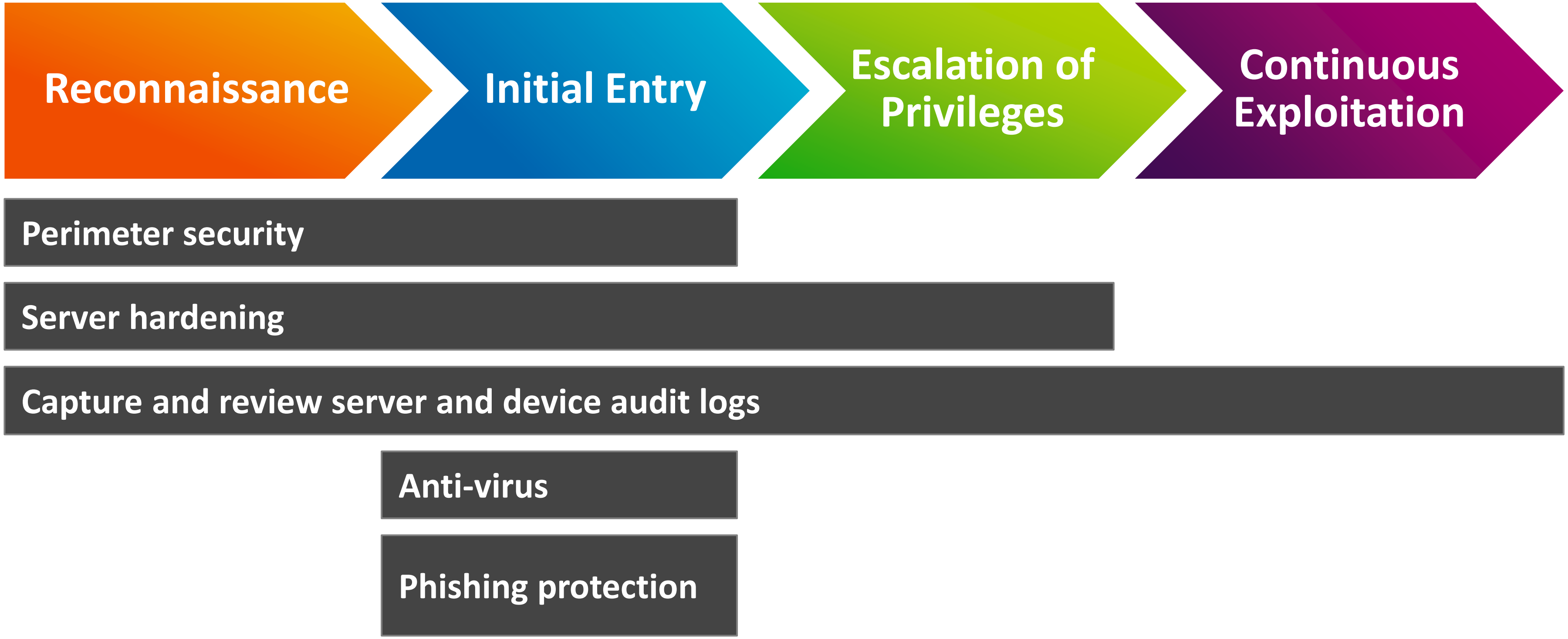
- Research
- Domain queries
- Port scans
- Vulnerability scans

- “Spear Phishing”
- Social Engineering
- Zero day vulnerability exploitation

- OS & application vulnerability exploitation
- Administrative access
- Compromise of new systems

- Continuous export of sensitive data
- Affect service availability
- Covering of tracks
- Rootkits

Traditional perimeter and infrastructure security capabilities only address part of the problem!



Reconnaissance

Initial Entry

Escalation of Privileges

Continuous Exploitation

Perimeter security

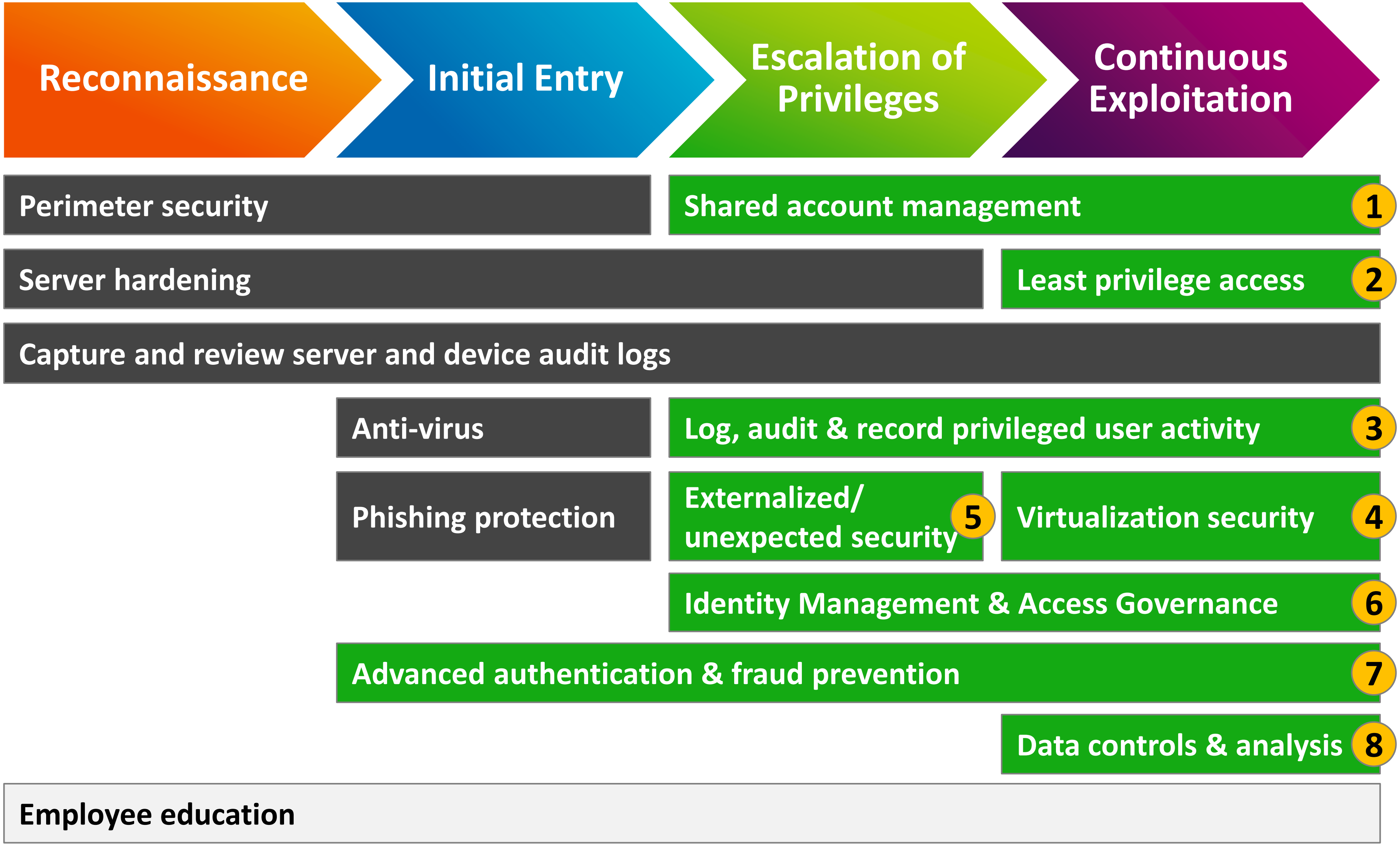
Server hardening

Capture and review server and device audit logs

Anti-virus

Phishing protection

Content-aware identity & access management bolster an APT defense!



Reconnaissance

Initial Entry

Escalation of Privileges

Continuous Exploitation

Perimeter security

Shared account management 1

Server hardening

Least privilege access 2

Capture and review server and device audit logs

Anti-virus

Log, audit & record privileged user activity 3

Phishing protection

Externalized/ unexpected security 5

Virtualization security 4

Identity Management & Access Governance 6

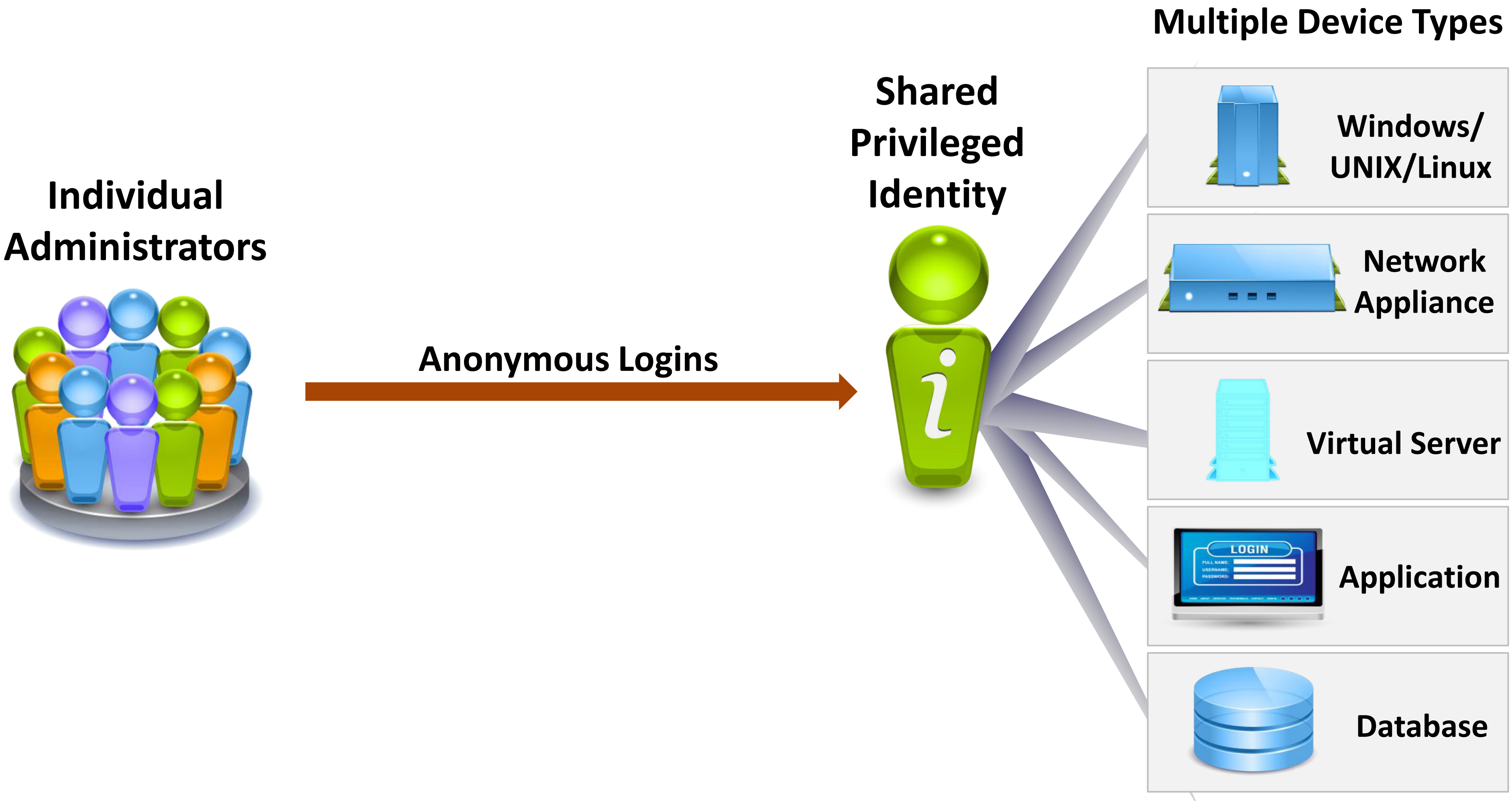
Advanced authentication & fraud prevention 7

Data controls & analysis 8

Employee education

1 Individual administrators can access shared accounts through password checkouts or automatic logins

Shared Account Management



Multiple Device Types

Individual Administrators

Anonymous Logins

Shared Privileged Identity

Windows/ UNIX/Linux

Network Appliance

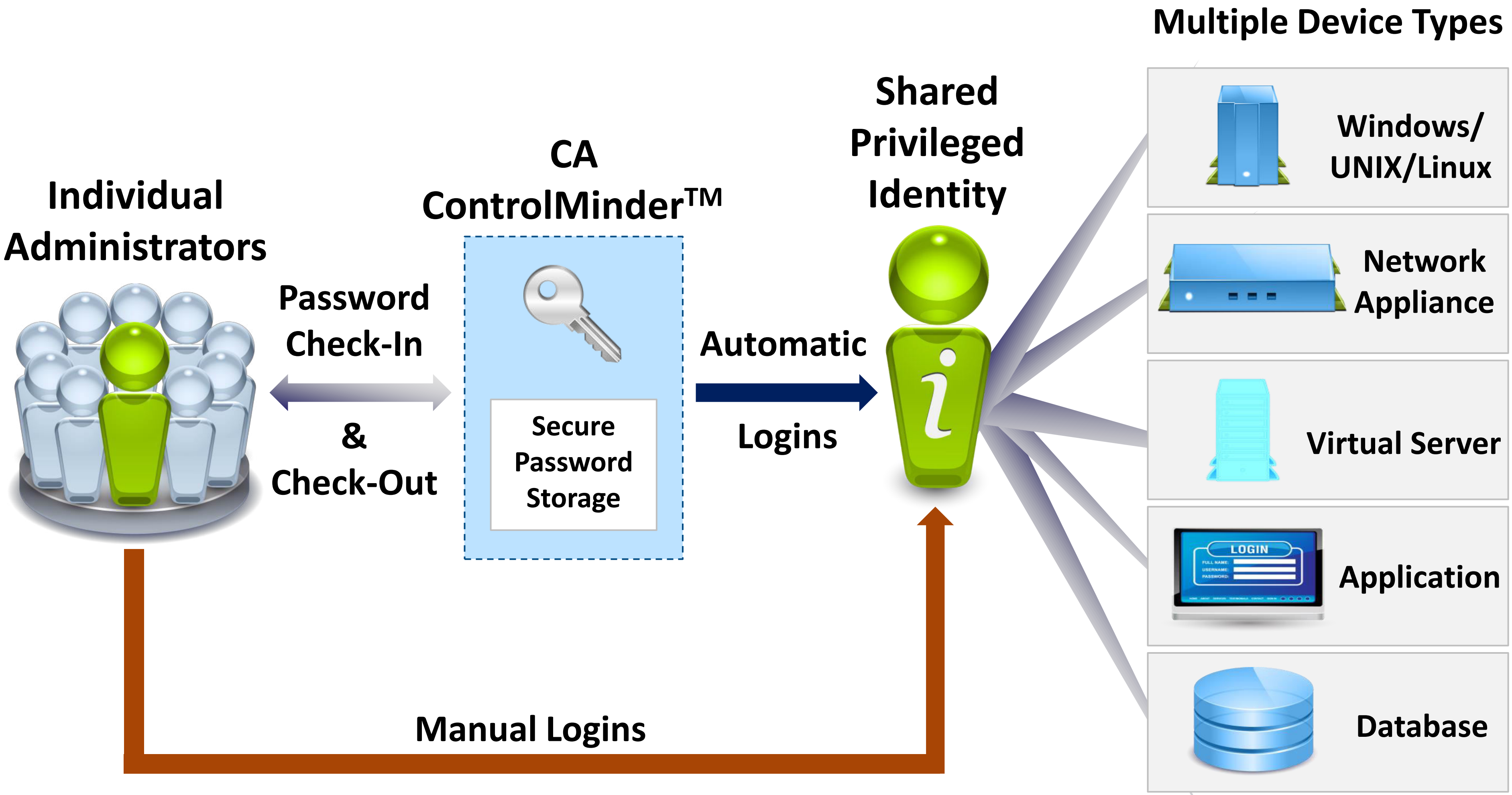
Virtual Server

Application

Database

1 Individual administrators can access shared accounts through password checkouts or automatic logins

Shared Account Management



Multiple Device Types

Shared Privileged Identity

CA ControlMinder™

Individual Administrators

Password Check-In & Check-Out

Secure Password Storage

Automatic Logins

Manual Logins

Windows/ UNIX/Linux

Network Appliance

Virtual Server

Application

Database

2

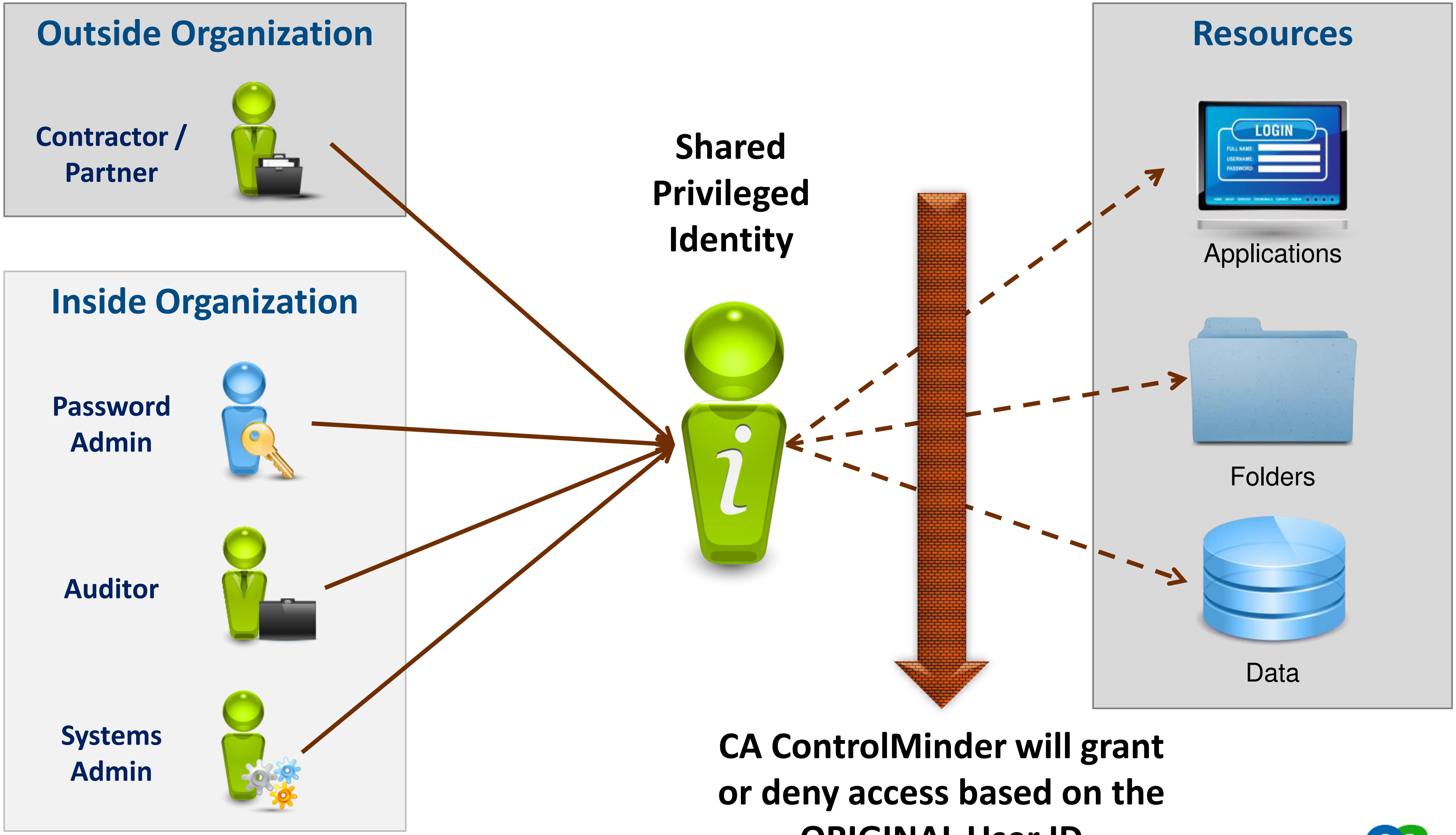
Do all your administrator’s privileges look the same?

Least Privilege Access (with Fine-Grained Controls!)

If your administrator privileges look like this, you have a problem!

2 Individuals accessing a shared account don't have to have the same privileges – make them job-specific!

Fine-Grained Controls



Outside Organization

Contractor / Partner

Inside Organization

Password Admin

Auditor

Systems Admin

Shared Privileged Identity

Resources

Applications

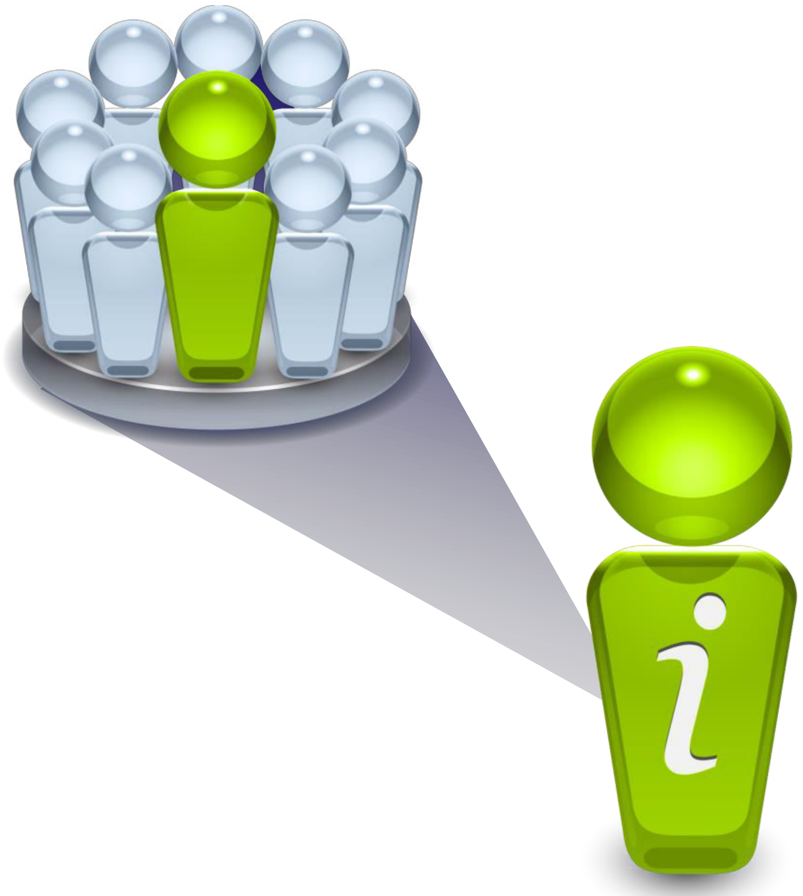
Folders

Data

CA ControlMinder will grant or deny access based on the ORIGINAL User ID

3 When there's a crowd behind a privileged identity, can you tell who did what?

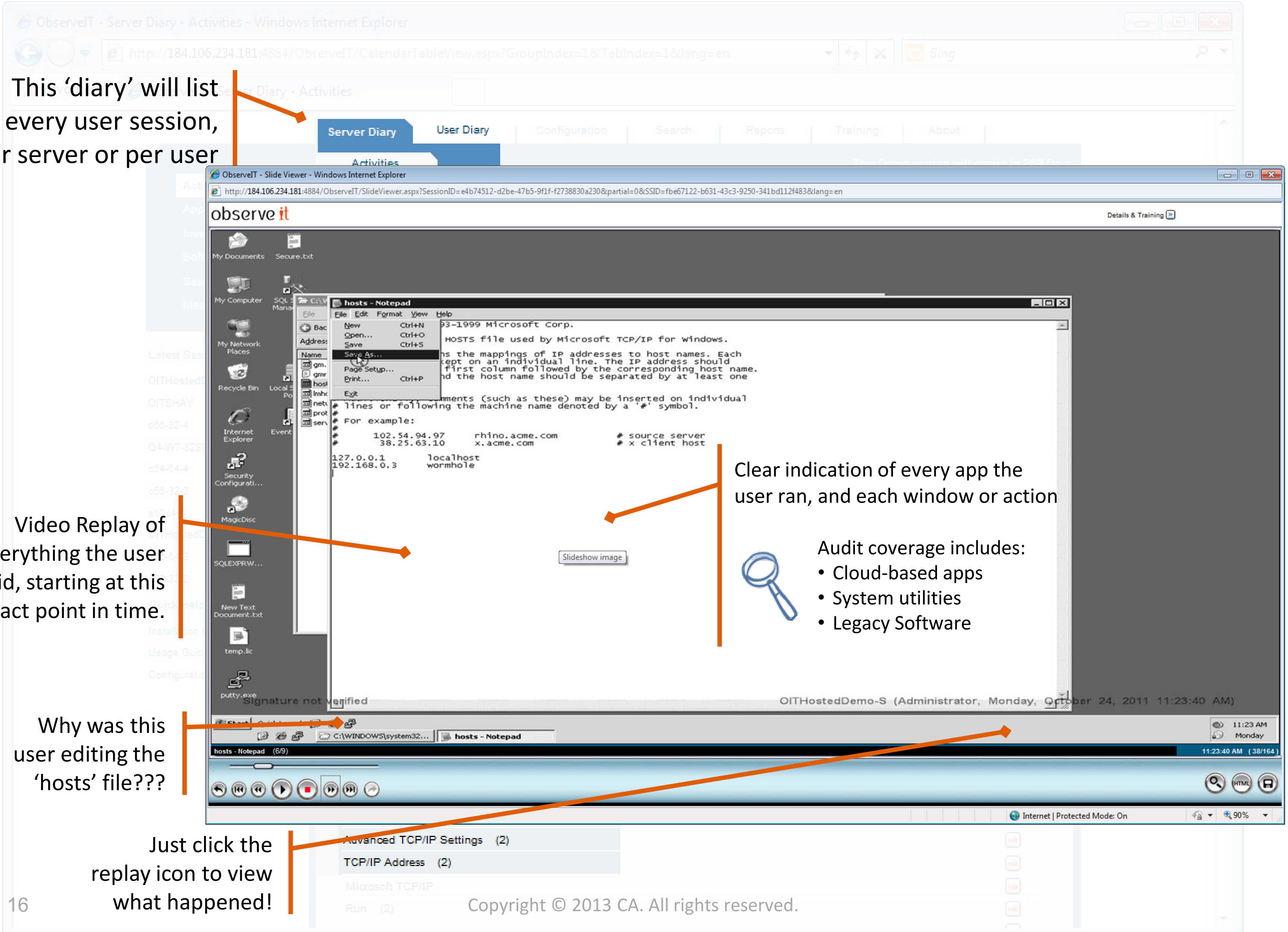
Log and Audit Privileged User Activity



Shared Account

Logs must capture all actions based on the original, *individual* identity!

3 CA Session Recording: in Windows



```
93-1999 Microsoft Corp.

 HOSTS file used by Microsoft TCP/IP for Windows.

hs the mappings of IP addresses to host names. Each
kept on an individual line. The IP address should
 first column followed by the corresponding host name.
nd the host name should be separated by at least one

        mments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

127.0.0.1       localhost
192.168.0.3     wormhole
```

This 'diary' will list every user session, per server or per user

Clear indication of every app the user ran, and each window or action

Video Replay of everything the user did, starting at this exact point in time.

Audit coverage includes:

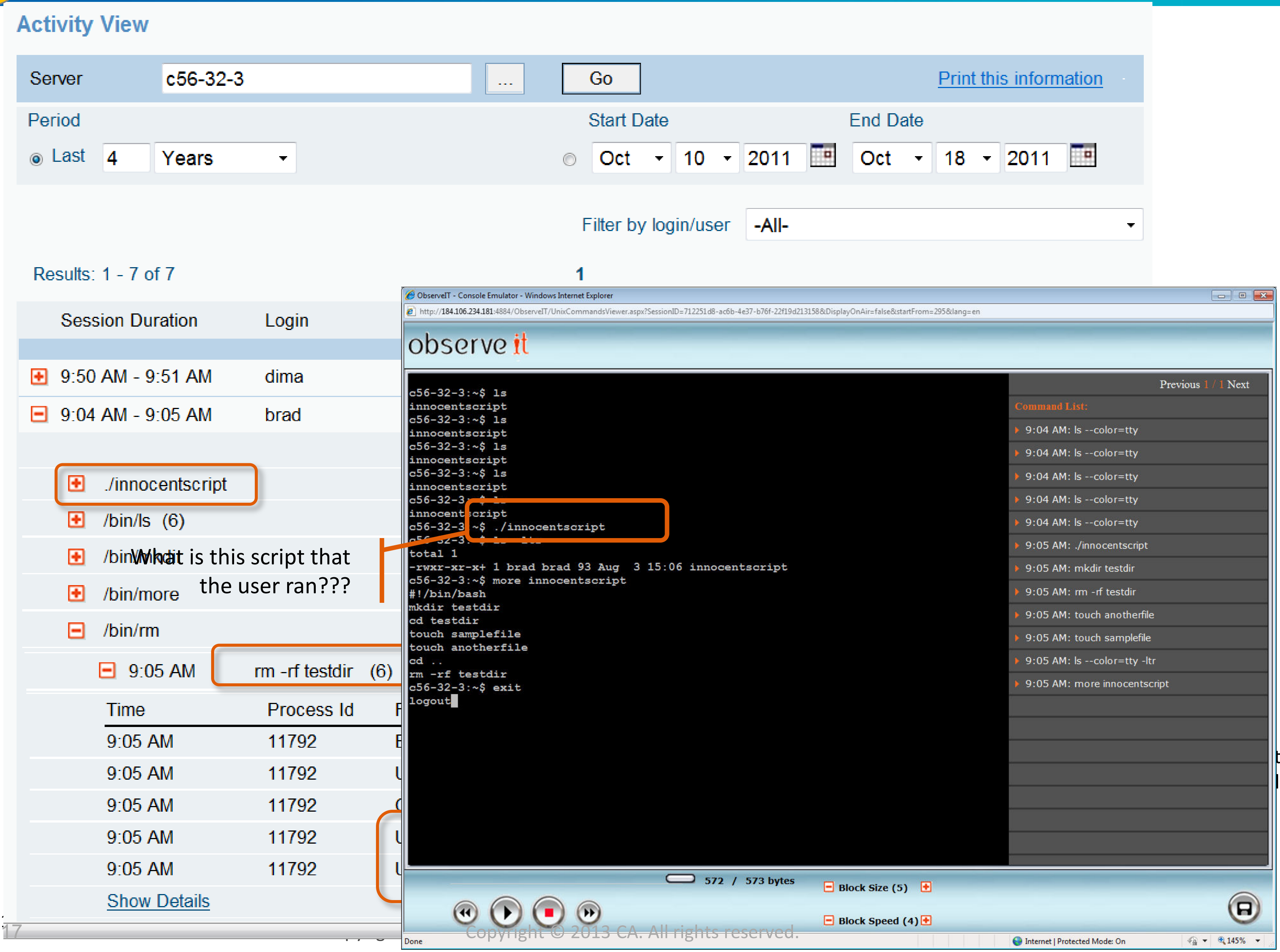
- Cloud-based apps
- System utilities
- Legacy Software

Why was this user editing the 'hosts' file???

Just click the replay icon to view what happened!

3

CA Session Recording: in Linux



Activity View

Server	c56-32-3	...	Go

Print this information

Period

● Last 4 Years

Start Date ○ Oct 10 2011

End Date Oct 18 2011

Filter by login/user -All-

Results: 1 - 7 of 7 1

Session Duration	Login
⊞ 9:50 AM - 9:51 AM	dima
⊟ 9:04 AM - 9:05 AM	brad

⊞ ./innocentscript

⊞ /bin/ls (6)

⊞ /bin/mkdir

⊞ /bin/more

⊟ /bin/rm

⊟ 9:05 AM rm -rf testdir (6)

Time	Process Id	F
9:05 AM	11792	E
9:05 AM	11792	U
9:05 AM	11792	C
9:05 AM	11792	U
9:05 AM	11792	U

Show Details

What is this script that the user ran???

ObserveIT - Console Emulator - Windows Internet Explorer

http://184.106.234.181:4884/ObserveIT/UnixCommandsViewer.aspx?SessionID=712251d8-ac6b-4e37-b76f-22f19d213158&DisplayOnAir=false&startFrom=295&lang=en

observe it

```
c56-32-3:~$ ls
innocentscript
c56-32-3:~$ ls
innocentscript
c56-32-3:~$ ls
innocentscript
c56-32-3:~$ ls
innocentscript
c56-32-3:~$ ls
innocentscript
c56-32-3:~$ ./innocentscript
c56-32-3:~$ ls -ltr
total 1
-rwxr-xr-x+ 1 brad brad 93 Aug  3 15:06 innocentscript
c56-32-3:~$ more innocentscript
#!/bin/bash
mkdir testdir
cd testdir
touch samplefile
touch anotherfile
cd ..
rm -rf testdir
c56-32-3:~$ exit
logout
```

Previous 1 / 1 Next

Command List:

- 9:04 AM: ls --color=tty
- 9:04 AM: ls --color=tty
- 9:04 AM: ls --color=tty
- 9:04 AM: ls --color=tty
- 9:04 AM: ls --color=tty
- 9:05 AM: ./innocentscript
- 9:05 AM: mkdir testdir
- 9:05 AM: rm -rf testdir
- 9:05 AM: touch anotherfile
- 9:05 AM: touch samplefile
- 9:05 AM: ls --color=tty -ltr
- 9:05 AM: more innocentscript

572 / 573 bytes

⊟ Block Size (5) ⊞

⊟ Block Speed (4) ⊞

Done

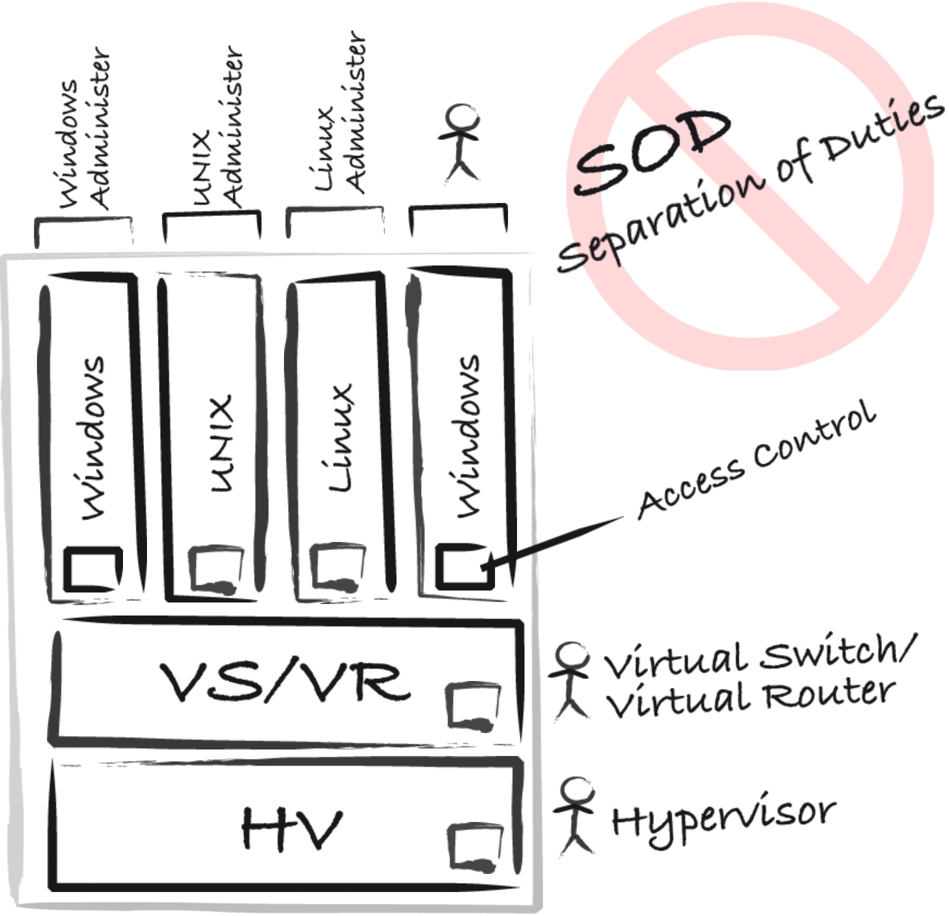
Internet | Protected Mode: On

145%

tadata

lying

4 Securing virtual environments requires "the fundamentals" as well as new capabilities



5 Adding unexpected elements to operating system security can help detect even careful attackers

Externalized / Unexpected Security

6

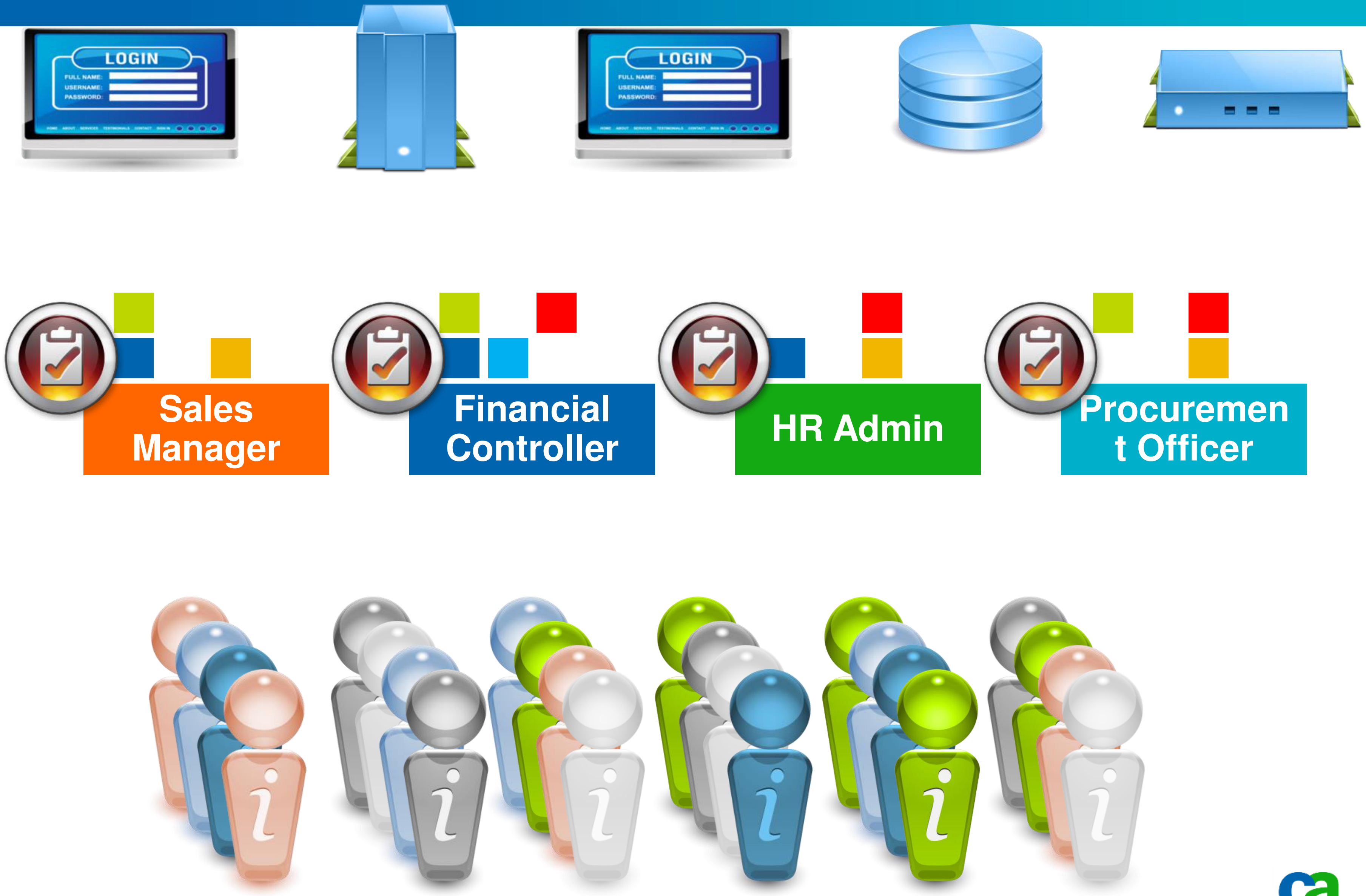
IMAG: Identity Cleanup

AConstantin12	AC1415	edvAS016	ksjdAS01	DalcHi02
HDalca01	HD3669	edvMN009	ksjdAS02	ConsAl10
ASala01	AS1842	edvRF016	ksjdAS03	FunaRa03
ASima02	AS4569	fdvAC037	ksjdRF01	SalaAd02
ASima04	AS6347	fdvHD007	ksrdtAC02	SimaAd03
MNicolescu02	MN3362	fdvAS005	ksrdYL03	SimaAd04
NGabor06	NG2542	fdvAS011	uadbHD01	NicoMo01
RFunar03	RF7397	xdvNG035	uadbMN02	LupeYa03
YLupei03	YL3492	xdvYL024	uadbNG03	GaboNi08
...	...	...	...	...

Adam Sima
Financial Controller

6

IMAG: Access Certification



Sales Manager

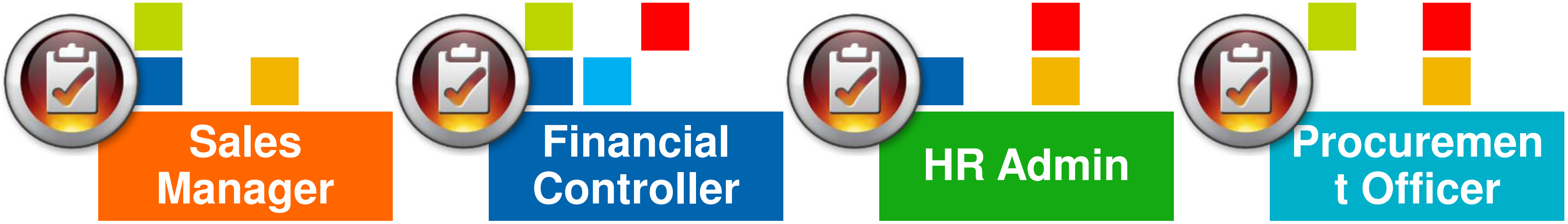
Financial Controller

HR Admin

Procuremen t Officer

6

IMAG: Provisioning



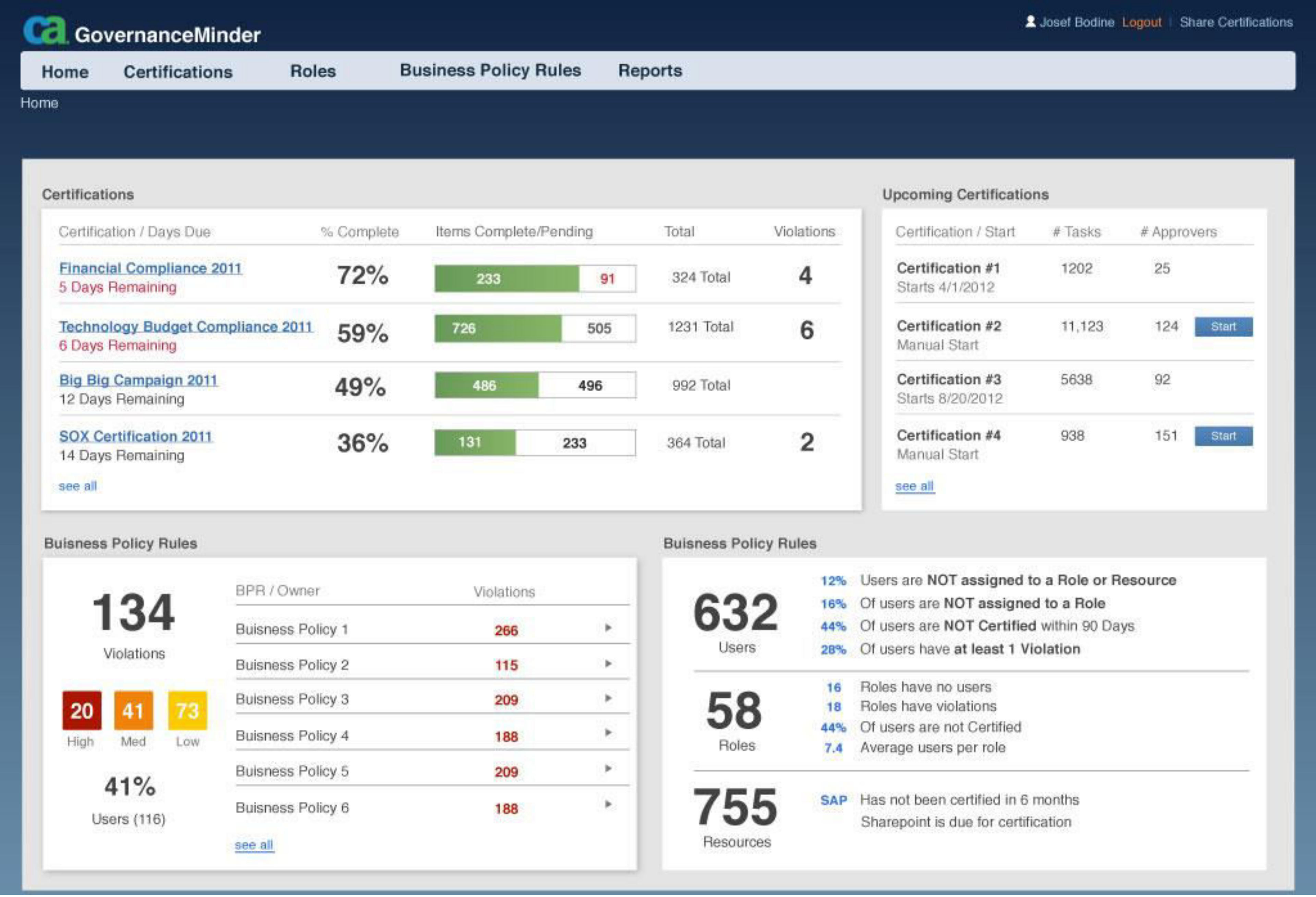
Sales Manager

Financial Controller

HR Admin

Procuremen t Officer

Joiners Movers Leavers



Certifications

Certification / Days Due	% Complete	Items Complete/Pending	Total	Violations
Financial Compliance 2011 5 Days Remaining	72%	233 / 91	324 Total	4
Technology Budget Compliance 2011 6 Days Remaining	59%	726 / 505	1231 Total	6
Big Big Campaign 2011 12 Days Remaining	49%	486 / 496	992 Total	
SOX Certification 2011 14 Days Remaining	36%	131 / 233	364 Total	2

see all

Upcoming Certifications

Certification / Start	# Tasks	# Approvers	
Certification #1 Starts 4/1/2012	1202	25	
Certification #2 Manual Start	11,123	124	Start
Certification #3 Starts 8/20/2012	5638	92	
Certification #4 Manual Start	938	151	Start

see all

Buisness Policy Rules

134

Violations

20	41	73
High	Med	Low

41%

Users (116)

BPR / Owner	Violations	
Buisness Policy 1	266	▸
Buisness Policy 2	115	▸
Buisness Policy 3	209	▸
Buisness Policy 4	188	▸
Buisness Policy 5	209	▸
Buisness Policy 6	188	▸

see all

Buisness Policy Rules

632

Users

12%	Users are **NOT assigned to a Role or Resource**
16%	Of users are **NOT assigned to a Role**
44%	Of users are **NOT Certified** within 90 Days
28%	Of users have **at least 1 Violation**

58

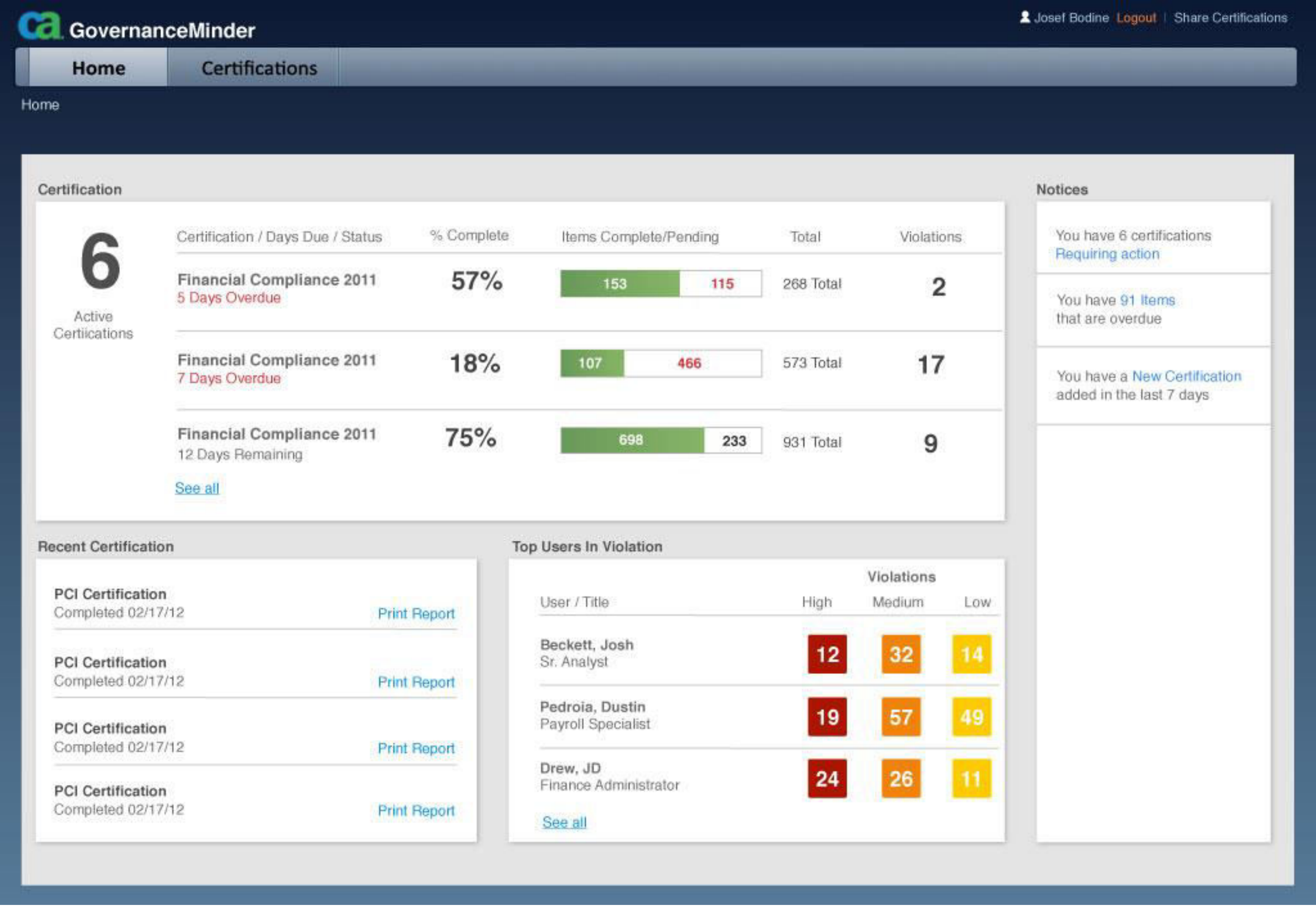
Roles

16	Roles have no users
18	Roles have violations
44%	Of users are not Certified
7.4	Average users per role

755

Resources

SAP	Has not been certified in 6 months
	Sharepoint is due for certification



Certification

6
Active Certiications

Certification / Days Due / Status	% Complete	Items Complete/Pending	Total	Violations
Financial Compliance 2011 5 Days Overdue	57%	153 / 115	268 Total	2
Financial Compliance 2011 7 Days Overdue	18%	107 / 466	573 Total	17
Financial Compliance 2011 12 Days Remaining	75%	698 / 233	931 Total	9

See all

Notices

You have 6 certifications Requiring action

You have 91 Items that are overdue

You have a New Certification added in the last 7 days

Recent Certification

PCI Certification
Completed 02/17/12 Print Report

PCI Certification
Completed 02/17/12 Print Report

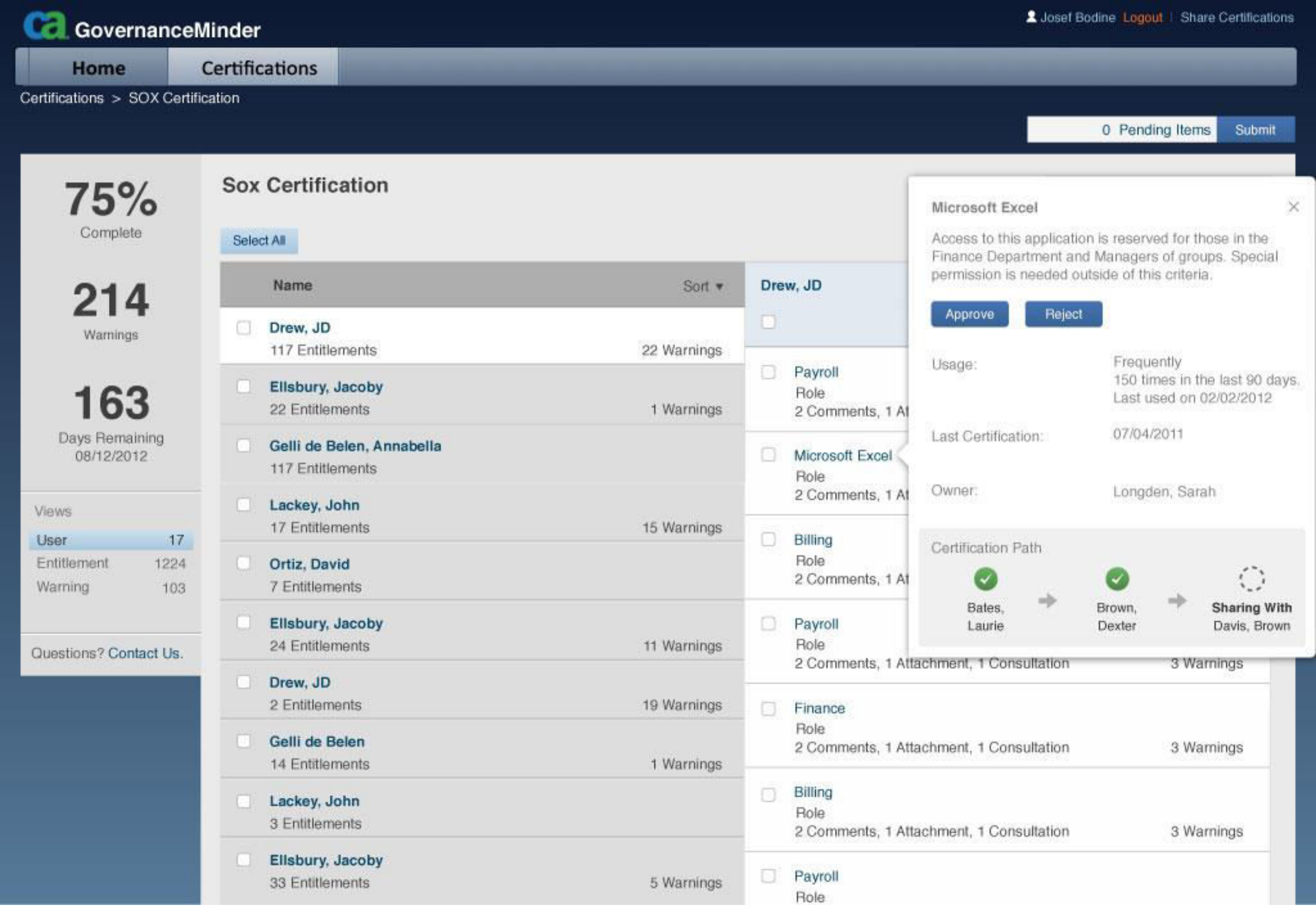
PCI Certification
Completed 02/17/12 Print Report

PCI Certification
Completed 02/17/12 Print Report

Top Users In Violation

	Violations		
User / Title	High	Medium	Low
Beckett, Josh Sr. Analyst	12	32	14
Pedroia, Dustin Payroll Specialist	19	57	49
Drew, JD Finance Administrator	24	26	11

See all



GovernanceMinder

Josef Bodine Logout | Share Certifications

Home | Certifications

Certifications > SOX Certification

0 Pending Items | Submit

75%
Complete

214
Warnings

163
Days Remaining
08/12/2012

Views

User	17
Entitlement	1224
Warning	103

Questions? Contact Us.

Sox Certification

Select All

	Name	Sort ▾
□	Drew, JD 117 Entitlements	22 Warnings
□	Ellsbury, Jacoby 22 Entitlements	1 Warnings
□	Gelli de Belen, Annabella 117 Entitlements	
□	Lackey, John 17 Entitlements	15 Warnings
□	Ortiz, David 7 Entitlements	
□	Ellsbury, Jacoby 24 Entitlements	11 Warnings
□	Drew, JD 2 Entitlements	19 Warnings
□	Gelli de Belen 14 Entitlements	1 Warnings
□	Lackey, John 3 Entitlements	
□	Ellsbury, Jacoby 33 Entitlements	5 Warnings

Drew, JD

□

□	Payroll Role 2 Comments, 1 At	
□	Microsoft Excel Role 2 Comments, 1 At	
□	Billing Role 2 Comments, 1 At	
□	Payroll Role 2 Comments, 1 Attachment, 1 Consultation	3 Warnings
□	Finance Role 2 Comments, 1 Attachment, 1 Consultation	3 Warnings
□	Billing Role 2 Comments, 1 Attachment, 1 Consultation	3 Warnings
□	Payroll Role	

Microsoft Excel ×

Access to this application is reserved for those in the Finance Department and Managers of groups. Special permission is needed outside of this criteria.

Approve | Reject

Usage:	Frequently 150 times in the last 90 days. Last used on 02/02/2012
Last Certification:	07/04/2011
Owner:	Longden, Sarah

Certification Path

✓ Bates, Laurie → ✓ Brown, Dexter → **Sharing With** Davis, Brown

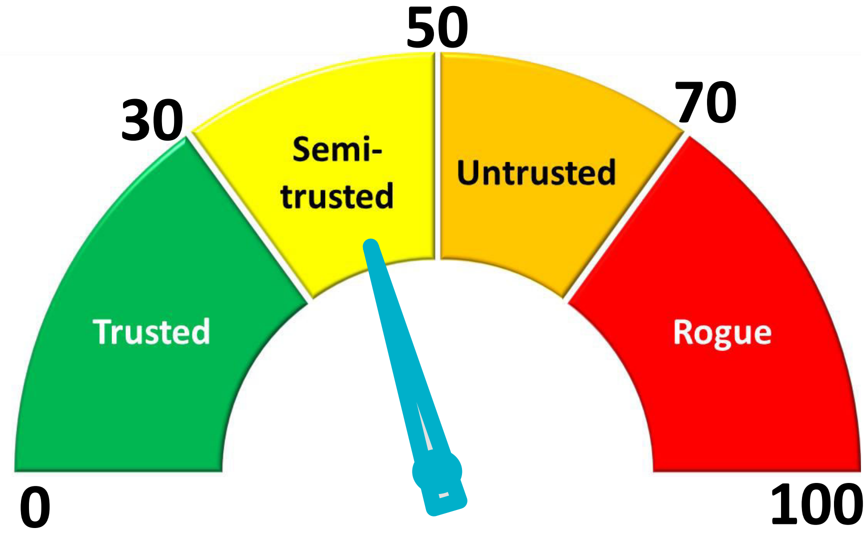
7

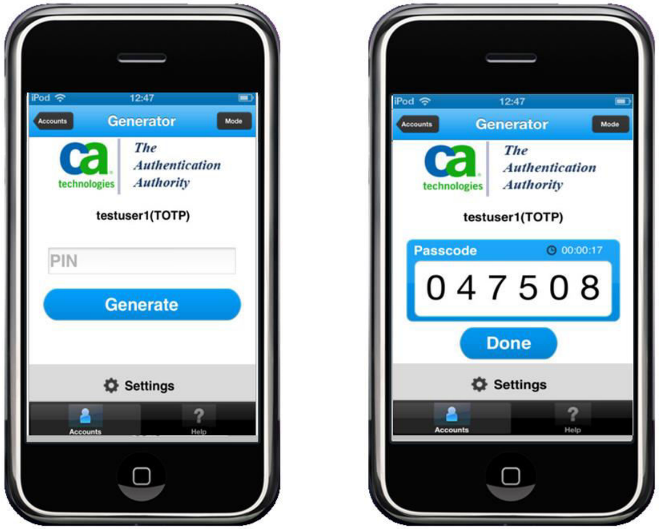
Advanced authentication & fraud detection

Security

Convenience

Cost





testuser1(TOTP)

PIN

testuser1(TOTP)

Passcode 00:00:17

047508

OTP can be delivered by SMS, voice or email

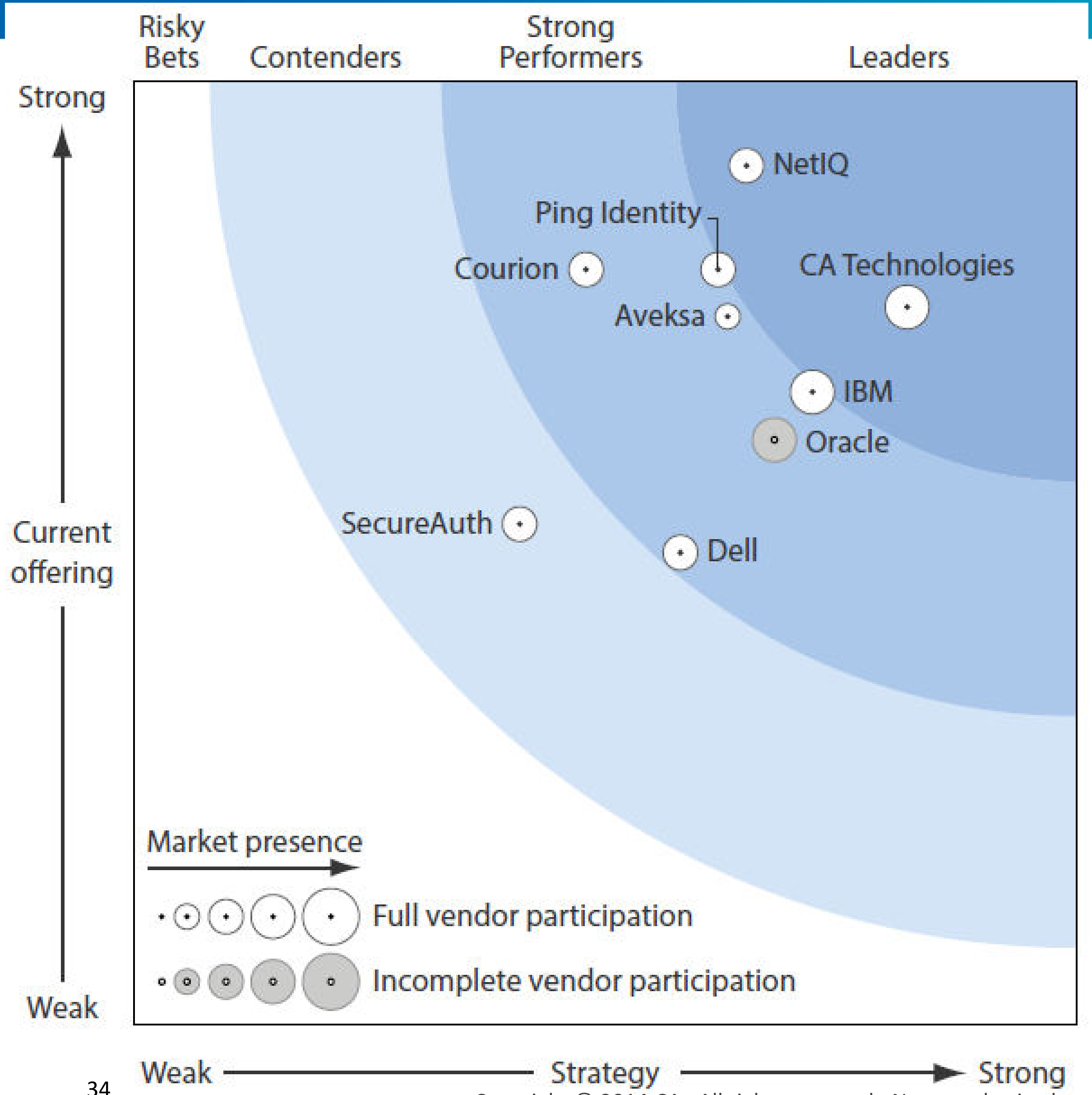
Layer 1

Invisible Risk-Based Authentication

Layer 2

Strong / Appropriate Authentication

IAM Forrester Wave Q3 2013



FORRESTER®

The Forrester Wave™: Identity & Access Management Suites, Q3 2013

Andras Cser and Eve Maler,

September 4, 2013

Industry Awards for CA Security Solutions

CA IdentityMinder™ – Best Identity Management Solution of 2012, 2013

Best Governance, Risk, & Compliance Solution, 2012*

*IdentityMinder, GovernanceMinder™

Identity Access Management/Single Sign-on Software – 2012

Best IAM Solution of 2012

Thank You

ca technologies®

Shirief Nosseir
Security Business Lead – Eastern & Africa
Shirief.Nosseir@ca.com

- @cainc
- Slideshare.net/CAinc
- linkedin.com/company/ca-technologies

ca.com