Trust in the Cloud

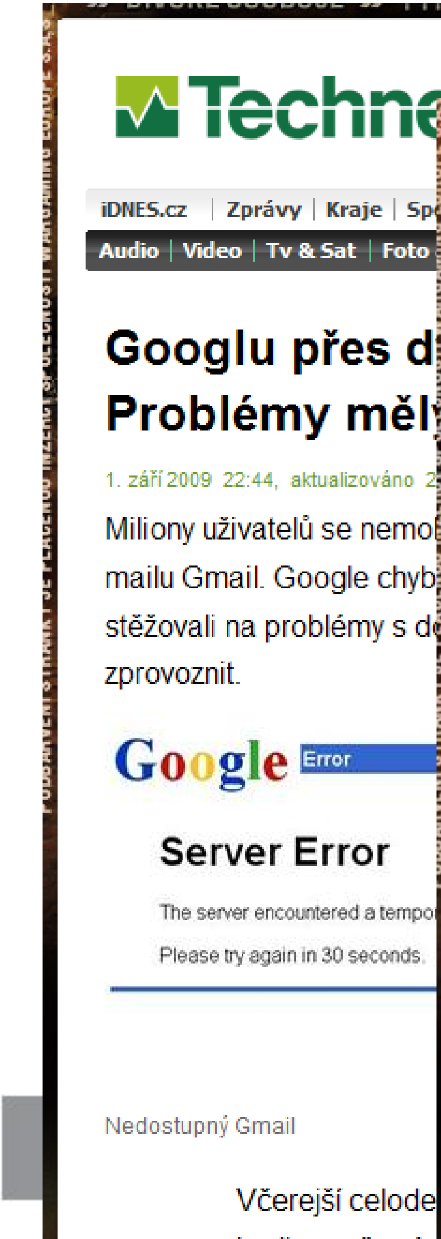
Zajištění bezpečnosti virtuálního datacentra a jeho souladu s předpisy a zákony

Ivan Svoboda
RSA, The Security Division of EMC

Microsoft
BBC
MasterCard
RSA
WIRED
Bank of America
Google
YAHOO!
SONY

New Threat Vectors

Cloud threats: examples



Technet.cz

iDNES.cz | Zprávy | Kraje | Sp

Audio | Video | Tv & Sat | Foto

Googlu přes d
Problémy měl

1. září 2009 22:44, aktualizováno 2

Miliony uživatelů se nemo mailu Gmail. Google chyb stěžovali na problémy s d zprovoznit.

Google Error

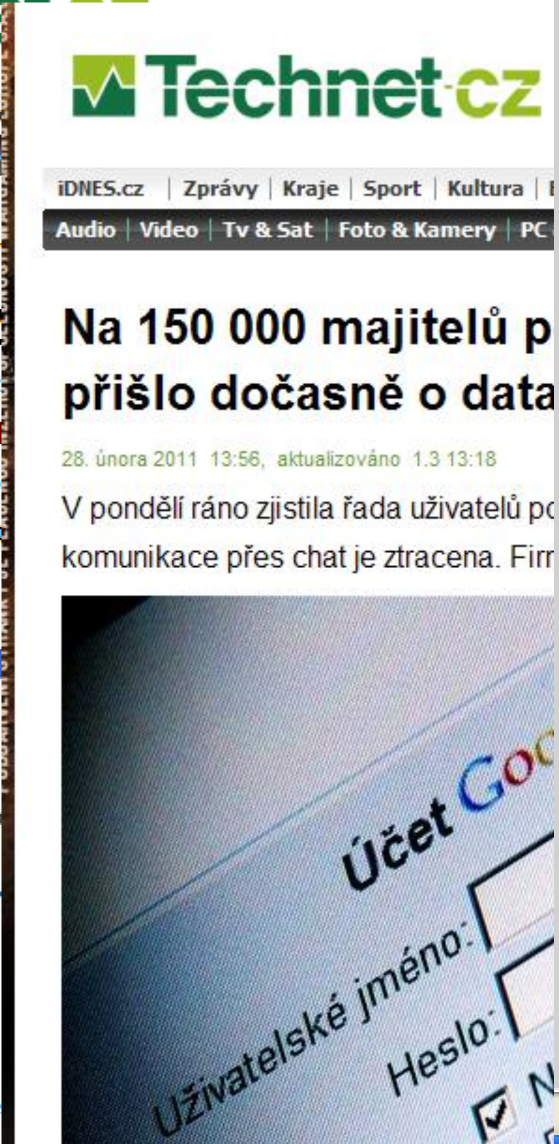
Server Error

The server encountered a tempo

Please try again in 30 seconds.

Nedostupný Gmail

Včerejší celode



Technet.cz

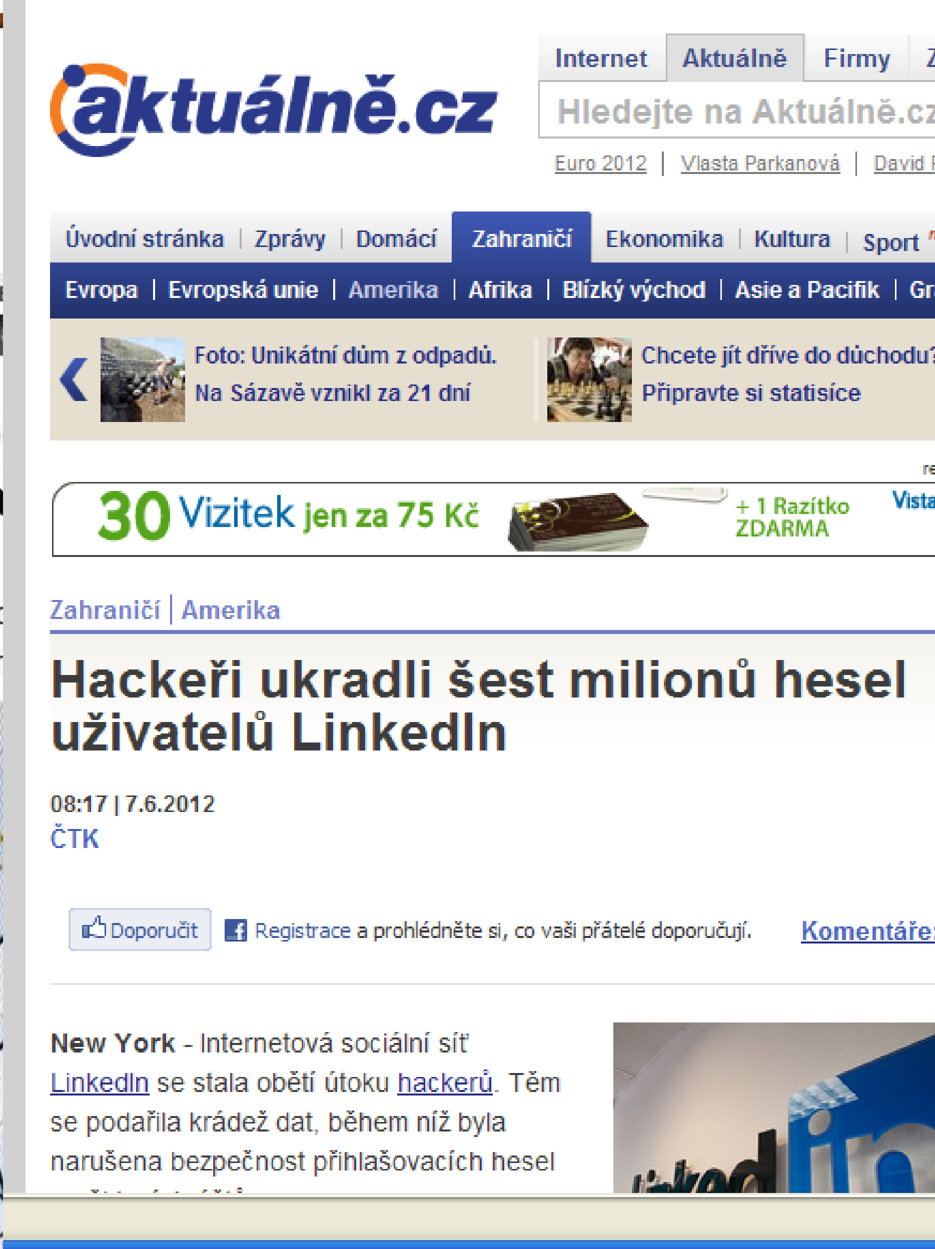
iDNES.cz | Zprávy | Kraje | Sport | Kultura |

Audio | Video | Tv & Sat | Foto & Kamery | PC

Na 150 000 majitelů p
přišlo dočasně o data

28. února 2011 13:56, aktualizováno 1.3 13:18

V pondělí ráno zjistila řada uživatelů po komunikace přes chat je ztracena. Fir



aktuálně.cz

Internet | Aktuálně | Firmy | Z

Hledejte na Aktuálně.cz

Euro 2012 | Vlasta Parkanová | David F

Úvodní stránka | Zprávy | Domácí | Zahraničí | Ekonomika | Kultura | Sport

Evropa | Evropská unie | Amerika | Afrika | Blízký východ | Asie a Pacifik | Gr

Foto: Unikátní dům z odpadů. Na Sázavě vznikl za 21 dní

Chcete jít dříve do důchodu? Připravte si statisíce

Zahraničí | Amerika

Hackeři ukradli šest milionů hesel uživatelů LinkedIn

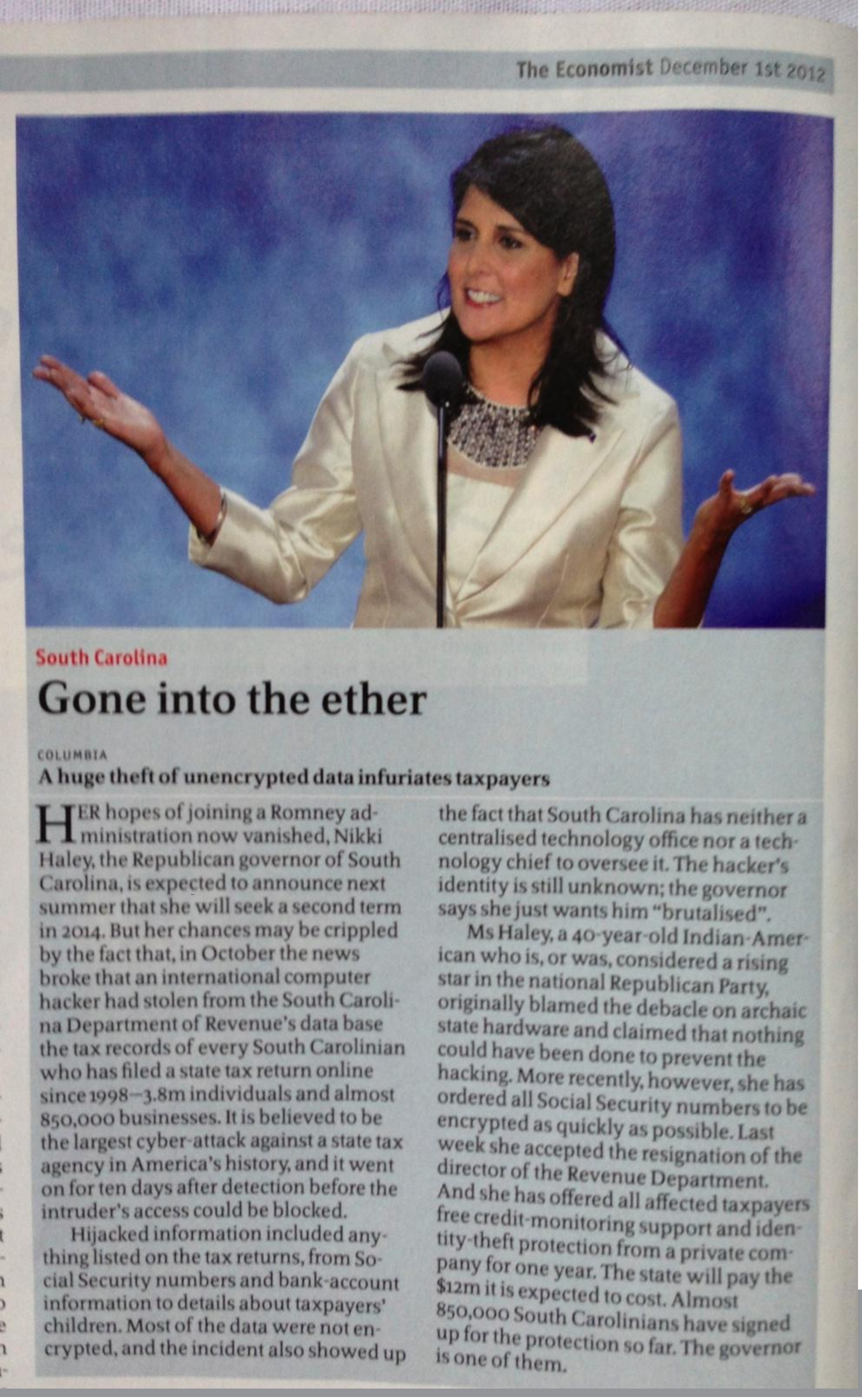
08:17 | 7.6.2012

ČTK

Doporučit Registrace a prohlédněte si, co vaši přátelé doporučují. Komentáře

New York - Internetová sociální síť LinkedIn se stala obětí útoku hackerů. Těm se podařila krádež dat, během níž byla narušena bezpečnost přihlašovacích hesel

Careers @ Risk



The Economist December 1st 2012

South Carolina

Gone into the ether

COLUMBIA

A huge theft of unencrypted data infuriates taxpayers

HER hopes of joining a Romney administration now vanished, Nikki Haley, the Republican governor of South Carolina, is expected to announce next summer that she will seek a second term in 2014. But her chances may be crippled by the fact that, in October the news broke that an international computer hacker had stolen from the South Carolina Department of Revenue's data base the tax records of every South Carolinian who has filed a state tax return online since 1998—3.8m individuals and almost 850,000 businesses. It is believed to be the largest cyber-attack against a state tax agency in America's history, and it went on for ten days after detection before the intruder's access could be blocked.

Hijacked information included anything listed on the tax returns, from Social Security numbers and bank-account information to details about taxpayers' children. Most of the data were not encrypted, and the incident also showed up the fact that South Carolina has neither a centralised technology office nor a technology chief to oversee it. The hacker's identity is still unknown; the governor says she just wants him "brutalised".

Ms Haley, a 40-year-old Indian-American who is, or was, considered a rising star in the national Republican Party, originally blamed the debacle on archaic state hardware and claimed that nothing could have been done to prevent the hacking. More recently, however, she has ordered all Social Security numbers to be encrypted as quickly as possible. Last week she accepted the resignation of the director of the Revenue Department. And she has offered all affected taxpayers free credit-monitoring support and identity-theft protection from a private company for one year. The state will pay the $12m it is expected to cost. Almost 850,000 South Carolinians have signed up for the protection so far. The governor is one of them.

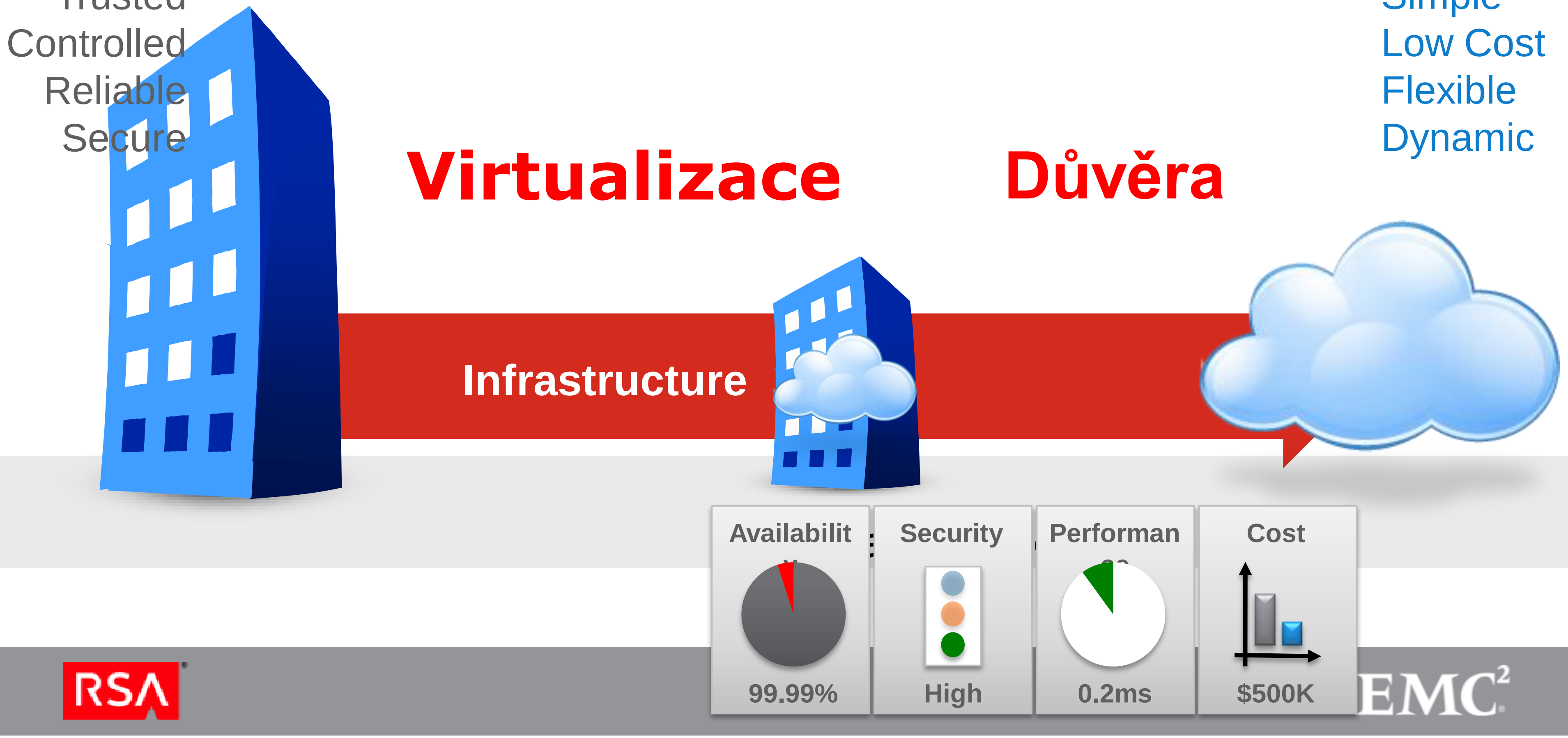
Cloud a Důvěra

Hlavní změny na cestě ke cloudu

Enterprise IT **Private Cloud** **Public Cloud**

Trusted
Controlled
Reliable
Secure

Simple
Low Cost
Flexible
Dynamic

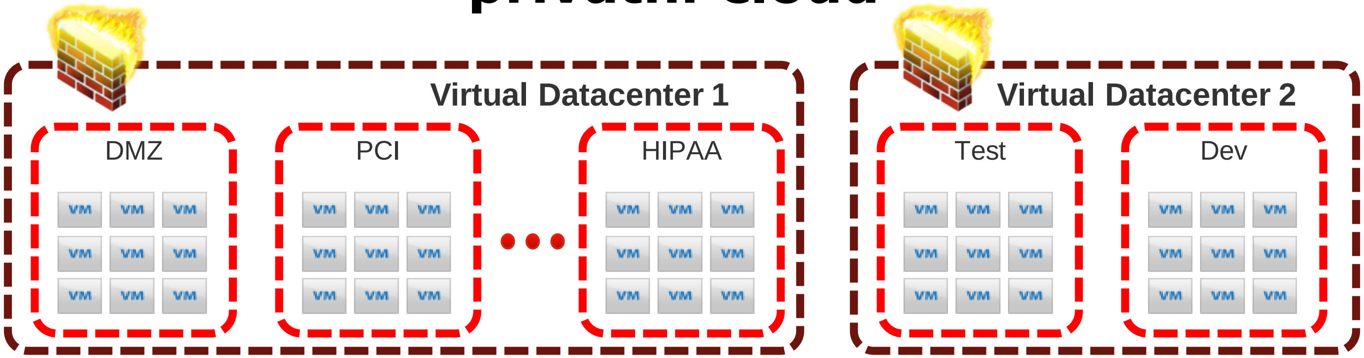


Virtualizace **Důvěra**

Hlavní změny na cestě ke cloudu: krok 1

DOHLED
(SIEM, DLP, GRC, …)

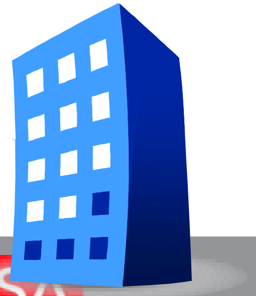
Bezpečnost virtualizace / privátní cloud

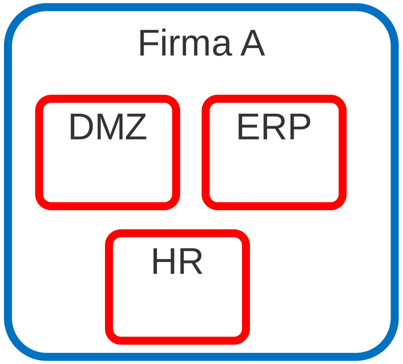


Síťová bezpečnost

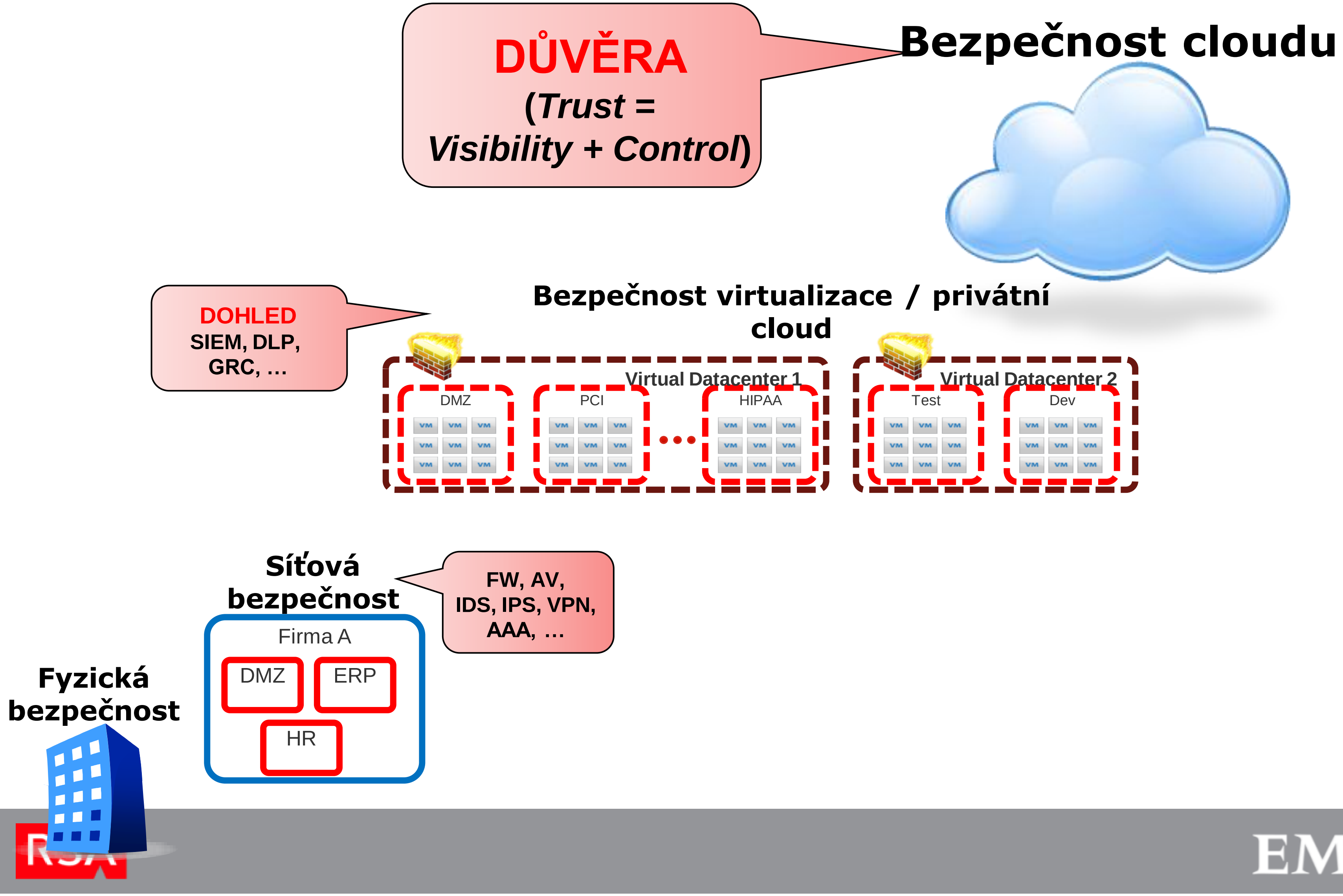
FW, AV, IDS, IPS, VPN, AAA, …

Fyzická bezpečnost





Hlavní změny na cestě ke cloudu: krok 2



DŮVĚRA
(Trust =
Visibility + Control)

Bezpečnost cloudu

DOHLED
SIEM, DLP, GRC, …

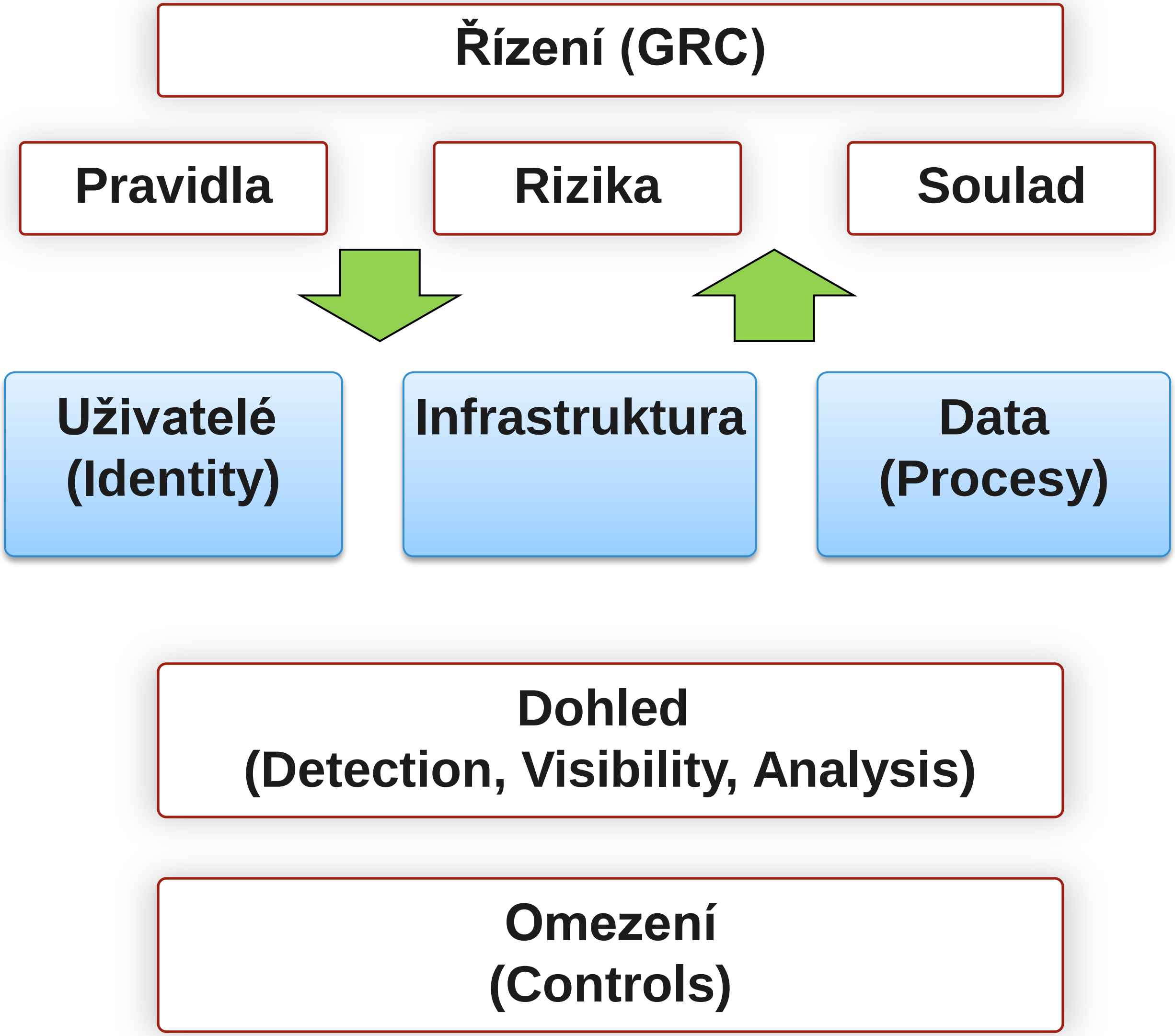
Bezpečnost virtualizace / privátní cloud

Síťová bezpečnost

FW, AV, IDS, IPS, VPN, AAA, …

Fyzická bezpečnost

Bezpečnost v cloudu



Řízení (GRC)

Pravidla

Rizika

Soulad

Uživatelé (Identity)

Infrastruktura

Data (Procesy)

Dohled (Detection, Visibility, Analysis)

Omezení (Controls)

Trust = Visibility + Control

Je to bezpečné ? A je to v soulad ?

- Jednoduchá odpověď provo
  - Na bezpečnost
  - M

Je to dostatečné ?
-pro Vás ?
- pro auditory ?

- „Vidíte dovnitř“? Poznáte útok?
  - Kde jsou Vaše data, kdo k nim přistoupil, co se stalo …
- Můžete vynutit pravidla a „změřit compliance“?
  - Jaká je aktuální realita (technická konfigurace) ?
  - Co přesně je/není splněno ?
- Můžete to dokázat/reportovat?

RSA

EMC²

RSA – Sada řešení (nejen) pro virtuální prostředí

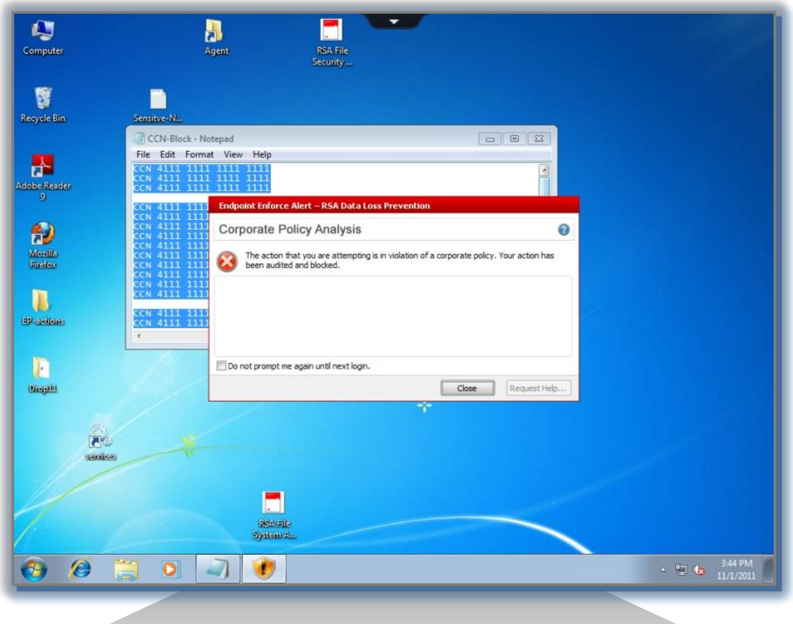
- Ochrana identit, řízení přístupu, detekce fraudu
  - Silná dvoufaktorová a multifaktorová autentizace, risk-based
  - Ochrana proti fraudu
- Ochrana citlivých dat před jejich únikem (DLP)
  - Na úložištích, na síti, na virtuálních desktopech, BYOD, ...
- Důkladný bezpečnostní monitoring a detekce
  - Kompletní SIEM 2. generace: Security Analytics: Logy, Pakety, Intelligence
- Archer GRC, zajištění shody s legislativou a interními předpisy
  - „měření/prokazování compliance“:
    - VMware (virtuální i fyzická infrastruktura, privátní cloud)
    - Cloud (compliance podle CSA)

RSA DLP for Virtual Desktops & Applications

New Threat Vectors Covered:

1) Copying sensitive data from virtual apps & VDI to physical device

2) Saving files from virtual apps & VDI to physical device



CCN-Block - Notepad

```
CCN 4111 1111 1111 1111
CCN 4111 1111 1111 1111
CCN 4111 1111 1111 1111
```

Endpoint Enforce Alert – RSA Data Loss Prevention

Corporate Policy Analysis

The action that you are attempting is in violation of a corporate policy. Your action has been audited and blocked.

□ Do not prompt me again until next login.

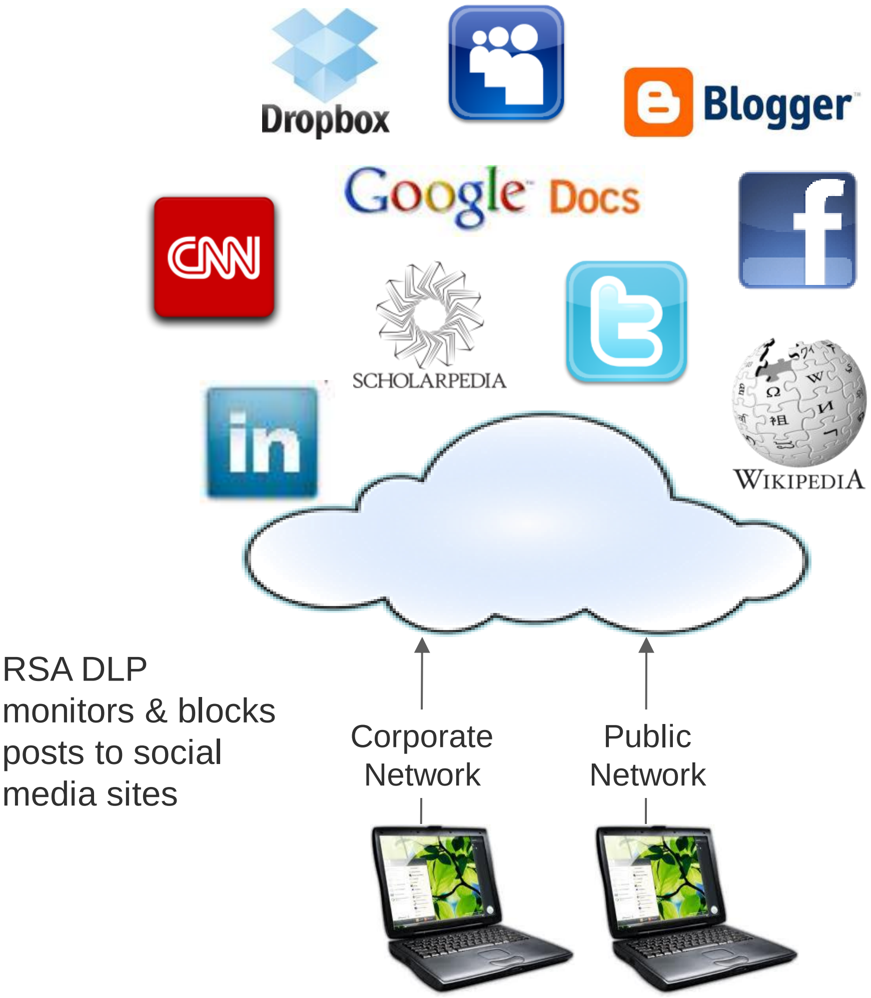
CITRIX

vmware

Key Benefits:

- No agent on endpoints
- Freedom & flexibility to BYOD

RSA DLP: Enhanced Support for Social Media



RSA DLP monitors & blocks posts to social media sites

Avoid Unauthorized Sharing

- Advanced monitoring for posts to popular social media sites
- Prevent company confidential information from being leaked

Monitor

- Log all datacenter actions
- Network monitoring
- Alerting
- Fine grained auditing of activity in the virtual environment

prevention

detection

How Fast To Detect & Act

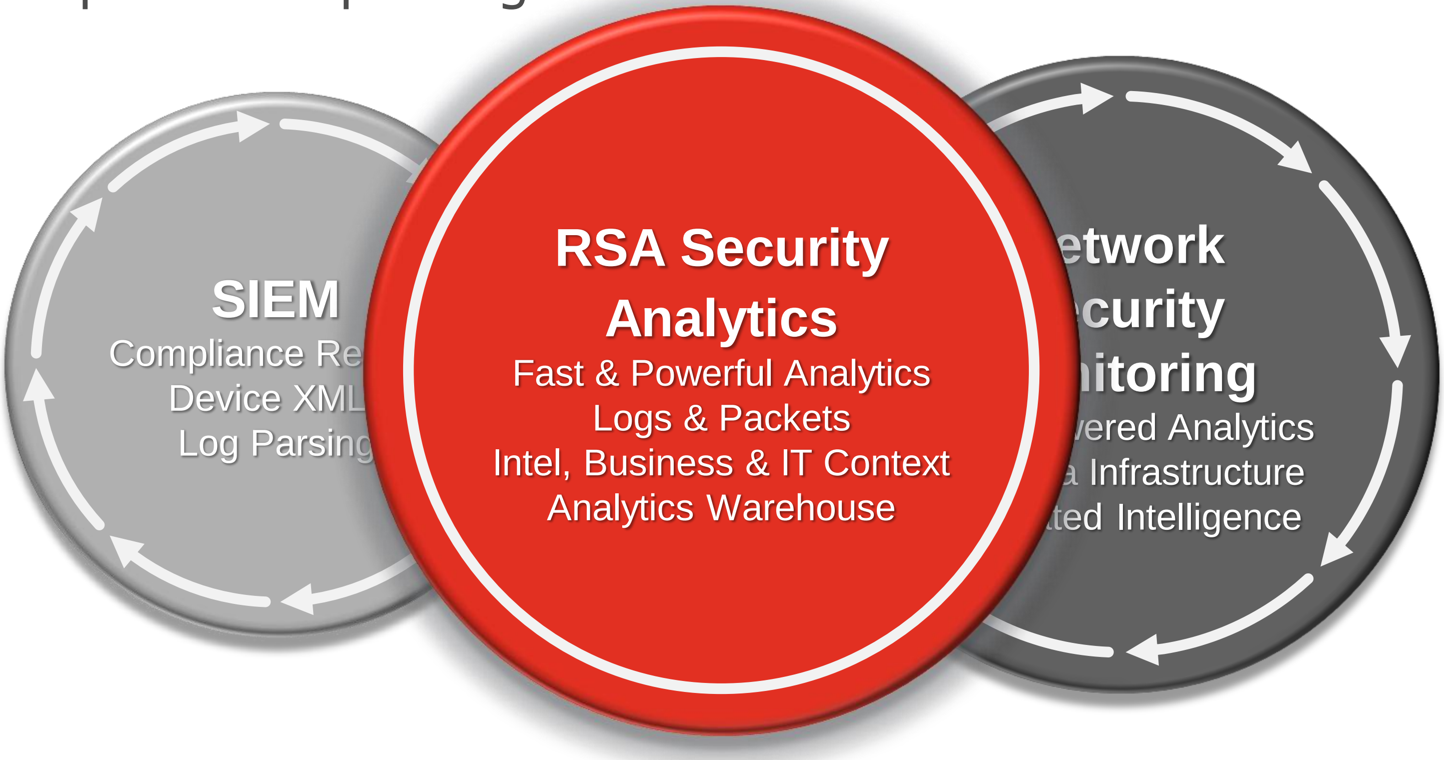
99% of breaches led to compromise within “days” or less with 85% leading to data exfiltration in the same time

85% of breaches took “weeks” or more to discover

Source: Verizon 2012 Data Breach Investigations Report

RSA Security Analytics: Changing The Security Management Status Quo

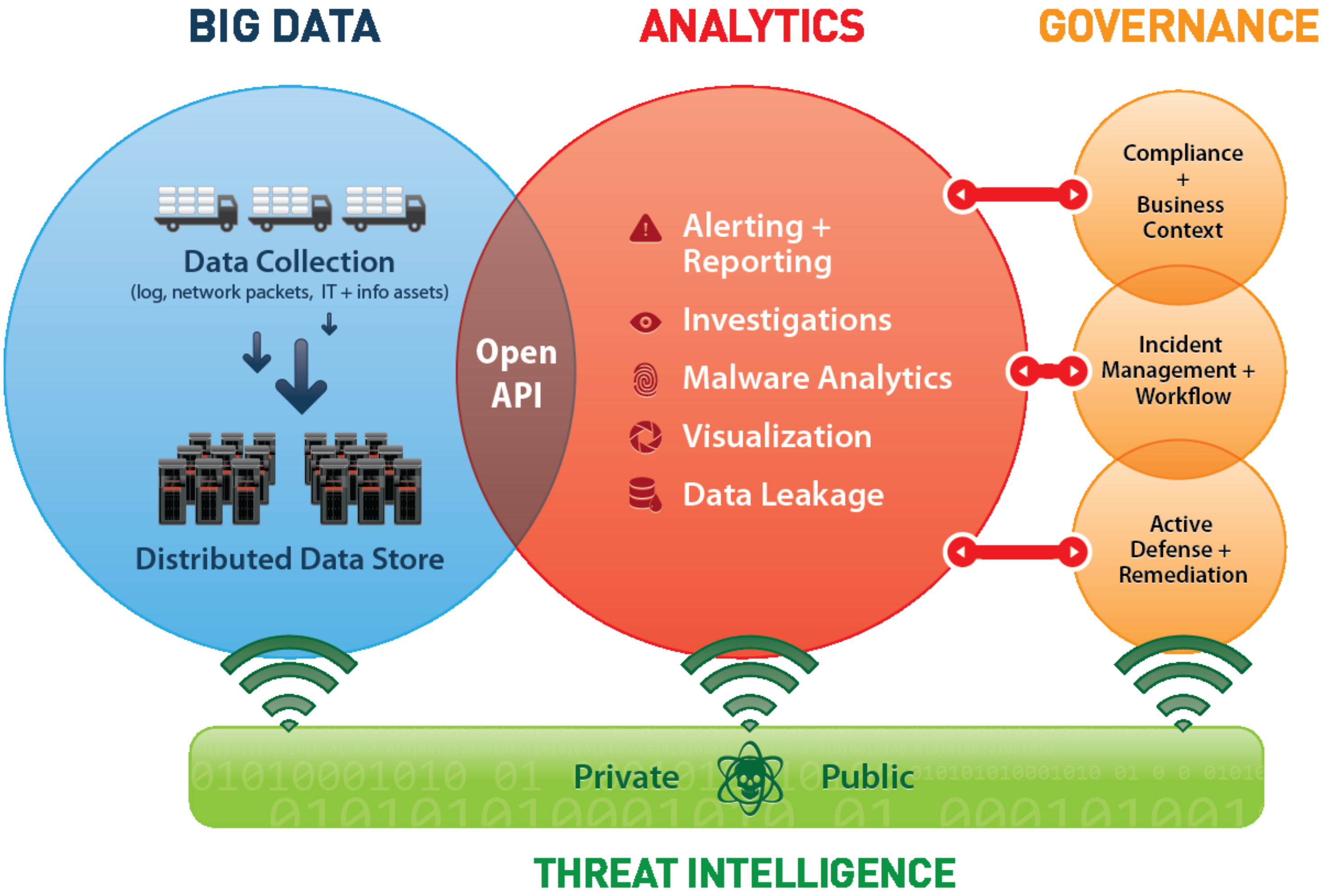
Unified platform for security monitoring, incident investigations and compliance reporting



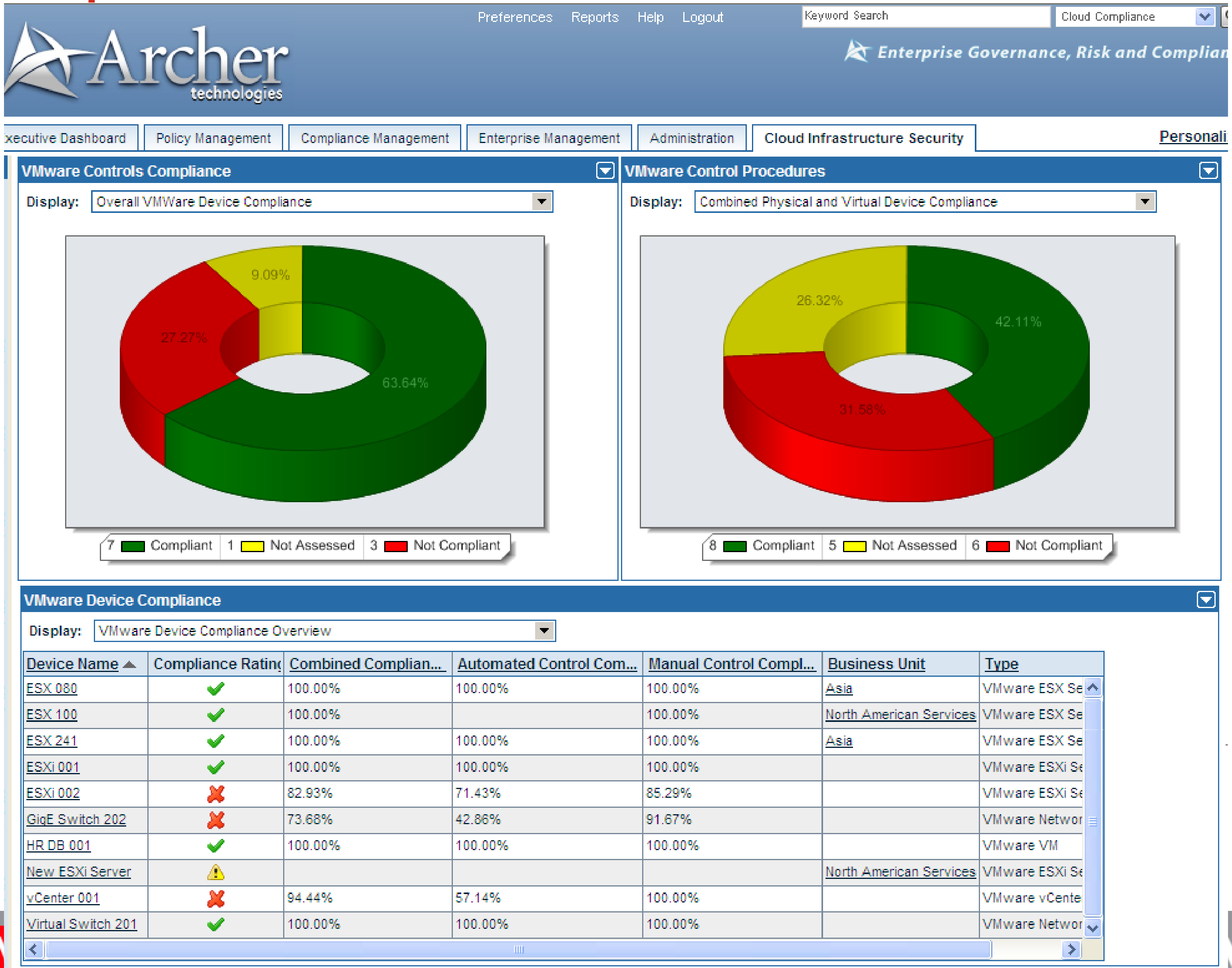
SEE DATA YOU DIDN'T SEE BEFORE,
UNDERSTAND DATA YOU DIDN'T EVEN CONSIDER BEFORE

RSA Security Management Compliance Vision

Delivering Visibility, Intelligence and Governance



Compliance Dashboard



VMware Controls Compliance

Display: Overall VMWare Device Compliance

7 🟩 Compliant | 1 🟨 Not Assessed | 3 🟥 Not Compliant

VMware Control Procedures

Display: Combined Physical and Virtual Device Compliance

8 🟩 Compliant | 5 🟨 Not Assessed | 6 🟥 Not Compliant

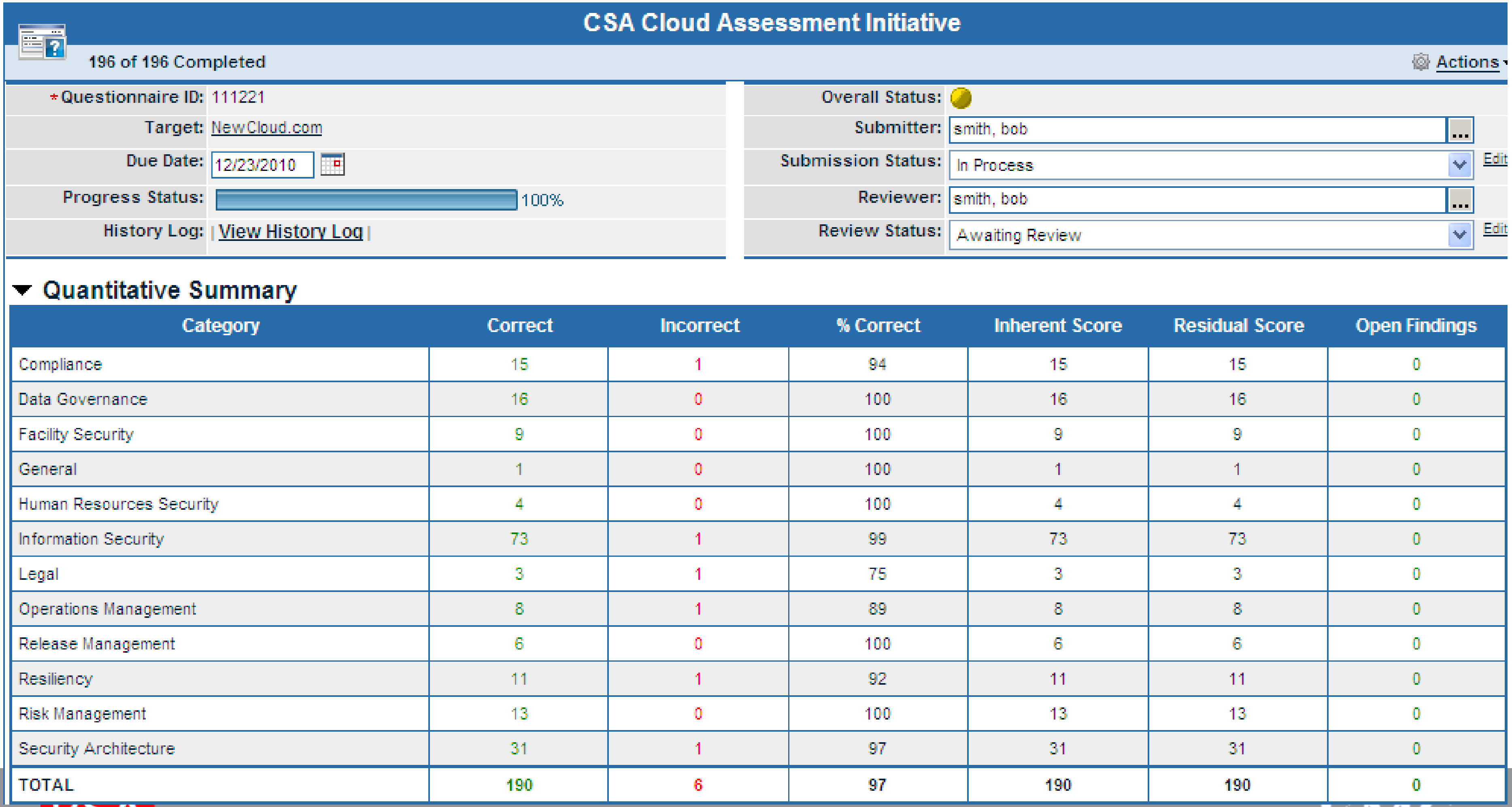
VMware Device Compliance

Display: VMware Device Compliance Overview

Device Name ▲	Compliance Ratin	Combined Complian...	Automated Control Com...	Manual Control Compl...	Business Unit	Type
ESX 080	✓	100.00%	100.00%	100.00%	Asia	VMware ESX Se
ESX 100	✓	100.00%		100.00%	North American Services	VMware ESX Se
ESX 241	✓	100.00%	100.00%	100.00%	Asia	VMware ESX Se
ESXi 001	✓	100.00%	100.00%	100.00%		VMware ESXi Se
ESXi 002	✗	82.93%	71.43%	85.29%		VMware ESXi Se
GigE Switch 202	✗	73.68%	42.86%	91.67%		VMware Networ
HR DB 001	✓	100.00%	100.00%	100.00%		VMware VM
New ESXi Server	⚠				North American Services	VMware ESXi Se
vCenter 001	✗	94.44%	57.14%	100.00%		VMware vCente
Virtual Switch 201	✓	100.00%	100.00%	100.00%		VMware Networ

Use Case: Assessing Cloud Service Providers

RISK: Choosing the wrong service provider



CSA Cloud Assessment Initiative

196 of 196 Completed

*Questionnaire ID:	111221	Overall Status:	●
Target:	NewCloud.com	Submitter:	smith, bob
Due Date:	12/23/2010	Submission Status:	In Process
Progress Status:	100%	Reviewer:	smith, bob
History Log:	View History Log	Review Status:	Awaiting Review

Quantitative Summary

Category	Correct	Incorrect	% Correct	Inherent Score	Residual Score	Open Findings
Compliance	15	1	94	15	15	0
Data Governance	16	0	100	16	16	0
Facility Security	9	0	100	9	9	0
General	1	0	100	1	1	0
Human Resources Security	4	0	100	4	4	0
Information Security	73	1	99	73	73	0
Legal	3	1	75	3	3	0
Operations Management	8	1	89	8	8	0
Release Management	6	0	100	6	6	0
Resiliency	11	1	92	11	11	0
Risk Management	13	0	100	13	13	0
Security Architecture	31	1	97	31	31	0
TOTAL	**190**	**6**	**97**	**190**	**190**	**0**

Results: Benchmarking vendors based on CSA standards

RSA řešení pro bezpečnost a compliance

RSA Vám zajistí:

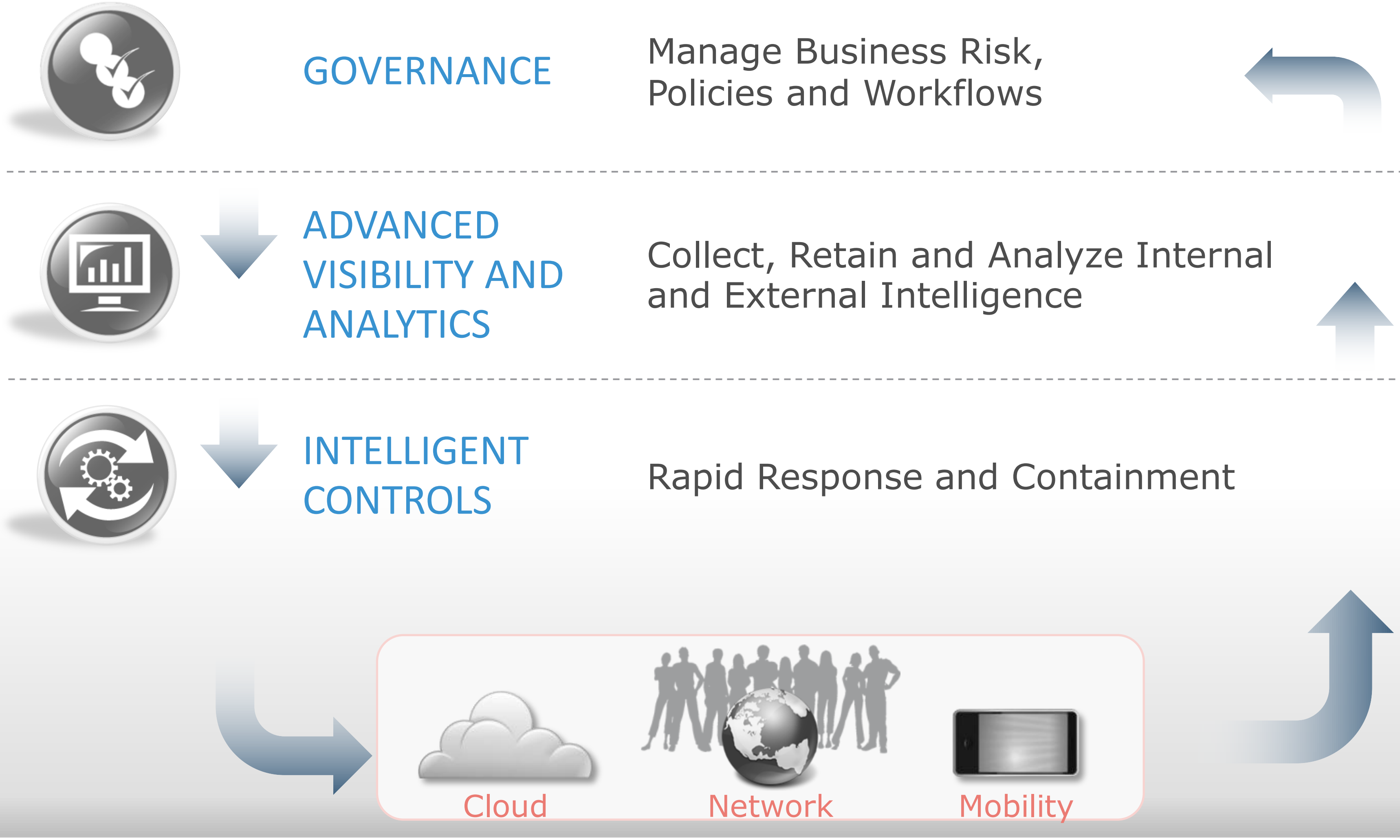
-„Pohled dovnitř“

-„Měřitelnou compliance“

-Důkazy a reporty

- „Vidíte dovnitř“? Poznáte útok?
  - Kde jsou Vaše data, kdo k nim přistoupil, co se stalo …
- Můžete vynutit pravidla a „změřit compliance“?
  - Jaká je aktuální realita (technická konfigurace) ?
  - Co přesně je/není splněno ?
- Můžete to dokázat/reportovat?

RSA Approach



GOVERNANCE

Manage Business Risk, Policies and Workflows

ADVANCED VISIBILITY AND ANALYTICS

Collect, Retain and Analyze Internal and External Intelligence

INTELLIGENT CONTROLS

Rapid Response and Containment

RSA Approach

GOVERNANCE

- RSA Archer eGRC Suite

ADVANCED VISIBILITY AND ANALYTICS

- RSA Security Analytics
- RSA Spectrum
- RSA DLP Suite
- RSA SilverTail
- RSA FraudAction
- RSA CCI
- RSA eFraud Network
- RSA NetWitness Live

INTELLIGENT CONTROLS

- RSA Adaptive Authentication
- RSA Access Manager
- RSA SecurID
- RSA Transaction Monitoring
- RSA Federated Identity Manager
- RSA Data Protection
- RSA DLP Suite
- RSA BSAFE

RSA Approach

- Risk-based: Common, flexible platform to manage risk throughout entire enterprise
- Contextual: Fusion of high-speed analytics and advanced visibility
- Agile: Controls that can be quickly adjusted based on changing risk posture

Otázky?

Ivan Svoboda

ivan.svoboda@rsa.com

+ 420 604 293 394

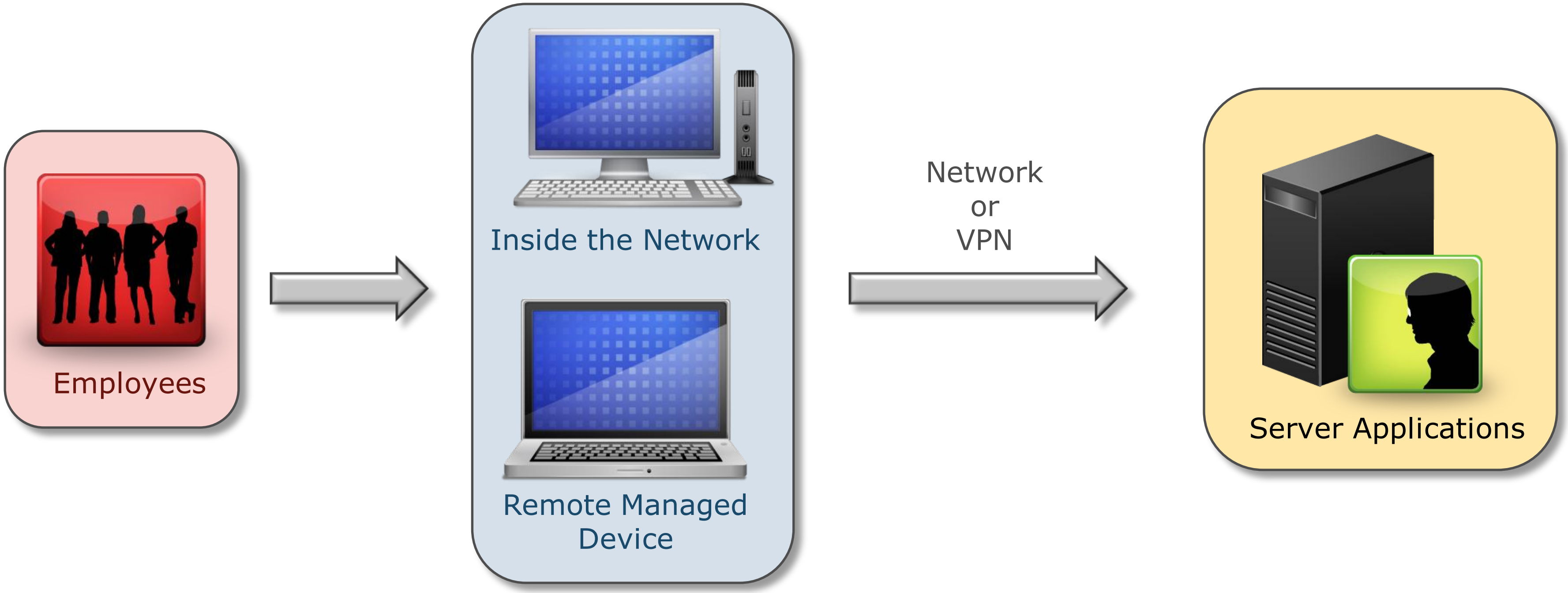
RSA®

The Security Division of EMC

rsa.com/rsavirtualization

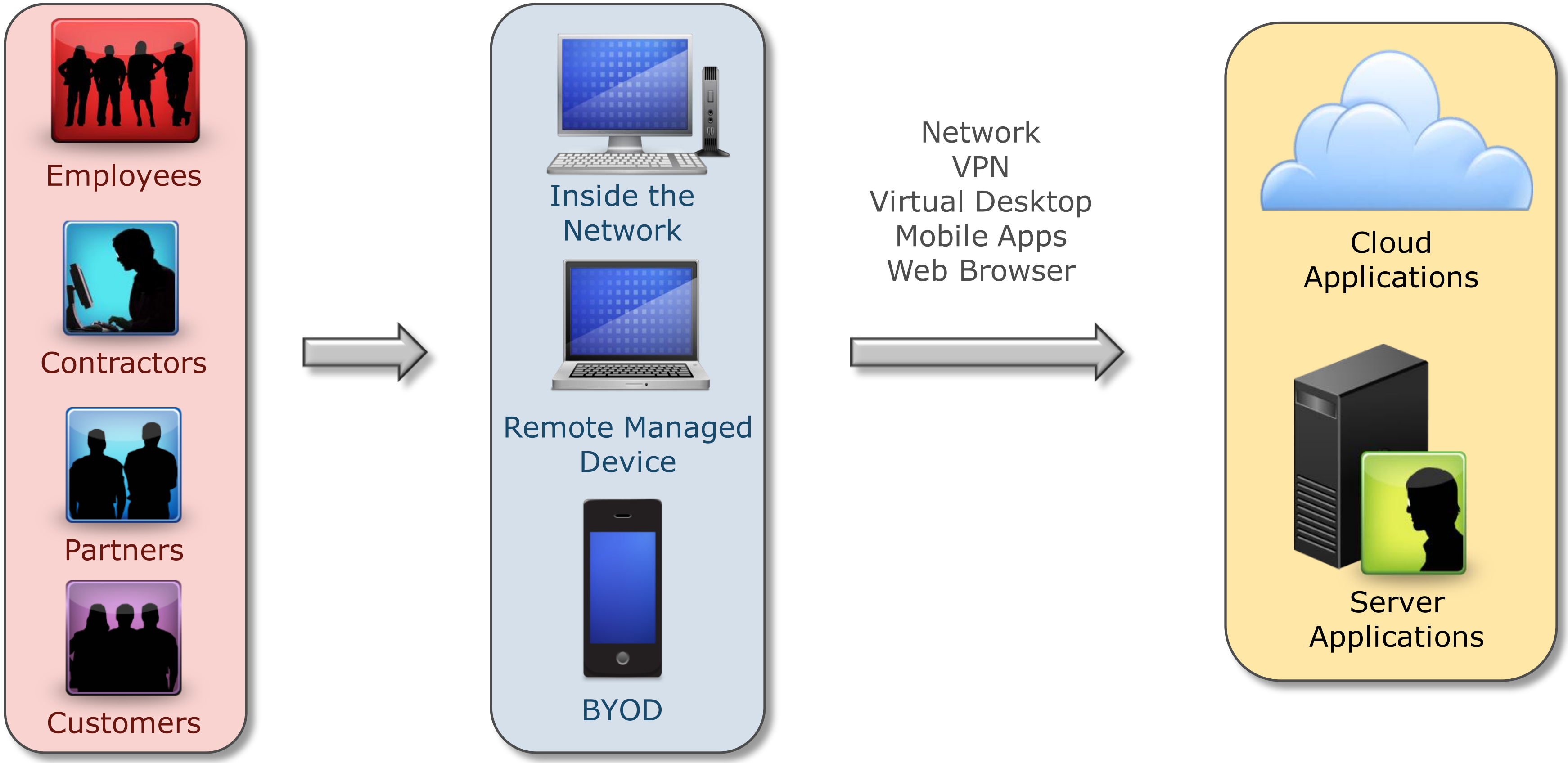
Before: Controlled Network Environment

Corporate Users	Managed Devices	Controlled Access Points	Information on a Network



Today: Any User, Any Device, Anywhere

External and **Temporary** Users | **Unmanaged** Devices | **Uncontrolled** Access Points | Information in Public **Cloud** and **Hosted** Applications



Employees

Contractors

Partners

Customers

Inside the Network

Remote Managed Device

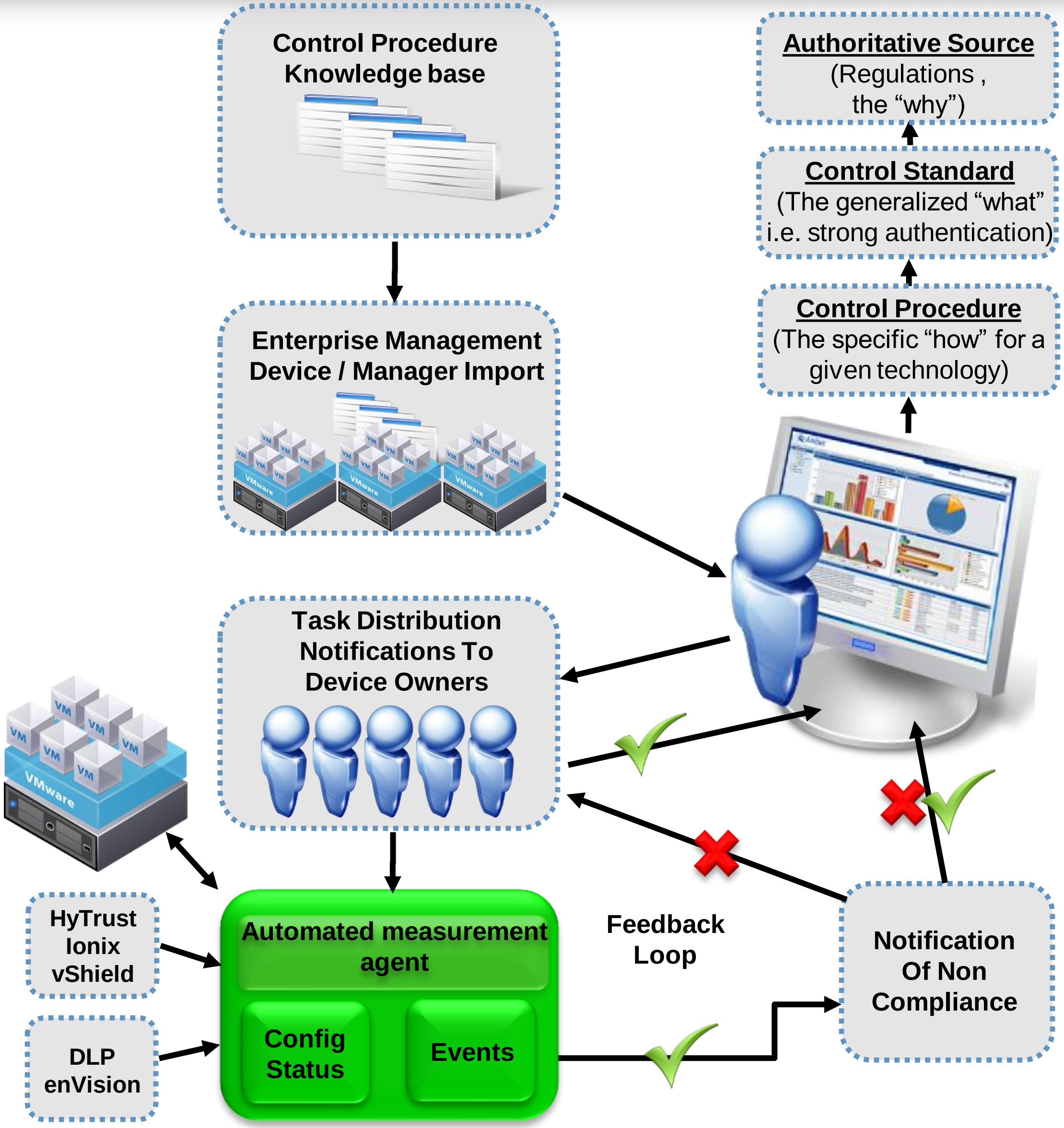
BYOD

Network
VPN
Virtual Desktop
Mobile Apps
Web Browser

Cloud Applications

Server Applications

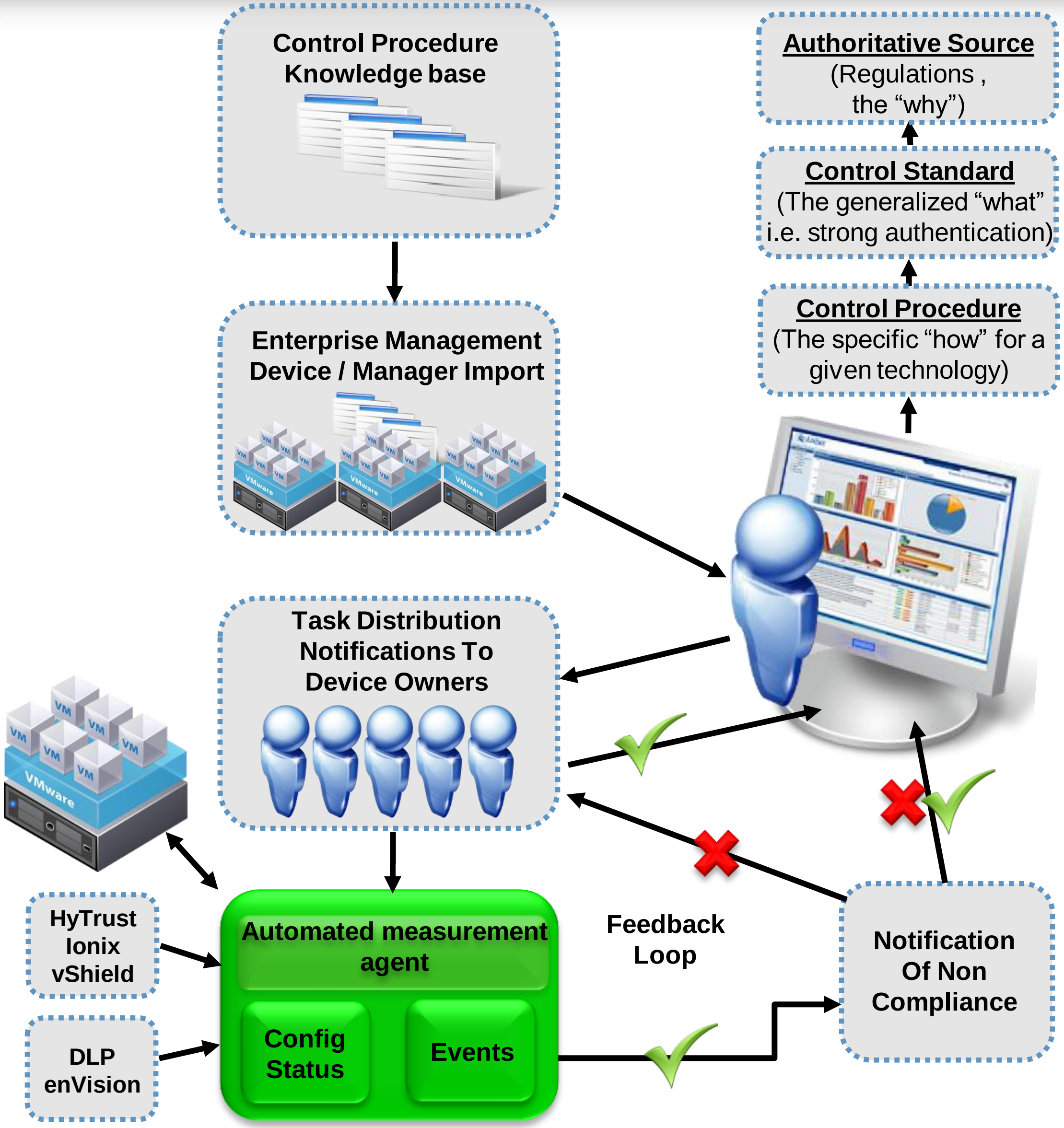
Compliance Cycle with Archer for VMware



- REGULACE: **PROČ** ?
- STANDARDY: **CO** ?
- PROCEDURY: **JAK** ?

The Security Division of EMC

Deployment and Measurement Cycle

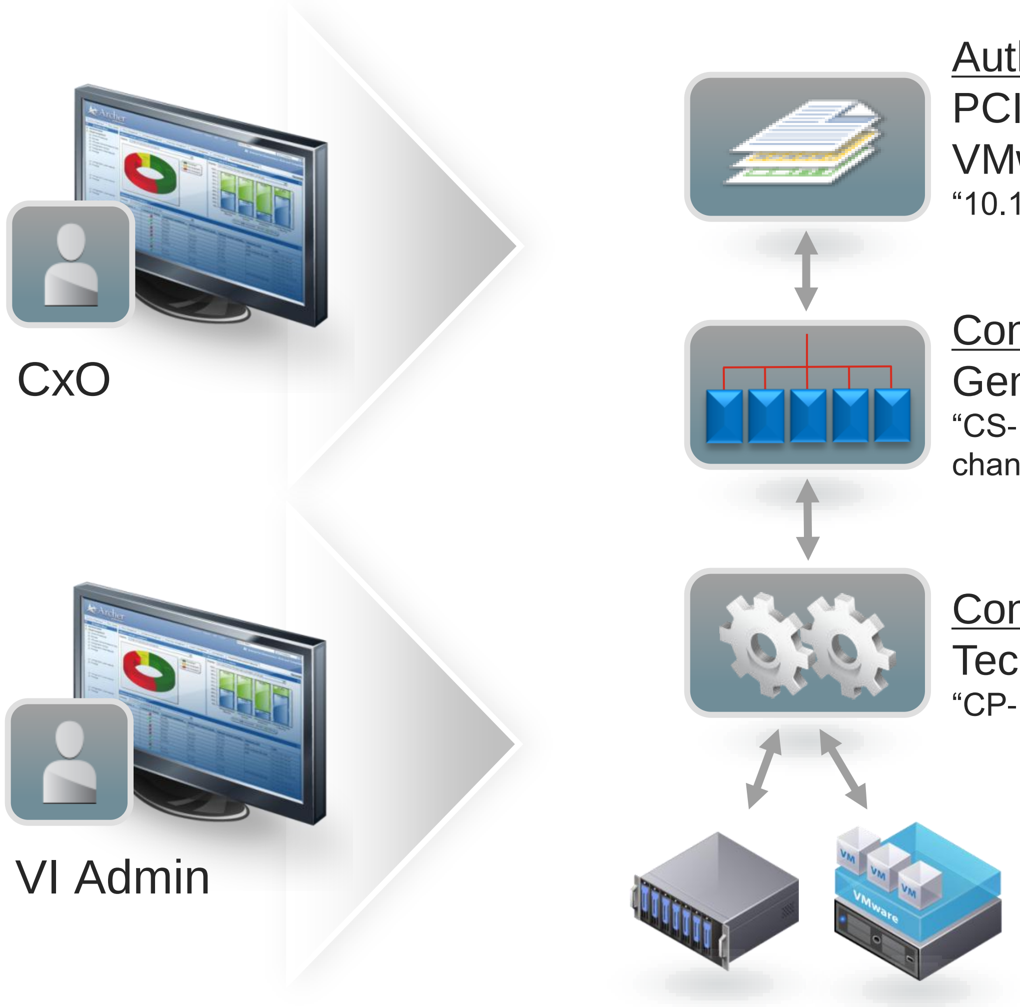


Control Procedure Knowledge base
Enterprise Management Device / Manager Import
Task Distribution Notifications To Device Owners
HyTrust
Ionix
vShield
DLP
enVision
Automated measurement agent
Config Status
Events
Feedback Loop
Notification Of Non Compliance
Authoritative Source
(Regulations , the "why")
Control Standard
(The generalized "what" i.e. strong authentication)
Control Procedure
(The specific "how" for a given technology)
VM
VMware

- Security / VI team begins deployment project plan
- Device data imported and mapped to CP's
- Distributes deployment tasks to device owners and receives feedback
- Measurement ecosystem gathers status and events
- Device owners notified of any remediation tasks needed
- Measurement ecosystem feedback confirms / denies "fix"
- Overall compliance status constantly updated

RSA®
The Security Division of EMC

RSA Archer: Mapping VMware security controls to regulations and standards



<u>Authoritative Sources</u>
PCI, HIPAA, SOX, CSA,
VMware Hardening Guide, etc.
"10.10.04 Administrator and Operator Logs"

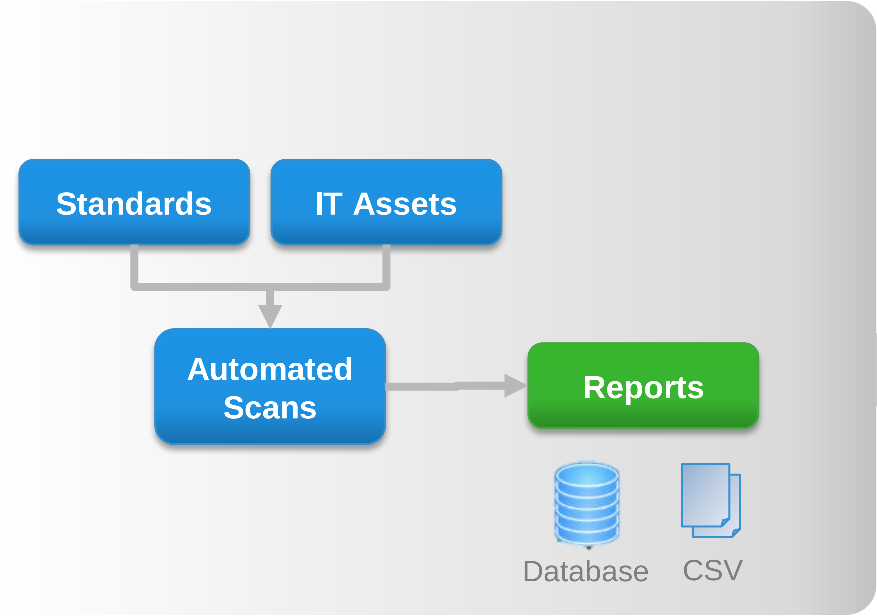
<u>Control Standard</u>
Generalized security controls
"CS-179 Activity Logs – system start/stop/config changes etc."

<u>Control Procedure</u>
Technology-specific control
"CP-108324 Persistent logging on ESXi Server"

Integrating RSA Archer & EMC/VMware

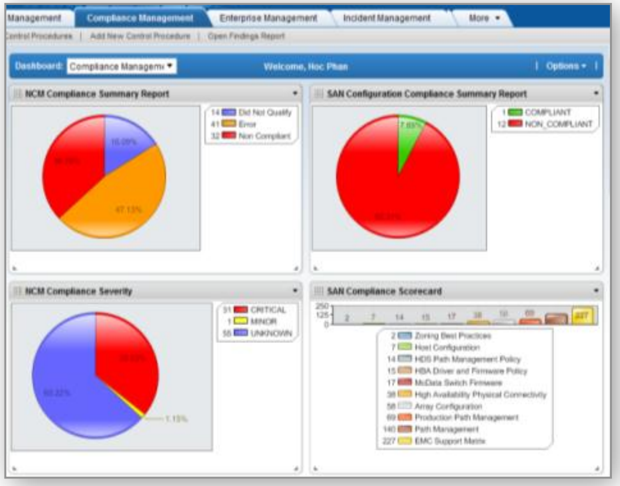
Measure
IT INFRASTRUCTURE

Pass the audit
ENTERPRISE COMPLIANCE



Data Feed Manager

RSA Archer



- ✓ Scan critical IT assets automatically
- ✓ Check compliance status
- ✓ Return assessment results

- ✓ Import results automatically
- ✓ Map to other solutions or policies
- ✓ Show relevant reports in dashboard