Extending SCAP into the VMware virtual infrastructure

Chris Farrow, VMware (cfarrow@vmware.com)

Rob Hollis, ThreatGuard (robert.hollis@threatguard.com)

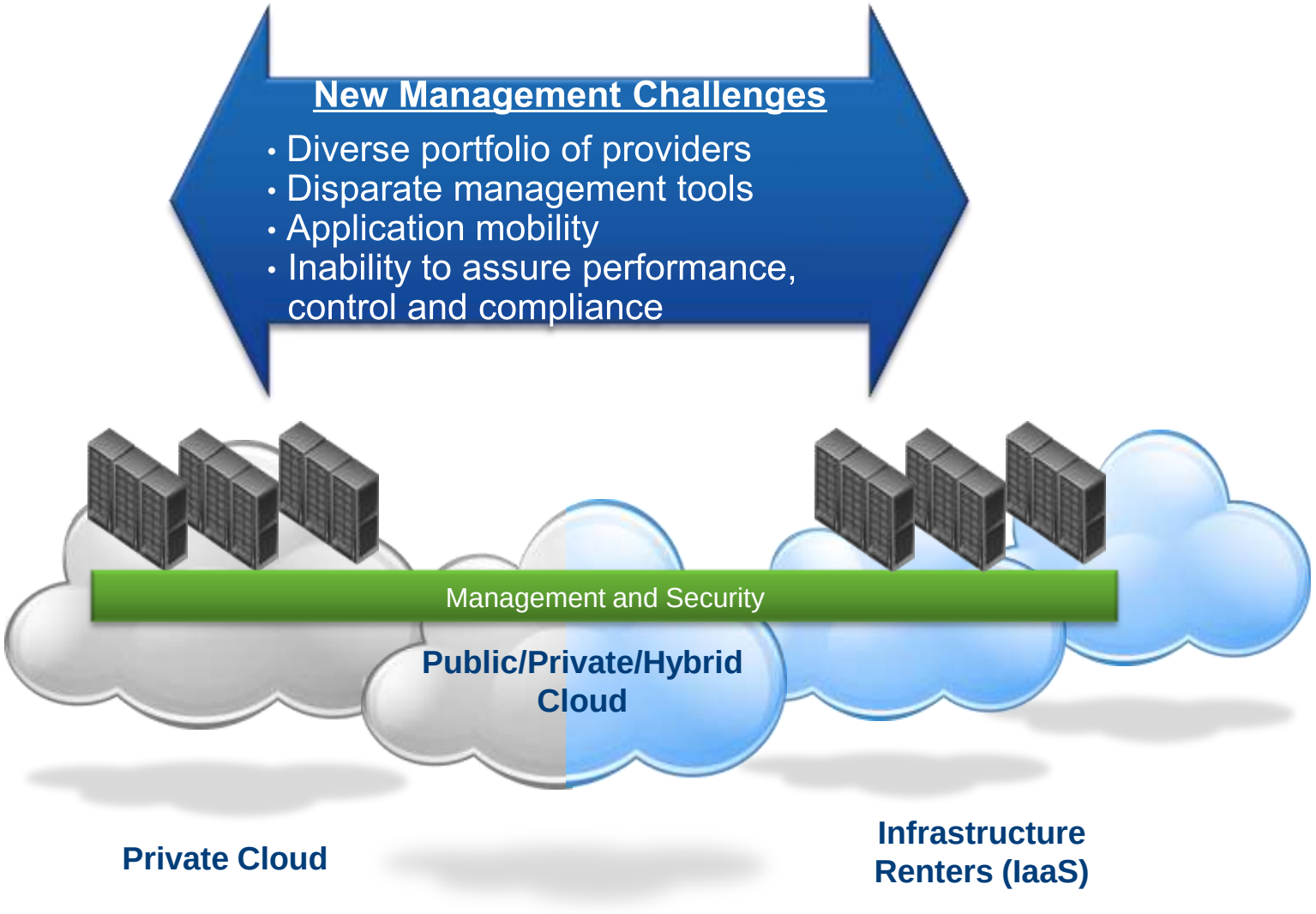
September 2010

Confidential

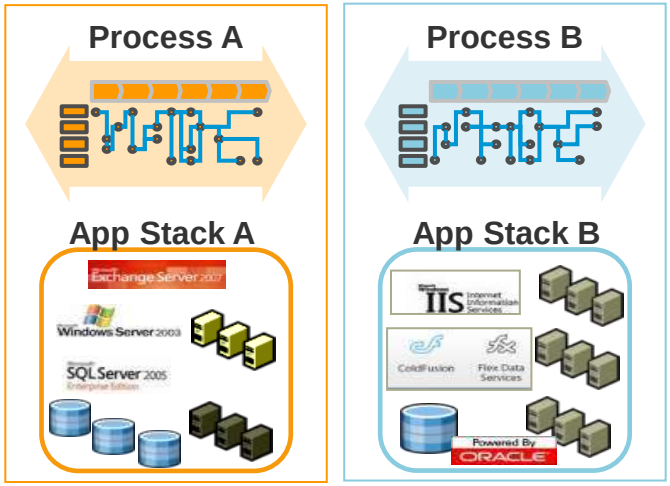
Agenda

- The Evolution of IT management, compliance & security
- VMware's commitment: open, interoperable & secure
- VMware Authoritative guidance & SCAP
  - VMware & ThreatGuard joint project
  - Extending the standards
  - Translating the authoritative guidance
- SCAP solutions from ThreatGuard
- VMware Configuration & Compliance Solution
  - Future VMware SCAP solutions

IT Management Is Changing in the Virtualization-Cloud Era

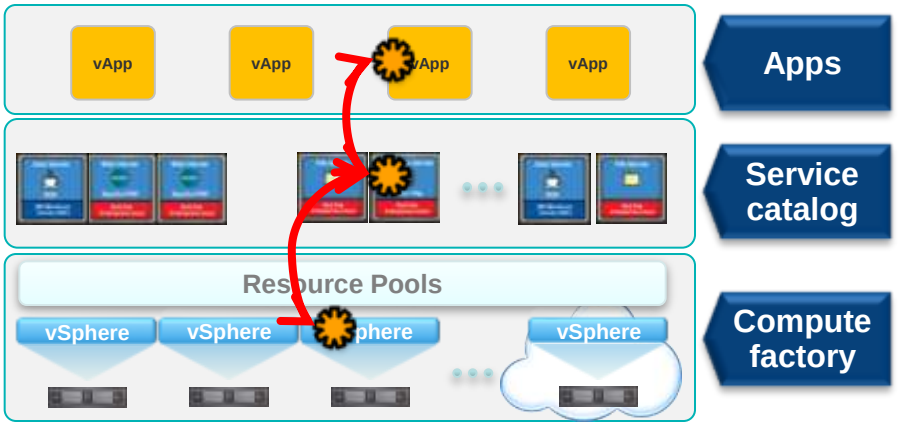


Cloud Drives Changes in Management Requirements



Traditional Management

- Static bindings between processes, applications, and infrastructure
- Change is carefully planned, risky, manual, and slow
- Heterogeneous elements and processes across silos
- Management software executes to the lowest common denominator



Cloud Management

- Dynamic relationships across all layers of the technology stack
- Change is constant and automated
- Normalization of data and elements
- Massive standardization and high-level abstraction
- Day-to-day is automated; management should focus on higher order tasks

Virtualization & Cloud Management: Why VMware?

VMware Virtualization & Cloud Management

From the leader in virtualization & cloud infrastructure – specifically for dynamic data centers – to simplify how IT is managed

Zero-Touch Automation

- Optimizes operational efficiency with built-in automation
- Native management designed-in, at each architectural layer
- Embedded expertise helps you make smarter use of virtual infrastructure

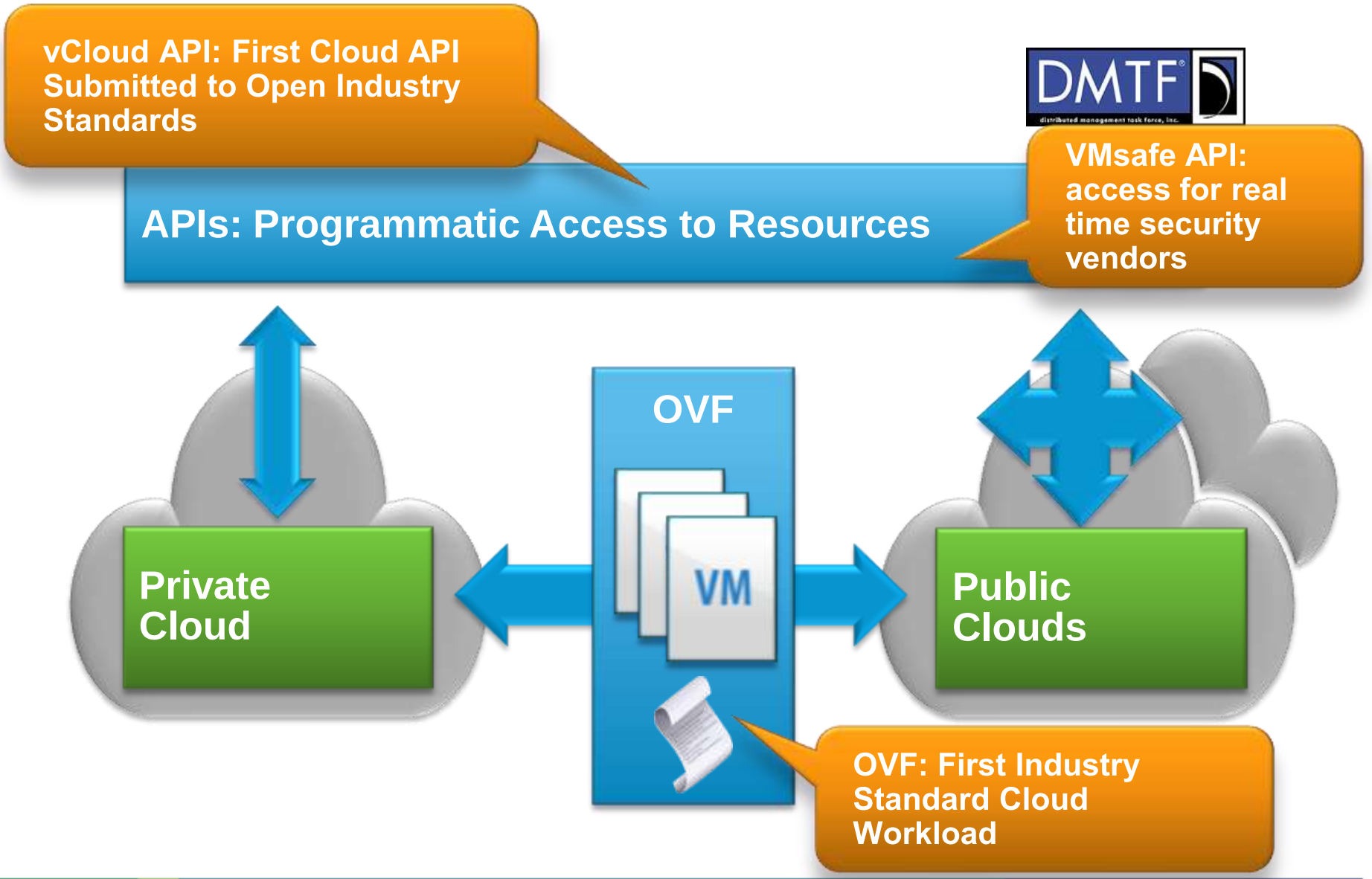
Policy-Driven Service Assurance

- Controls dynamic environments to assure compliance & performance
- Delivers self-service with control
- Self-manages to desired state
- Reduces risk & ensures compliance and security

Management & Cloud Interoperability

- Freedom of choice via management interoperability with ecosystem partners
- Cloud interoperability across service providers
- Open and standards-based approach
- Enables application mobility across clouds

VMware's Commitment: open, interoperable & secure



VMware's Commitment to Authoritative Guidance & SCAP

- Publication of vSphere Security Hardening Guide
- Publication of vCloud Director Security Hardening Guide
- ThreatGuard & VMware partnership
  - Extension of OVAL & SCAP standard to include virtual infrastructure
  - Translation of vSphere Security Hardening Guide to SCAP
- VMware SCAP solutions in the works (more later in this deck)

ThreatGuard

Extending SCAP into the VMware virtual infrastructure

Setting the Standard

About ThreatGuard

Engineering Company

- Founded: 2002; Standards: 2004; SCAP: 2006
- Goal: Be the BASF of SCAP
- Goal: Provide most widely used SCAP engine in the world

Business Concepts

- Technical Socializing
  (NIST, NSA, MITRE)
- Enable, extend, innovate
  (Secutor Prime, S-CAT)
- Drive the standards
  (Remediation, Deviations, Scoring)

Cadre-driven Outreach

- Top contributor for OVAL
  (9 straight quarters)
- Foundational SCAP Support
  (Key roles in FDCC)
- Donated technology
  (Make SCAP tangible)

The Forerunner of SCAP Technology

- Commitment to SCAP languages since 2004
- Primary tool used to establish the FDCC images in the OMB lab
- Leveraged in OMB demonstration as exemplary SCAP

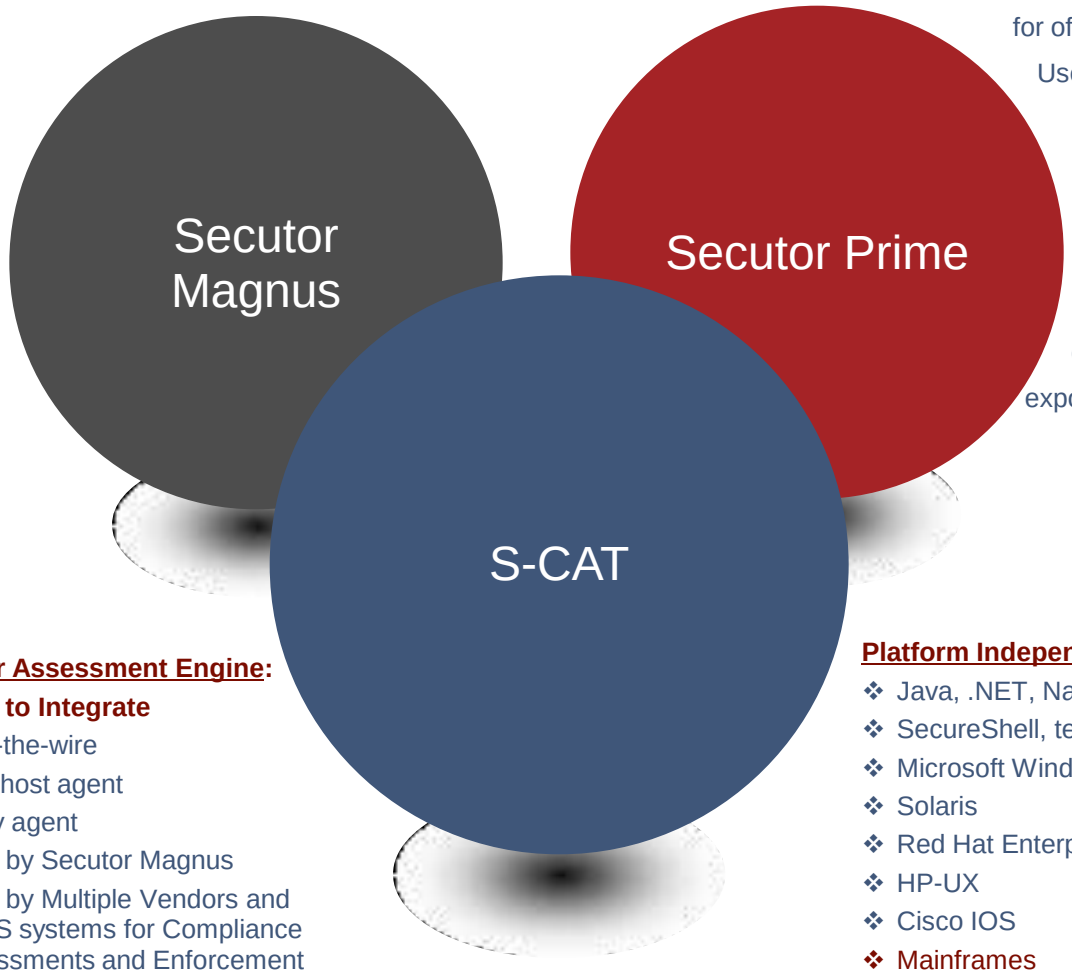
Our Task for SCAP 1.2

- Task Dates
  - Official Start: June 24
  - OVAL 5.8 cutoff: July 21
  - SCAP 1.2 cutoff: August 15
- Create OVAL Extensions for VMware
  - visdkmanagedobject_test in the ESX schema
  - Extensions submitted June 25
  - Officially announced as part of OVAL 5.8 on July 2
- Create Sample Content for Extensions
  - Sample content generated: June 25
  - Extended content: July 2
  - Remediation content: July 7

Flexibility

Hybrid architecture to support multiple deployment requirements

An enterprise tool for the trenches. High-level views easily show problem areas and quickly drill down to expose guidance on how to make things better.



Desktop module can stand alone or be used for off-line reconnaissance. Use in closed labs to test software operability under tightened security. Use in remote offices with degraded comm lines; export results for Magnus.

Modular Assessment Engine:

- **Easy to Integrate**
- Over-the-wire
- Localhost agent
- Proxy agent
- Used by Secutor Magnus
- Used by Multiple Vendors and GOTS systems for Compliance Assessments and Enforcement

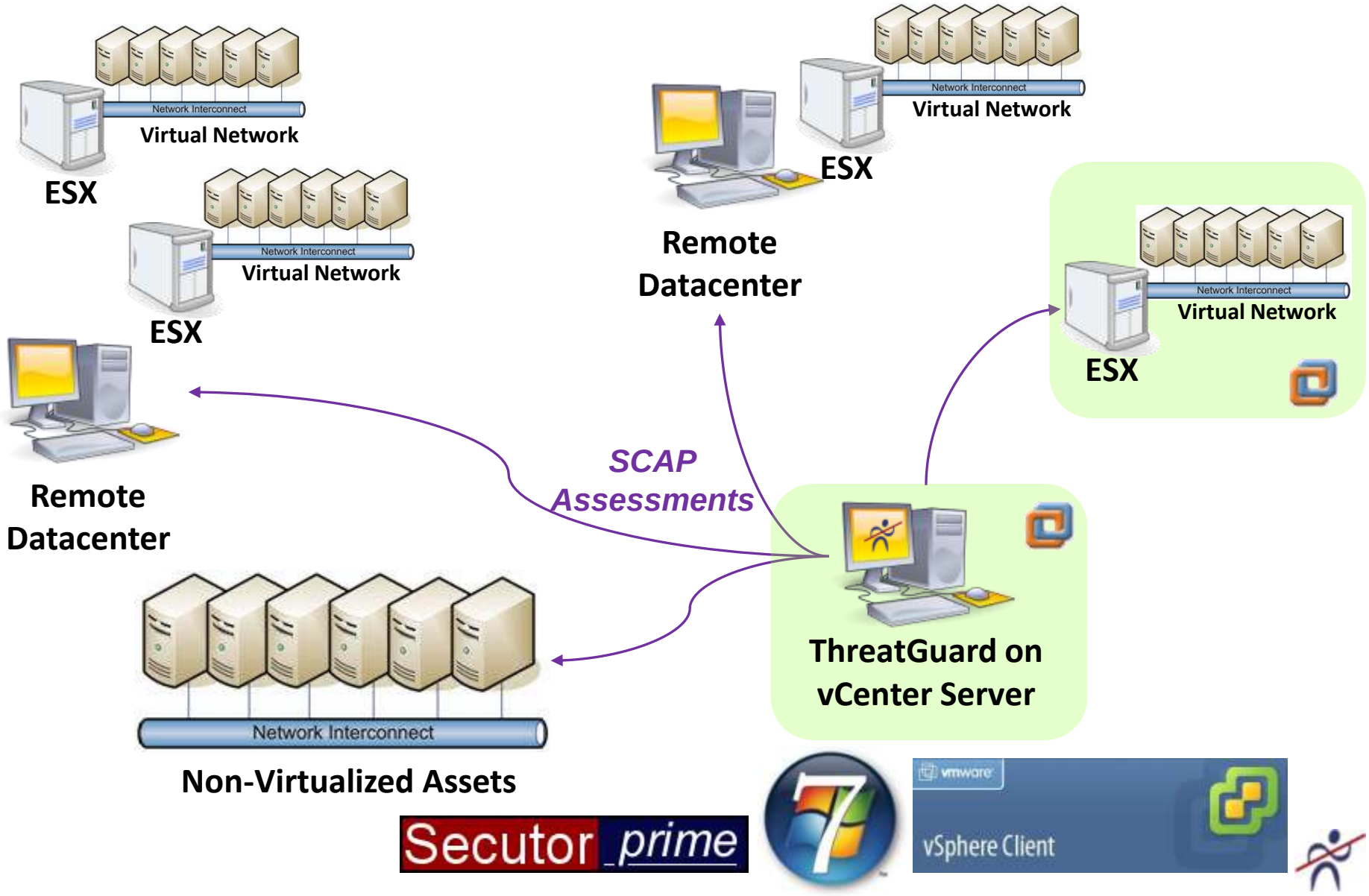
Platform Independent Design:

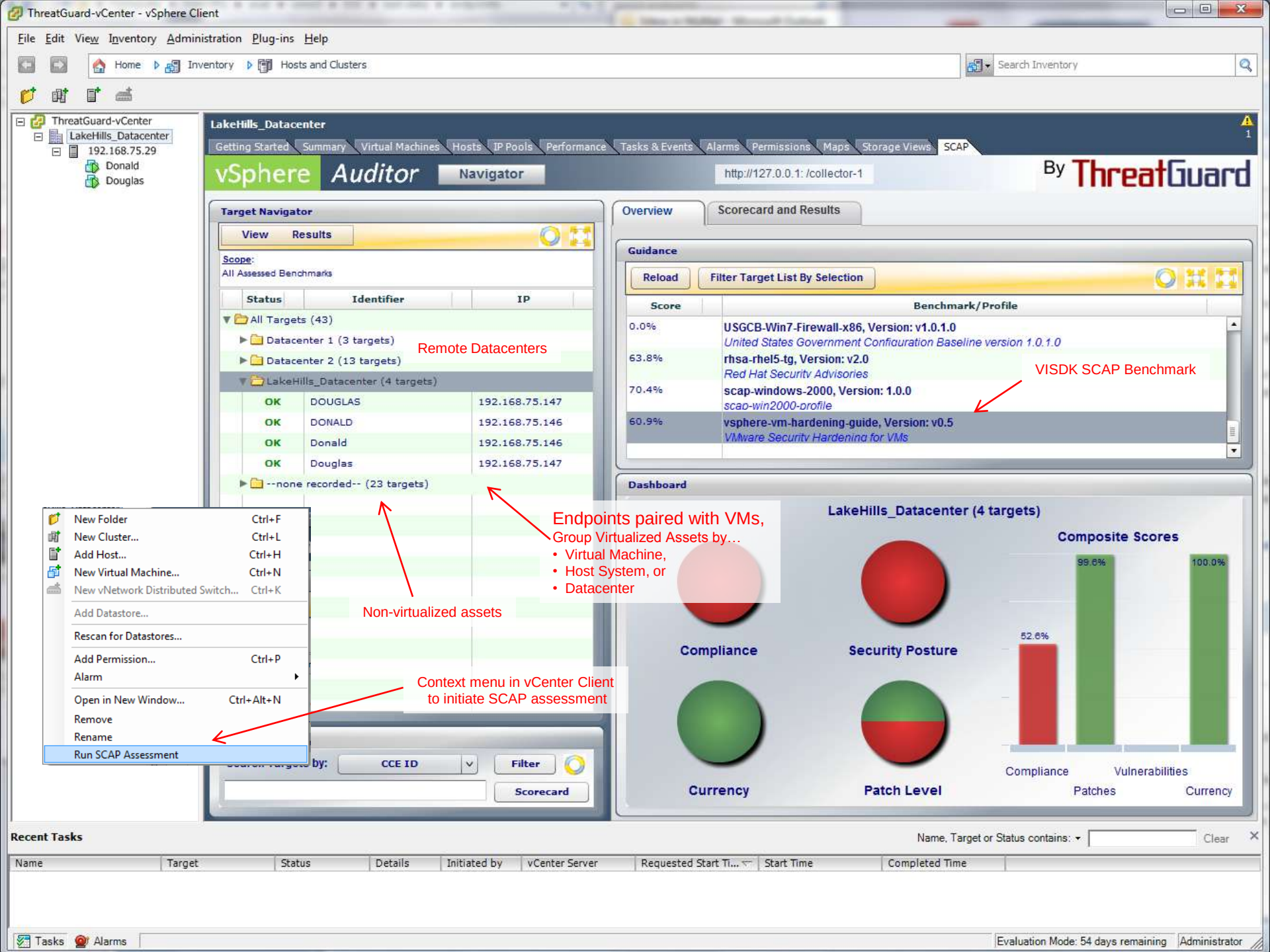
- Java, .NET, Native Binary
- SecureShell, telnet, rexec
- Microsoft Windows
- Solaris
- Red Hat Enterprise Linux
- HP-UX
- Cisco IOS
- Mainframes
- MacOSX
- And more…

Today's Demo

- SCAP Assessment
  - Target: VirtualMachine Objects in the VI
  - Secutor Prime
    - *Desktop SCAP Tool*
    - *Used in every Federal Agency, across DoD, and in 80+ foreign countries*
    - *Remediation*
  - S-CAT
    - *Embeddable SCAP Engine*
    - *Used to SCAP-enable existing products quickly*
    - *SCAP Data in vSphere Client*
  - Secutor Magnus (aka vSphere Auditor)
    - *ThreatGuard Enterprise SCAP Product*
    - *Correlation*
    - *Aggregation*
- Advanced Topics
  - **O**pen **R**emediation and **A**djustment **L**anguage
  - **S**CAP **I**ntegration through **M**anageable **P**rocess **L**inks
  - **C**orrelation **L**inkages **O**f the **U**nderlying **D**evices
  - **C**yberScope **A**ggregation of **F**ederal **E**numerations

Demo Environment




ThreatGuard-vCenter - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory Hosts and Clusters
Search Inventory
ThreatGuard-vCenter
LakeHills_Datacenter
192.168.75.29
Donald
Douglas
LakeHills_Datacenter
Getting Started Summary Virtual Machines Hosts IP Pools Performance Tasks & Events Alarms Permissions Maps Storage Views SCAP
vSphere Auditor Navigator
http://127.0.0.1: /collector-1
By ThreatGuard
Target Navigator
View Results
Scope:
All Assessed Benchmarks
Status Identifier IP
All Targets (43)
Datacenter 1 (3 targets)
Datacenter 2 (13 targets)
LakeHills_Datacenter (4 targets)
OK DOUGLAS 192.168.75.147
OK DONALD 192.168.75.146
OK Donald 192.168.75.146
OK Douglas 192.168.75.147
--none recorded-- (23 targets)
Remote Datacenters
Non-virtualized assets
Overview
Scorecard and Results
Guidance
Reload
Filter Target List By Selection
Score
Benchmark/Profile
0.0%
USGCB-Win7-Firewall-x86, Version: v1.0.1.0
United States Government Configuration Baseline version 1.0.1.0
63.8%
rhsa-rhel5-tg, Version: v2.0
Red Hat Security Advisories
70.4%
scap-windows-2000, Version: 1.0.0
scap-win2000-profile
60.9%
vsphere-vm-hardening-guide, Version: v0.5
VMware Security Hardening for VMs
VISDK SCAP Benchmark
Dashboard
LakeHills_Datacenter (4 targets)
Compliance
Security Posture
Currency
Patch Level
Composite Scores
52.6%
99.6%
100.0%
Compliance
Vulnerabilities
Patches
Currency
Endpoints paired with VMs,
Group Virtualized Assets by…
• Virtual Machine,
• Host System, or
• Datacenter
New Folder Ctrl+F
New Cluster... Ctrl+L
Add Host... Ctrl+H
New Virtual Machine... Ctrl+N
New vNetwork Distributed Switch... Ctrl+K
Add Datastore...
Rescan for Datastores...
Add Permission... Ctrl+P
Alarm
Open in New Window... Ctrl+Alt+N
Remove
Rename
Run SCAP Assessment
Context menu in vCenter Client
to initiate SCAP assessment
CCE ID
Filter
Scorecard
Recent Tasks
Name, Target or Status contains:
Clear
Name Target Status Details Initiated by vCenter Server Requested Start Ti... Start Time Completed Time
Tasks Alarms
Evaluation Mode: 54 days remaining
Administrator

What is SCAP good for, and how does your product support it?

- Compliance Assessments
- Vulnerability Assessments
- ***Virtual Devices***
- Configuration Management
- System Diagnostics
- Automated Threat Response
- Standardized Decision Intelligence Systems
- ***Service Level Agreements***
- ***Offline Assessments***

Avoid Configuration Drift & Maintain Compliance

Only full-coverage IT compliance solution spanning physical and virtual server & desktop environments

Eliminate manual, error-prone and time-consuming work

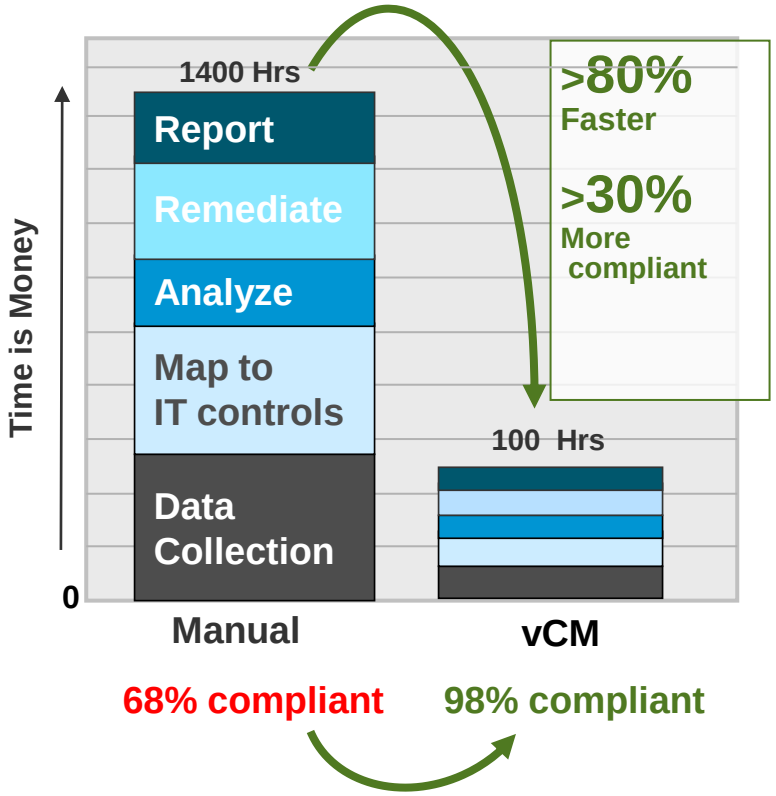
Apply out-of-the box compliance toolkits to automate audit data collection, analysis, remediation & verification

Continuously manage compliance with regulations and IT best practices, including VMware Hardening Guidelines

Massively reduce your risk posture & eliminate costly audit "events"

Supports DISA STIGs, CIS Benchmarks and many other standards

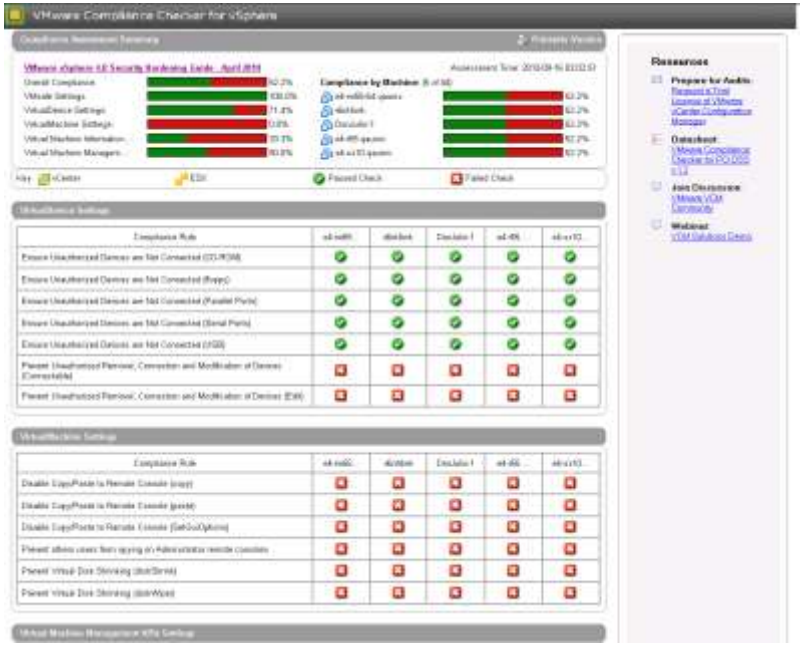
Automating IT Compliance with vCenter Configuration Manager

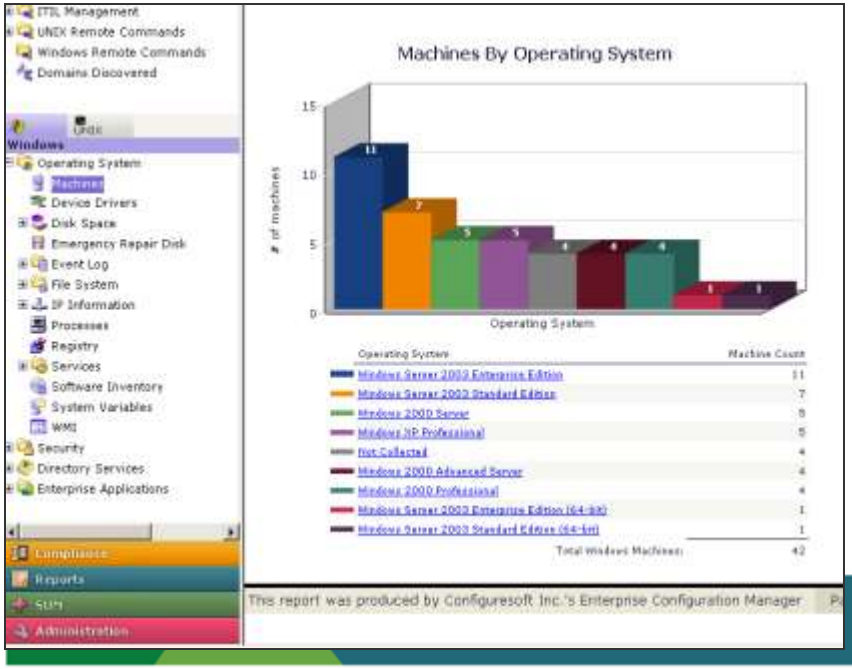


Future VMware SCAP Solutions

VMware Compliance Checker for vSphere

- Free download available by November 1st, 2010
- Leverages SCAP driven vSphere security assessment





vCenter Configuration Manager to be SCAP validated 1H2011

- Enterprise assessment & remediation of physical and virtual infrastructure
- Includes xPlatform patch management

Questions & Answers