Smarter Security – Compliance

mit Tivoli Endpoint Manager for Security & Compliance

Heutige Sicherheitsanforderungen

Smarter Security

Identitäten vertrauen

Kunde oder Krimineller?

Partner oder Mitbewerber?

Mitarbeiter Oder Hacker?

Zugriff verwalten

Service sichern

Lohnabrechnung

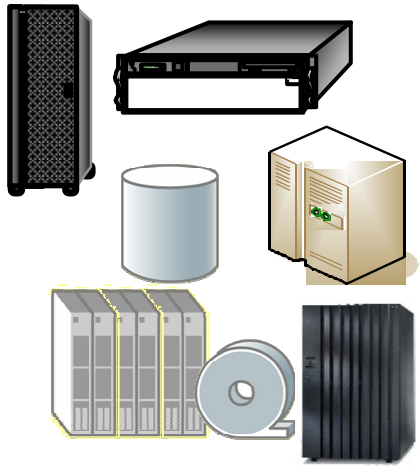
Online Banking

Darlehnsverwaltung

Wiederverkauf

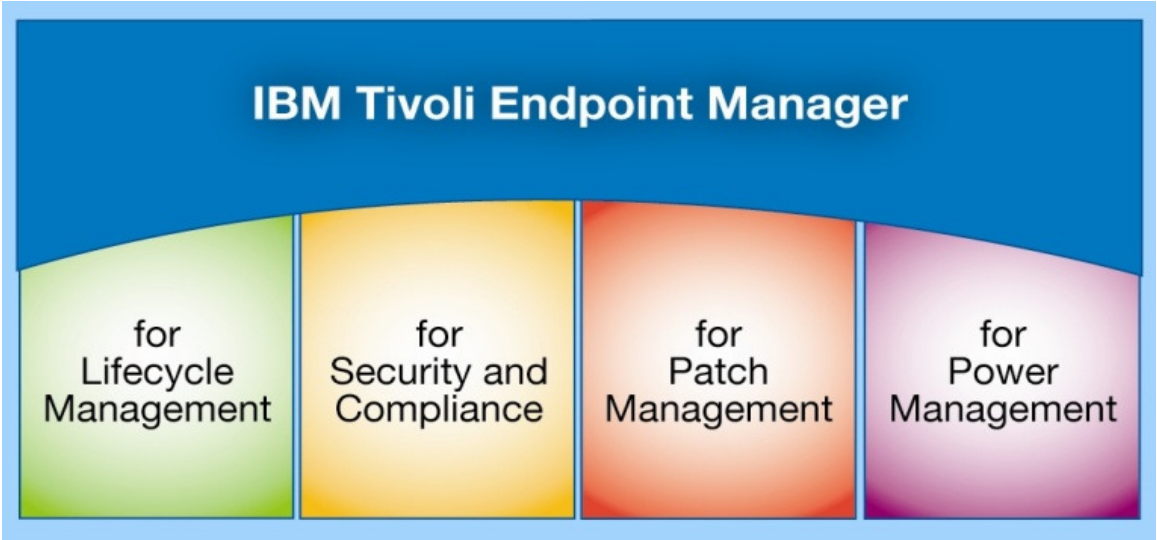
Inventar

Daten schützen



Sicherheit muß im Rahmen der Anforderungen in die Geschäftsprozesse integriert werden und nicht als Ding verstanden werden, das die nächste Sicherheitsbedrohung löst

Tivoli Endpoint Manager



Tivoli Endpoint Manager:

„Richtlinienbasierter“ Ansatz mit über 175.000 sofort einsatzfähigen Richtlinien (sogenannte Fixlets)

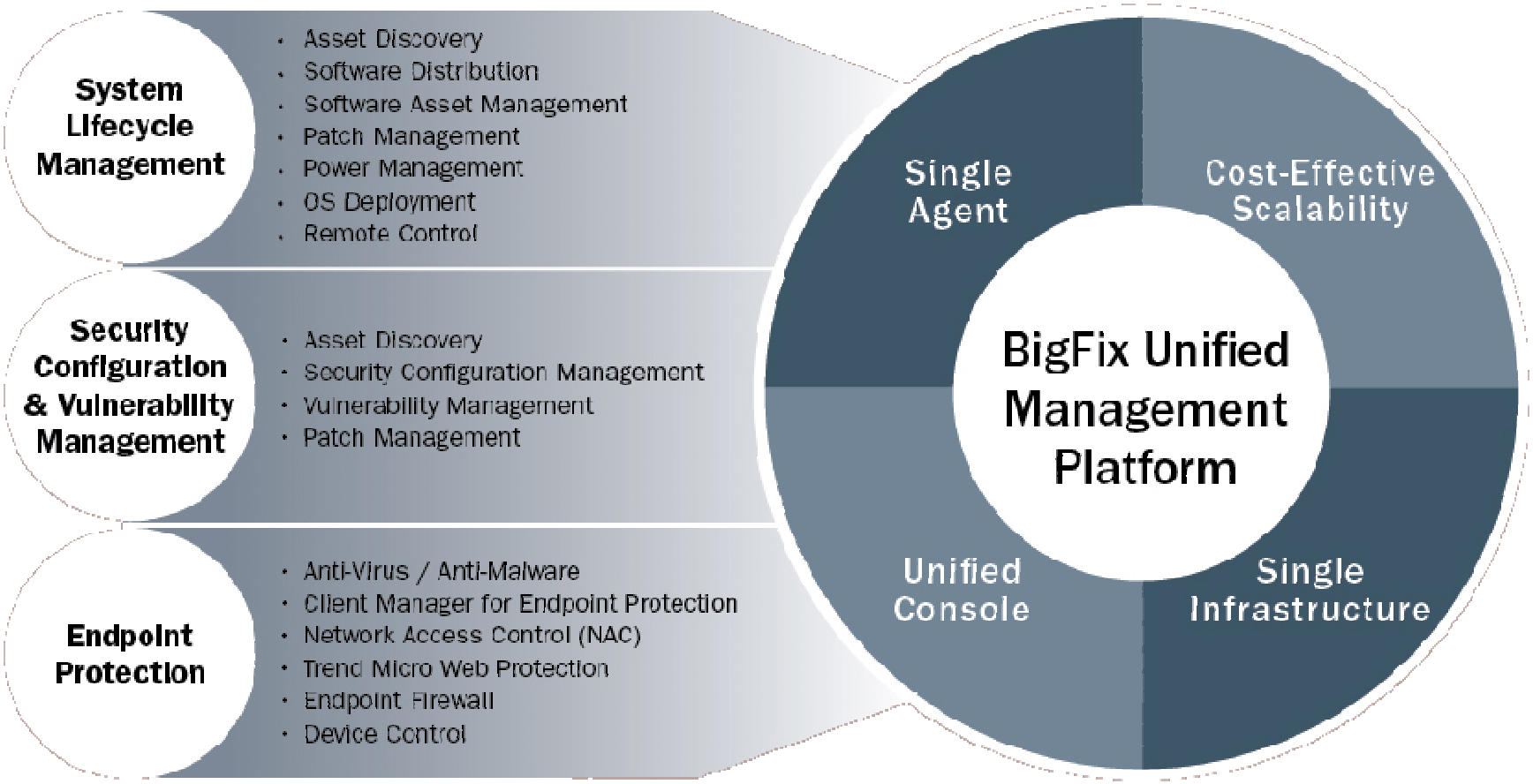
Integrierte Security Configuration- und Power Management-Lösung

Vollständiger Patch Automation-Service

Breites Spektrum an Betriebssystem- und Endpunktunterstützung:

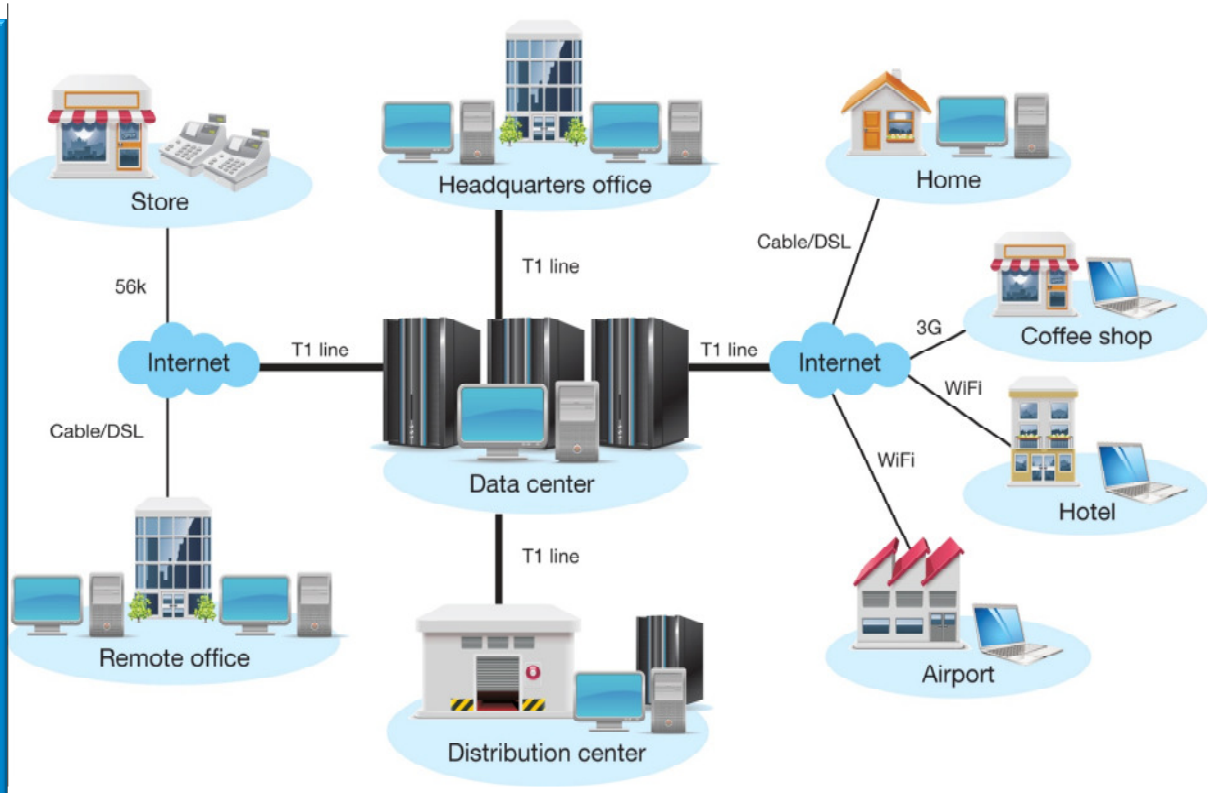
Windows-Desktopsysteme und -Server (einschließlich Win7), Windows Point of Sale und mobile Endgeräte, MacOS, Linux (RedHat, RedHat Enterprise, Fedora, SUSE/SLES, Oracle Linux), zLinux, AIX, HP-UX und Solaris

Übersicht



Schnelleres und smarteres IT Management

- *Network Asset Discovery*
- *Endpoint HW, SW Inventory*
- *Patch Management*
- *Software Distribution*
- *OS Deployment*
- *Remote Desktop Control*
- *Software Use Analysis (add on)*
- *Power Management (add on)*

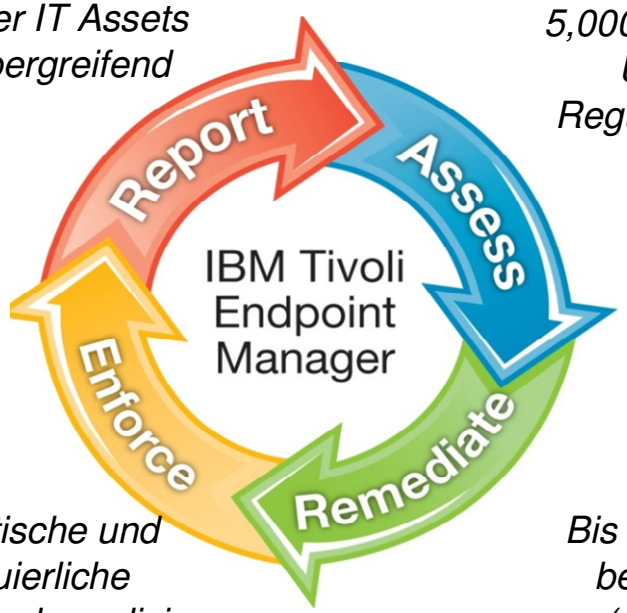


Whether it's a Mac connecting from hotel wi-fi, or a Windows laptop at 30K feet, or even a Red Hat Linux Server in your data center, Tivoli Endpoint Manager has it covered. In real-time, at any scale.

Mehr sehen, besser kontrollieren, umfassend automatisieren

- *Patch Management*
- *Security Configuration Management*
- *Vulnerability Management*
- *Asset Management*
- *Network Self Quarantine*
- *Multi-Vendor Endpoint Protection Management*
- *Anti-Malware & Web Reputation Service (add on)*

Erkennen der IT Assets plattformübergreifend



5,000+ compliance settings Unterstützung von Regularien (FDCC SCAP, DISA STIG)

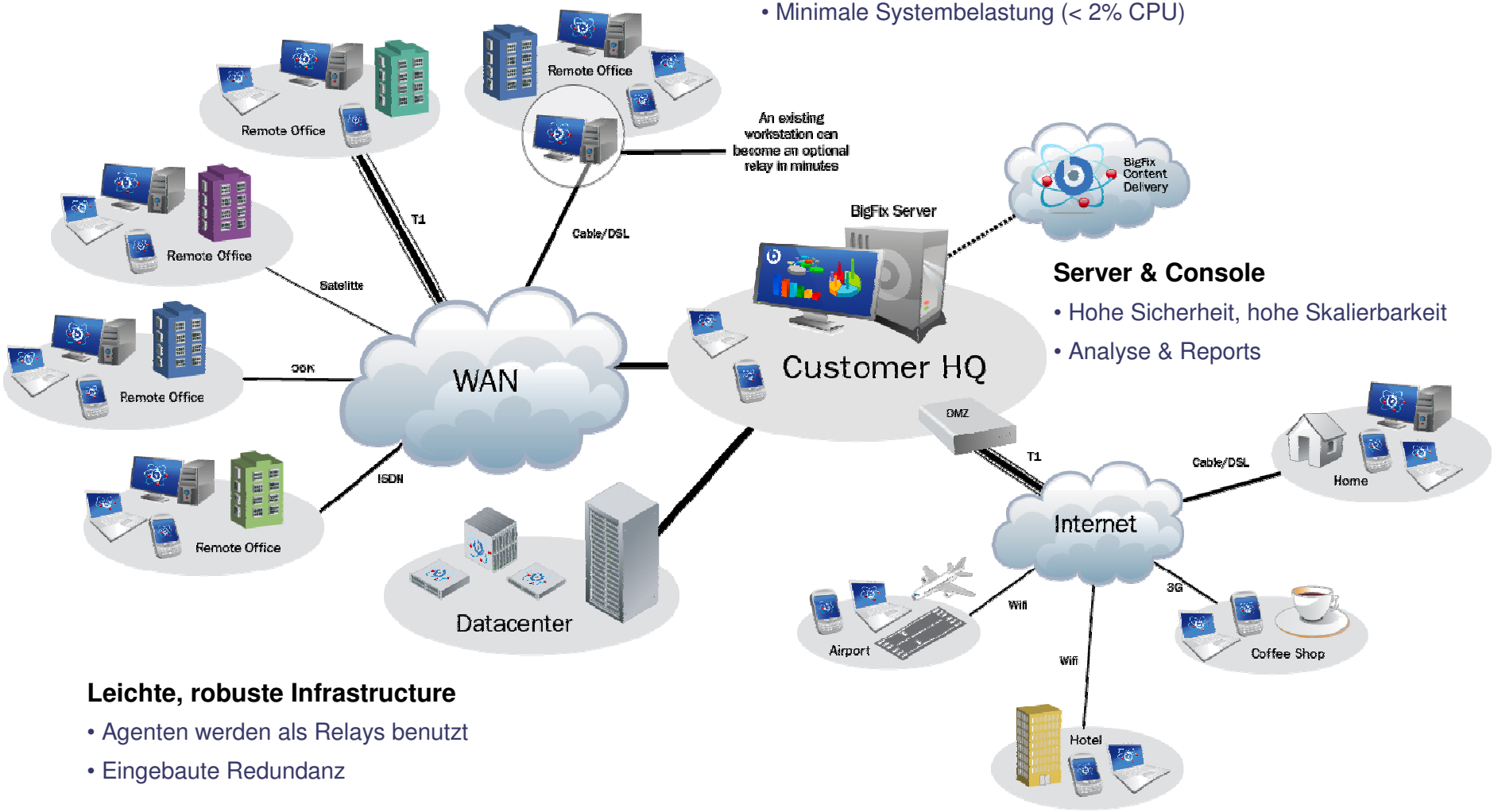
Automatische und kontinuierliche Anwendung der policies

Bis zu 95% Erfolgsrate beim ersten roll-out (patches, policies)

Architektur

Intelligenter Agent

- Führt multiple Funktionen
- Kontinuierliches self-assessment & policy enforcement
- Minimale Systembelastung (< 2% CPU)



Server & Console

- Hohe Sicherheit, hohe Skalierbarkeit
- Analyse & Reports

Leichte, robuste Infrastructure

- Agenten werden als Relays benutzt
- Eingebaute Redundanz

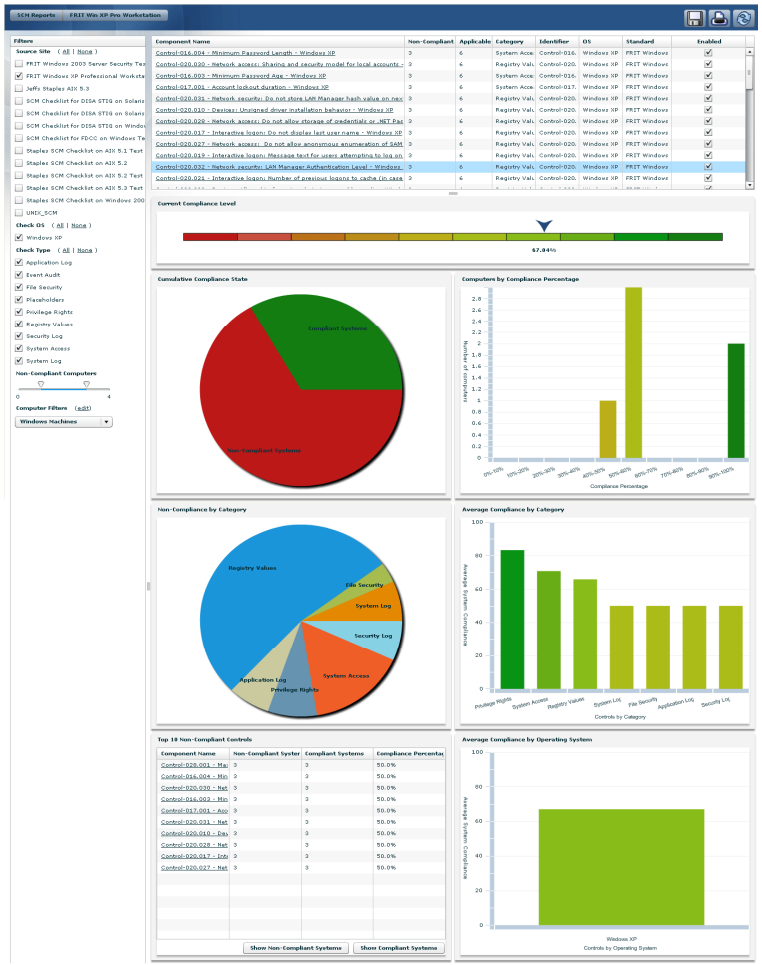
Tivoli Endpoint Manager for Security and Compliance

- Vereint mehrere Sicherheits und Konfigurationsmanagement Funktionen in einer einzelnen policy-basierten plattformübergreifenden Lösung.

- Anhaltende Compliance mit definierten Industriestandards und Security best practices.

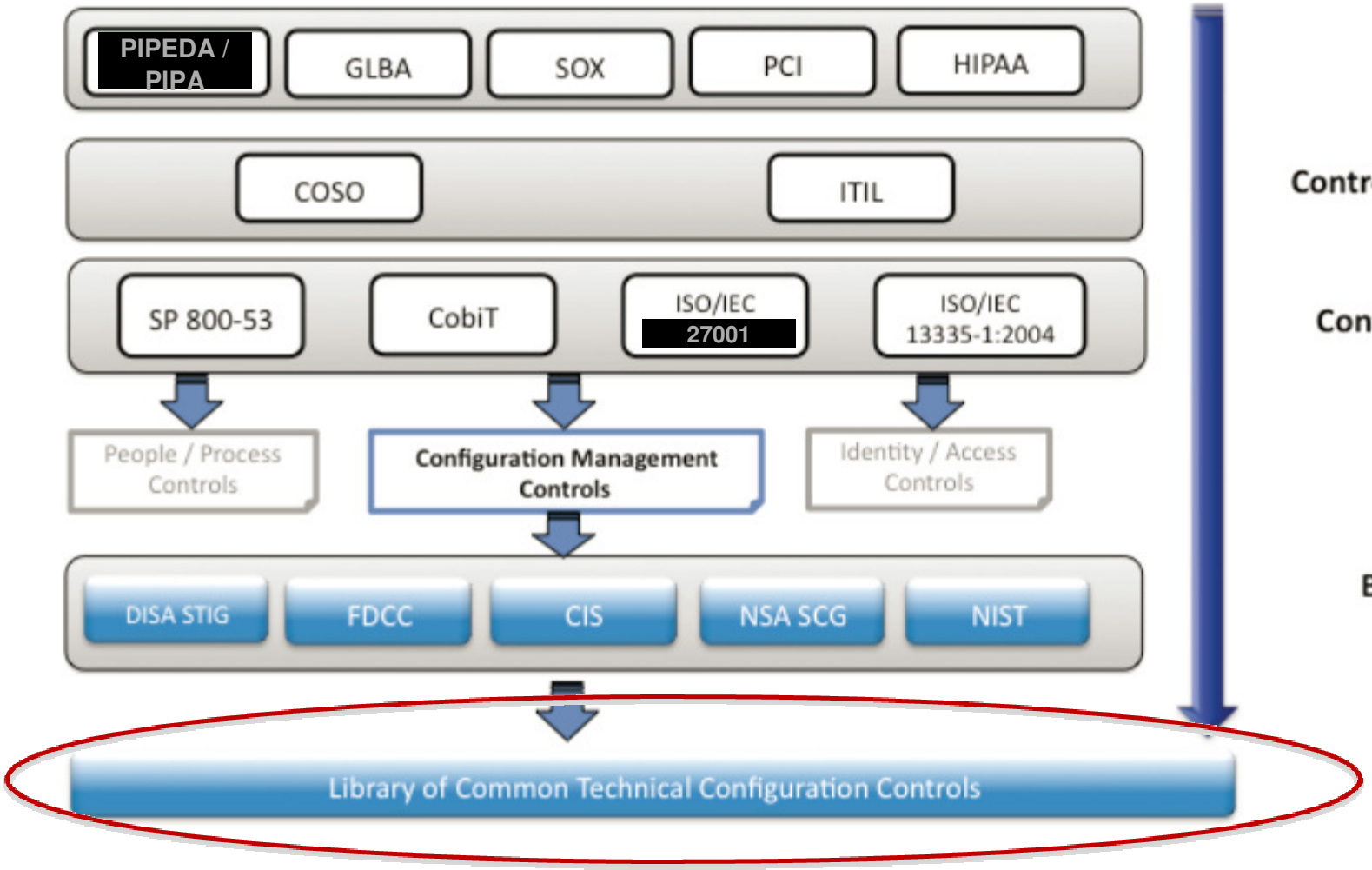
Herausforderungen	**TEM Beitrag zu Lösung**
• Fehlgeschlagene Audit / Compliance Initiative • Komplexe / teurer manueller Audit, Reporting und Remediation von Konfigurationen • Mangel an zentraler Einsehbarkeit von System Konfigurationen • Lange und aufwändige Zyklen um Konfigurationen zu Ändern, unter Verwendung bestehender Lösungen.	• Echtzeit Einsicht in Konfigurationen • Vielfältiger Plattform Support • Manuelle oder automatisierte Remediation • Einfaches Compliance Dashboard • Anhaltende Compliance und akkurates, Auditfähiges Reporting. • Standardisierter Ansatz für Konfigurationsmanagement

Auswertung über die IT-Umgebung



- Echtzeit Sicht in den aktuellen Compliance Status.
- Identifizieren von kritischen Lücken in der Compliance zur definierten Policy
- Anpassen des Dashboards um verschiedene Ansichten (“lenses”) auf den Compliance Status zu bekommen
  - Computer Groups
  - Kategorien
  - Policy Templates
- Drill-down in spezifische Details von Systemen die Compliant oder non-Compliant sind.

Unterstützung von Regularien und Standards



Reporting and Enforcement on 5,000+ Controls

Unterstützung von Regularien und Standards

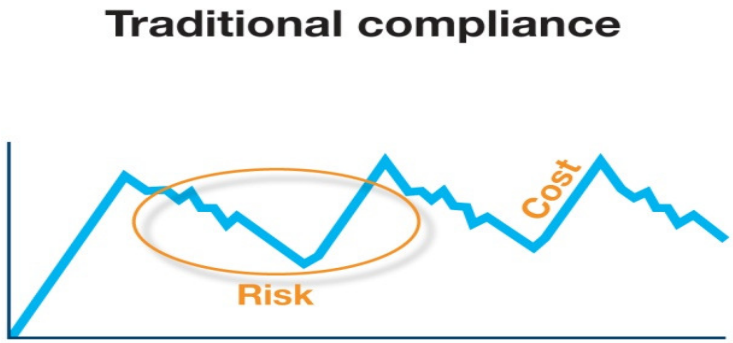
Requirement	PCI	ISO 27001	CobIT	NIST 800-53
Implementierung von 'anti-malware' Aktualisierung der IT-Endgeräte	5.1, 5.2	A12.6	DS5.9	SI-3
Definierne, implementieren & durchsetzen von grundlegenden Sicherheitskonfigurationen	2.1, 2.2, 6.2	A12.1, A15.2	DS9	CM-2,4,6
IT-Endgeräte auf aktuellem Patch-Level	6.1	A12.6	DS5.9	CM-2
Reguläre Vulnerability Scans Probleme (findings) adressieren	11.2	A12.6	PO9.3	RA-5
Akuelle IT-Network Übersicht Wissen über neue Geräte	1.1	A7.1	DS13.3	CM-8
Installation & Pflege Firewalls, etc auf IT-Endgeräten	1.4	A11.4	DS5.10	AC-19

Regularien und Standards - Abkürzungen

- Verwendete Standards – alle US:
  - DISA STIG (Windows, UNIX, Linux)
  - FDCC (Windows XP, Vista)
- Basieren auf sog. Best Practices – Benchmarks für Security Configuration

- Abkürzungen:
  - DISA: Defense Information System Agency
  - STIG: Security Technical Implementation Guide
  - NIST: National Institute of Standards and Technology
  - FDCC: Federal Desktop Core Configuration
  - SCAP: Security Content Automation Protocoll

Kontinuierliches Compliance Management



1. Entwickeln von Compliance Richtlinien.
2. Umsetzen der Richtlinien mit einem/mehreren Lösungen
3. Erkennen von findings
4. Korrigieren der findings
5. Benutzer ändert Zustand des IT-Endgerätes (Installation von Software), die Folge Non-Compliance
6. Wiederholung ab Punkt 3

1. Definition von Richtlinien und SLAs
2. Implementierung der Definitionen
3. Richtlinien werden kontinuierlich überwacht und durchgesetzt. Änderungen werden umgehend angezeigt
4. Jeder Zeit umfassendes Wissen über Sicherheit und Compliance
5. Fortlaufende Verbesserung von Richtlinien, SLAs und Compliance

Plattformen

- Plattform Unterstützung (Managed Assets)
  - ✓ Windows NT SP6a/95/98/ME/2000/XP/2003/Vista/Windows 7/Windows 2008 (Incl. x86, x64 and Itanium)
  - ✓ Suse Linux (32 & 64-bit), Suse Linux Enterprise Desktop
  - ✓ Redhat Linux (32 and 64-bit)
  - ✓ Solaris (incl. Sparc and x86)
  - ✓ HPUX
  - ✓ IBM AIX
  - ✓ Mac OSX
  - ✓ VMWare ESX
  - ✓ IBM zLinux
  - ✓ Wyse Thinclients
  - ✓ Windows XPembedded, WePOS, and Embedded Standard 2009
  - ✓ Windows Mobile 5 and 6, Windows CE
  - ✓ Nicht offiziell unterstützt: Debian, Ubuntu, CentOS

Beispiele aus den umfassenden Richtlinien

- Non-authorised users/group (e.g. anonymous, guest)
- Privileged users/group
- Account capabilities
- Password integrity (e.g. strength, how often changed)
- Inactive Accounts
- Service additions/deletions
- Existence of mandatory services (e.g. ssh)
- Existence of forbidden services (e.g. rpc dependant)
- Security settings and configuration (e.g. registry settings)
- Application configuration files
- Software patch and hotfix levels
- Incorrect weak ACL/permissions (e.g. world writable)
- Mandatory/forbidden files
- Check of installed software packages and versions (e.g. firewall, antivirus)
- ...

Auf einem Blick

IBM Tivoli Endpoint Manager for Security & Compliance ist ein Produkt, das Systeme und Anwendungen auf Angriffspunkte hin überprüft und Verstöße gegen die “Security Policy” des Unternehmens aufdeckt

Wesentliche Vorteile für die Kunden:

- ✓ Hilft Unternehmensdaten zu schützen
- ✓ Identifiziert Sicherheitslöcher
- ✓ Reduziert IT Kosten durch Automation und Zentralisierung
- ✓ Unterstützt bei der Einhaltung von Regularien und Standards