4ª edição
IBM Security Forum

Uma abordagem inovadora para reduzir custos e otimizar a gestão de segurança dos endpoints

Rodolfo de Souza
Sales Leader
Tivoli Endpoint Manager

Tivoli software

Agenda

Contextos – Externo e Interno

A Solução e a Ação

Os Resultados

Tivoli software

Agenda

4ª edição IBM Security Forum

- Contextos – Externo e Interno
- A Solução e a Ação
- Os Resultados

Tivoli software

As perspectivas de um mundo mais inteligente

4ª edição IBM Security Forum

O planeta esta cada vez mais **Instrumentado**, **Interconectado** **e** **Inteligente**.

1 trilhão

É estimado que no próximo ano 2 bilhões de pessoas estarão na Web… e teremos **1 trilhão** de dispositivos conectados – carros, estradas, câmeras, equipamentos móveis, compreendendo a **"Internet das Coisas."**

90%

Próximo a **90%** das inovações em automóveis são relacionados a software e sistemas eletrônicos. 30-60% do valor do carro corresponde ao software.

162 milhões

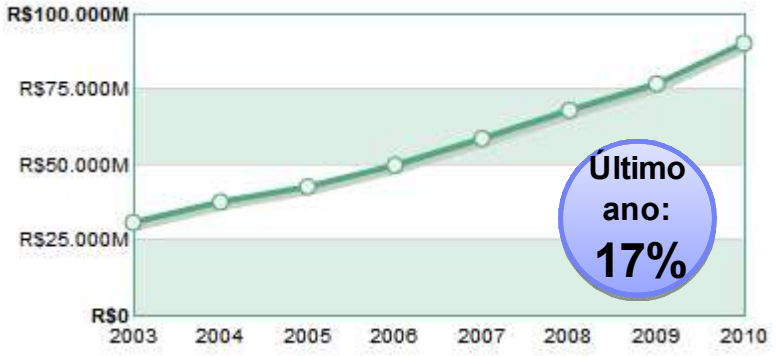
Quase **162 milhões** **de** "Smart Phones" foram vendidos em 2008, ultrapassando as vendas de laptop pela primeira vez na história.

Aproximadamente 70% do universo digital é criado por pessoas, **mas as empresas são responsáveis por 85%** **da segurança, privacidade, confiabilidade e compliance**

Brasil, uma economia em crescimento

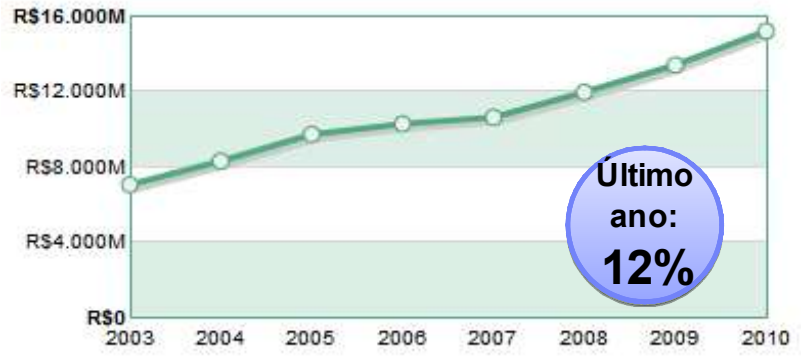
Evolução do Segmento A

R$ milhões



Evolução do Segmento B

R$ milhões

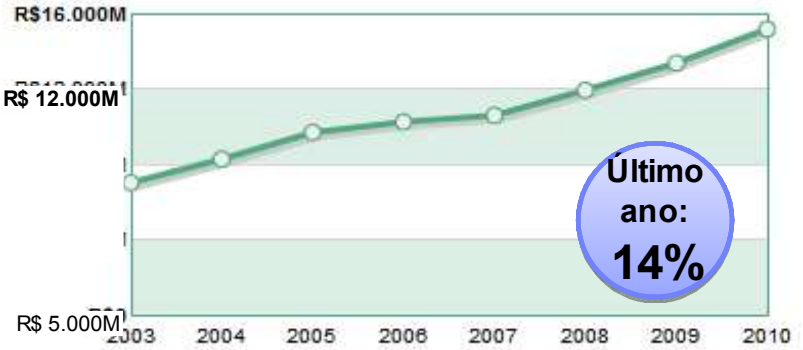


Evolução do Segmento C

R$ milhões

Evolução do Segmento D

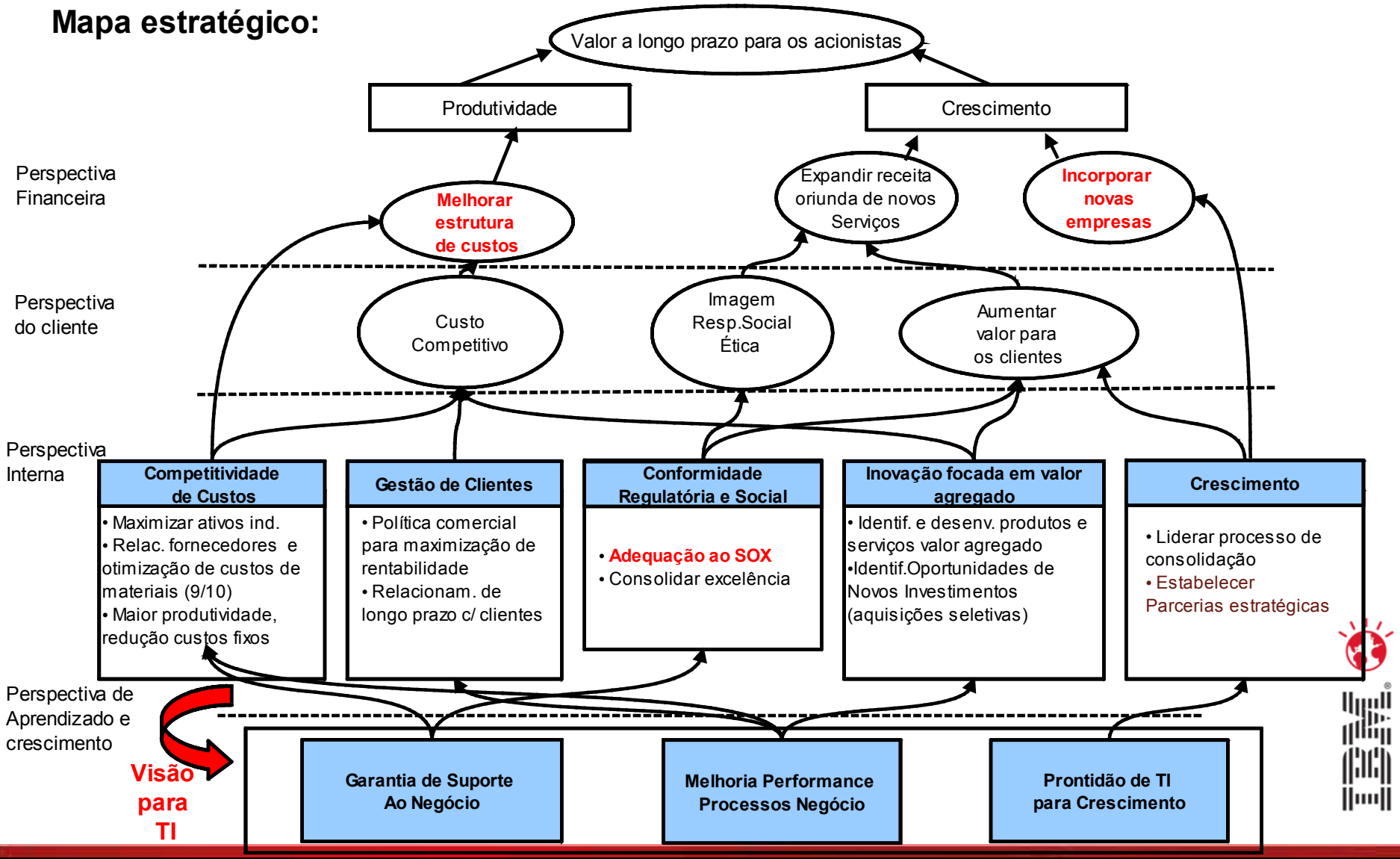
R$ milhões



Drivers de valor de TI

4ª edição IBM Security Forum

Mapa estratégico:



Gereciamento de Risco – O que é Risco?

- Risco: Qualquer coisa que possa impedir o atingimento de objetivos.

Risco Externo

- Clima
- Mudanças políticas
- Mudança regulatória

Risco de Mercado

- Eventos Competitivos
- Preço
- Avanço tecnológicos

Risco Operacional

- Acesso seguro aos dados, aplicações
- Proteção de todos os assets e recursos operacionais
- Gerenciar e remediar as vulnerabilidades dos sistemas
- Disponibilidade e resiliência

Risco de Crédito

- Mudança econômica
- Manutenção da taxa de crédito
- Outsourcing
- Custo

Risco operacional está relacionado com a operação com sucesso dos processos de negócio, e é o risco mais controlável.
SEGURANÇA é o elemento mais importante do Risco Operacional.

Principais desafios de segurança de Endpoint

- Falha na auditoria de conformidade e regulamentação
- Brechas de Segurança
- Explosão de Malware e “Zero day Attack”

Desafios: Falha de Auditoria de conformidade e regulamentação

1. Você teve alguma falta de conformidade de auditoria, relacionada a gerenciamento de patches, configuração de segurança ou gestão de anti-virus?

§ O quanto é difícil estar em conformidade e apresentar os dados requisitados pelos auditores?

§ Quantas áreas e ferramentas precisam ser envolvidas para a coleta destas informações?

Desafios: Brechas de Segurança

1. Você já teve alguma experiência com brecha de segurança, envolvendo assets não gerenciados, falta de patches, configuração não conforme com as política corporativas?

2. Você acredita saber aonde todos os seus sistemas estão e como eles estão protegidos?

3. As políticas de segurança são respeitadas através das centenas de servidores e milhares de workstation e Smart Phones?

Desafios: Explosão de Malware e “Zero day Attack”

1. Você já teve alguma experiência com explosão de Malware (virus, worms, trojans, etc) que impactou o negócio?
2. Você fez alguma avaliação e tem comprovação que as ferramentas de anti-virus estão instaladas e atualizadas em todos os dispositivos da sua empresa?
3. Como você evita que os colaboradores e terceiros não acessem sites Web com reputação duvidosa?
4. Você já vivenciou algum risco de segurança através de estações com serviços e portas TCP/UDP abertas sem necessidade?

Existem vários desafios para atender o crescimento, garantir a segurança e as operações de TI

Conformidade

Reduzir Custos

Aumentar eficiência

Gestão de Riscos

Maior controle e velocidade

Fazer mais com menos

12

Agenda

4ª edição IBM Security Forum

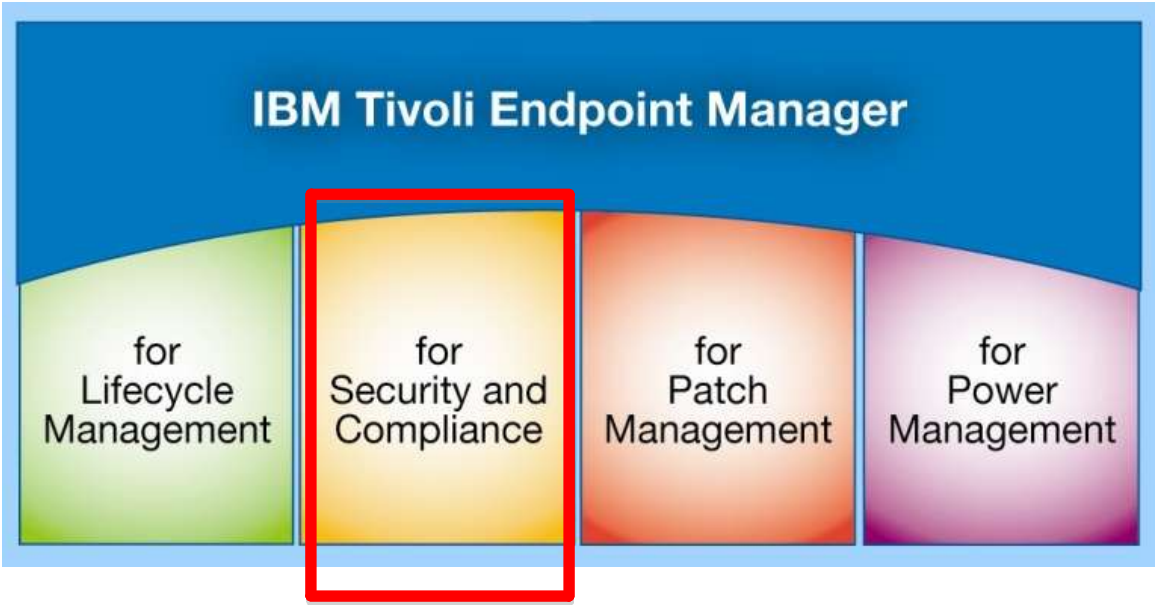
Contextos – Externo e Interno

A Solução e a Ação

O Resultado

Tivoli software

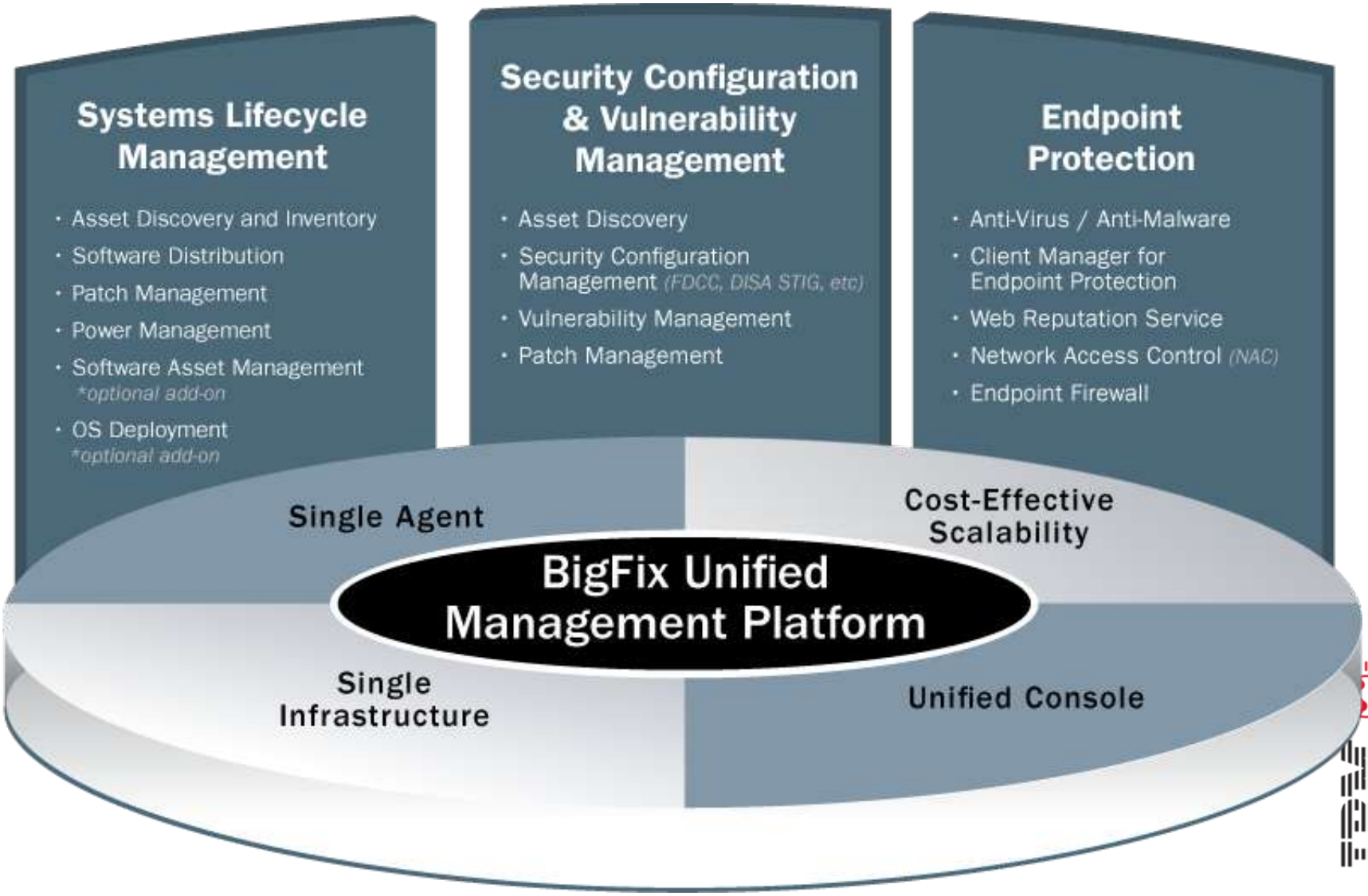
Tivoli Endpoint Manager, usando a tecnologia BigFix



Usando o Tivoli Endpoint Manager, os clientes podem:

- Visualizar todos os endpoints: físico, virtual, fixo ou móvel
- Corrigir problemas de qualquer lugar em minutos, desconsiderando banda ou conectividade
- Implementação em dias, sobre qualquer rede ou geografia
- Entrega conformidade contínua através de diversas plataformas
- Operação e gerenciamento automatizados e simplificado

Portfolio TEM/BigFix



15 15

TEM: Como funciona?

Infraestrutura Robusta e Leve

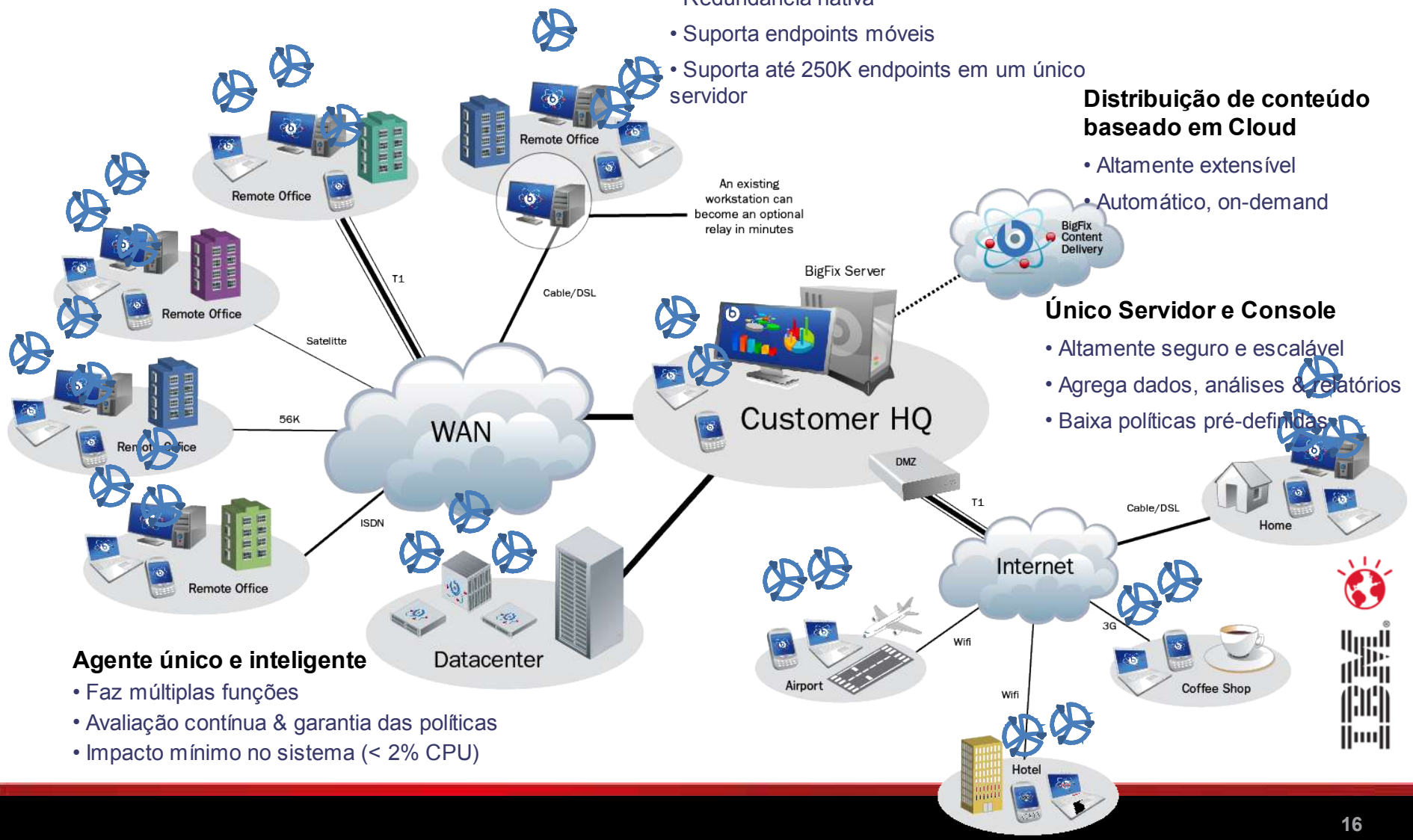
- Usa sistemas existentes como Relays
- Redundância nativa
- Suporta endpoints móveis
- Suporta até 250K endpoints em um único servidor

Distribuição de conteúdo baseado em Cloud

- Altamente extensível
- Automático, on-demand

Único Servidor e Console

- Altamente seguro e escalável
- Agrega dados, análises & relatórios
- Baixa políticas pré-definidas



Agente único e inteligente

- Faz múltiplas funções
- Avaliação contínua & garantia das políticas
- Impacto mínimo no sistema (< 2% CPU)

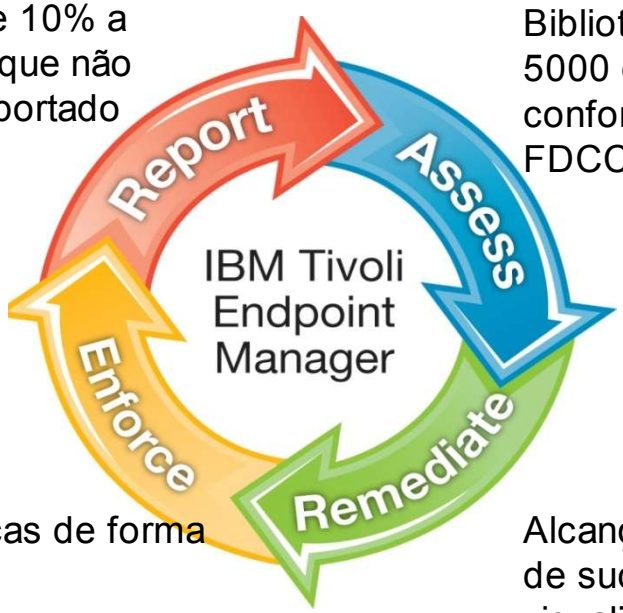
Agente Inteligente: Visibilidade em tempo real multi-plataforma

- Suporte a plataforma hetereogênea(Ativos Gerenciados):
  - ✓ Windows NT SP6a/95/98/ME/2000/XP/2003/Vista/Windows 7/Windows 2008 (Inc. x86, x64 e Itanium)
  - ✓ Suse Linux (32 e 64-bit), Suse Linux Enterprise Desktop
  - ✓ Redhat Linux (32 e 64-bit)
  - ✓ Solaris (incl. Sparc e 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
  - ✓ Debian, Ubuntu, CentOS e Oracle Enterprise Linux
  - ✓ Visibilidade em qualquer dispositivo IP através do escaneamento de rede em qualquer ativo gerenciado pelo TEM. (dispositivos não gerenciados)

Tivoli Endpoint Manager: See More, Secure More

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

Descobre de 10% a 30% assets que não tinha sido reportado



Biblioteca com mais de 5000 configurações de conformidade, incluindo: FDCC SCAP, DISA STIG

Aplica políticas de forma contínua

Alcança por volta de 95%+ de sucesso na visualização e remediação de políticas e patches logo na primeira execução.

Common Criteria Certified EAL3

oval.mitre.org

cve.mitre.org

FIPS VALIDATED 140-2

FIPS 140-2 Inside

Tivoli Endpoint Manager: traz equilíbrio na conformidade de endpoints

Traditional compliance

1. Time de segurança desenvolve as políticas de conformidade
2. Time de segurança executa ferramentas de avaliação contra as políticas
3. Time de segurança passa as descobertas para operação
4. Operação executa correções, normalmente utilizando uma ou mais ferramentas, diferente da ferramenta utilizada pela segurança, gerando diferentes resultados
5. Usuários realizam mudanças, causando novamente falhas nas políticas de conformidade
6. Inicia o ciclo de avaliação novamente

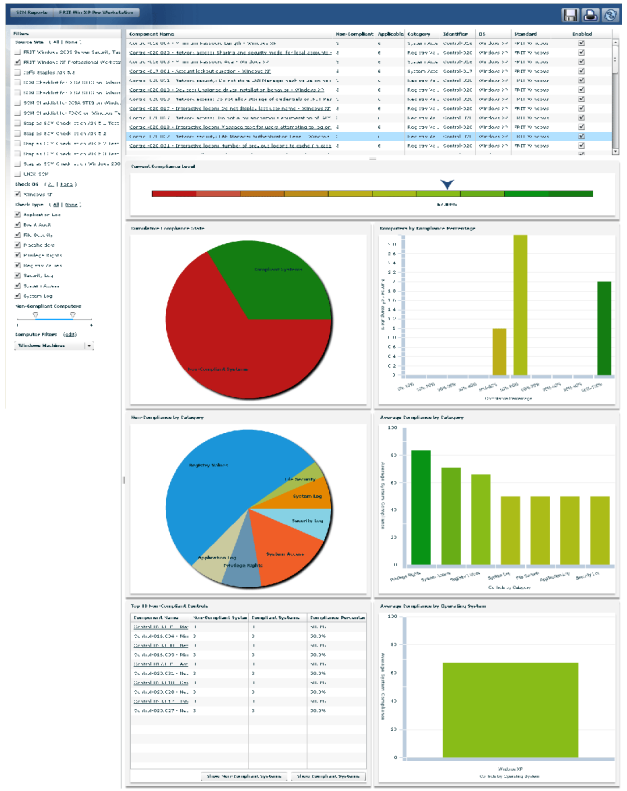
Continuous compliance

1. Time de segurança e operação trabalham juntos para formular as políticas e SLAs
2. Operação implementa uma baseline (patch, configuração, AV,etc) através da organização
3. Política de conformidade é executada e monitorada de forma contínua, mudanças são relatadas imediatamente.
4. Time de segurança pode checar instantaneamente o status de segurança e conformidade a qualquer momento
5. Time de segurança e operação trabalham juntos para reforçar a segurança e realizar os ajustes necessários baseados nos requerimentos de segurança

Tivoli Endpoint Manager for Security & Compliance

Solução compreensiva de segurança fim-a-fim que inclue:

- Descoberta de Ativos
- Gerenciamento de Patches
- Gerenciamento de Configuração de Segurança
- Gerenciamento de Vulnerabilidades

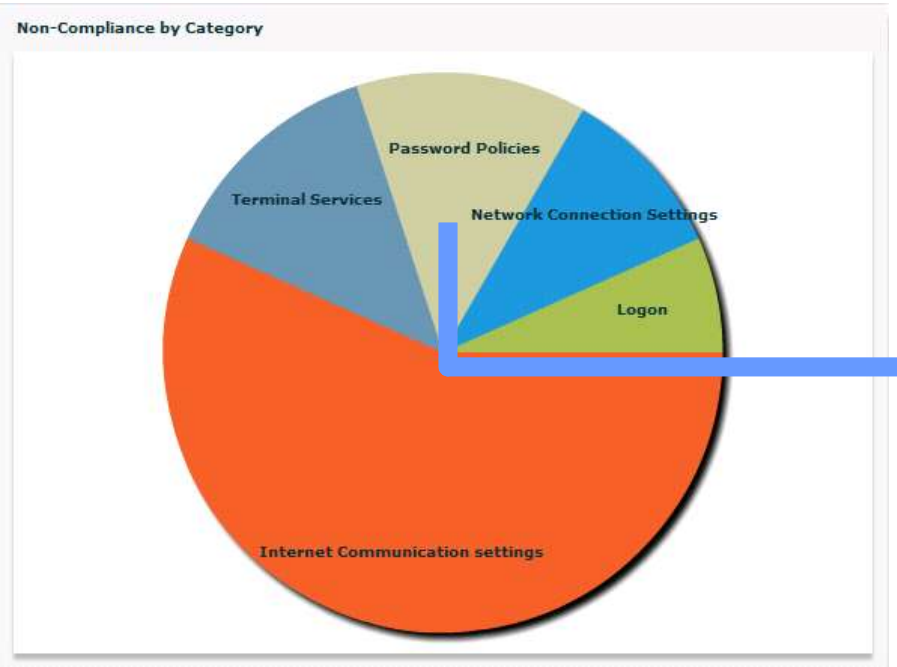


Benefícios e Funcionalidades

- Aplicação contínua das políticas de segurança, independente do estado da rede
- Análise de vulnerabilidade baseada em Host com escore de severidade e 99.9% de acerto
- Define e avalie a conformidade de segurança de clientes com políticas e baselines
- Suporte para plataformas heterogêneas: Windows, UNIX, Linux, and MacOS

Tivoli Endpoint Manager for Security & Compliance

Drill Down para entender as não conformidades



Non-Compliance by Category

Component Name	Non-Comp	Su	Category	Identifie	Type	Standard
Enforce Password History	2	2	Password Policies	CCE-299	xp-1.	SCM Checl
Maximum Password Age	2	2	Password Policies	CCE-292	xp-1.	SCM Checl
Minimum Password Length	2	2	Password Policies	CCE-298	xp-1.	SCM Checl
Passwords Must Meet Complexity	2	2	Password Policies	CCE-273	xp-1.	SCM Checl
Store Passwords Using Reversible		2	Password Policies	CCE-288	xp-1.	SCM Checl
Minimum Password Age		2	Password Policies	CCE-243	xp-1.	SCM Checl

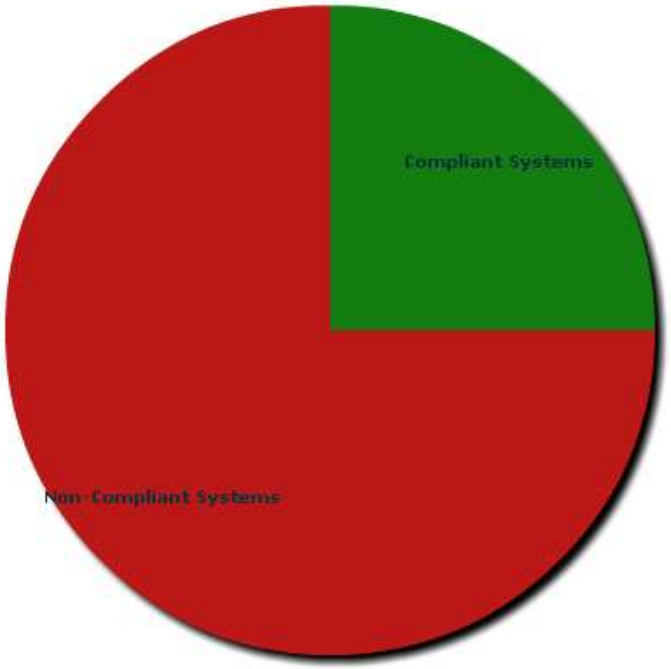
Return to Chart | Show Non-Compliant Systems | Show Subscribed Systems

Computer Name	OS	CPU	Last Report Time	Locked	BES Relay Sele...	Relay	User Name
IBM-D360A5FB33A	WinXP 5.1.2600	1600 MHz Penti...	9/18/10 10:48:...	No	Manual	IBM-6B34B5050...	aparra
IBM-6B34B505090	WinXP 5.1.2600	2500 MHz Core ...	9/21/10 9:11:0...	No	Manual	BES Root Server	aparra

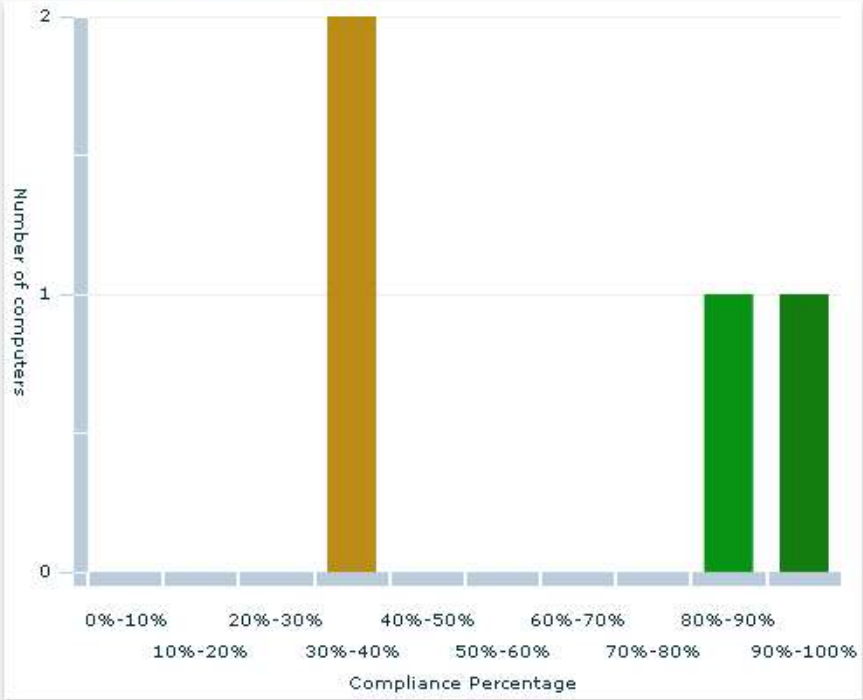
Security Configuration Management

Current Compliance Level

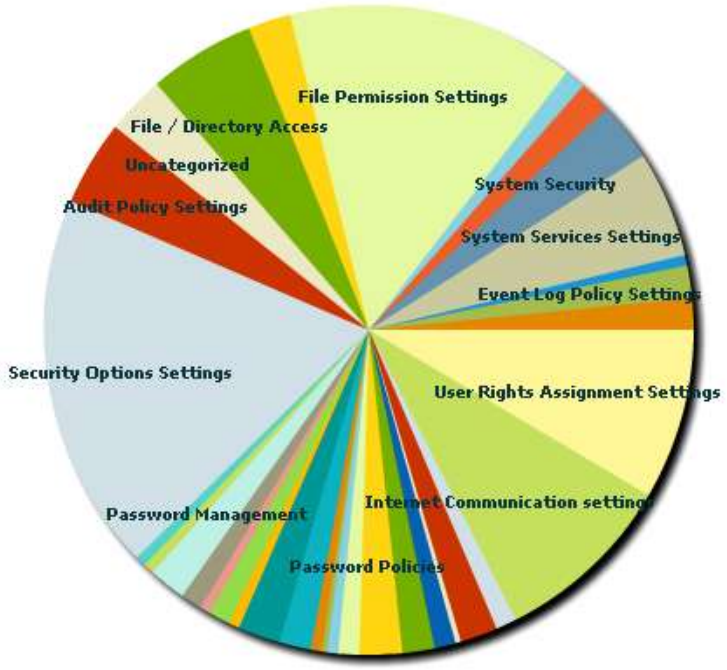
Cumulative Compliance State



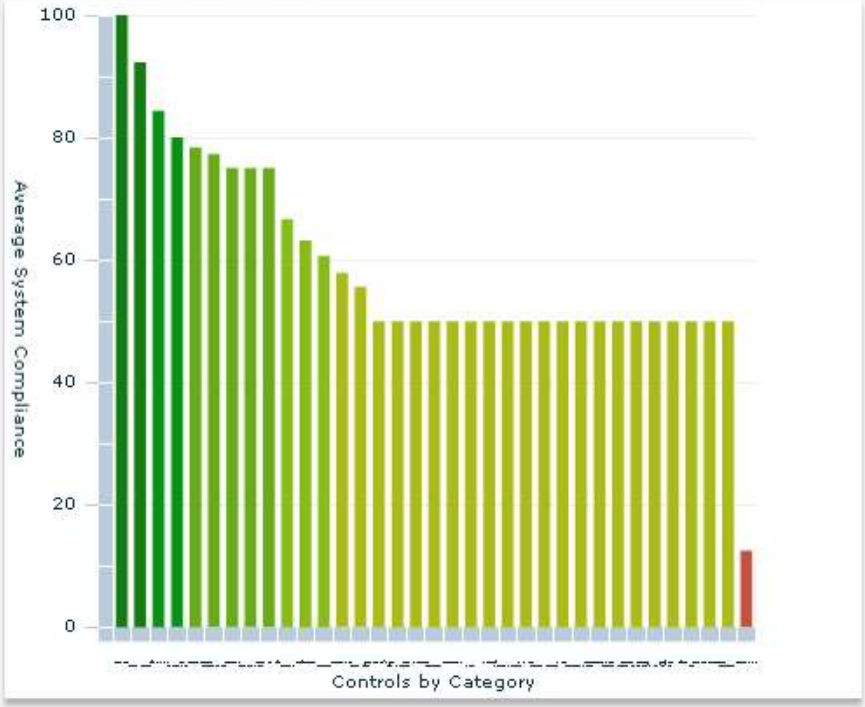
Computers by Compliance Percentage



Non-Compliance by Category



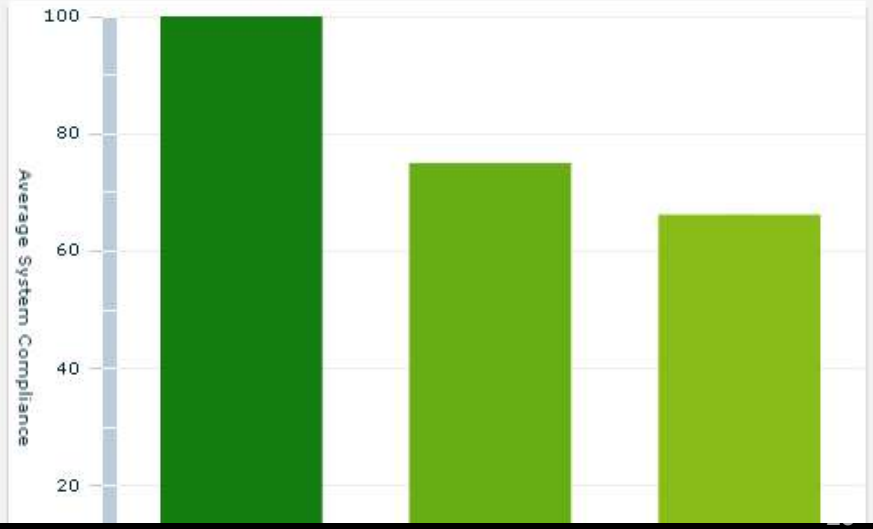
Average Compliance by Category



Top 15 Non-Compliant Controls

Component Name	Non-Compliant Syst	Compliant Systems	Compliance Percent
at.exe Permissions	2	2	50.0%
regsvr32.exe Permis	2	2	50.0%
Right To Back Up Fil	2	2	50.0%
Right To Remove Cc	2	2	50.0%
Turn Off Microsoft Pe	2	2	50.0%
Registry Policy Proce	2	2	50.0%
Turn off downloadin(	2	2	50.0%
regini.exe Permissio	2	2	50.0%
Right To Bypass Tra	2	2	50.0%
sc.exe Permissions	2	2	50.0%
mshta.exe Permissi	2	2	50.0%
WebClient Service	2	2	50.0%
arp.exe Permissions	2	2	50.0%

Average Compliance by Type

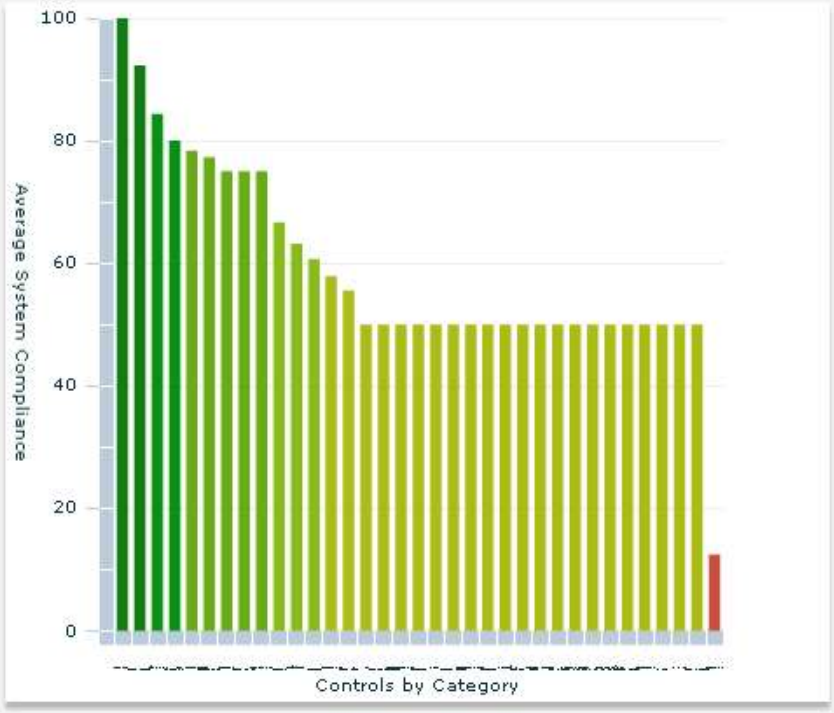


Non-Compliance by Category

Component Name	Non-Con	Subscrib	Categor	Identifie	Type	Standarc
WebClient Service	2	4	System	CCE-329	xp-1.2.1	SCM Che
Universal Plug And Play De	2	4	System	CCE-304	xp-1.2.1	SCM Che
NetMeeting Remote Desktc	2	4	System	CCE-289	xp-1.2.1	SCM Che
Simple Service Discovery Pr	2	4	System	CCE-266	xp-1.2.1	SCM Che
Indexing Service Disabled	2	4	System	CCE-291	xp-1.2.1	SCM Che
Fast User Switching Compa	2	4	System	CCE-295	xp-1.2.1	SCM Che
Error Reporting Service Dis	2	4	System	CCE-323	xp-1.2.1	SCM Che
Computer Browser Service I	2	4	System	CCE-288	xp-1.2.1	SCM Che
Wireless Zero Configuratior	2	4	System	CCE-249	xp-1.2.1	SCM Che
Background Intelligent Trar	1	4	System	CCE-281	xp-1.2.1	SCM Che
Telnet Service Disabled	1	4	System	CCE-232	xp-1.2.1	SCM Che
Routing And Remote Acces	0	4	System	CCE-303	xp-1.2.1	SCM Che
Messenger Service Disablec	0	4	System	CCE-291	xp-1.2.1	SCM Che
FTP Publishing Service Disa	0	4	System	CCE-288	xp-1.2.1	SCM Che
ClipBook Service Disabled	0	4	System	CCE-271	xp-1.2.1	SCM Che
Fax Service Disabled	0	4	System	CCE-284	xp-1.2.1	SCM Che

Return to Chart | Show Non-Compliant Systems | Show Subscribed Systems

Average Compliance by Category



Fixlet: Telnet Service Disabled

Take Action | Edit | Copy | Export | Hide Locally | Hide Globally | Remove

Description | Details | Applicable Computers (1) | Action History (0)

Description

Unnecessary services should not be running on the system. Services typically run under the local System Account, which generally have more permissions than are required by the service. Compromising a service could allow an intruder to obtain System permissions and open the system to a variety of attacks.

Supplied Configuration Reference Data:
dc:type = GPO
dc:source = Computer Configuration\Windows Settings\Security Settings\System Services

---

- Benchmark Information:

Accepted Date: 2009-04-08
Reference:
http://nvd.nist.gov/chklst_detail.cfm?config_id=76
Publisher: National Institute of Standards and Technology
Identifier: SP 800-68
Version: v1.2.1.0
Platform: cpe:/o:microsoft:windows_xp
Identifier: http://cce.mitre.org: CCE-2326-7
Identifier: cce.mitre.org/version/4: CCE-75

- References:

ID: CM-6
Title: Configuration Settings
Reference: NIST 800-26: 10.2.6, 10.3.1, 16.2.2, 16.2.3, 16.2.11
Reference: DOD 8500.2: DCSS-1, ECSC-1, E3.3.8
Reference: DCID 6/3: 4.B.2.a(10)
ID: CM-7
Title: Least Functionality
Reference: NIST 800-26: 10.3.1
Reference: DOD 8500.2: DCPP-1, ECIM-1, ECVI-1, E3.3.8
Reference: DCID 6/3: 4.B.2.a(10), 7.D.2.b

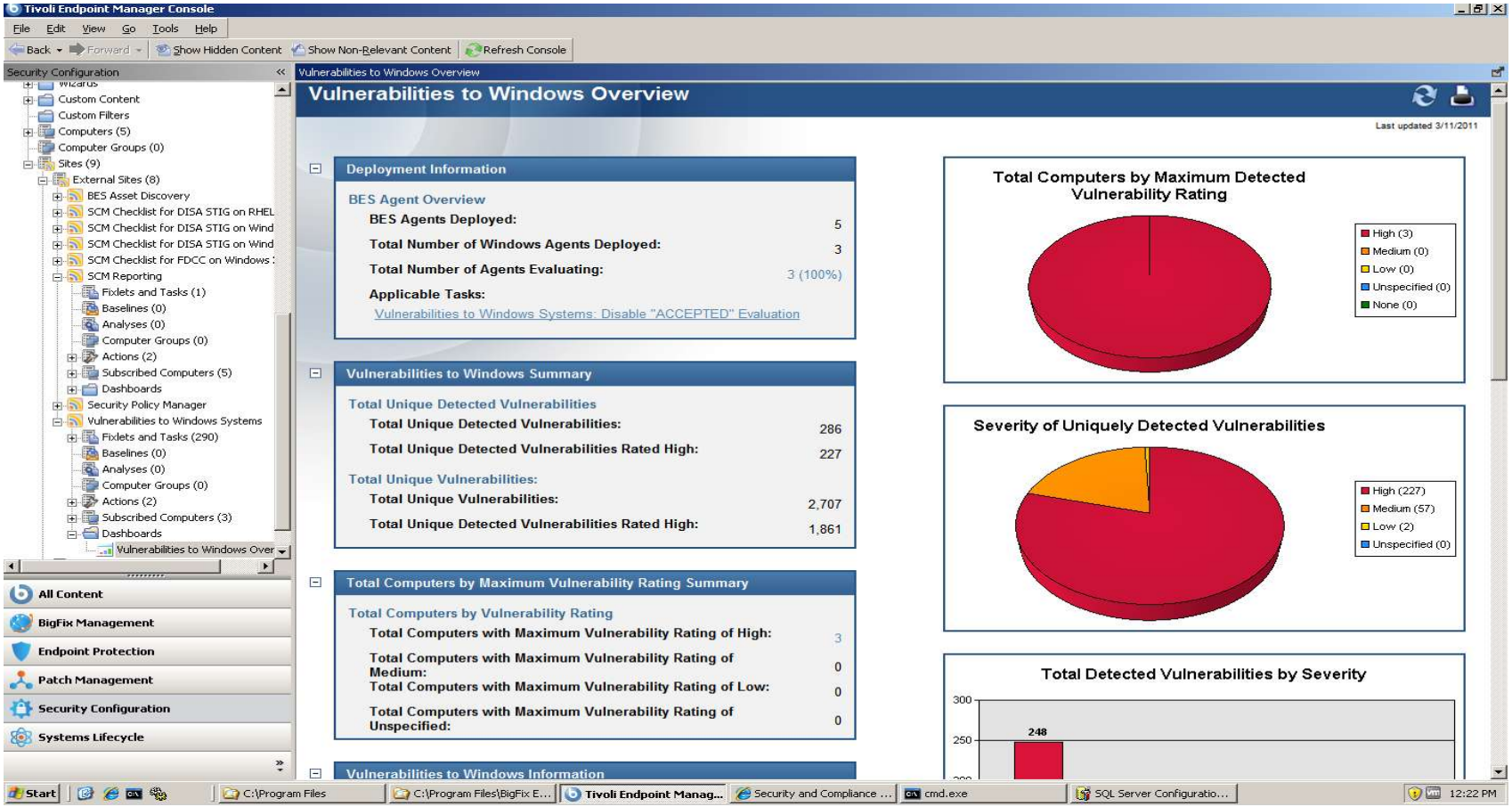
+ OVAL Definition:

Actions

- Click here to remediate this security issue.

TEM for Security & Compliance – Vulnerability for Windows

Avalia vulnerabilidades através de Base de Dados internacional



Common Criteria Certified EAL3

oval.mitre.org

cve.mitre.org

FIPS VALIDATED 140-2

FIPS 140-2 Inside

Vulnerabilities to Windows Overview

Last updated 2/6/20

Deployment Information

BES Agent Overview

BES Agents Deployed:	4
Total Number of Windows Agents Deployed:	3
Total Number of Agents Evaluating:	3 (100%)
Applicable Tasks:	
Vulnerabilities to Windows Systems: Disable "ACCEPTED" Evaluation	

Vulnerabilities to Windows Summary

Total Unique Detected Vulnerabilities

Total Unique Detected Vulnerabilities:	274
Total Unique Detected Vulnerabilities Rated High:	213

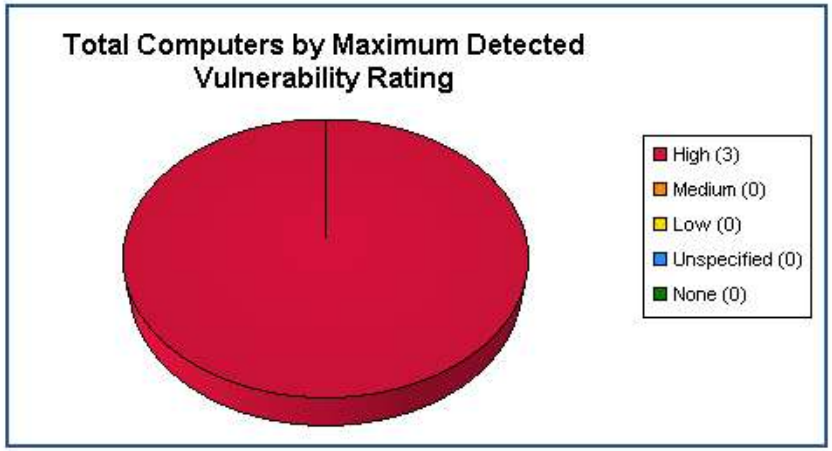
Total Unique Vulnerabilities:

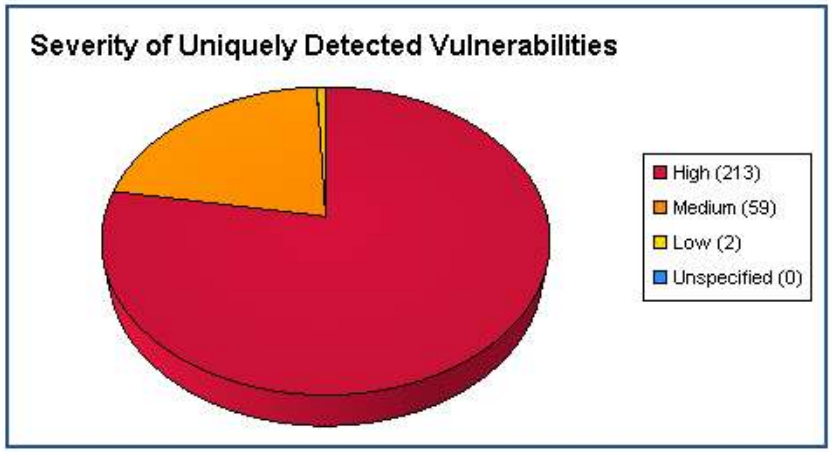
Total Unique Vulnerabilities:	2,768
Total Unique Detected Vulnerabilities Rated High:	1,904

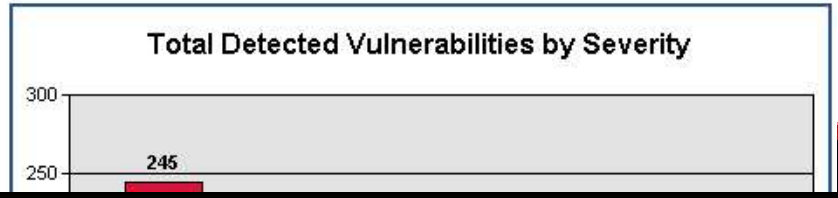
Total Computers by Maximum Vulnerability Rating Summary

Total Computers by Vulnerability Rating

Total Computers with Maximum Vulnerability Rating of High:	3
Total Computers with Maximum Vulnerability Rating of Medium:	0
Total Computers with Maximum Vulnerability Rating of Low:	0
Total Computers with Maximum Vulnerability Rating of Unspecified:	0







Average Number of Detected Vulnerabilities Per Computer

Total Detected Vulnerabilities:	103.00
Total Detected Vulnerabilities Rated High:	81.67

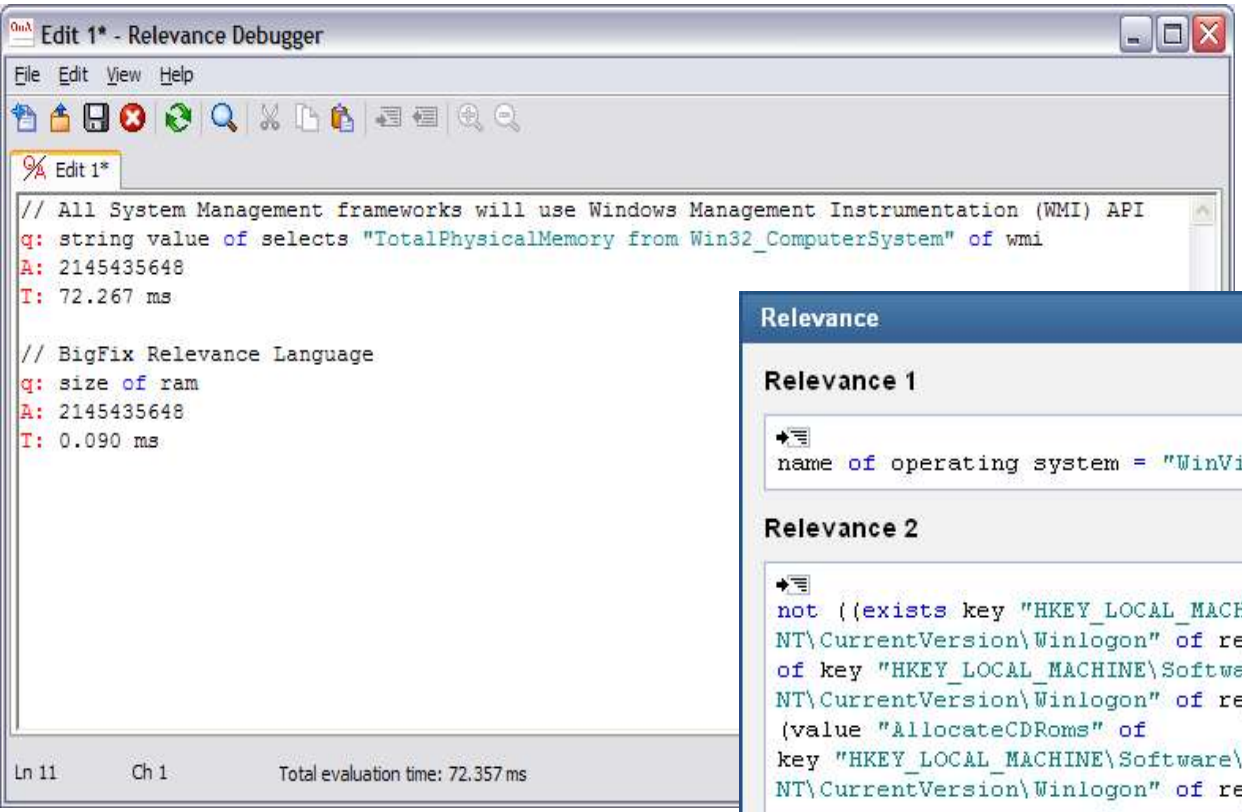
Rank	Vulnerability	Severity	OVAL-ID	Total Applicable Computers
1.	GDI+ GIF Parsing Vulnerability	High	OVAL5986	3
2.	GDI+ WMF Buffer Overrun Vulnerability	High	OVAL6004	3
3.	GDI+ EMF Memory Corruption Vulnerability	High	OVAL6040	3
4.	GDI+ VML Buffer Overrun Vulnerability	High	OVAL6055	3
5.	Microsoft Internet Explorer CSS Tags Remote Code Execution Vulnerability	High	OVAL11574	3
6.	Untrusted search path vulnerability in Microsoft Windows Progman Group Converter	High	OVAL12209	3
7.	GDI+ PNG Heap Overflow Vulnerability	High	OVAL5800	2

Top 10 Detected Vulnerabilities

Rank	Vulnerability	Severity	OVAL-ID	Total Applicable Computers
1.	GDI+ GIF Parsing Vulnerability	High	OVAL5986	3
2.	GDI+ WMF Buffer Overrun Vulnerability	High	OVAL6004	3
3.	GDI+ EMF Memory Corruption Vulnerability	High	OVAL6040	3
4.	GDI+ VML Buffer Overrun Vulnerability	High	OVAL6055	3
5.	Microsoft Internet Explorer CSS Tags Remote Code Execution Vulnerability	High	OVAL11574	3
6.	Untrusted search path vulnerability in Microsoft Windows Progman Group Converter	High	OVAL12209	3
7.	GDI+ PNG Heap Overflow Vulnerability	High	OVAL5800	2
8.	GDI+ TIFF Buffer Overflow Vulnerability	High	OVAL5898	2
9.	TCP/IP Orphaned Connections	High	OVAL5965	2

TEM: Definindo políticas de segurança através da linguagem “Relevance”

- Executada no endpoint gerenciado
- > 100 mais rápida que outras soluções



Relevance

Relevance 1

```
name of operating system = "WinVista"
```

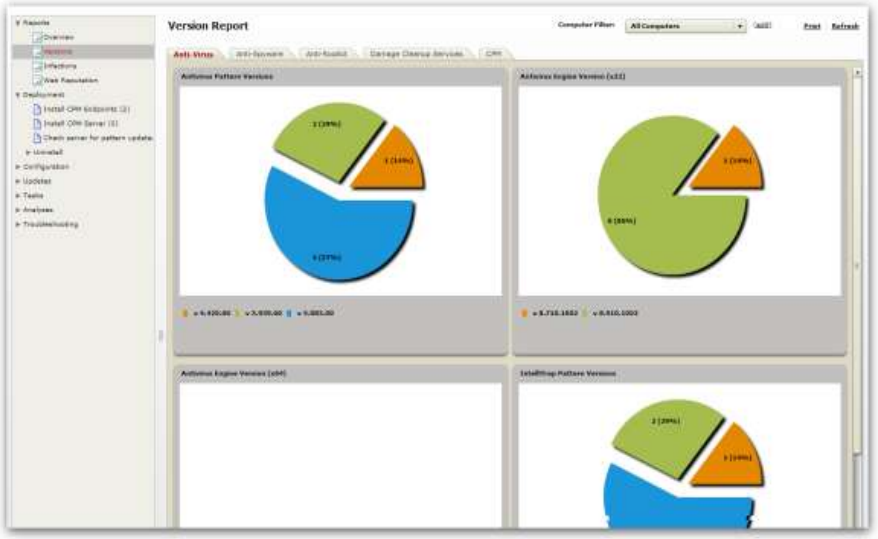
Relevance 2

```
not ((exists key "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon" of registry AND exists value "AllocateCDRoms"
of key "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon" of registry) AND exists
(value "AllocateCDRoms" of
key "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon" of registry) whose( it as string = "0" ))
```

TEM – Agregando mais segurança com o Endpoint Protection

O Módulo de Endpoint Protection inclui:

- Anti-Virus
- Anti-Malware
- Endpoint Firewall
- Web Protection
- Client Manager for Endpoint Protection
- Network Access Control (NAC)



Características e Benefícios

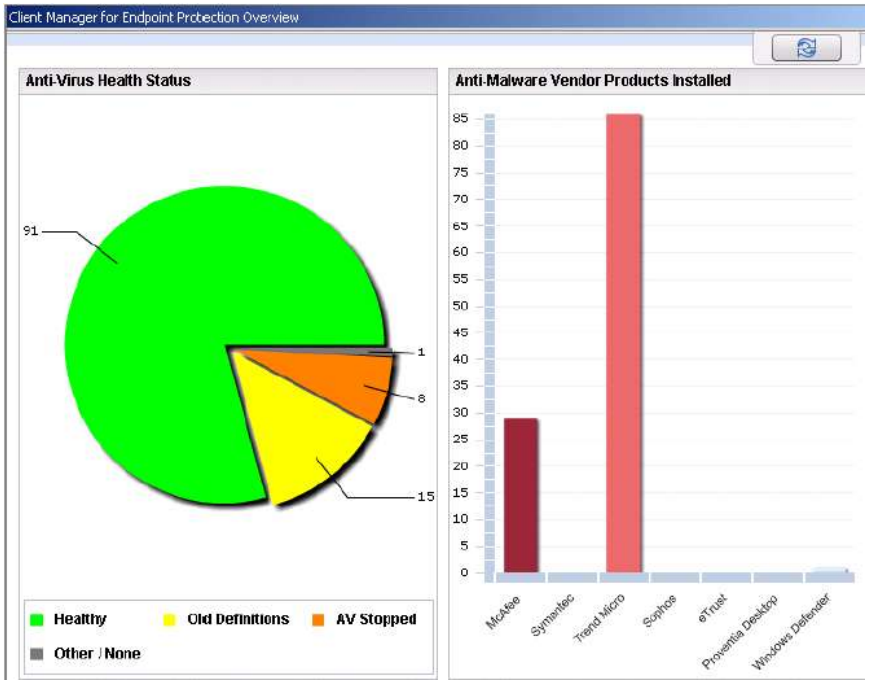
- Previne contra infecção, roubo de informações, perda de produtividade, interrupção de rede e violação de conformidade.
- Elimina falhas de segurança com monitoração real time contra ameaças
- Alcança visibilidade sem precedentes com uma solução de proteção corporativa
- Complementa a solução de configuração, gerenciamento de patches e políticas de conformidade.

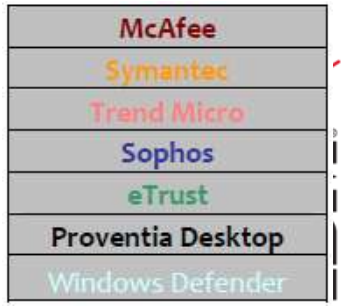
TEM for Security & Compliance – CMEP

Avalia a saúde e gerencia de forma centralizada ferramentas de proteção

O Client Manager for Endpoint Protection realiza:

- Visibilidade em tempo real da "saúde" e status de solucões de Endpoint Security de terceiros
- Gerênciamento e remediação dos Endpoint Protection quando não estão atualizados
- Remove ferramentas não mais utilizadas
- Device Control, para gerenciamento de periféricos como USB e CD-ROMs





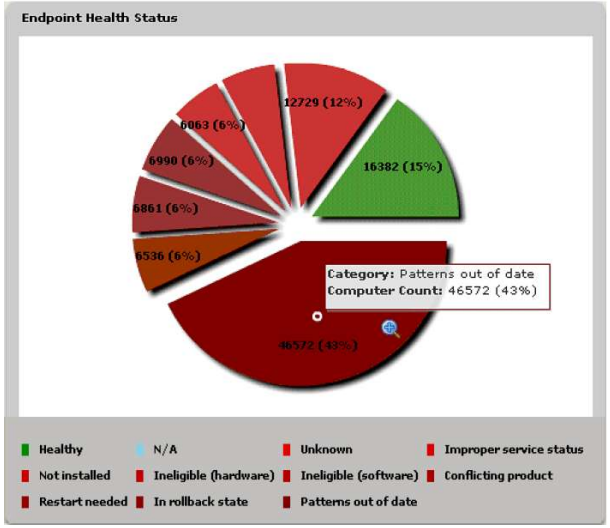
TEM for Security & Compliance – Core Protection Module

Reforça a segurança das estações através do "Trend Endpoint Protection"

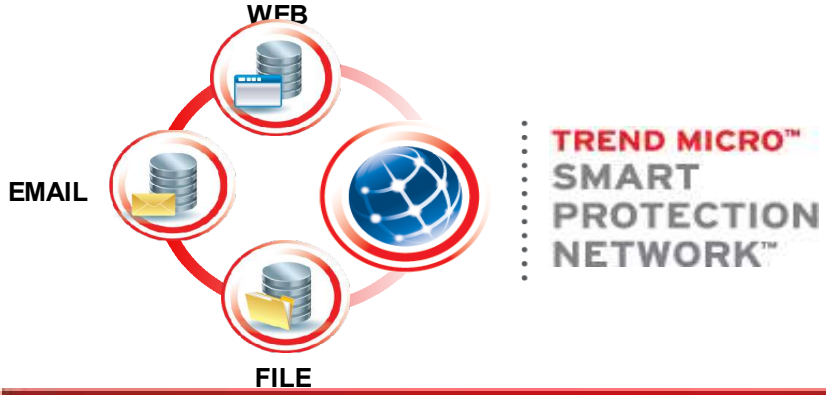
TREND MICRO

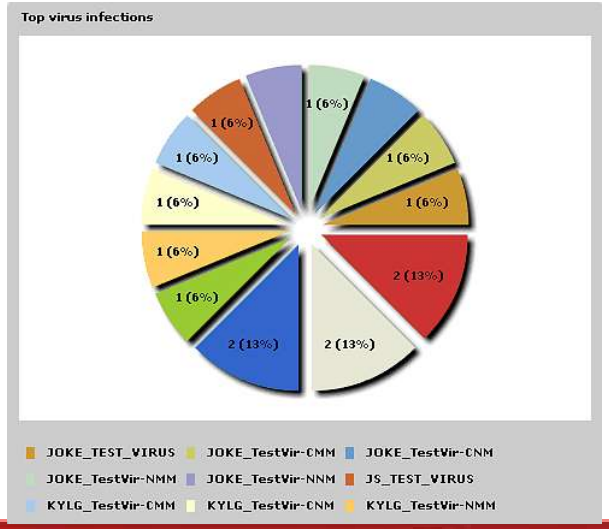
O Core Protection Module inclui:

- Web Reputation
- Endpoint Firewall
- Relatórios (anti-virus, top infections, sites acessados, port violation, etc)
- Anti-virus e Anti-Malware



Maio/2011 chegará a nova versão com novas funcionalidades





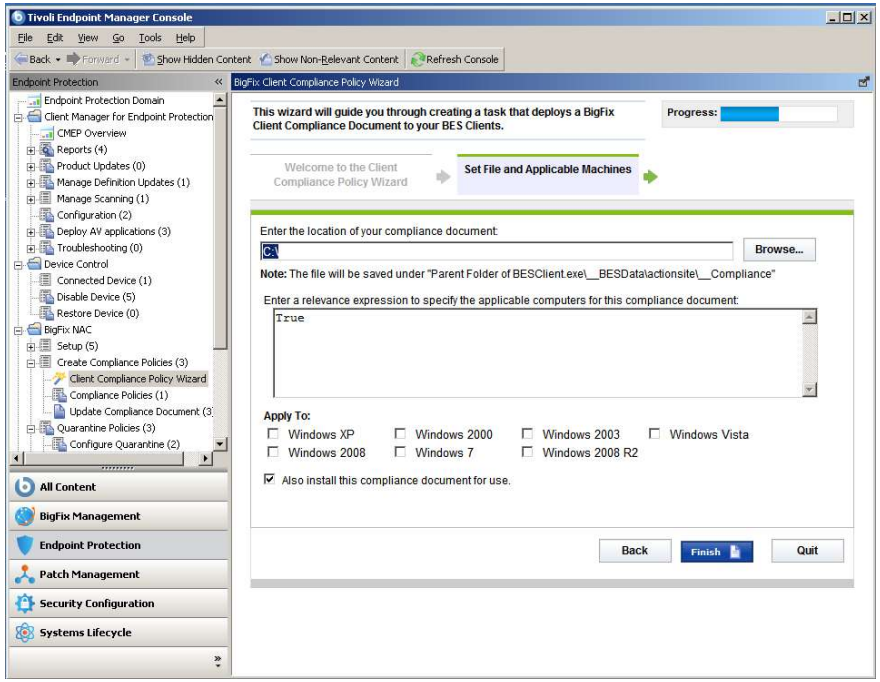
TEM – Endpoint Protection NAC

Diminuindo riscos de invasão através de políticas de compliance

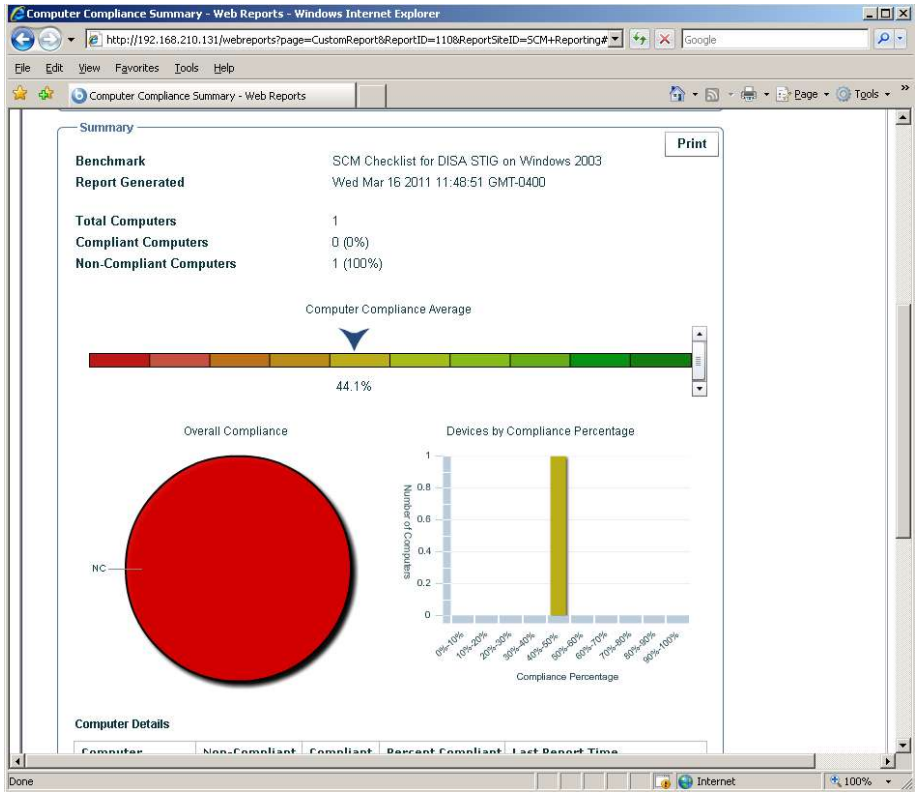
4ª edição IBM Security Forum

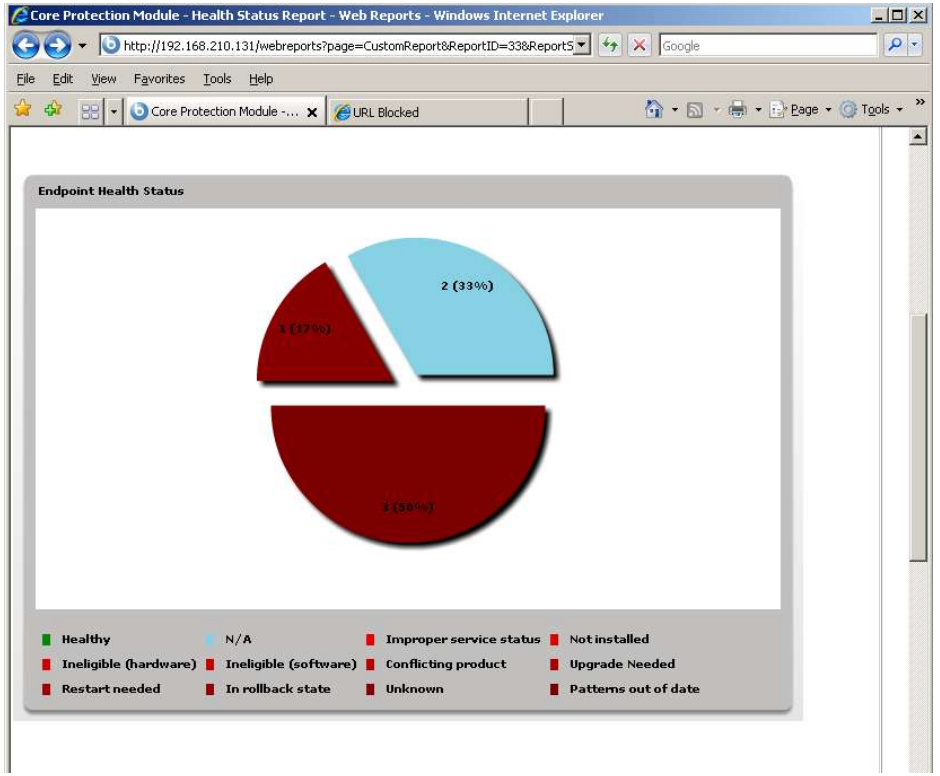
O Core Protection Module realiza:

- Validação da política de compliance
- Se não estiver conformidade, irá para quarentena
- Durante quarentena endpoint só tem acesso ao servidor TEM para correção de compliance
- Possui APIs que podem ser utilizadas por provedores de NAC para consulta de políticas de compliance

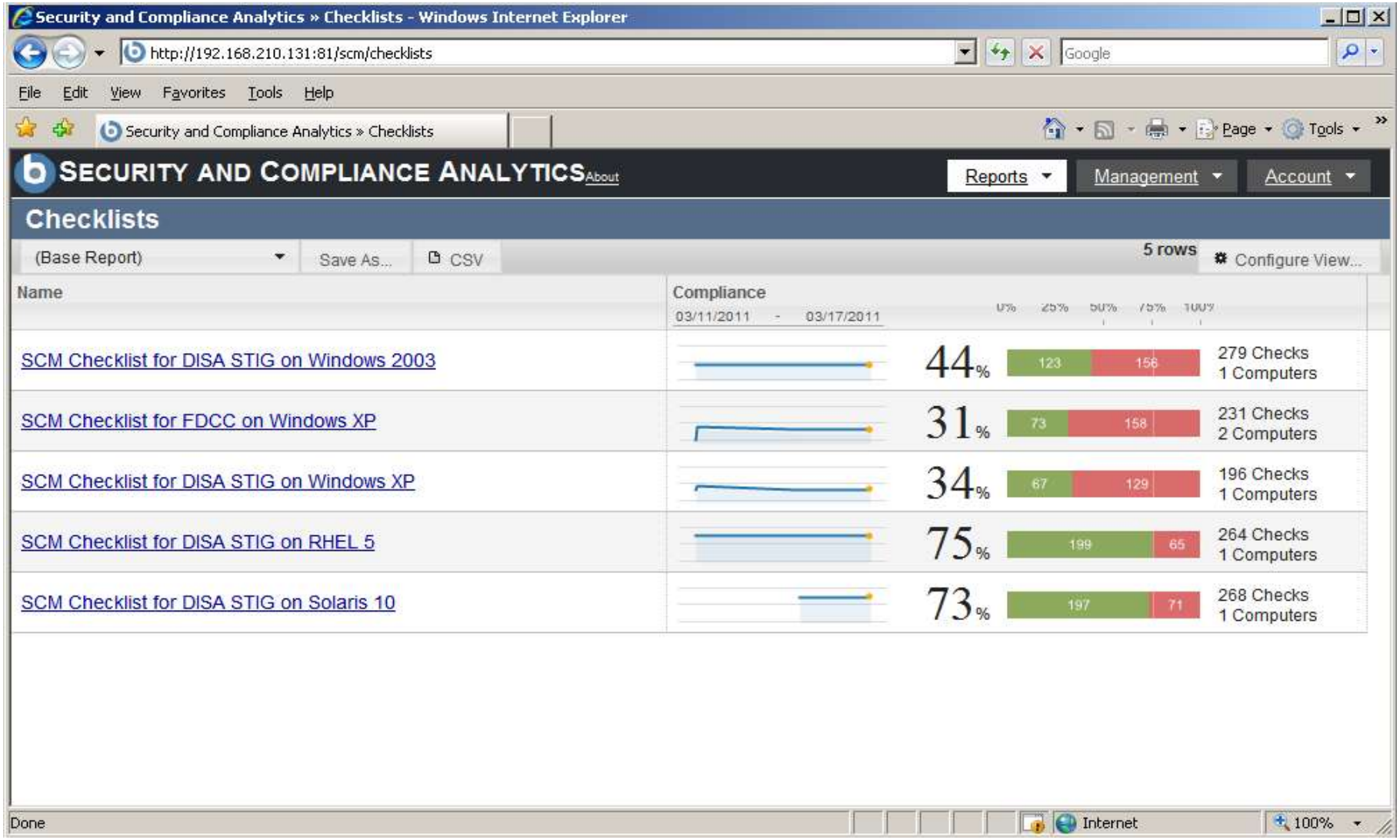


TEM – Web Reports





TEM – Compliance Analytics



BigFix User Group

Index Rules Search Register Login

You are not logged in.

BES Technical Discussions **(RSS Feed)**

Forum	Topics	Posts	Last post
BES Deployment Questions and issues with your BES deployment *(Moderated by* **Ben Kus, Doug Coburn, Lee Wei, Tyler Duni, brolly33***)* **(RSS Feed)**	1437	6064	**Today 09:53:04** by tsikma
BES Customizations Customize your BES deployment *(Moderated by* **Ben Kus, Doug Coburn, Lee Wei, Tyler Duni, brolly33***)* **(RSS Feed)**	519	2450	**2011-03-07 08:08:26** by cstoneba
BES Web Reports and Custom Reports Find those reports that you need *(Moderated by* **Ben Kus, Doug Coburn, Lee Wei, Tyler Duni, brolly33***)* **(RSS Feed)**	650	3255	**Yesterday 15:46:00** by jonrobinson
BES Performance Tuning Get the most out of your BES deployment *(Moderated by* **Ben Kus, Doug Coburn, Lee Wei, Tyler Duni, brolly33***)* **(RSS Feed)**	179	837	**2011-03-06 22:40:08** by Stacy Lee
Fixlet Authoring Share your custom Fixlet ideas and request help with those tricky relevance clauses *(Moderated by* **Ben Kus, Doug Coburn, Lee Wei, Tyler Duni, brolly33***)* **(RSS Feed)**	1828	8344	**Today 08:44:24** by Lee Wei

Solution Forums **(RSS Feed)**

BIGFIX
An IBM Company

Request a Demo

Complete this form and we will follow up to see how BigFix can meet your systems and security management needs.

First Name *

Last Name *

Company *

Title *

Email *

Phone *

No free accounts, please

Please enter use the format (xxx) yyy-zzzz OR +xx yyy zzz-zzzz

Country *

Select One

State/Province

U.S./Canada Only

Purchase time frame *

Select One

Is this a budgeted project? *

☐ Yes ☐ No

Total computers managed *

Select One

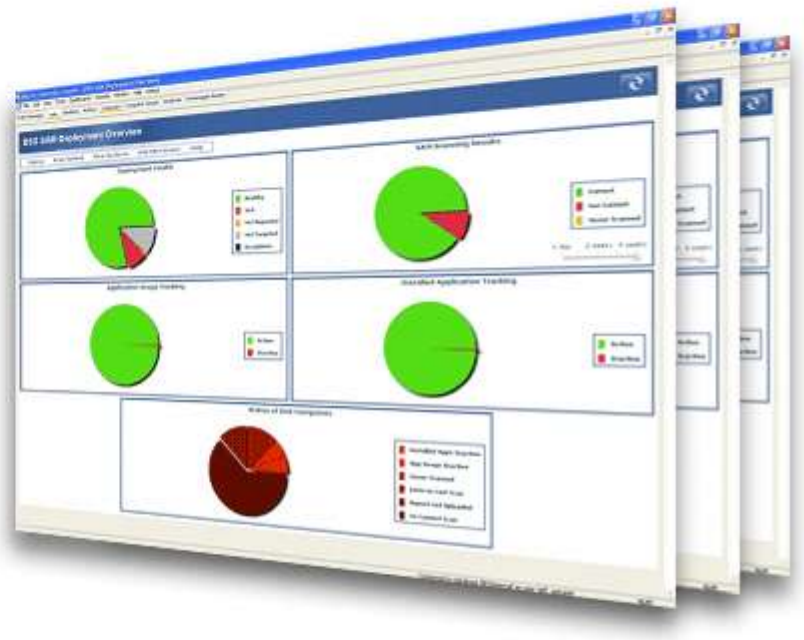
IBM and affiliates may use the information you have provided to keep you informed about IBM products, services and offerings.

No, do not send me e-mail. ☐

No, do not call me. ☐

No, do not send me postal mail. ☐

Submit



Agenda

4ª edição IBM Security Forum

Contextos – Externo e Interno

A Solução e a Ação

Os Resultados

Tivoli software

Por que os clientes escolhem o TEM?

4ª edição IBM Security Forum

Visibilidade em tempo real

- Agente único vê tudo e faz tudo

Escalabilidade inigualável

Um servidor para > 250K endpoints

Ampla cobertura

Multi-platforma, multi-propósito, com rede, sem rede

Rápido retorno

Instalação em poucas horas, remediação em poucos minutos

VAREJO

"**TEM** *simplifica os processos e nos propicia menos fornecedores para gerenciar – economizando dinheiro, reduzindo o estresse e melhorando a qualidade de serviço que entregamos à organização"*

Michael Schaefer
Sr. Wide Area Network Analyst

EDUCAÇÃO (K-12)

*" A econonia de $4.2M [através do **TEM for Power Management**] é impressionante, e isto é só o começo"*

Tom Sims
Director, Network Systems

FINANÇAS

*"Não é uma briga justa [entre o **TEM** e os concorrentes]". A capacidade de superar multiplos desafios através da alavancagem de um agente multi-propósito, residindo em uma única console foi o principal apelo para BGC escolher o **TEM**. Adicionamente, a velocidade do produto foi outro fator importante levado em consideração."*

Chris Marino
SVP of Global IT Procurement

Caso de Sucesso – Deutsche Bank

Ganhos:

- Implantado em 90.000 máquinas dentro de uma semana.
- Redução significativa de TCO: redução de 25 servidores dedicados para 01;redução do número de 20 administradores dedicados para 4.
- Alta taxa de sucesso – para 95%.

Deutsche Bank

CHALLENGES

- Grande variedade de aplicativos financeiros desenvolvidos internamente que necessitam de distribuição e atualização.
- Ferramenta titular implantada em apenas 40 mil dos 90 mil dispositivos.
- 15 ferramentas de configuração de software para gerenciamento do ambiente de TI.
- Experimentou uma baixa taxa de sucesso de 80% com recursos de relatórios limitada.

SOLUTION

- **TEM implantado em todos os 90 mil aparelhos em menos de uma semana.**

RESULTS

- **Consolidação de 15 ferramentas de gerenciamento de configuração em 7.**
- **Redução do número de servidores dedicados de 25 para 1.**
- **Redução do número de administradores dedicados de 20 para 4.**
- **Cumprindo a taxa de sucesso de 95%, com relatórios em tempo real.**

Retorno Comprovado

Área de Preocupação	Abordagem Anterior	Com TEM
Implantação em 90 mil terminais	6 meses	1 semana
Quantidade de Servidores	25	1
Custos anuais de eletricidade	$6.9M	$4M
Ciclo de atualização de Patch	7 dias	5 minutos
Ciclo de Inventário de Software (license “true-up”)	3 semanas	20 minutos
Avaliação do ciclo de vulnerabilidades	6 meses	3 dias
Ciclo de Configuração de Segurança	5 meses 6 FTEs	2 semanas 1 FTE

parâmetros ...

41

Caso de Sucesso – SunTrust

IBM Security Forum

SUNTRUST

Ganhos:

- Amplo sistema de infra-estrutura agora com visibilidade e controle.
- Atualização de Patchs reduzido de 2-3 semanas a 2-3 dias.
- Gerenciamento pró-ativo em vez de uma gestão reativa.

CHALLENGES

- **Ganhar visibilidade sobre uma infra-estrutura distribuída em todas as filiais do banco e sedes da empresa.**
- **Descobrir e trazer todos os componentes para um controle de gestão.**
- **Manter todos os sistemas a nivel de pacth atual e reduzir o tempo de padrões de configuração e atualização.**
- **Conformidade com a segurança e com os grupos de gestão de riscos.**

SOLUTION

- Instalado em mais de 50 mil PCs, servidores e computadores móveis.
- TEM - principal recurso para a correção de software e atualização de sistemas e aplicativos.
- Mantém a vigilância de computadores não gerenciados e periféricos em situação irregular.

RESULTS

- 98,5 % dos patchs atualizados e em conformidade com as politicas de segurança.
- Atualização e tempos de ciclo de atualização de patchs reduzida de 2-3 semanas a 2-3 dias.
- Mudança geral de reativo para pró-ativo com um sistema de gestão de eventos levados a abordagem da gestão do nível de serviço.

Cases - Universidades

MIAMI-DADE PUBLIC SCHOOLS

“ A economia de $4.200.000,00 [através do TEM/BigFix Power Management] é impressionante, e isto é só o começo”

--Tom Sims, Director of Network Systems

EDMONT PUBLIC SCHOOLS

"Recentemente, corrigido e atualizado 16.000 clientes do Microsoft Outlook durante a noite .... Antes isso teria nos levado pelo menos uma semana."

—Richard D’Amours, Senior Network Analyst,Edmonton Public School Board

43

Clientes TEM

44

Clientes TEM

nab
VISA
LG.PHILIPS LCD
SEOUL NATIONAL UNIVERSITY
中国海洋石油总公司
CHINA NATIONAL OFFSHORE OIL CORP.
Western Digital
CJNU
CHUNGJU NATIONAL UNIVERSITY
NANYANG TECHNOLOGICAL UNIVERSITY
NCDEX
TATA BP SOLAR
EMERSON
Process Management
대구은행
DGB
WOORI
INVESTMENT & SECURITIES
PRAXAIR
Honeywell
kepco
CLSA
ASIA-PACIFIC MARKETS
Bank Rakyat Indonesia
Mengutamakan Kepuasan Nasabah
HOUSING & DEVELOPMENT BOARD

Clientes TEM

Finar / Banking — 130,000

Merrill Lynch · Goldman Sachs · Deutsche Bank

Technology

LSI LOGIC · KRONOS

Retail / Consumer — 80,000

Marriott · BLOCKBUSTER

Pharma/Biotech — 230,000

IVAX · Wyeth · KAISER PERMANENTE

Manufacturing — 30,000

SOLECTRON · Western Digital · TRW Automotive

Education — 110,000

Miami-Dade County Public Schools · STANFORD UNIVERSITY · HARVARD · Princeton University

Government

SEC · CALIFORNIA REPUBLIC

Energy — 30,000

FPL · Progress Energy · Entergy THE POWER OF PEOPLE · 中国海洋石油总公司 CHINA NATIONAL OFFSHORE OIL CORP.

+ Clientes

TEM Customer	Managed Devices
US Agency 1	430,000
World's Largest Chip Manufacturer	350,000
World's Largest Retailer	240,000
US-based Healthcare Provider	230,000
Los Angeles Unified School Dist	226,000
Sinopec (China Petroleum)	180,000
Large US Telco	166,000
Wall-Street Firm 1	130,000
China Ministry of Rails	120,000
US Agency 2	111,000
Miami Dade County School Dist	110,000
Wall-Street Firm 2	110,000
US Agency 2	100,000
Wall-Street Firm 3	100,000

Top 50 clients' average deployment is 90,000 endpoints on single management server

Conclusão: Benefícios Framework Tivoli Endpoint Manager

4ª edição IBM Security Forum

SOX	• Assegura que todos os terminais estejam em conformidade com as políticas corporativas, políticas de segurança e políticas de regulação: SOX,GLBA, IE PCI_DSS,etc..
REDUÇÃO DE CUSTOS	• Gerenciamento de energia: economia anual de US$ 30k a US$50k por máquina, controles granulares de opções para hibernação/standby, shutdown de apenas sub-sistemas e trabalhos são salvos antes do shutdown. • Licenças: Identifica os softwares realmente utilizados reduzindo o número de licenças; • Infraestrutura de gerenciamento: um único servidor BigFix gerencia até 250.000 máquinas; • Redução de FTE's: automatiza os processos de gerenciamento reduzindo a dedicação de recursos para as atividades relacionadas.
AMPLA COBERTURA	• Controle em todos os terminais, independentemente do sistema operacional, localização, largura de banda ou de conectividade. • Atualização de Patch's do Windows, Unix, Linux, Mac e todos os aplicativos (Adobe, Firefox, Java, Quicktime, etc).
DISPONIBILIDADE E CONTROLE	• Única Console: Somente um agente e uma console que utiliza menos de 2% dos recursos da CPU. • Relatórios em tempo real: todos os softwares instalados e patchs atualizados, agentes corrompidos, número de maquinas que necessitam de correção, entre outros.
VELOCIDADE	• Rápida Instalação : 02 a 04 horas. • Rápida Atualização: centenas de milhares de máquinas em alguns dias ou poucas semanas em diversas localizações geográficas. • Agente único: melhora o desempenho e permite gerenciamento e ações em tempo real.

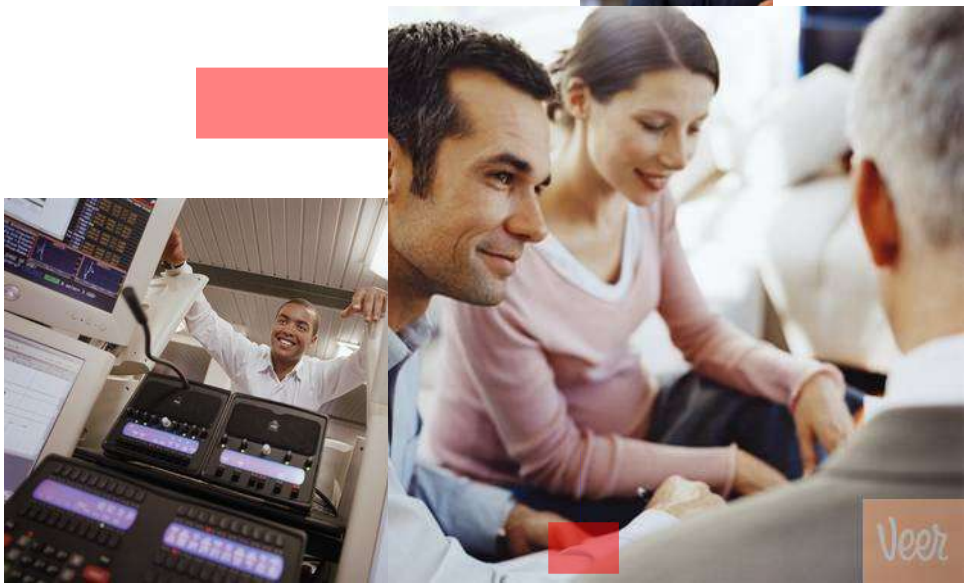
Dúvidas Finais

Mais informações

Utilize o contato abaixo:

Rodolfo de Souza
Sales Leader – Tivoli Endpoint Manager
Telefone: 55 11 2322-6004
Mobile: 55 11 7153-8709
E-Mail: **rodolfo.souza@br.ibm.com**

Obrigado!!



50