

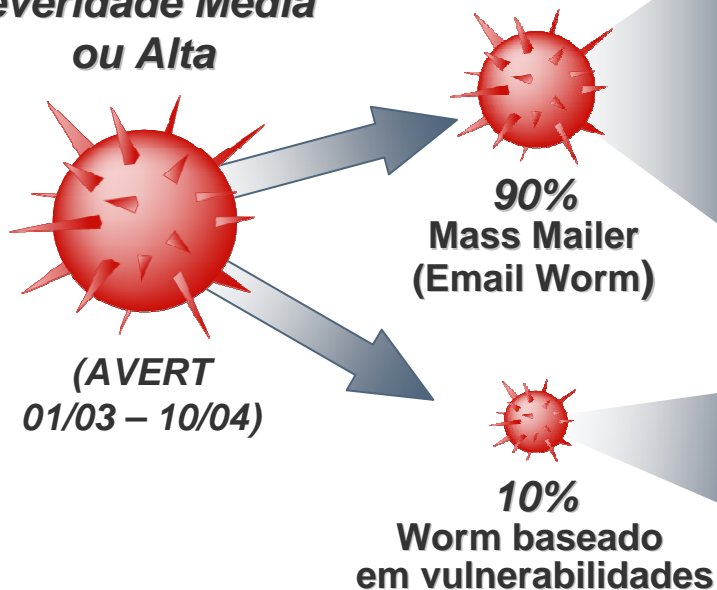


McAfee

Ameaças e Gestão de Risco
Prevenção de Intrusões
Gestão de Conteúdos Seguros

Panorama actual

**66 Ameaças com
severidade Média
ou Alta**



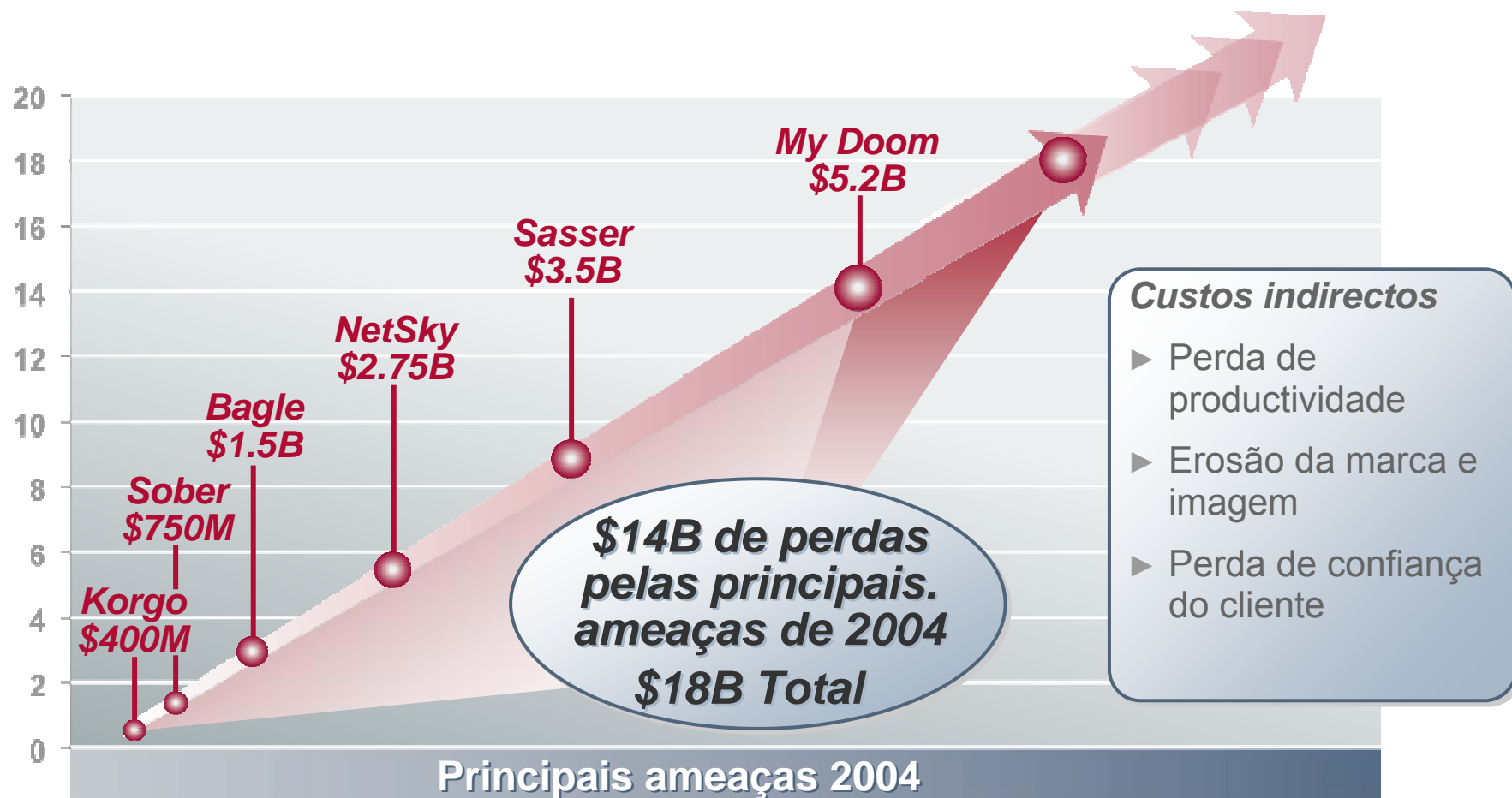
Metodologias e acções adicionais

Email 100%	Remote Access 73%
P2P 45%	Terminate Process 42%
Share Hopper 23%	Download 17%
Remote File Copy 10%	Key Logger 12%
Exploit 10%	Registry Delete 10%
File Infector 8%	DOS 10%
Application Spoof 5%	File Deletion 2%

Exploit 100%	Remote Access 83%
Download 33%	DOS 17%

Metodologia de infecção inicial

Impacto no negócio por ameaças



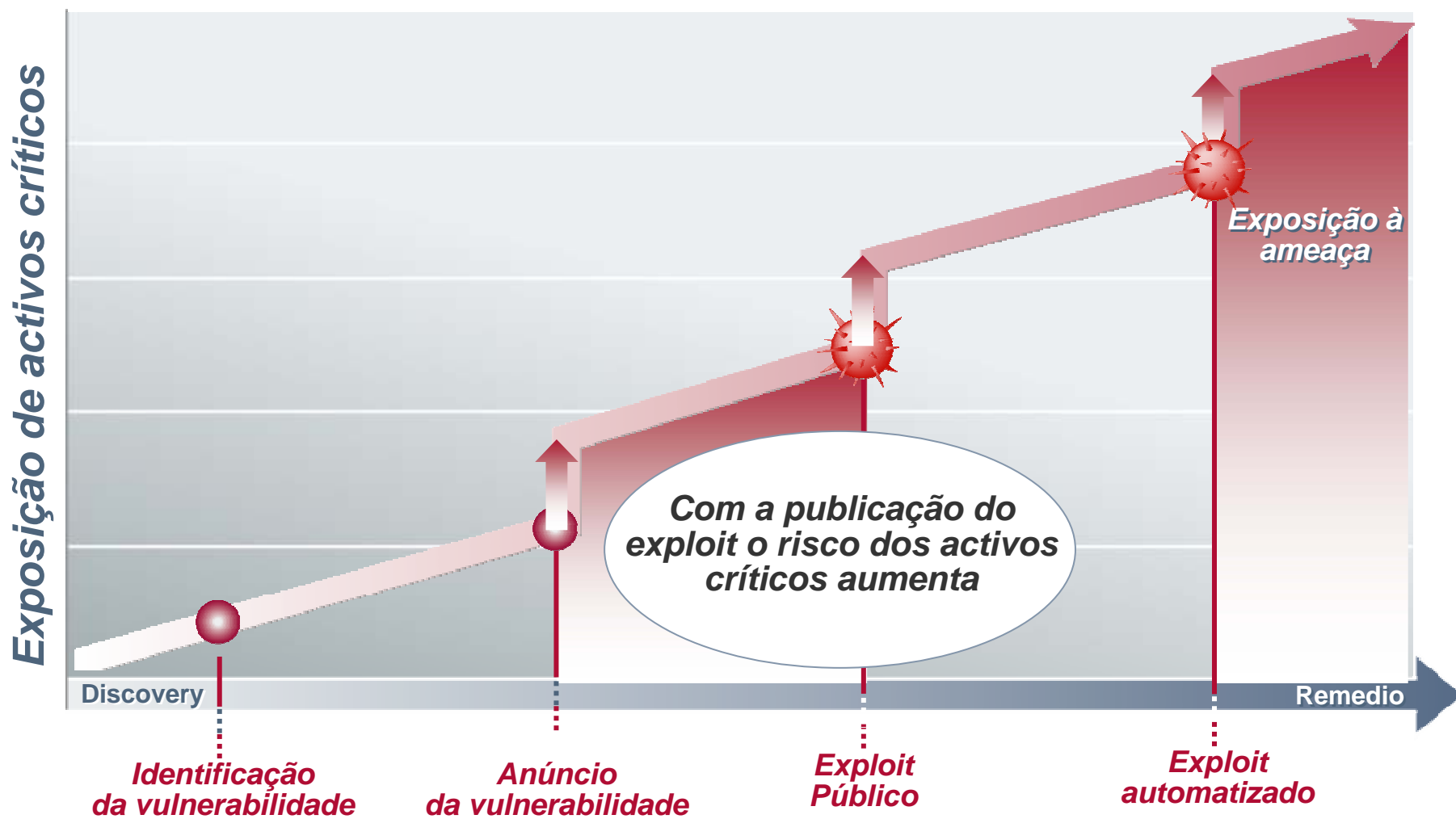
Source: Computer Economics 12/04



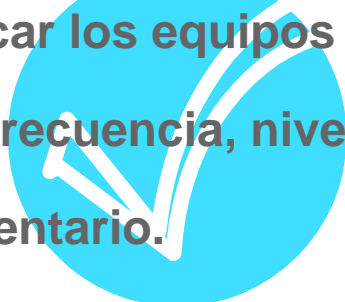

McAfee

Detecção Day 0

Desde a vulnerabilidade à ameaça



Sistemas de Detección de Vulnerabilidades

- 
- 
- ▶ Ayudan a identificar los equipos con problemas.
 - ▶ Se actualiza con frecuencia, nivel de actualización adecuado.
 - ▶ Capacidad de inventario.
 - ▶ Visión/evolución histórica.
 - ▶ Priorización de los activos/optimización de recursos.
 - ▶ Medición del riesgo.
 - ▶ Adecuación a la política existente.

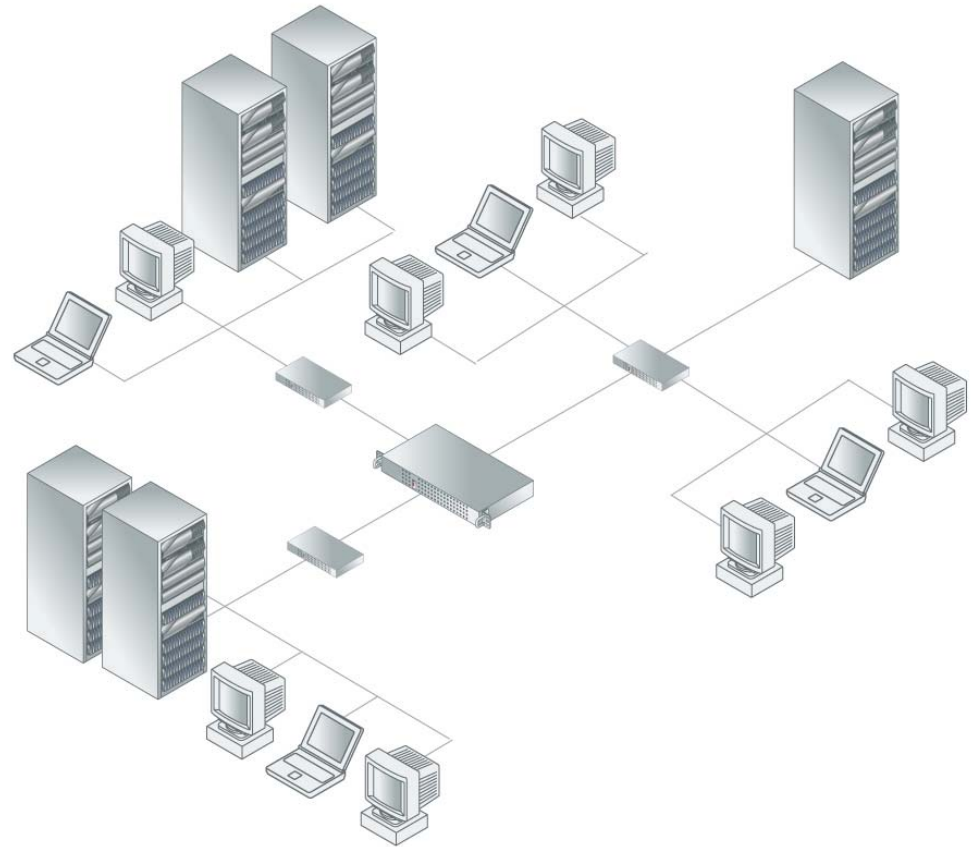
Mudança da estratégia referente à segurança

- ▶ Filosofia de **GESTÃO de RISCO**
- ▶ Mudança de estratégia
 - Protecção contra a metodologia, não contra o ataque
- ▶ Protecção da infra-estrutura
 - Protecção desde o 'cabo' até à aplicação
 - 'Enforcing' de políticas

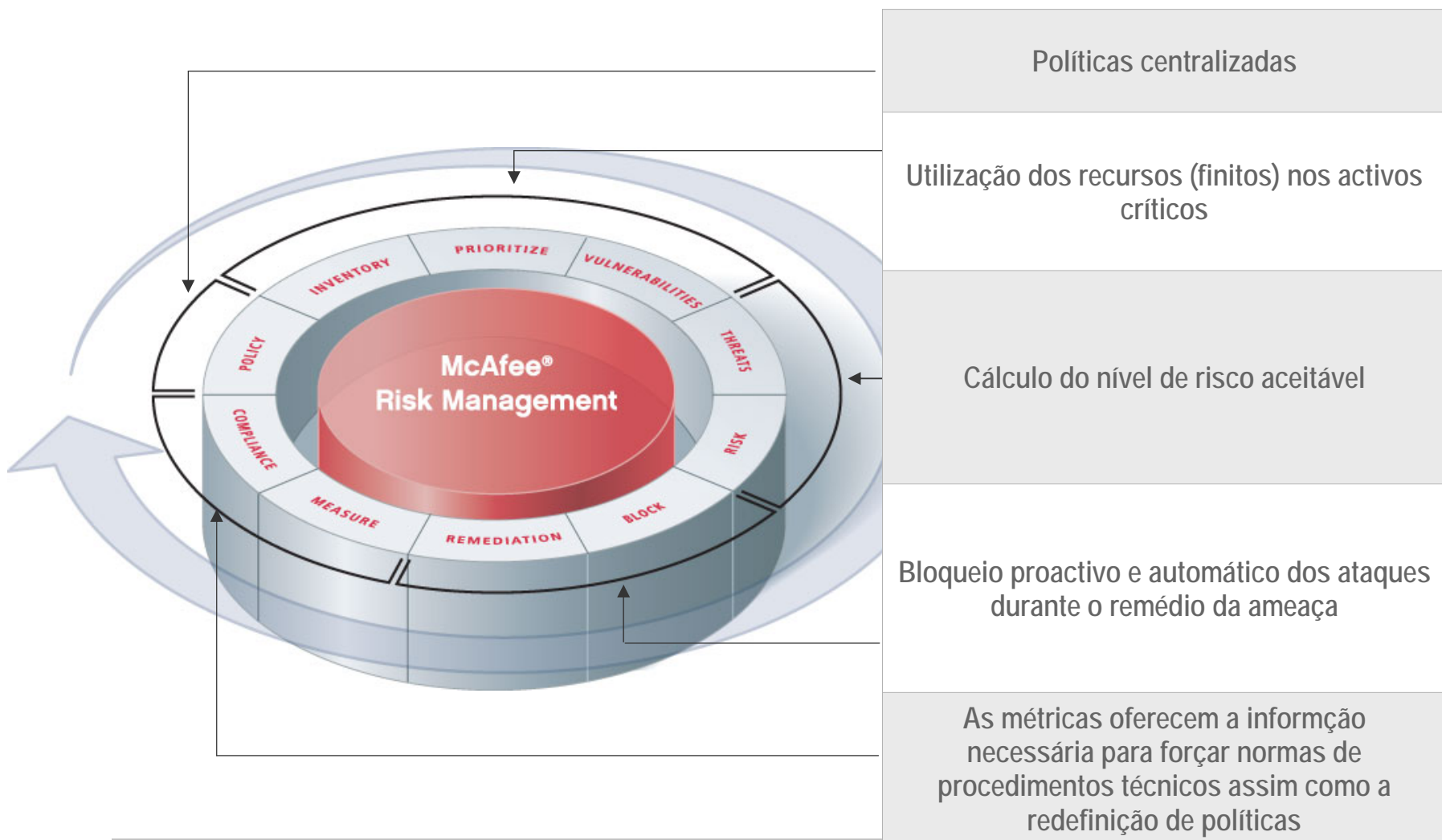


As organizações consideram a necessidade

- ▶ Os activos são cada vez mais complexos e mais distribuídos
- ▶ Alguns activos são mais críticos que outros
- ▶ Os recursos são limitados
- ▶ É necessário melhorar a produtividade dos recursos para chegar a todos os activos críticos



McAfee Gestão de Riscos — Aplicação da disciplina de negócio à segurança



McAfee Gestão de Riscos — Aplicação da disciplina de negócio à segurança



Políticas centralizadas	McAfee ePolicy Orchestrator
Utilização dos recursos (finitos) nos activos críticos	McAfee ePolicy Orchestrator McAfee Foundstone
Cálculo do nível de risco aceitável	McAfee Foundstone
Bloqueio proactivo e automático dos ataques durante o remédio da ameaça	McAfee IntruShield McAfee Entercept (HIPS) McAfee VirusScan Family of Products McAfee Anti-Spyware McAfee SCM
As métricas oferecem a informação necessária para forçar normas de procedimentos técnicos assim como a redefinição de políticas	McAfee ePolicy Orchestrator McAfee Foundstone



McAfee

Resposta

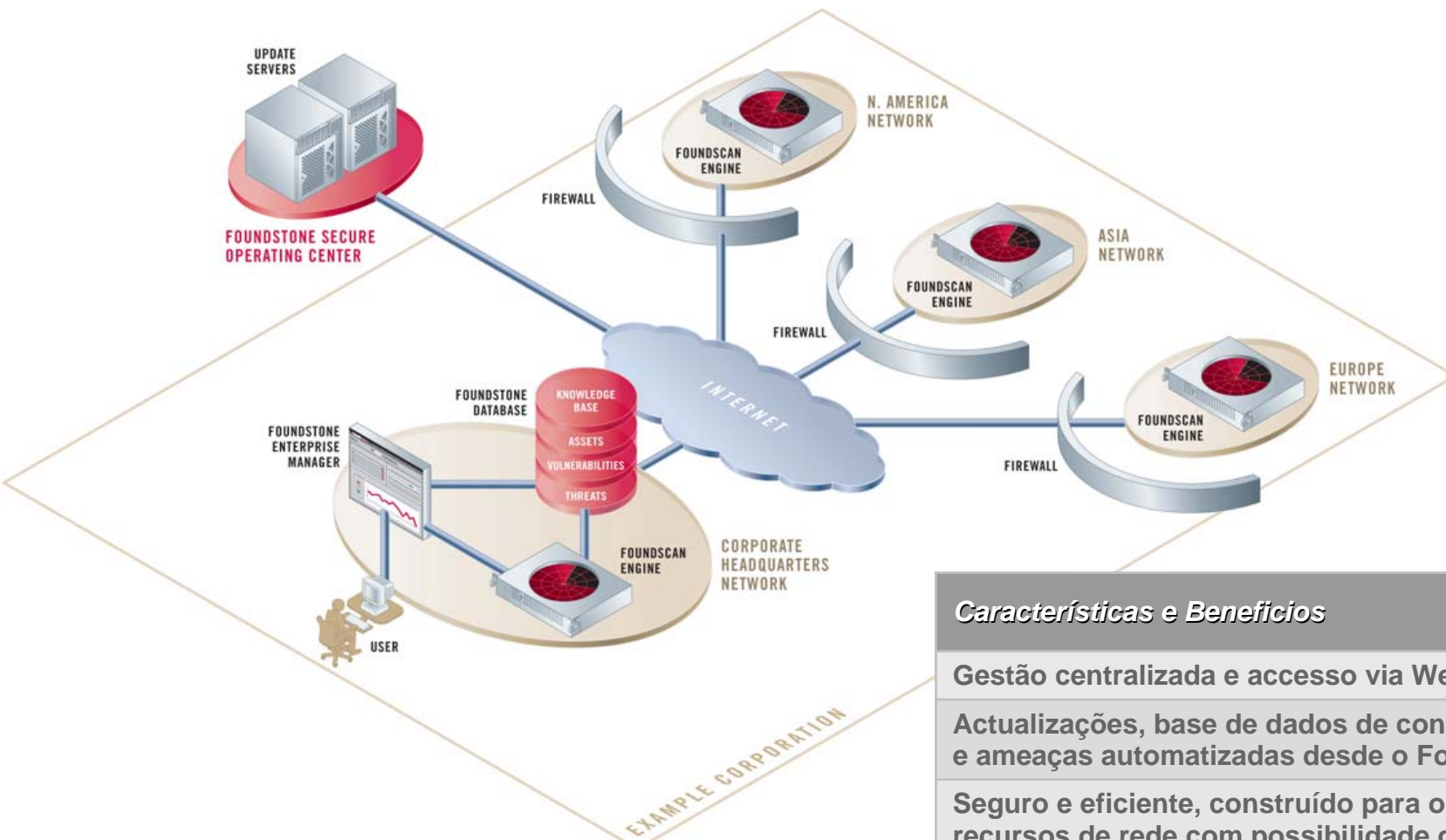
McAfee Foundstone

Características



- ▶ Baseado em *Appliances* dedicadas
- ▶ Alto rendimento nas análises de inventario
- ▶ Actualizações automáticas
- ▶ Escalável. Supervisão de ambientes complexos com instalações distribuídas.
- ▶ Facilidade de acesso. Interface Web.
- ▶ Administração delegada.

Produto empresarial



Características e Benefícios

Gestão centralizada e acesso via Web

Atualizações, base de dados de conhecimento e ameaças automatizadas desde o Foundstone

Seguro e eficiente, construído para otimizar recursos de rede com possibilidade de balanço de carga

Produto Empresarial

FOUNDSTONE SCAN ARCHITECTURE



Características e Benefícios

Arquitectura paralela única que permite executar distintos 'scans' em simultâneo

Un único escaneo se distribuye automáticamente en múltiples subescaneos para mejorar el rendimiento

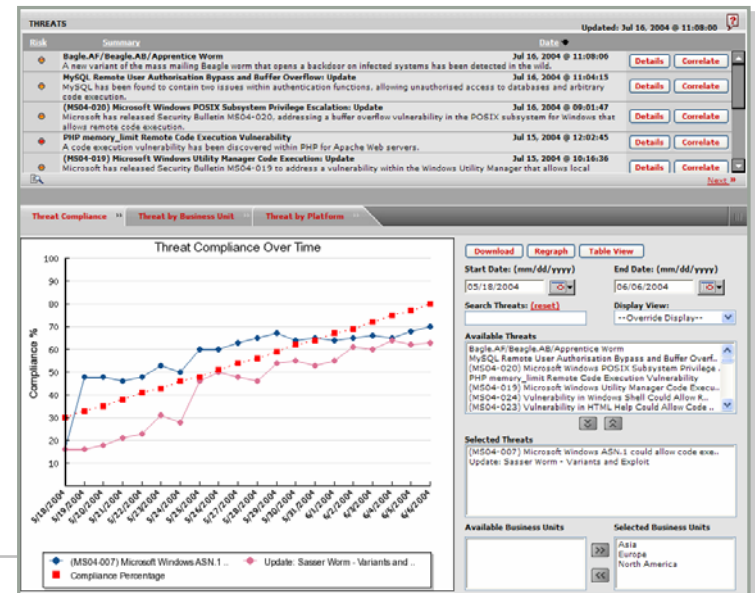
Recuperación de escaneos sin pérdidas de información gracias a su diseño de procesos por lotes

Gestão de Ameaças

- ▶ Alertas inteligentes sobre ameaças, como *worms* e *exploits*...
- ▶ Mostra o impacto de uma ameaça, imediatamente e sem necessidade de realizar um novo scan.
- ▶ 'Ranking' de riscos , para proteger primeiro os sistemas mais importantes.
- ▶ Resposta às ameaças por unidades de negócio.
- ▶ Mede os esforços de resposta contra as metas de remédio estabelecidas.

THREAT DETAILS: Update: (MS04-011) Microsoft Windows Security Rollup Patch (835732)

Risk	System	IP Address	Criticality	Matched By	Operating System	Vulnerability
37	[Unknown]	10.0.30.163	5	✖️🔍🔒🔒🔒	Windows XP	(MS04-011) Microsoft Windows ASN.1 Double Free Heap Corruption via DCOM
63	[Unknown]	10.0.30.175	5	✖️🔍🔒🔒🔒	Windows 2000	
51	[Unknown]	10.0.30.155	4	✖️🔍🔒🔒🔒	Windows 2000	
38	[Unknown]	10.0.30.137	3	✖️🔍🔒🔒🔒	Windows NT 4.0	
38	[Unknown]	10.0.30.152	3	✖️🔍🔒🔒🔒	Windows 2000	
14	[Unknown]	10.0.30.160	1	✖️🔍🔒🔒🔒	Windows NT 4.0	(MS04-011) Microsoft Windows ASN.1 Double Free Heap Corruption via SUB
38	[Unknown]	10.0.30.167	-	✖️🔍🔒🔒🔒	Windows XP	
38	[Unknown]	10.0.30.169	-	✖️🔍🔒🔒🔒	Windows 2000	
38	[Unknown]	10.0.30.170	-	✖️🔍🔒🔒🔒	Windows 2000	
38	[Unknown]	10.0.30.195	-	✖️🔍🔒🔒🔒	Windows 2000	
38	[Unknown]	10.0.30.159	-	✖️🔍🔒🔒🔒	Windows 2000	(MS04-011) Microsoft Windows ASN.1 Double Free Heap Corruption via SMTP
38	[Unknown]	10.0.30.156	-	✖️🔍🔒🔒🔒	Windows 2000	
38	[Unknown]	10.0.30.164	-	✖️🔍🔒🔒🔒	Windows 2000	
14	[Unknown]	10.0.30.165	-	✖️🔍🔒🔒🔒	Windows NT 4.0	
14	[Unknown]	10.0.30.166	-	✖️🔍🔒🔒🔒	Windows NT 4.0	
14	[Unknown]	10.0.30.179	-	✖️🔍🔒🔒🔒	Windows 9x/Me	(MS04-011) Microsoft Windows ASN.1 Double Free Heap Corruption via SMTP
14	[Unknown]	10.0.30.187	-	✖️🔍🔒🔒🔒	Windows NT 4.0	
14	[Unknown]	10.0.30.189	-	✖️🔍🔒🔒🔒	Windows NT 4.0	



Workflow

- ▶ Introduzido em 2002 .
- ▶ As vulnerabilidades convertem-se facilmente em *tickets*.
- ▶ A atribuição de *tickets* está baseada em regras flexíveis.
- ▶ Criação, atribuição e fecho automáticos.
- ▶ Compatibilidade com terceiros.

New Tickets: You have 10 new tickets to review, out of 2216.

<input type="checkbox"/>	ID	Scan Name	Risk	Vulnerability	System	Criticality	OS
<input type="checkbox"/>	73623	Sales Network Scan	●	Sun Solaris Common Desktop Environment (CDE) displayed Information Leaks	66.192.0.176 (66.192.0.176)	-	Solaris 2.7 - 2.8
<input type="checkbox"/>	73624	Sales Network Scan	●	rshd Detected	66.192.0.176 (66.192.0.176)	-	Solaris 2.7 - 2.8
<input type="checkbox"/>	73626	Sales Network Scan	●	RLugin Service	66.192.0.176 (66.192.0.176)	-	Solaris 2.7 - 2.8
<input type="checkbox"/>	73628	Sales Network Scan	●	Solaris in-fined User Enumeration	66.192.0.176 (66.192.0.176)	-	Solaris 2.7 - 2.8
<input type="checkbox"/>	73629	Sales Network Scan	●	Solaris in-fined User Enumeration	66.192.0.176 (66.192.0.176)	-	Solaris 2.7 - 2.8
<input type="checkbox"/>	73630	Sales Network Scan	●	Chargen Denial of Service	66.192.0.176 (66.192.0.176)	-	Solaris 2.7 - 2.8
<input type="checkbox"/>	73631	Sales Network Scan	●	revocd Detected	66.192.0.176 (66.192.0.176)	-	Solaris 2.7 - 2.8
<input type="checkbox"/>	73634	Sales Network Scan	●	Telnet Daemon is Running	66.192.0.176 (66.192.0.176)	-	Solaris 2.7 - 2.8
<input type="checkbox"/>	73635	Sales Network Scan	●	LPD Information Leaks	66.192.0.176 (66.192.0.176)	-	Solaris 2.7 - 2.8
<input type="checkbox"/>	73636	Sales Network Scan	●	SSH-V Protocol Enabled	Frank Laptop (66.192.0.190)	1	OpenBSD 3.0 - 3.3

Make all due on: 08/16/2004 Assign all to: None

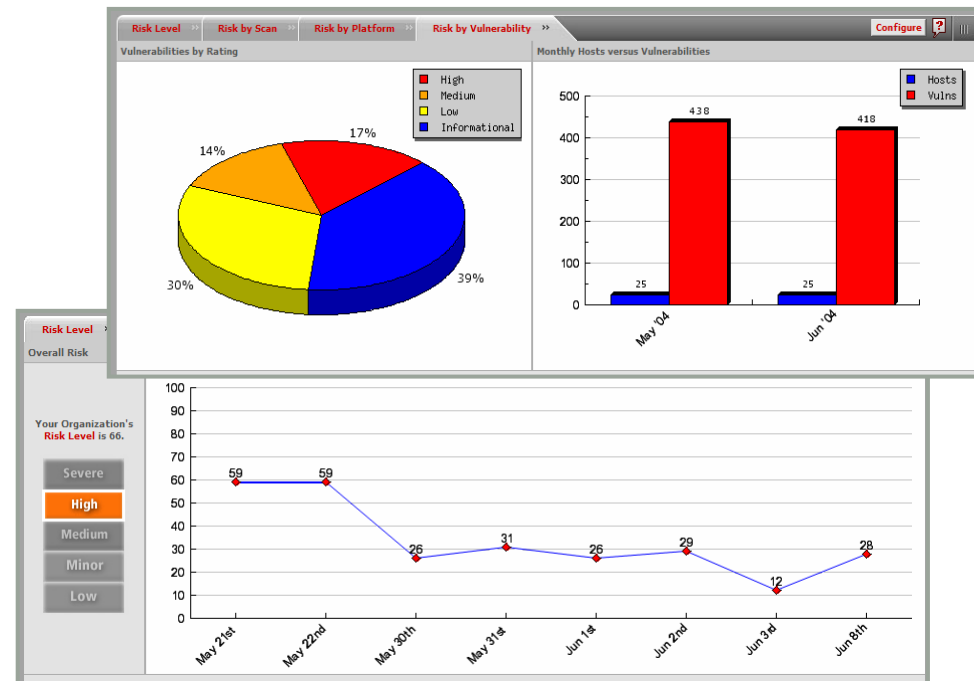
Rules » Global Options »

Name	Description	Status					
Assign to asset owner	Assign any tickets with an asset owner to the asset owner	Active	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Run"/>	<input type="button" value="Up"/>	<input type="button" value="Down"/>
Assign to John	Assign all high risk vulns to John Smith	Active	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Run"/>	<input type="button" value="Up"/>	<input type="button" value="Down"/>
Assign to Rob	Assign all wireless issues to Rob in San Francisco	Inactive	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Run"/>	<input type="button" value="Up"/>	<input type="button" value="Down"/>
Export for Ecommerce Farm	Export Ecommerce web farm tickets to Remedy HelpDesk system	Active	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Run"/>	<input type="button" value="Up"/>	<input type="button" value="Down"/>
Ignore Anonymous FTP in Extranet	Anonymous FTP allowed a policy exception for the Extranet only.	Active	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Run"/>	<input type="button" value="Up"/>	<input type="button" value="Down"/>
Assign to Linux System Administrators	Assign all RedHat Linux tickets to the Linux administrators in Chicago	Active	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Run"/>	<input type="button" value="Up"/>	<input type="button" value="Down"/>
Assign to Network Administrators	Send all Cisco Router, Extreme Switch, and Check Point Firewall-1 vulnerabilities to the network administrators	Active	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Run"/>	<input type="button" value="Up"/>	<input type="button" value="Down"/>
Assign Solaris Configuration Issues	Assign all Sun issues (i.e. policy problems with configuration) to Sally	Active	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Run"/>	<input type="button" value="Up"/>	<input type="button" value="Down"/>

Métricas – Relatórios

- ▶ FoundScore: Valores intuitivos de 0-100 baseado em vulnerabilidades
- ▶ MyFoundScore: FoundScore é personalizável.
- ▶ Risk Score: Visão imediata do risco global da empresa.

- ▶ *Dashboard* interactivo para comparações entre unidades de negócio, regiões, plataformas etc...





McAfee

Medidas de Contenção

McAfee System Protection



► Mobile Devices

McAfee VirusScan Mobile



► Laptop, Desktop & Servers

McAfee VirusScan Enterprise & AntiSpyware

McAfee LinuxShield

McAfee Host Intrusion Prevention System

McAfee Policy Enforcer

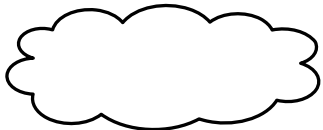


► eMail & Groupware Servers

McAfee GroupShield Exchange & Domino

McAfee SpamKiller Exchange & Domino

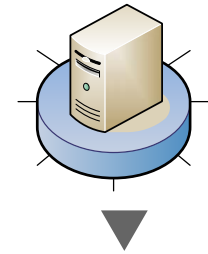
McAfee PortalShield for Ms Sharepoint



► Internet gateway

SCM Appliances

McAfee SecurityShield for Ms ISA

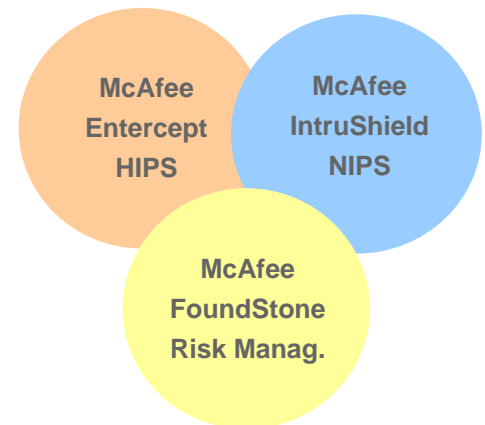


Management

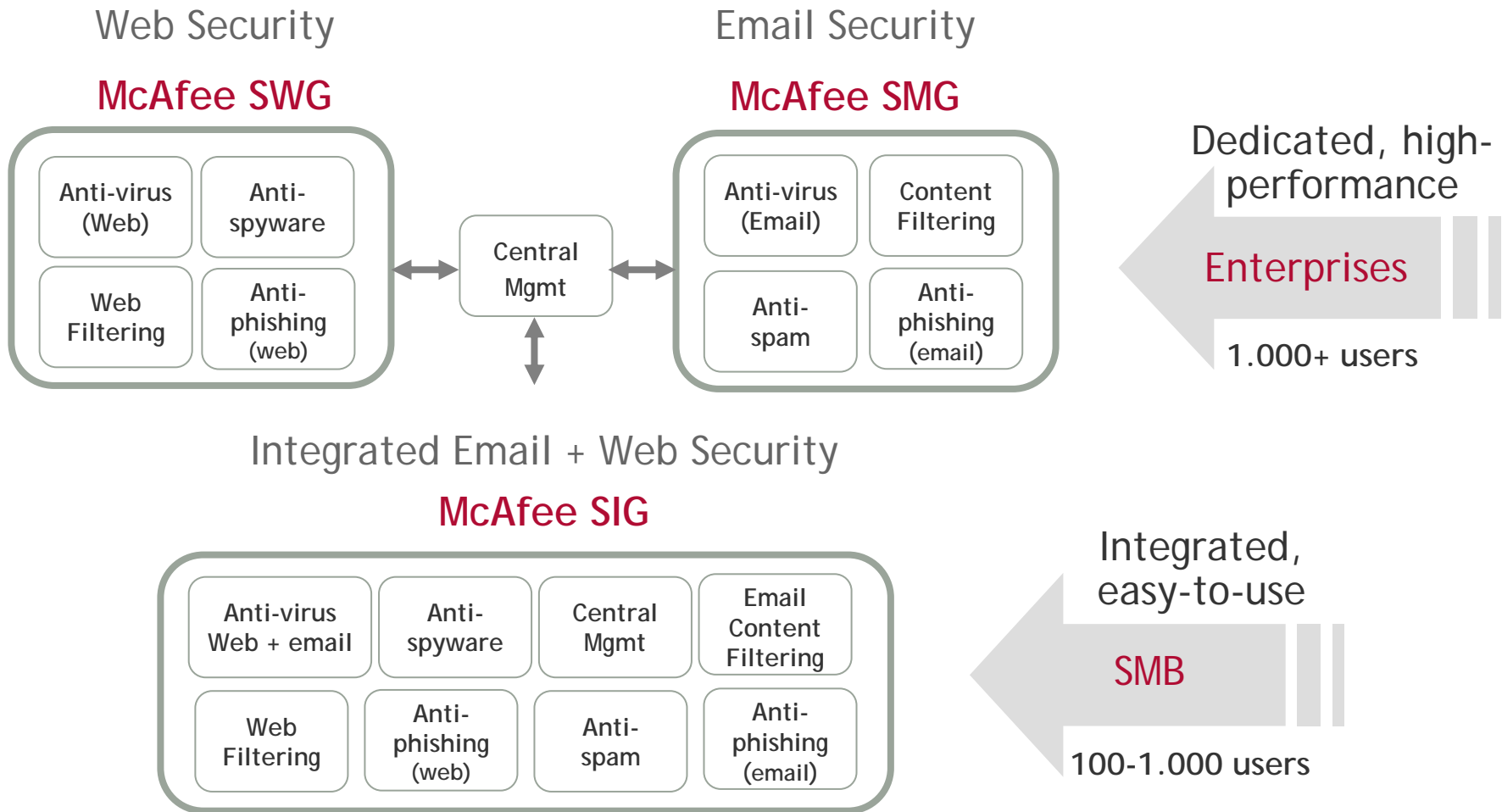
McAfee ProtectionPilot (SMB)

McAfee ePolicy Orchestrator

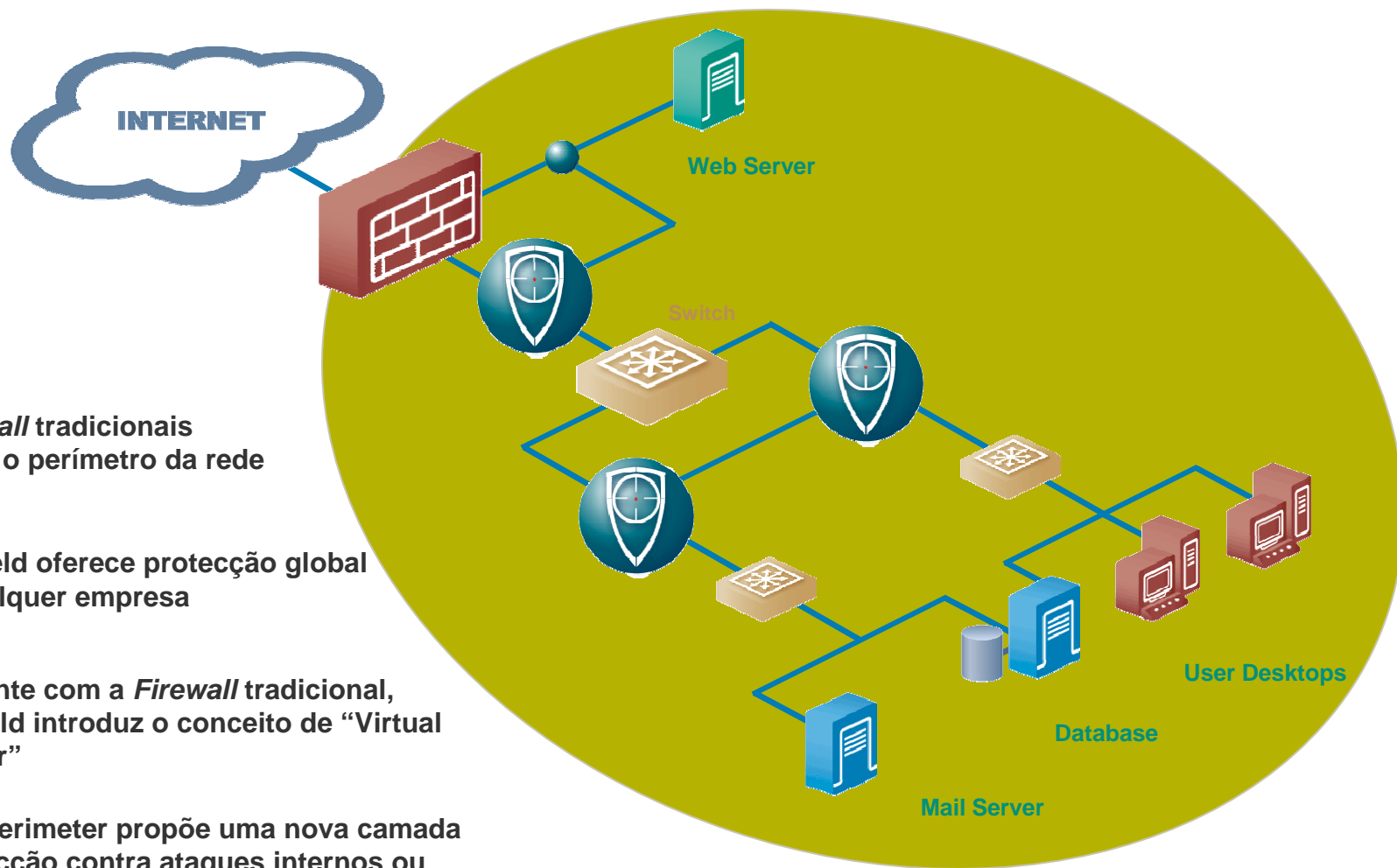
- **Support HIPS strategy**
- **High availability**
- **Threat information**
- **Named policy**



McAfee SCM 4.0 Appliance



Novo conceito: “Virtual Perimeter”



- 1 As *Firewall* tradicionais definiam o perímetro da rede
- 2 IntruShield oferece protecção global para qualquer empresa
- 3 Juntamente com a *Firewall* tradicional, IntruShield introduz o conceito de “Virtual Perimeter”
- 4 Virtual Perimeter propõe uma nova camada de protecção contra ataques internos ou ataques que ultrapassam a *Firewall* tradicional

IntruShield Sensor Appliances



IntruShield 1200
PME e escritórios remotos



IntruShield 1400
PME e escritórios remotos e perímetro



IntruShield 2600
Perímetro corporativo



IntruShield 4000
Redes backbone

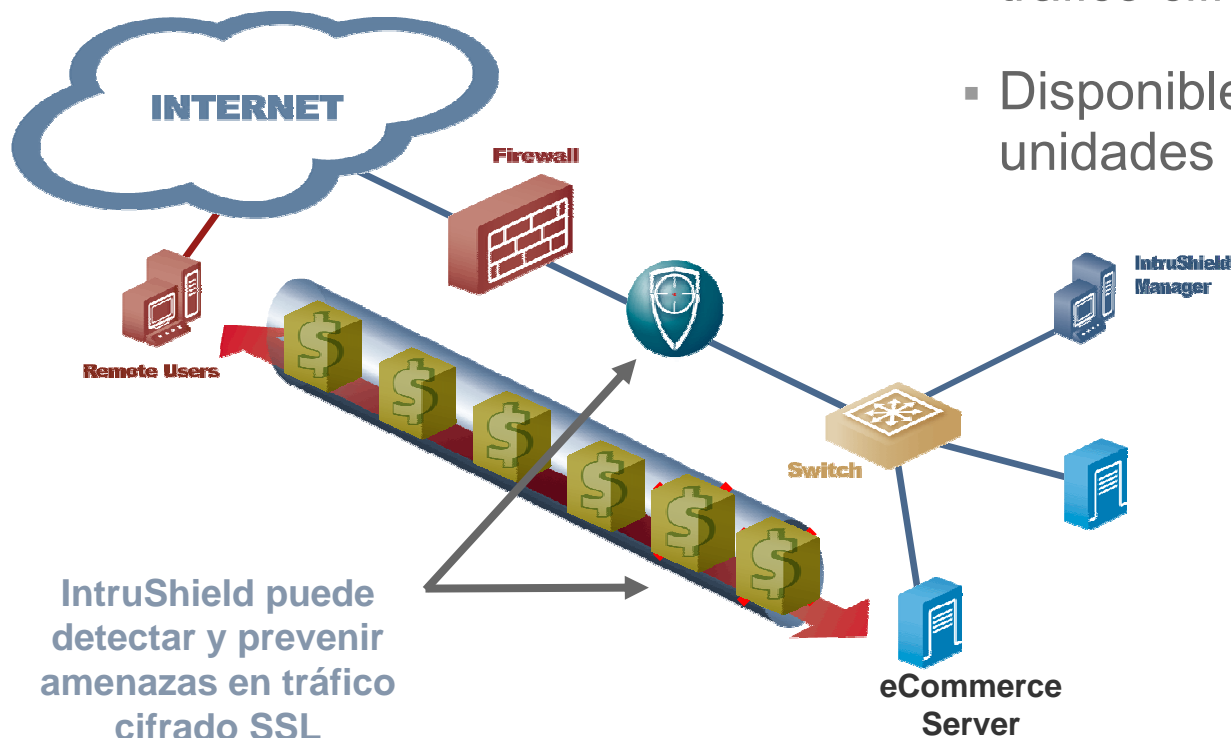
SENSOR	PERFORMANCE	Monitoring Ports			Response Ports
		10/100 Base-T	Gigabit	Taps	10/100 Base-T
IntruShield 1200	100 Mbps	2		Yes	1
IntruShield 1200	200 Mbps	4		Yes	1
IntruShield 2600	600 Mbps	6	2	Yes	3
IntruShield 4000	2 Gbps		4	No	2
IntruShield 4000	2 Gbps		12	No	2
		1 - 10/100 Base-T Management Port			
		1 Console Port & 1 Aux Port			

IntruShield: Características competitivas

Característica	Benefício
Solução <i>Appliance</i>	Redução do custo de propriedade eliminando custos separados como Hardware, software, sistema operativo e protecção do Sistema Operativo.
Solução de detecção e prevenção integradas	Elimina a necessidade de adquirir ou re-licenciar productos que conduzam ao nível de prevenção.
Gestão remota baseada em Web	Sistema de gestão remota centralizado. A gestão granular de politicas reduz falsos positivos.
Virtual IDS/IPS	Um único IntruShield pode substituir muitos IDS tradicionais.
Inclusão interna de Fast Ethernet Network Taps	Permite a modificação remota de um sistema para passar de detecção a prevenção.
Tolerância a falhas	As portas do sensor podem actuar como “fail-closed” ou “fail-open”.
Implementação flexível: SPAN, Tap, In-line, Agrupamento de portas, Alta-disponibilidade	IntruShield pode adaptar-se a qualquer topologia de rede.

Protección en tráfico cifrado SSL

- Primer IPS de red con capacidad de inspección y protección sobre tráfico cifrado SSL
- Disponible como upgrade para unidades existentes

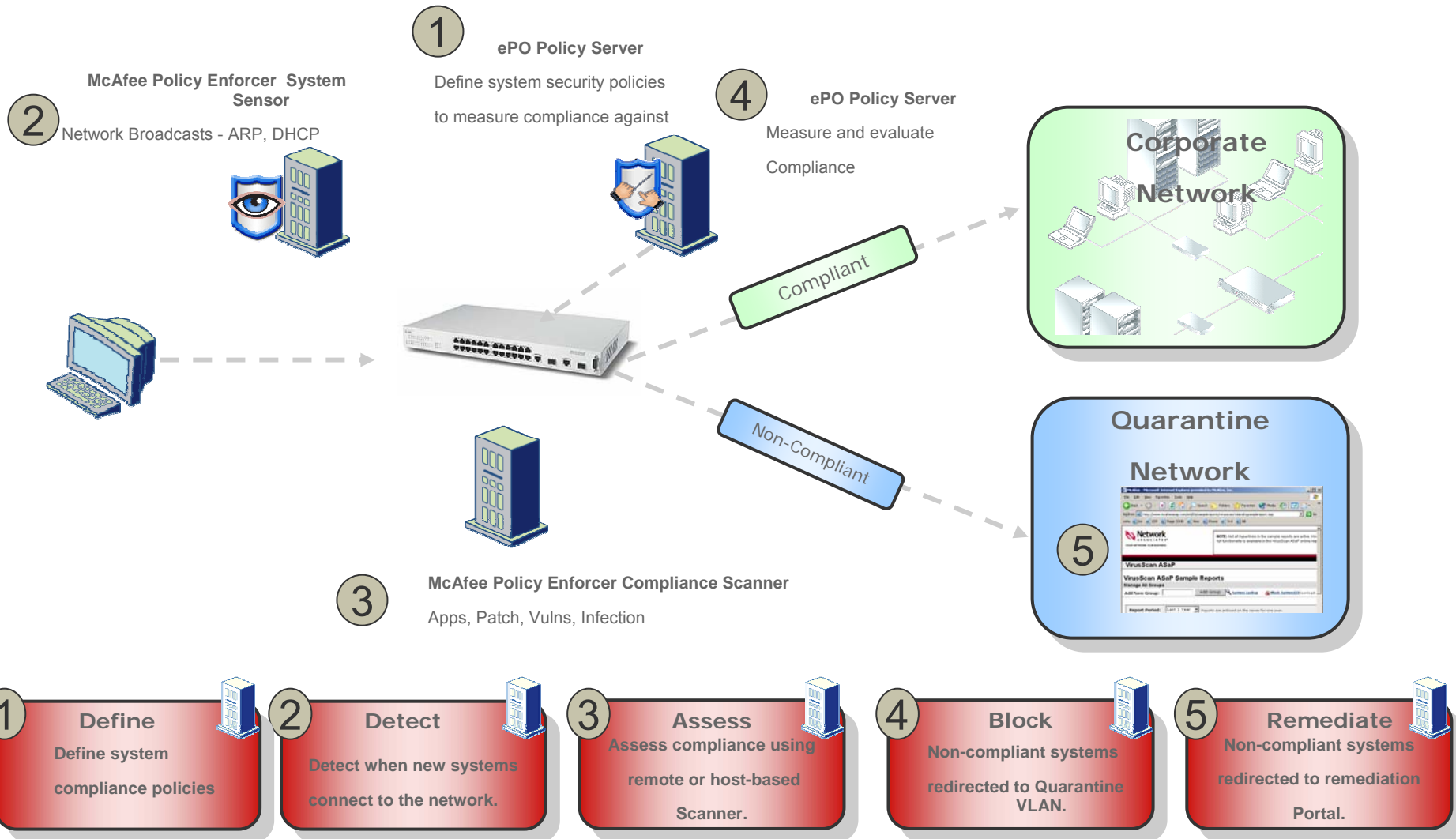




McAfee

Evolução Tecnológica

McAfee Policy Enforcer – Em 5 pasos





McAfee

Serviços e Formação

Expert Services

Custom Consulting

On-Site AV Security Consultancy Project Leader
AV Security Consultancy (1-9 days)
AV Security Consultancy (10+ days)
Intrushield Consultancy
Foundstone Consultancy

Packaged Consulting

Anti-Virus Policy Check On/Off site
Anti-Virus Policy Check and Implementation On/Off Site
Anti-Virus Self Start (VSS) on site
ePolicy Orchestrator Self Start on site
ePolicy Orchestrator Installation on site
Gateway Services Groupshield on site
Gateway Services WebShield Appliance on site

Training Courses

McAfee Live Virus Workshop
Anti-Virus Administrator Training - VirusScan & Epo
Anti-Virus Administrator Training - VirusScan
Anti-Virus Administrator Training - ePolicy Orchestrator
Mastering Groupshield for AV Administrators
Mastering Webshield for AV Administrators

Entercept Essentials

Intrushield Essentials

McAfee Product Training

Ultimate Hacking

Ultimate Hacking Expert

Ultimate Web Hacking

Building Secure Software

Incident Response & Forensics

Foundstone Scripting Language Trn

Foundstone Enterprise Product Trn

Training Courses

Ultimate Hacking

Ultimate Hacking Expert

Principles of Security

Ultimate Hacking: Windows Security

Ultimate Web Hacking

Building Secure Software

Incident Response & Forensics

Cyber Law

One day Seminar

AV Trainer 1 day (certified trainer)



Obrigado