IBM Security Forum

Soluções para um ambiente seguro

Proteja sua Rede e Dados, Reduzindo Custos Operacionais e Perdas

Ricardo Marques
Senior Security Engineer
marquesr@br.ibm.com

Agenda

- Cenário atual de Segurança de TI, Custos, Ameaças, Soluções
- Reduzindo custos com Soluções de Segurança IBM ISS

É cada vez mais complexo proteger o ambiente de negócio das empresas

Proteger os sistemas contra ataques

- Virus
- Malware
- Intrusões

Proteger os dados

- parados
- Em transito
- Em uso
- transações

Realidade Atual dos Negócios: Maior Risco, Menos Recursos

Economia Atual...

***Computerworld* – 14 Outubro 2008**

"With a faltering economy resulting in increased jobs cuts and corporate belt tightening, security analysts are warning companies to be especially vigilant about protecting their data and networks against disgruntled employees."

"Tough economic times create uncertainty in the workplace. When there is uncertainty, it creates stress for employees. It makes the company more vulnerable to threats."

Shelley Kirkpatrick
Management Concepts

...Realidade

Cortando Custos Operacionais

- Adiando contratações de staff adicional de TI, projetos de longo prazo e novas iniciativas em favor de ROI a curto prazo
- Procurando aumento em produtividade na infraestrutura existente

Gerenciando Riscos Maiores

- Aumento de riscos de fraude e outras atividades criminosas
- Aumento de ameaças de empregados insatisfeitos
- Custos associados a downtime não planejado

Mantendo ou Definindo uma Postura sobre Compliance

- Exemplo americano +/- 114,000 normativas ou regras foram impostas sobre negócios e instituições americanas desde 1981
- *33% dos clientes notificados de uma quebra de segurança terminam o relacionamento com a empresa fornecedora*

Custos e Complexidade Sem Precedentes

Novos Métodos e Motivos

Aumento da complexidade e quantidade de riscos

"Web Facing Applications"

Custos associados a iniciativas de Compliance:
Investimentos em mais produtos pontuais para resolver mais problemas pontuais

A Economia Global:
Clima económico oscilando

Inovação TI:
Necessidade de novas maneiras de proteger as novas formas de colaboração (virtualização)

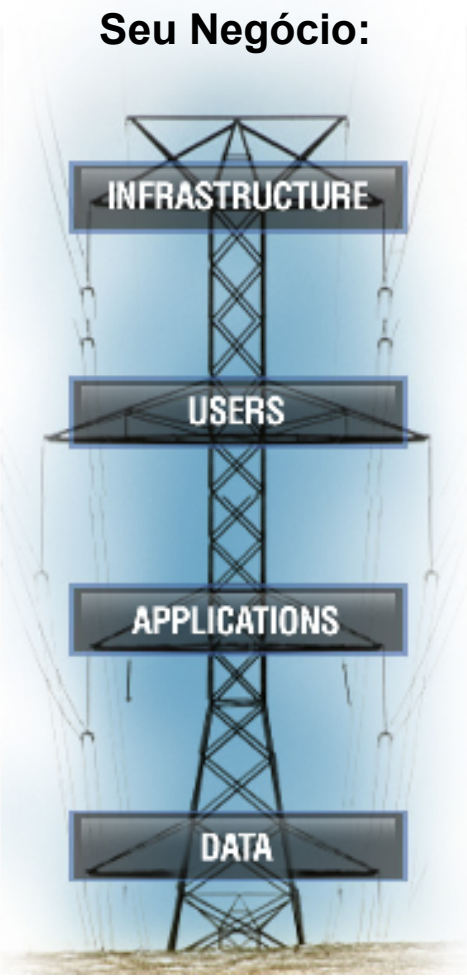
Flexibilidade nos Métodos de Fazer Negócios:
Para melhorar operações e serviços aos clientes

A Complexidade Permanece o Maior Desafio da Segurança de TI!

Integração é a chave para gerenciar custo e complexidade no ambiente de transformação constante

Questões de Segurança que Permanecem sem Respostas:

Seu Negócio:



Pergunte-se:

- **Posso proteger contra ameaças de segurança internas e externas?**

  (Information Technology)

- Posso proteger minhas iniciativas de negócios?

  (Linha de Negócios)

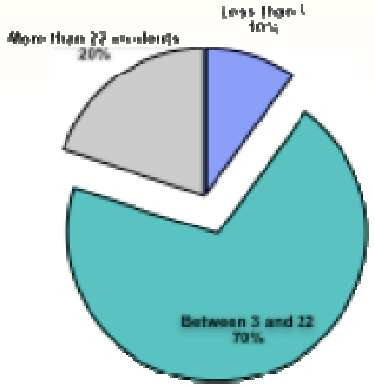
  – Quem pode entrar?
  – Que podem fazer?
  – Posso provar isso facilmente a um auditor?

A RESPOSTA SIMPLES:

"Não, não posso."

Disclosures of Sensitive Business Data

(IT Policy Compliance Group)



Soluções de Segurança devem Endereçar Desafios-Chave para o Negócio

REDUZIR CUSTOS

MITIGAR RISCOS

AUMENTAR A PRODUTIVIDADE

- **Entregar economia imediata e reduzir o custo total de propriedade**
- **Assegurar a continuidade do negócio**
- **Permitir inovação**

A Complexidade Permanece o Maior Desafio da Segurança de TI!

Integração é a chave para gerenciar custo e complexidade no ambiente de transformação constante

**InformationWeek 2008 Security Survey*

Uma conversa franca sobre: *Redução de Custos Enquanto Aumentamos a Segurança e Produtividade*

- Qual é a sua atual estrutura de custo para segurança de TI?
- Como você assegura que a sua infraestrutura de TI seja suportada pelas mais modernas tecnologias e processos de segurança?
- Você tem dificuldades durante a contratação de profissionais qualificados em segurança de TI?

Uma conversa franca – cont.

- Sua organização está protegida contra todas as ameaças de TI conhecidas na atualidade?
- Você sabia que 99% das empresas que tiveram quebras de segurança tinham firewalls e antivirus implementados?
- Existe alguma parte da infraestrutura de segurança de TI prestes a entrar em ciclo de renovação?
- Quem é seu suporte em segurança? Ele/Ela consegue acompanhar as demandas 24x7 da operação de segurança?

Sofa no Museu Sigmund Freud

Reduzindo Custos Enquanto Aumentamos a Segurança e Produtividade

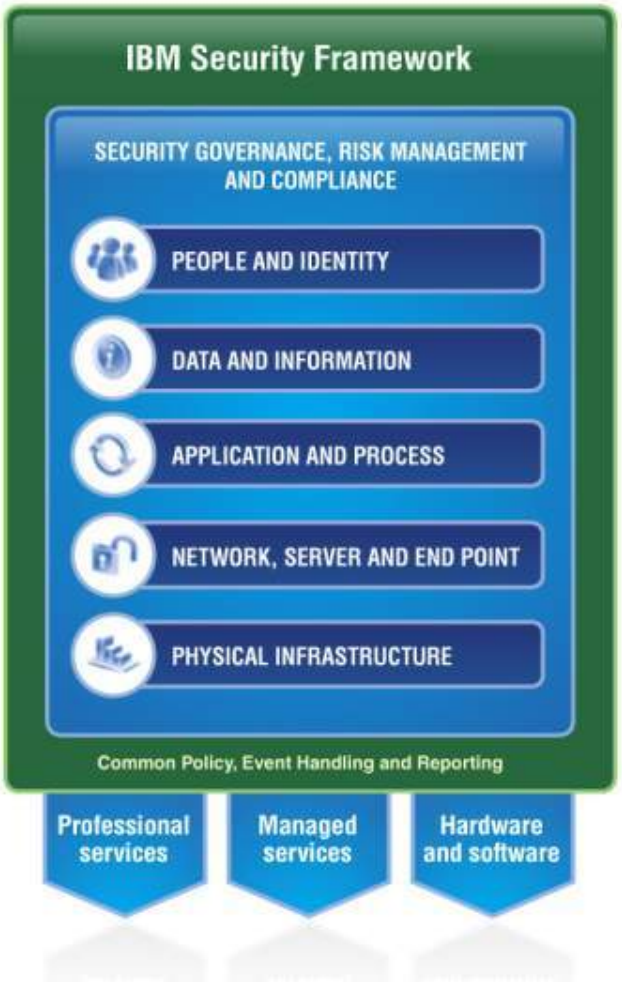
- A sua solução de proteção de servidores protege contra ambos ataques de rede e de aplicação automaticamente?
- O processo de implementar “patches” em servidores cria um peso ou desfalque na operação dos seus negócios?
- Sua equipe consegue lidar com as demandas da implementação e gerenciamento de soluções de segurança de hosts?
- Sua organização está sujeita a algum tipo de conformidade ou normativa externa?

Lego - Dr. Octopus

IBM oferece uma nova visão para sustentabilidade de negócios através de segurança gerenciável

Desenvolvida para:

- **Permitir inovação através de infraestruturas, sistemas e plataformas seguras**
- **Reduzir o número e complexidade dos controles de segurança necessários**
- **Reduzir gastos redundantes em segurança**
- **Melhorar a agilidade e disponibildade operacional**
- **Explorar nosso expertise para unificar o gerenciamento**
- **Entregar visibilidade, controle e automação**



Soluções de Segurança IBM ISS entrega as soluções de negócios que você precisa em tempos de incertidão

Reduzindo custo e complexidade sem comprometer a segurança

1. ***Reduza os cursos de implementar as mais modernas tecnologias e processos de segurança***
2. *Combata, monitore e gerencie as mais recentes ameaças online e vulnerabilidades*
3. *Identifique e combata os riscos de estar em descumprimento de normativas*
4. ***Reduza o custo ao limitar o acesso interno a informação e a perda de dados sensíveis***
5. *Redução de custos de **identity and access management***
6. *Combata riscos associados a **application-level vulnerabilities***

Como a IBM faz frente aos desafios de Segurança

- Processo inovador que protege clientes "Ahead of the Threat"
- Proteção preventiva = Menor custo operacional
- Enterprise Security Platform = Menor custo operacional e liberdade de escolha
- Altamente escalável e poderosa capacidade de adaptação para enfrentar as atuais e futuras ameaças digitais = Permite que o cliente ganhe/retome controle sobre seus negócios e processos
- IBM ISS Enterprise Security Platform = a mais avançada, integrada e completa solução de segurança multi-camadas

IBM Internet Security Systems X-Force® Research Team

Pesquisa → Tecnologia → Soluções

- Original Vulnerability Research
- Public Vulnerability Analysis
- Malware Analysis
- Threat Landscape Forecasting
- Protection Technology Research

X-Force Protection Engines

- Extensions to existing engines
- New protection engine creation

X-Force XPU's

- Security Content Update Development
- Security Content Update QA

X-Force Intelligence

- X-Force Database
- Feed Monitoring and Collection
- Intelligence Sharing

The X-Force team delivers reduced operational complexity –
helping to build integrated technologies that feature "baked-in" simplification

SiteProtector

Unified Enterprise Security Console for all products

Enterprise Protection Products

proventia™ Vulnerability Assessment

Enterprise Scanner

Helps to ensure the availability of your revenue producing services and protects your corporate data by identifying where risk exists, prioritizing and assigning protection activities, and then reporting on results

proventia™ Network Protection

Proventia Mx
Proventia Gx

High performance network security with real-time attack, malicious code and hybrid threat blocking. Allows secure open transactions in a SOA environment which is an effective way to preserve network availability, reduce the burden on your IT resources and prevent security breaches.

proventia™ Server Protection

Proventia Server
RealSecure Server Sensor

Data Security -- Provides historical data that enables companies to find the origin of a change, breach or string of behavior
Insider Threats -- Tracks the who, what, when, where of user/administrator behavior
Compliance -- Provides the reporting necessary to prove the security of sensitive information

Data Security Services

FIDELIS SECURITY SYSTEMS

Fidelis XPS

Data Leakage – A Holistic approach to ensure that data does not find it's way outside of controlled environments… Accidently, or Intentionally.

IBM Proventia® SiteProtector™ System

Redução de custos e complexidade no gerenciamento de segurança na corporação

- Plataforma de gerenciamento escalável, de gerenciamento centralizado
  - Redução de tempos e custos associados ao gerenciamento de segurança
  - Relatórios
  - Redução de riscos graças à visibilidade e capacidade de prevenção

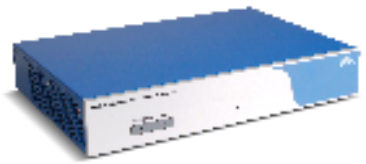
- **Extensão nas capacidades de “monitoração baixo demanda”**

INTERNET|SECURITY|SYSTEMS®

proventia® network

Enterprise Scanner

Proventia ES1500 Vulnerability Management (VM) Appliance

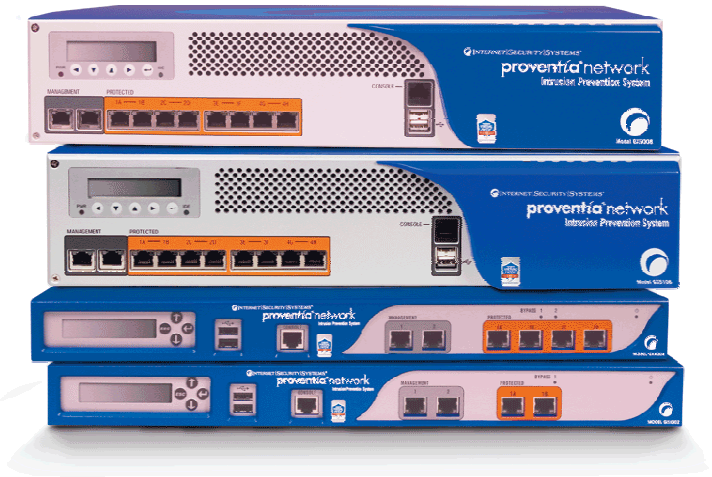


Proventia ES750 Vulnerability Management (VM) Appliance

Enterprise Scanner, é parte do sistema de gerenciamento de vulnerabilidades da Internet Security Systems, que garante a disponibilidade dos serviços e protege seus dados identificando a existência de riscos, priorizando e definindo Atividades de proteção e relatórios.

Proventia® Network IPS
Bloqueio de Ataques

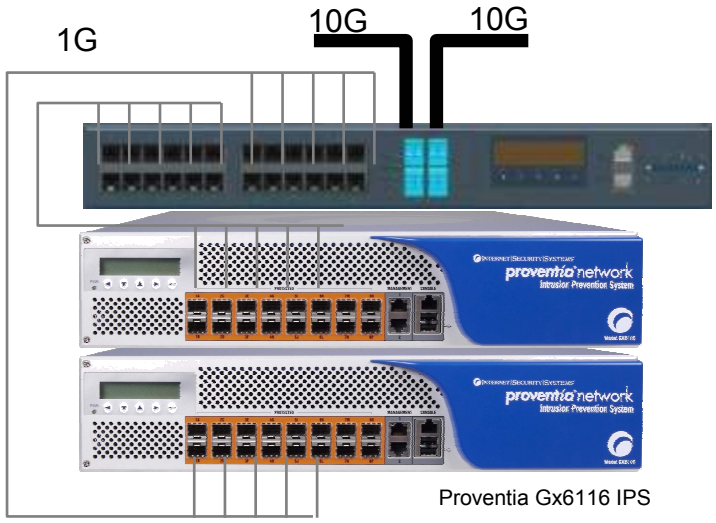
- O que faz?
  - Proativamente bloqueia ataques e tráfego malicioso deixando tráfego ligítimo passar intacto.
- Como isto ajuda?
  - Proteção máxima para a rede
  - Recupera banda
  - Evita perdas e danos
- Por que IBM…
  - Somos o único fabricante a receber “perfect scores” constantes em eficiência de proteção



Proventia Network Security Controller

- Permite conectividade 10Gb para appliances da série Gx5000 e Gx6000
- Permite expansão de performance
- Bypass Unit Integrado
- Melhor escalabilidade
- Valoriza Investimentos Passados

IBM Proventia® Network Security Controller



Proventia Gx6116 IPS

- **10 Gig Interface**
- **Integrated bypass**

IBM Internet Security Systems

Reduzindo custo e complexidade sem comprometer a segurança

- **Proventia G - VIPS (Virtual IPS) Appliance *FUTURO***
  - Permite que clientes acelerem o processo de migração a ambientes do tipo virtual datacenter ao tratar diligentemente sobre segurança e compliance
  - IPS baseado em Software sobre VMware permite flexibilidade na implementação
  - Permite que usuários implementem seus próprios appliances economizando dinheiro
  - Permite o compartilhamento de hardwares (ex. Ips + fw)
  - Caminho de migração ideal para quem tem Proventia A ou real secure
  - Gerenciamento centralizado via SiteProtector

Virtual Security Appliances

VIPS

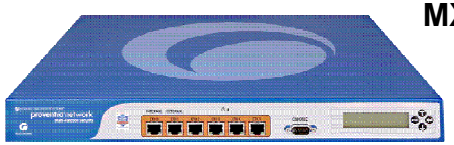
- **Virtual Network Protection**
- **Redução do CapEx**
- **Green data center**

Proventia® Network MX
Multi-Funcional

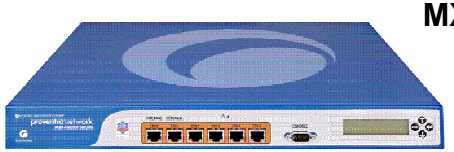
- O que faz?
  - Proativamente bloqueia múltiplos tipos de ataques e deixa o tráfego legítimo passar.
- Como funciona?
  - Usa as melhores tecnologias da indústria
  - IPS, AV, AS, WF, FW & VPN
- Como isto ajuda?
  - Recupera banda
  - Evita ataques, virus, spyware e spam
- Por que IBM…
  - Reconhecido pioneiro e líder no mercado ISA.

MX0804

MX1004

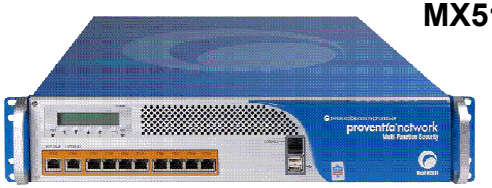


MX3006



MX4006

MX5008



MX5110

IBM ESC Endpoint Protection

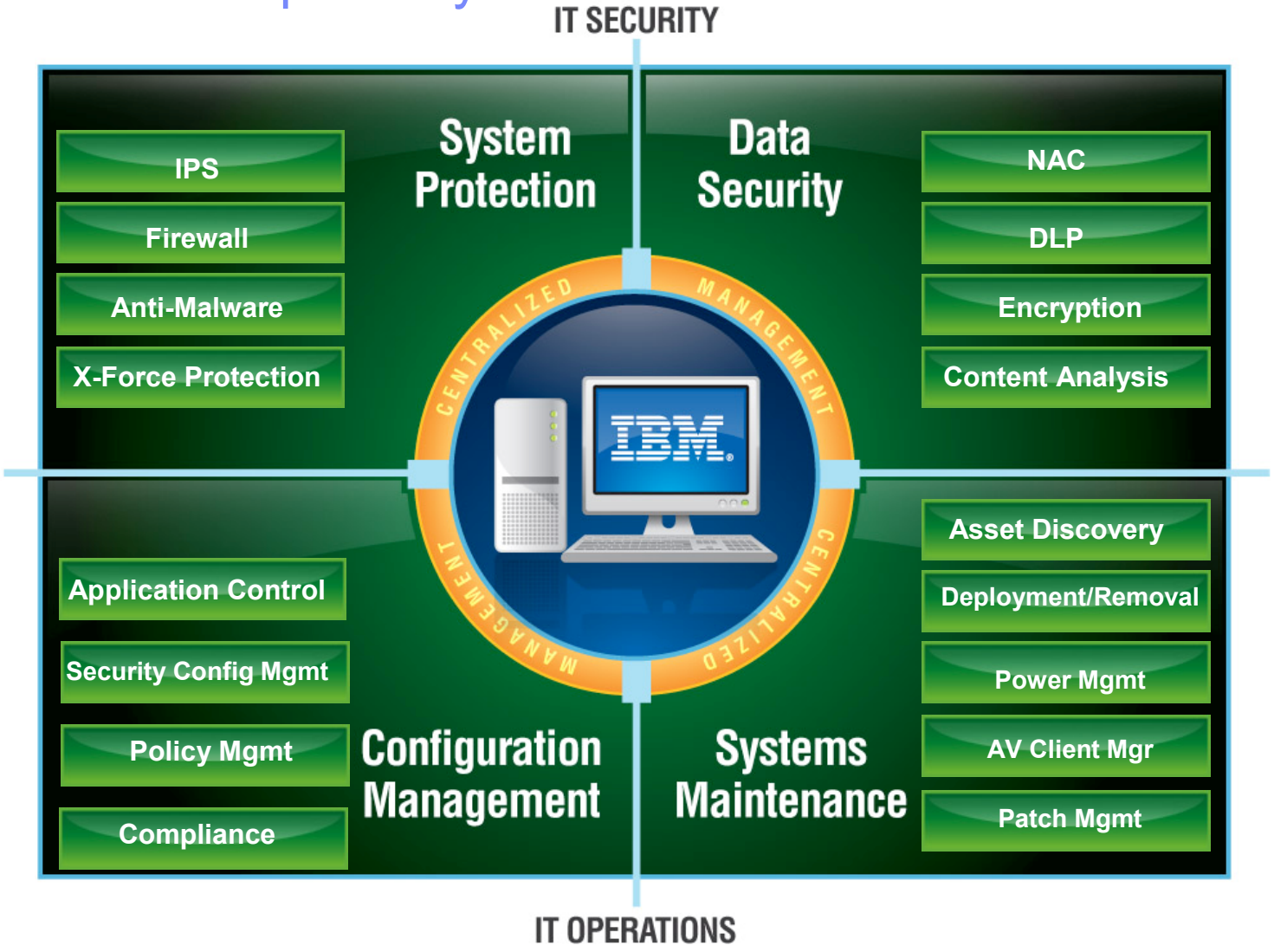
Endpoint Protection

O que é o IBM ESC Endpoint Protection?

- **Cobertura completa para proteção de estações de trabalho**
- **Estrutura simplificada, tudo sob uma console de gerenciamento unificada.**

Desafios Comuns	IBM Endpoint Protection – Valor
1. **Falta de uma estrutura de gerenciamento única para produtos de segurança para estações de trabalho** 2. **Brechas na cobertura permitem oportunidades de exploração** 3. **Ambientes corporativos altamente distribuídos** 4. **Custos de propriedade e suporte demasiado altos** 5. **Múltiplos agentes que consomem grandes quantidades de recursos computacionais**	1. **Cobertura padronizada e completa para a estação de trabalho e notebooks, dentro e fora da rede** 2. **TCO menor que o de soluções pontuais** 3. **Elimina brechas de cobertura associadas com soluções anti-Malware** 4. **Reduções significativas em tempo de remediação e carga de trabalho na equipe.**

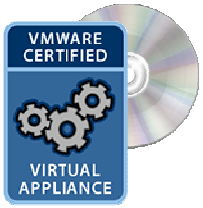
Solução IBM Endpoint System Protection



Proventia Network Mail Security System

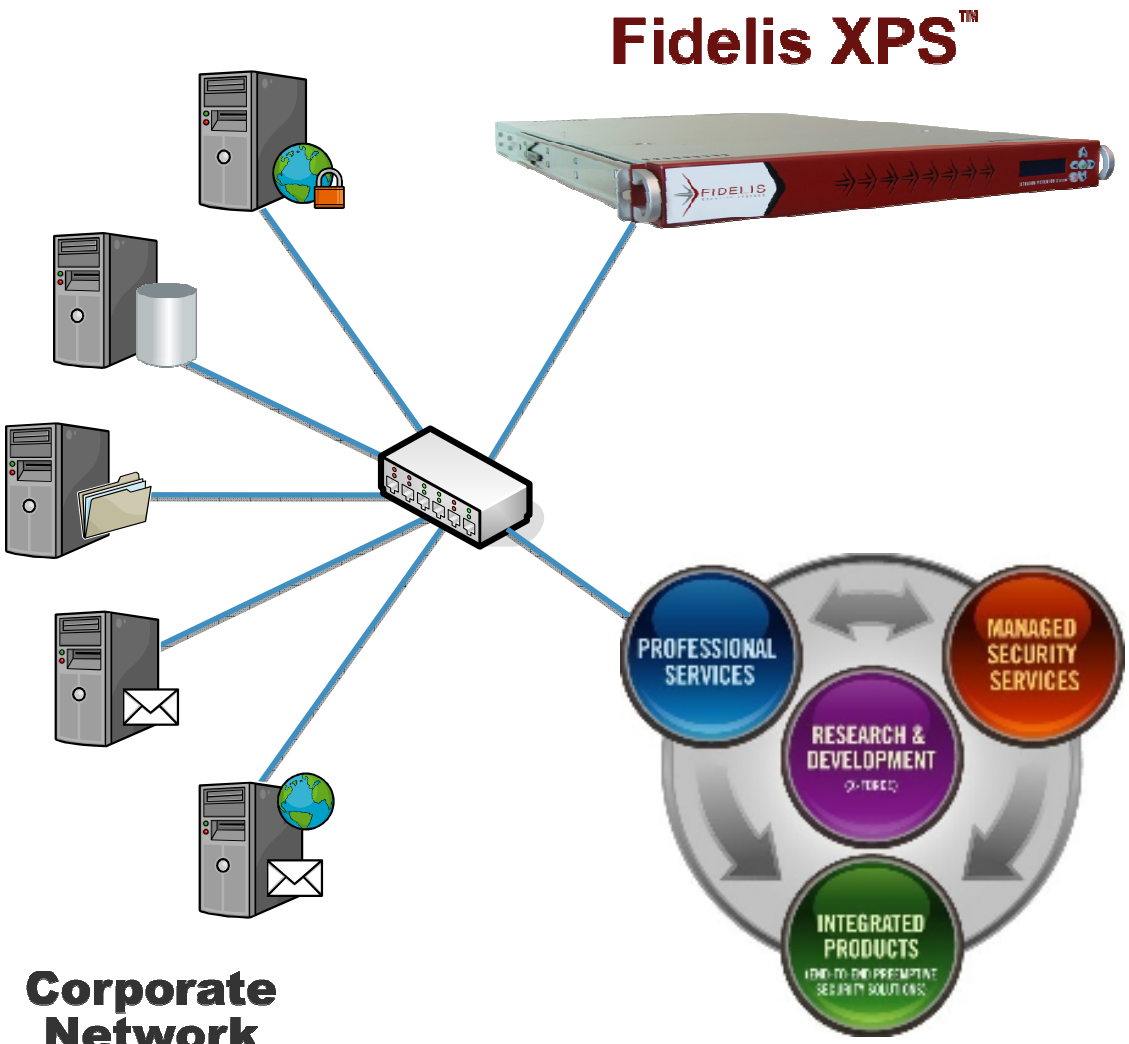
- O que faz?
  - Proativamente bloqueia ataques contra a infraestrutura de email corporativo
  - Controle contra SPAM
- Como funciona?
  - Tecnologias VPS e IPS analisam e protegem contra ataques em tempo real
  - IBM ISS Filter Database
- Como isto ajuda?
  - Infra corporativa e usuários são totalmente protegidos
  - Aumenta produtividade
  - Protege contra conteúdo malicioso, phishing, malwares, spywares
- Por que IBM?
  - Tecnologia líder mundial em proteção proativa IPS e VPS
  - Proventia Filter Database é a maior base do mercado 60+ milhões de registros (Web pages e spam signatures)

Proventia Network Mail Security System MS3004N



Proventia Network Mail Security System Virtual Appliance – MS1002-VM

Fidelis – IBM Partnership



FIDELIS SECURITY SYSTEMS

- Next-generation Network Data Loss Prevention
- Prevenção para todas as portas, todos os protocolos
- Gigabit performance
- Advanced content profiling

IBM

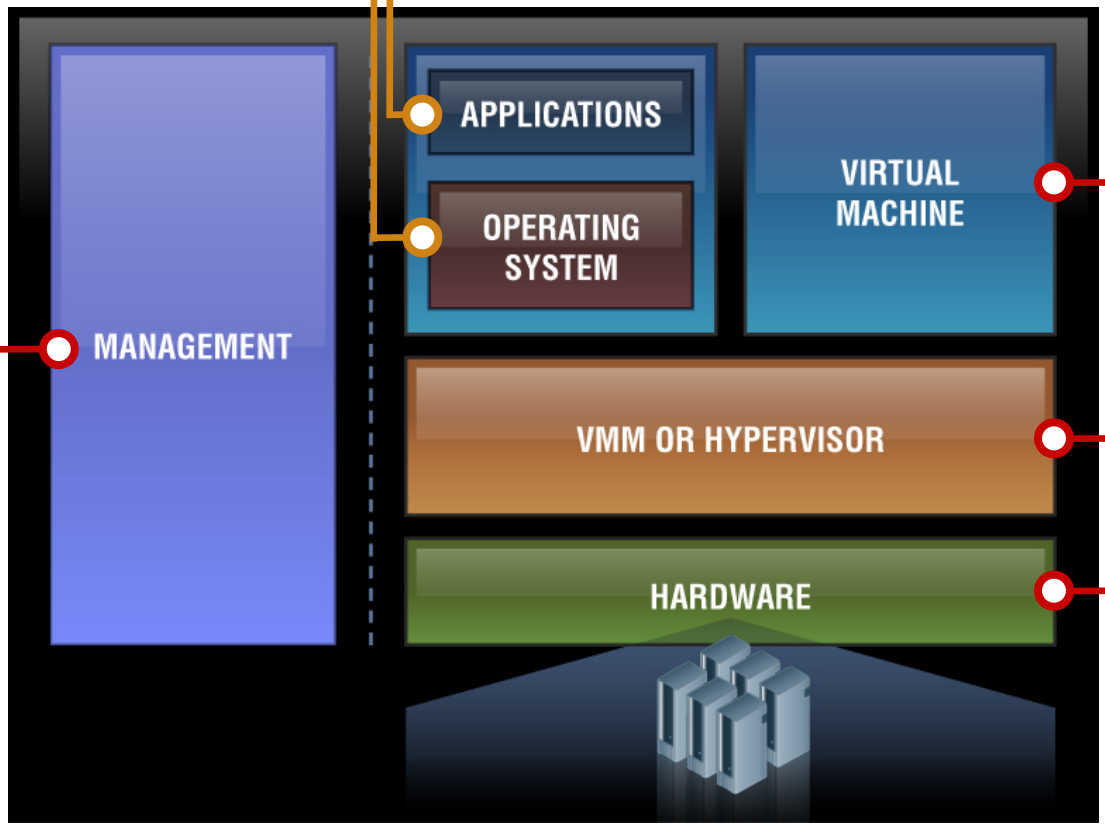
- Expertise em Segurança Comprovado
- Soluções Completas
- Suporte Global

Proteção de Dados Sensíveis com IBM ISS

Gerencie os riscos associados a Virtualização e economize!

- **Ameaças tradicionais**
- **Novas ameaças para ambientes VM's**

Ameaças tradicionais podem atacar VM's da mesma maneira que sistemas tradicionais



Vulnerabilidades de Gerenciamento

Guarda segura de VMs e dados de gerenciamento

Necessita de novas capacidades

Expansão virtual

Dynamic relocation

Roubo de VM's

Compartilhamento de recursos

Ponto único de falha

Stealth rootkits no hardware

Virtual NICs & Virtual Hardware são alvos

MAIS COMPONENTES = MAIS EXPOSIÇÃO

Server Protection

Proteção multi-camadas para servidores

IBM Proventia Server (Linux e Windows)

IBM RealSecure Server Sensor (AIX, Solaris, HP-UX e Windows)

Unificando Segurança e compliance

- Multi-layer Protection ***(backed by X-Force)***
  - Tecnologias de proteção preventiva - inclui: firewall, intrusion prevention/detection, buffer overflow protection, application black/white listing, e SSL inspection
- Policy Compliance / Integridade de Sistema
  - Tecnologias Compliance: file integrity monitoring (FIM), OS auditing, registry integrity monitoring, third party log monitoring

Professional Services

- **Assessment Services**
  - **Application Security Assessment**
  - **Information Security Assessment**
  - **Penetration Testing**
  - **PCI Assessment (US and International)**
  - **SCADA Assessment**
  - Policy and ISO 17799 Gap Analysis

- **Design Services**
  - Implementation Planning
  - Network Security Architecture Design
  - Policy Design and Development
  - QuickStart Programs for Regulatory Compliance
  - Standards and Procedures Development

- **Deployment Services**
  - Migration Services

- **Manage & Support Services**
  - **Emergency Response Services**
  - **Subscription**
  - **On Demand**
  - Staff Augmentation and Support

Managed Services da IBM ISS

Gama de Serviços

Managed Security Services

Benefícios

- Proteção dos recursos de TI, reputação da empresa, continuidade do negócio, monitoração 24x7
- Redução de custos internos de até 55%
- Alinhamento com normativas internas e externas
- Maximiza investimentos de segurança atuais
- Libera recursos
- Reafirma a clientes, parceiros e acionistas que os dados críticos da empresa estão sendo resguardados e gerenciados por equipes competentes
- Redução de complexidade

Gama de Serviços

Enablement Services

Benefícios

- Visão e controle centralizado
- Relatórios e métricas a qualquer momento
- Automação e análise avançada
- Archiving ilimitado
- Acesso controlado ao portal
- Integrado com dados de inteligência Xforce

Reduzindo o custo total de propriedade e a complexidade. Ao mesmo tempo melhorando a produtividade e otimizando a infraestrutura

- **Open vendor architecture**
- **Consolidated security views**
  - Managed Security Services
  - Security Enablement Services
- **Powerful query & reporting options**
- **Automated event/ log analyses**

- **Unlimited event/ log archive**
- **Granular permissions system**
- **Guaranteed availability**
- **Integrated trouble ticketing & workflow**
- **Integrated IBM Internet Security Systems X-Force® intelligence**

Virtual-SOC Portal

Por que Serviços Gerenciados da IBM?

RESEARCH

- **Pesquisa Xforce**
- **Expertise**
- **Knowledge base**
  - 4B Eventos/dia
  - 2,500+ clientes
  - milhares de dispositivos

INNOVATION

- **Tecnologia Preventiva**
- **Adaptabilidade e Inteligência**
  - Evolving threat
  - Dynamic
- **Escalabilidade**
- **Plataforma Integrada**

INTEGRATION

- **Automação**
- **Segurança acima de tudo**
- **Automated Policy Management**
- **Workflow**
- **Lifecycle Management**
- **Escolha = controle**

VALUE

- **Alinhamento e compliance**
- **Eficiência tecnológica**
- **Proatividade!!!**
- **SLA's**
- **Redução de custo e complexidade**

IBM ISS cria verdadeiro valor – entregando um TCO menor

IBM Security: Sum is Greater Than its Parts

Forrester	 Wave: ISS Managed Security Services	Leader
Forrester	 Wave: User Account Provisioning and Enterprise Security Information Management	Leader
Gartner	 MQ: ISS Network Security, Firewalls and Managed Services	Leader
Gartner	 MQ: Web Access Management	Leader
Gartner	 MQ: Security Information & Event Management	Challenger
Gartner	 MQ: User Provisioning (TIM)	Leader
Gartner	#1 Marketshare: Web Access Management, Worldwide, (FIM, TAM)	Ranked #1
Gartner	#1 Marketshare : Application Security Vulnerability Scanning, (Rational AppScan)	Ranked #1
Frost & Sullivan	#1 ISS Managed Security Services and Vulnerability Assessment	Ranked #1
Frost & Sullivan	#1 Identity Management (TIM , TAM, FIM, TDI, TDS)	Ranked #1
IDC Analyze the Future	#1 Marketshare: Identity and Access Management	Ranked #1
IDC Analyze the Future	#1 Marketshare: Application Vulnerability Assessment (Rational AppScan)	Ranked #1

OBRIGADO!

Perguntas?

Ricardo Marques
Senior Security Engineer
marquesr@br.ibm.com