



# Serviços Gerenciados e Profissionais da IBM para Segurança de TI

**Marco Antonio Almeida**

Security Services Manager - IBM Latin America

# Agenda

- Aspectos e Riscos que impactam a Segurança de TI
- Framework e Visão IBM
- Serviços de Segurança IBM e Symantec
- “New” – Mobile Security Services
- IBM HA/DR, Virtualization and Storage Management Services
- Por que a IBM ?

O conceito de Smarter Planet cria novas oportunidades mas também novos riscos

**O planeta está ficando mais equipado, interconectado e inteligente.**

**Novas possibilidades**  
**Novas complexidades**  
**NOVOS riscos...**



**“We have seen more change in the last 10 years than in the previous 90.”**

*Ad J. Scheepbouwer,  
CEO, KPN Telecom*

Proteção a  
infraestrutura de I/T



Proteção a Privacidade  
e Identidade



Novas Ameaças



Cloud  
Security



# Uma série de aspectos impactam os Riscos e Gerenciamento de Segurança

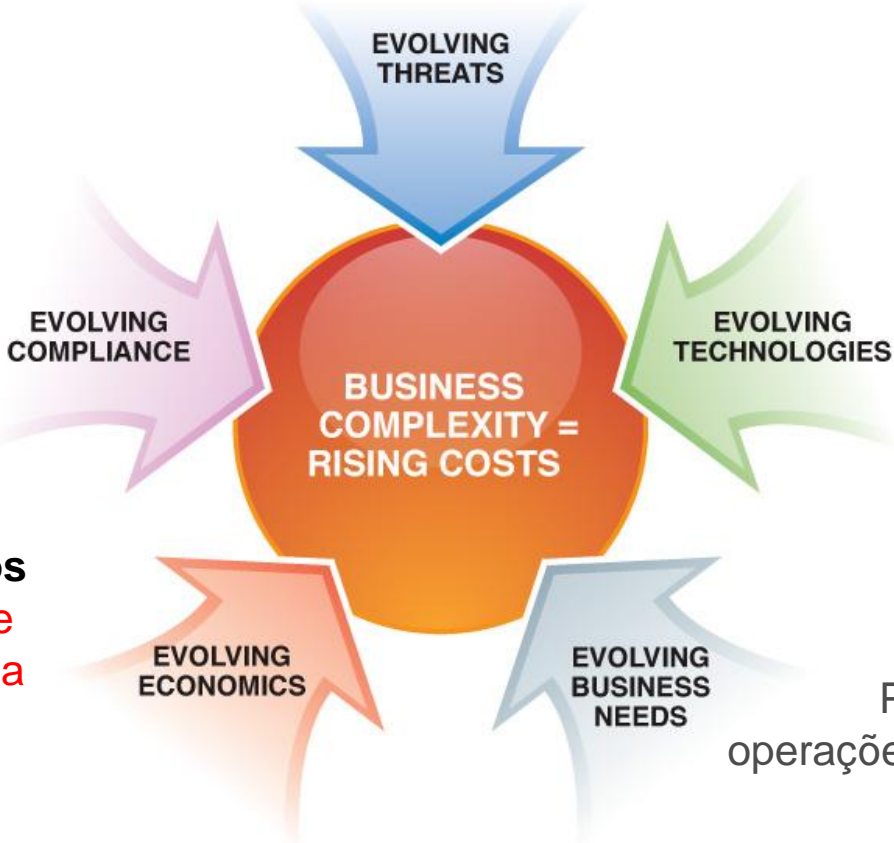
## Novos Ataques e Motivações:

Adicionando novos riscos e complexidade

### Necessidade de Compliance:

Diferentes Industrias possuem diferentes regulamentações e leis que devem ser cumpridas

**Aumento de Dados / informações:** que acaba provocando a necessidade crescente de proteção



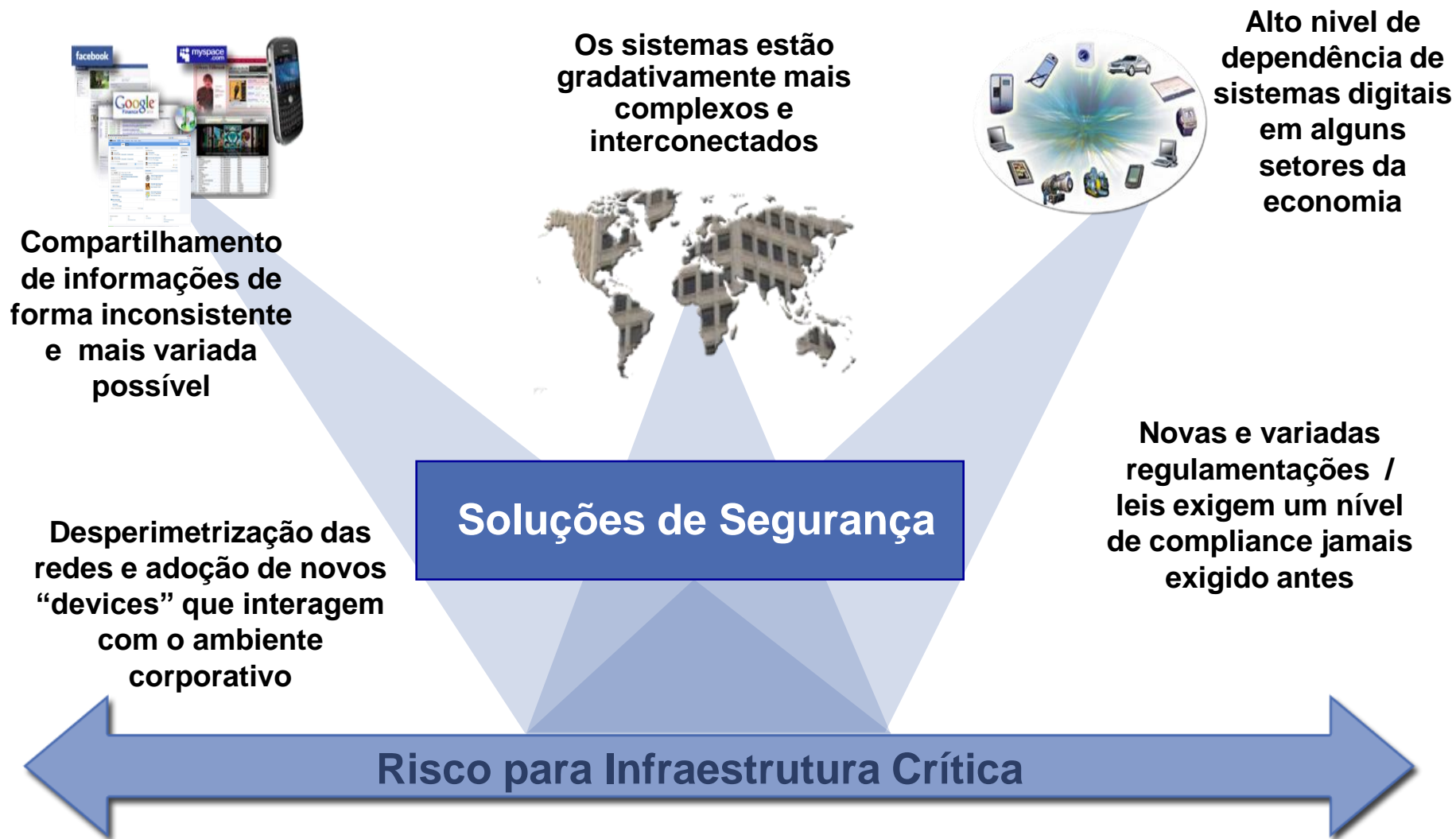
**Inovação em IT:**  
Os sistemas estão cada vez mais integrados e cada vez mais novos "aparelhos" se conectam as redes

**Flexibilidade nos Modelos de Negócio:**  
Para melhorarr as operações e melhor servir os Clientes

**Complexidade continua a ser o maior desafio !**

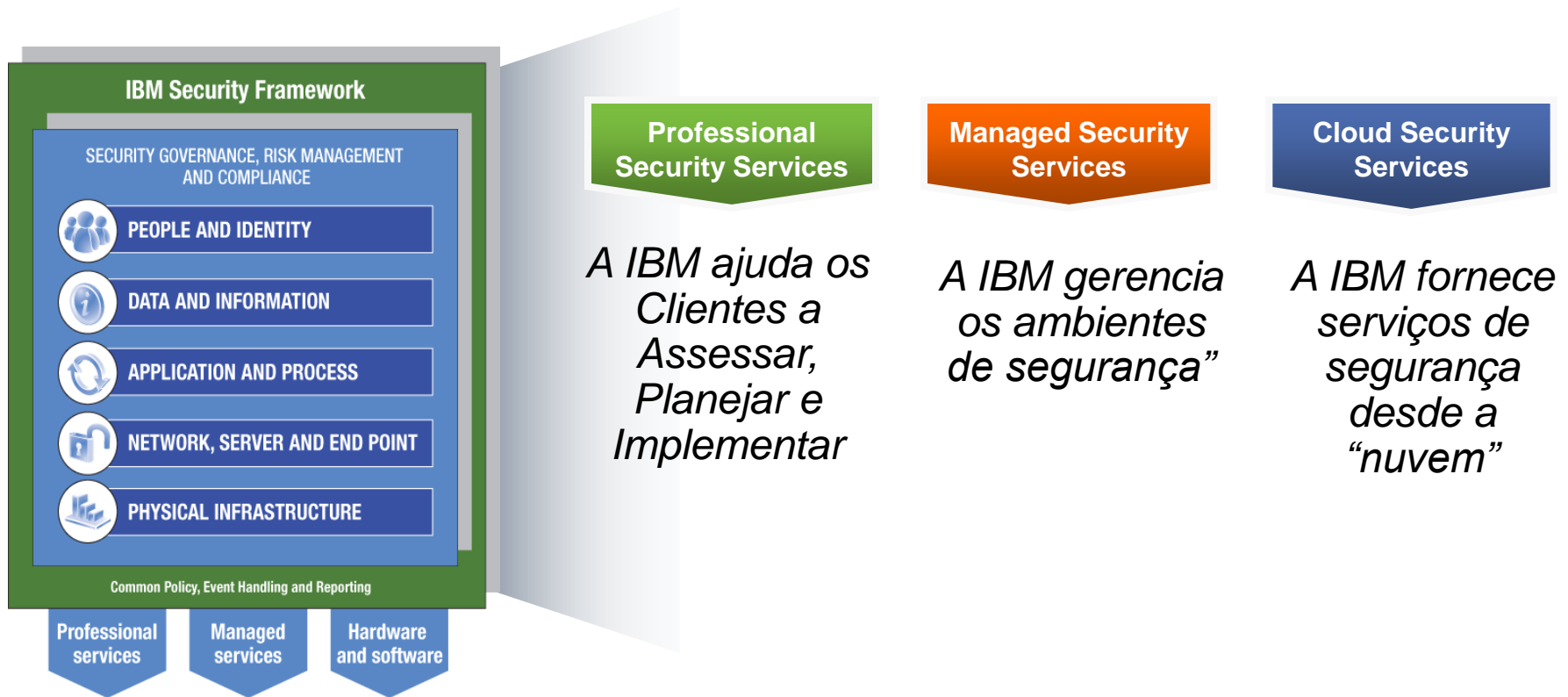
**Integração é chave no gerenciamento do custo e complexidade dos ambientes de T/I**

# Muitos fatores definem o nível e a natureza do risco



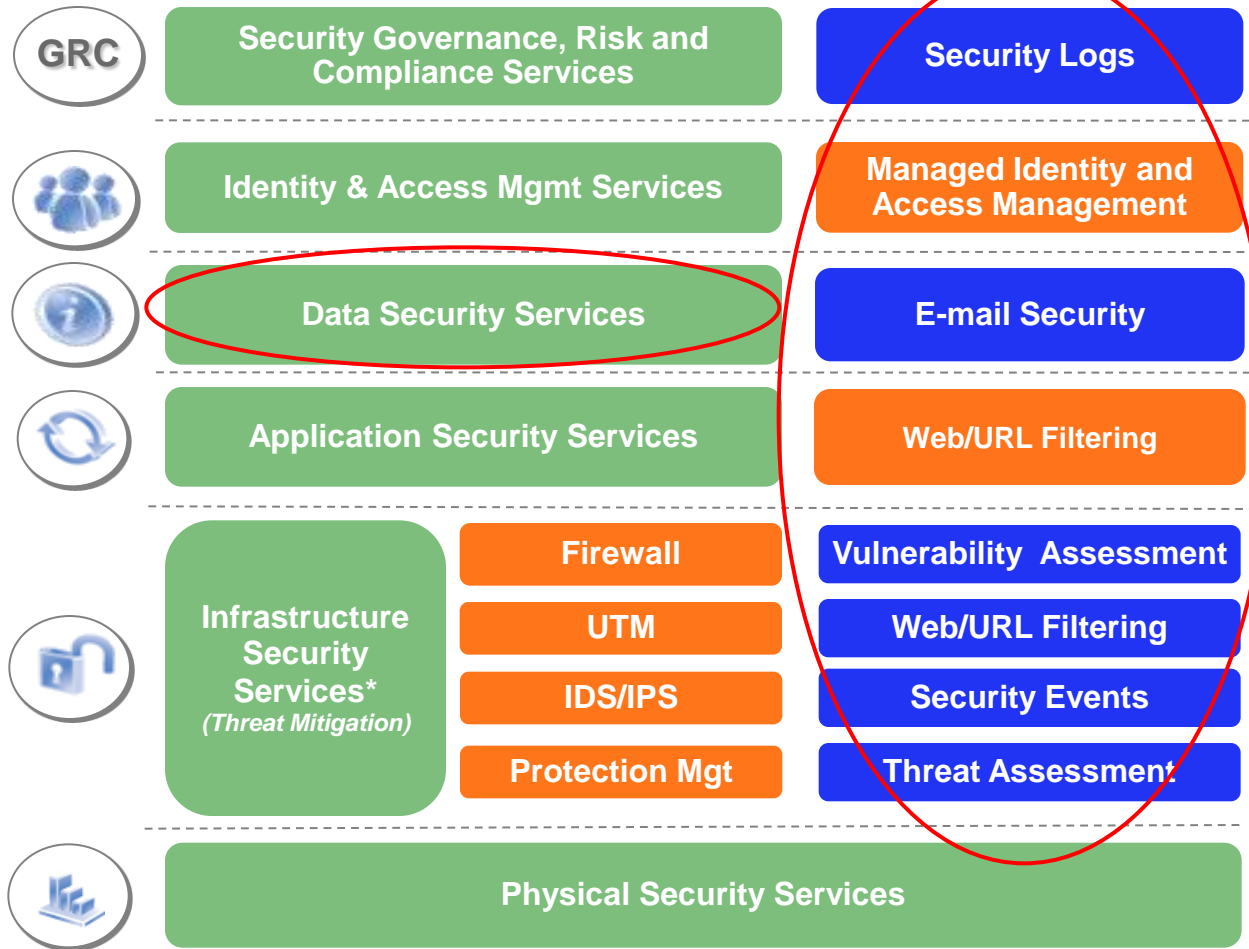
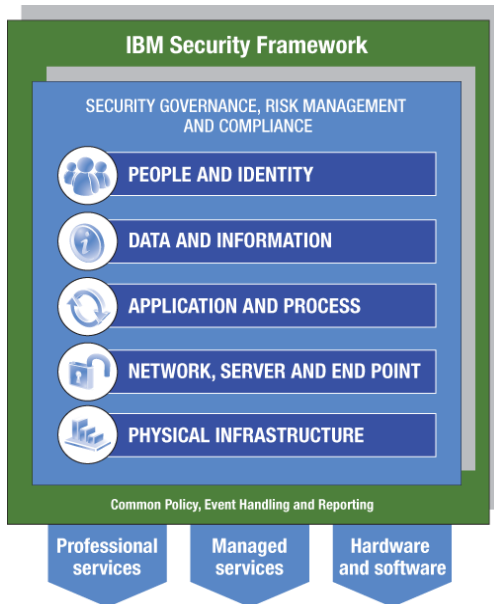
# Um Único Modelo não se aplica a todas as Empresas:

## Serviços de Segurança da IBM – Framework e Visão



# Security Services portfolio – Visão detalhada

- = Professional services
- = Managed services
- = Cloud services



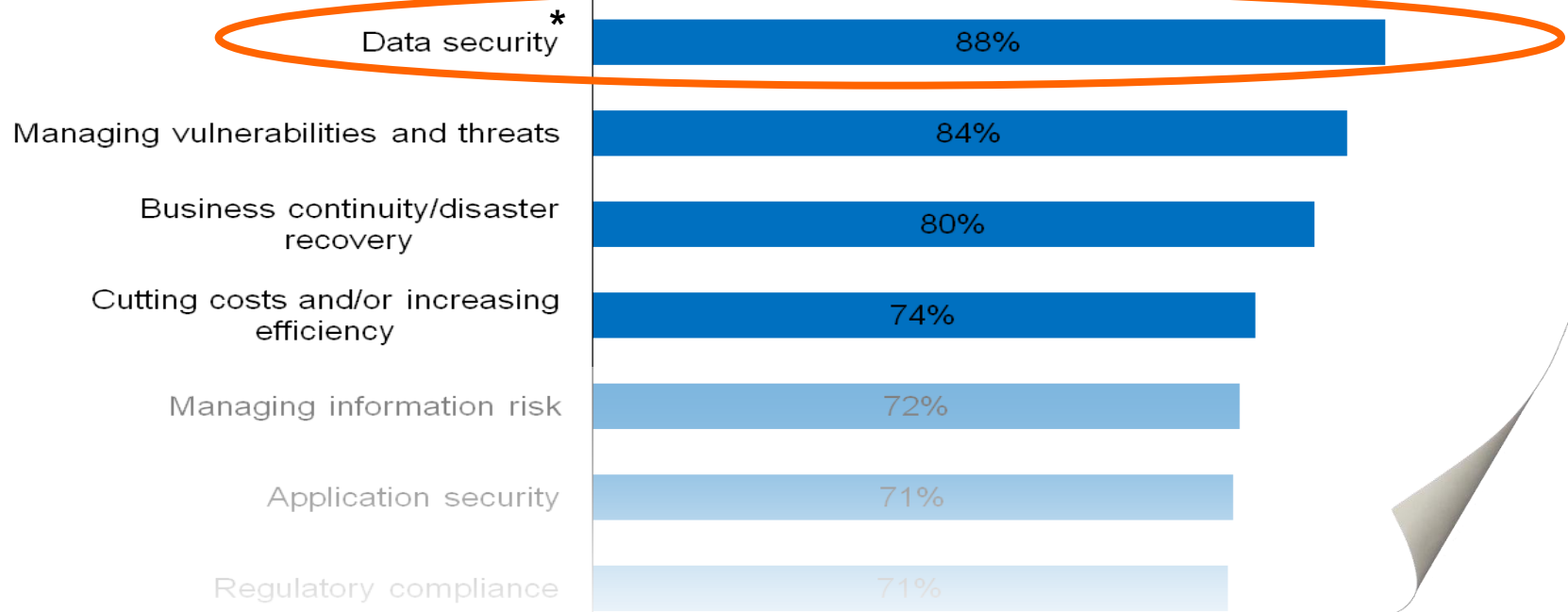
# IBM Data Security Services



# Segurança de Dados é “top priority” em novos projetos de TI hoje

## Data security and vulnerability and threat management are top priorities

Which of the following initiatives are likely to be your firm's/organization's top IT security priorities over the next 12 months?



Base: 2,058 North American and European Security decision-makers

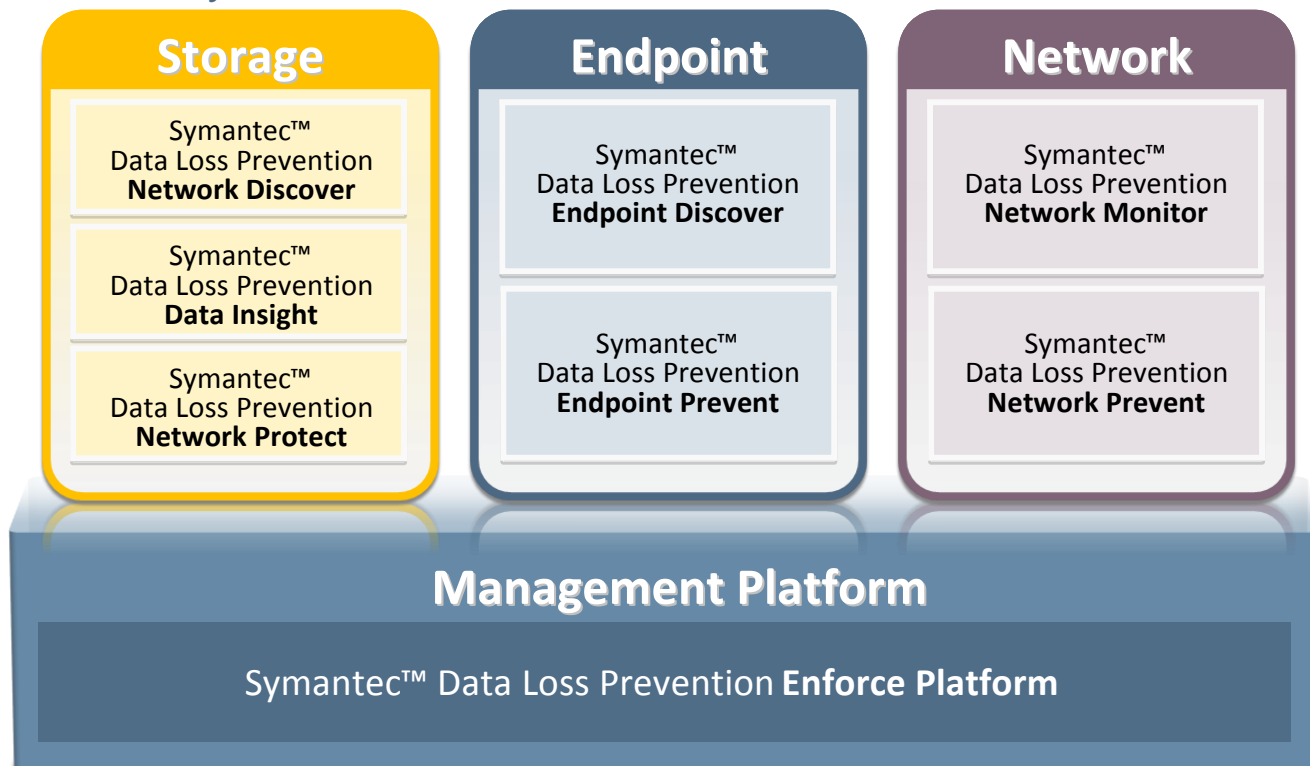
Source: Forrsights Security Survey, Q3 2010

\* ***“Data leak prevention (DLP) and full disk encryption are the two technologies expected to grow adoption the fastest relative to their existing market penetration.”***

“The State of Enterprise IT Security and Emerging Trends: 2009 to 2010,” Forrester Research Inc. – Jan. 25, 2010

# IBM Data Security Services – usando a solução da Symantec para “data loss prevention”

## Symantec Data Loss Prevention – Products



**Através de uma Aliança Mundial, a IBM vende e implementa as Soluções Symantec para DLP**

# Implementando a solução Symantec DLP com a IBM

O IBM “Data Security Assessment” inclui uma metodologia que endereça os pontos principais na questão de proteção de dados, através da coleta de informações e entrevistas que auxiliam na “descoberta” dos dados e a melhor forma de protegê-los



- Definir / levantar os requerimentos do negócio, de IT e de compliance
- Desenvolver um approach high-level para implementar a solução de data loss prevention

- Identificar os dados críticos e sensíveis nos servidores e workstations
- Avaliar o uso atual dos dados nos endpoints
- Prover recomendações de solução e eventualmente de processos

- Desenhar a arquitetura da solução ;
- Planejar a implementação ;
- Configurar um piloto ;
- Definir políticas e regras de proteção ;
- Implementar o piloto e testá-lo ;
- Realizar o roll-out do projeto ;
- Realzar o treinamento técnico e “transfer skills” para equipe de gerenciamento ;

# Os Serviços IBM contemplam uma efetiva estratégia que engloba as múltiplas dimensões na proteção de dados

## Criação de uma Estratégia para Proteção de Dados

### Corporate Imperatives

- Compliance com as regulamentações de mercado
- Aderência aos processos e regras de negócio da empresa

### Marketplace Developments

- Proteção a marca e confiabilidade da empresa
- Tecnologias diferentes fazendo “Overlapping”

### Management Challenges

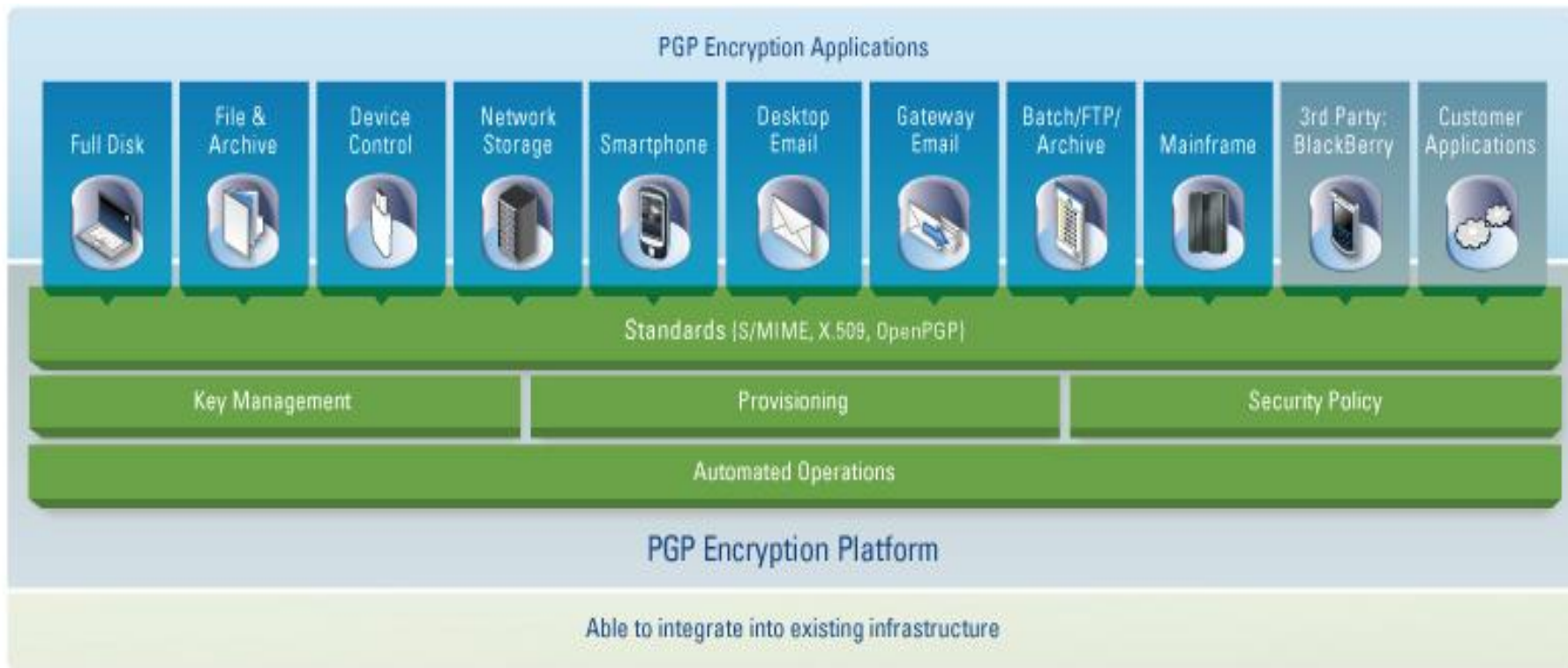
- Roubo de dados intencional
- Perda de dados acidental
- Balanceamento entre o controle de proteção de dados e produtividade

### Technology Issues

- Múltiplas soluções existentes e diferentes para DLP
- Implementações Complexas
- Novas ameaças
- Prioridades em TI

# IBM Data Security Services – Solução de Encriptação PGP

Proteção através de encriptação com o **PGP Encryption** da  Symantec.



**Através de uma Aliança Mundial, a IBM vende e implementa as Soluções Symantec PGP**

# O que a solução de Encriptação IBM e Symantec pode fazer pelos Clientes

## Com o PGP software, voce pode ...

**Melhorar a proteção de dados** armazenados em endpoint's **mesmo quando o device foi perdido ou roubado**

**Proteção de dados** mais efetiva **enquanto os mesmos estão em uso** no endpoint device

**Monitorar e controlar o uso de devices de storage externos** para armazenamento e transporte de dados

**Melhorar a segurança do trafego** “inbound” e “outbound” **de e-mail**

## Usando

Whole disk encryption

Encriptação de arquivos, folders, discos virtuais (VDisks) e shared media

Removable media encryption

Encriptação e “digital signing” dos e-mail's



# IBM Managed Security Services

# O que são os Serviços Gerenciados de Segurança ?



**Reduce  
Costs**



**Manage  
Risk**



**Improve  
Service**

Os **IBM Managed Security Services (MSS)** são desenhados para :

- Oferecer Serviços em **Cloud Computing** ;
- **Reduzir custos** operacionais e de pessoal ;
- **Melhorar a postura** e **cobertura em Segurança**;
- Auxiliar no gerenciamento de segurança / compliance através do **“outsourcing” de alguns aspectos chave** neste contexto;
- Contar com **Skill e profissionais experts 24x7** no tema de Segurança.





# Serviços Gerenciados IBM - Overview



Suporte a Múltiplos Tipos Device/Vendors



# Portal do IBM MSS

Gerenciamento Integrado dos serviços, reduzindo a Complexidade, aumentando a produtividade e otimizando a Infraestrutura

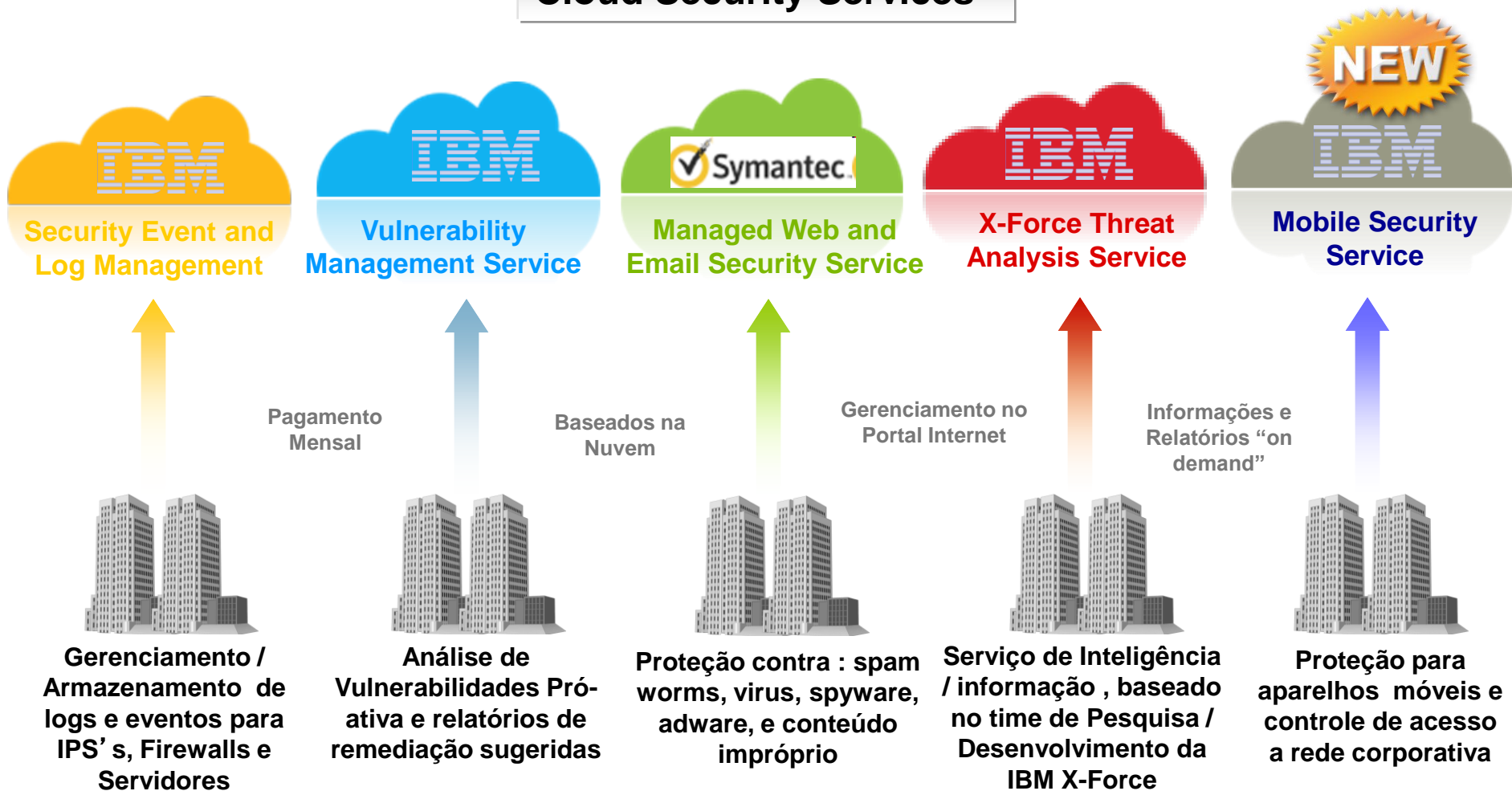
- Open vendor architecture
- Consolidated security views
  - Managed Security Services
  - Security Enablement Services
- Powerful query & reporting options
- Automated event/log analyses



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

# Serviços Gerenciados de Segurança entregues desde a 'nuvem'

## Cloud Security Services



# Hosted Mail and Web Security

MessageLabs

SYMANTEC HOSTED SERVICES™

## Overview da Solução

O “Hosted Mail and Web security services” permite o combate a ameaças (como virus, spam e spyware) aos serviços de email e roubo de dados, através de uma tecnologia de verificação / filtragem - sem a necessidade de investimento do Cliente na compra de tecnologia para este fim.



## Benefícios

- **Implementação rápida** baseada na nuvem, acelera o retorno do investimento e reduz o consumo de banda de rede do Cliente.
- **É fácil de usar** não necessitando de compra de HW ou SW a ser instalado no ambiente do Cliente.
- Melhora a produtividade dos usuários de email pois evita mensagens indesejáveis ou conteúdo impróprio.

## Características Principais :

- Aliança IBM e Symantec para delivery do Serviço
- Filtro de Spam
- Proteção contra Virus
- Proteção contra Spyware
- Detecção de links maliciosos
- Bloqueio de acesso a sites indesejados

# A IBM tem experiência local e global na entrega de serviços de segurança ao redor do Mundo

9 Security Operations Centers

9 Security Research Centers

11 Security Solution Development Centers

133 Monitored Countries

900+ Professional Services Security Consultants

600+ field security specialists

4,500 Security Delivery Experts

400+ security operations analysts



- 3,700+ Clientes em MSS no Mundo
- Mais de 13 Bilhões de Eventos gerenciados por dia
- Centros de Pesquisa e Desenvolvimento espalhados globalmente

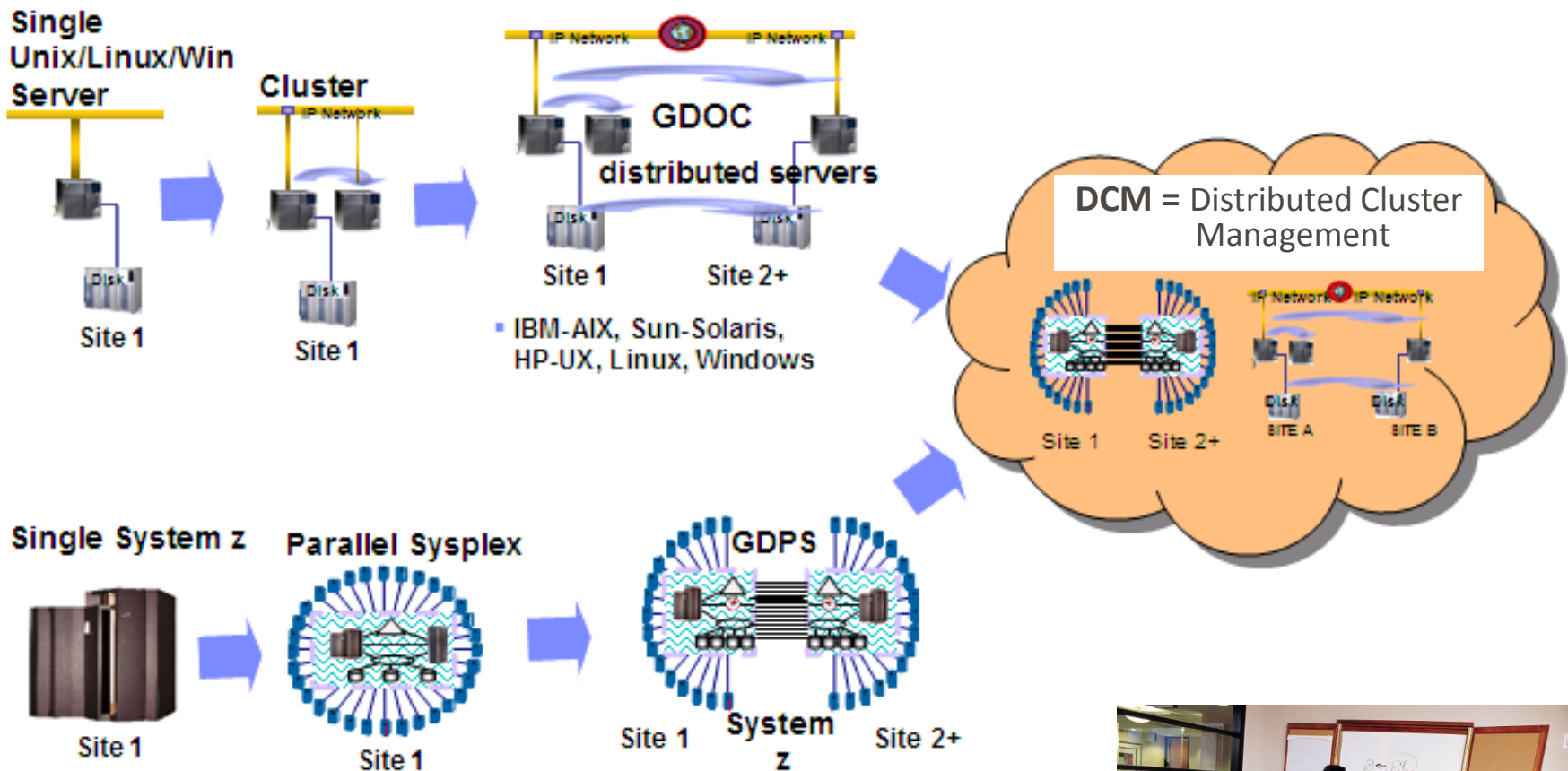


# IBM HA/DR, Virtualization and Storage Management Services

**Adriano Barreto**

Solution Sales Manager

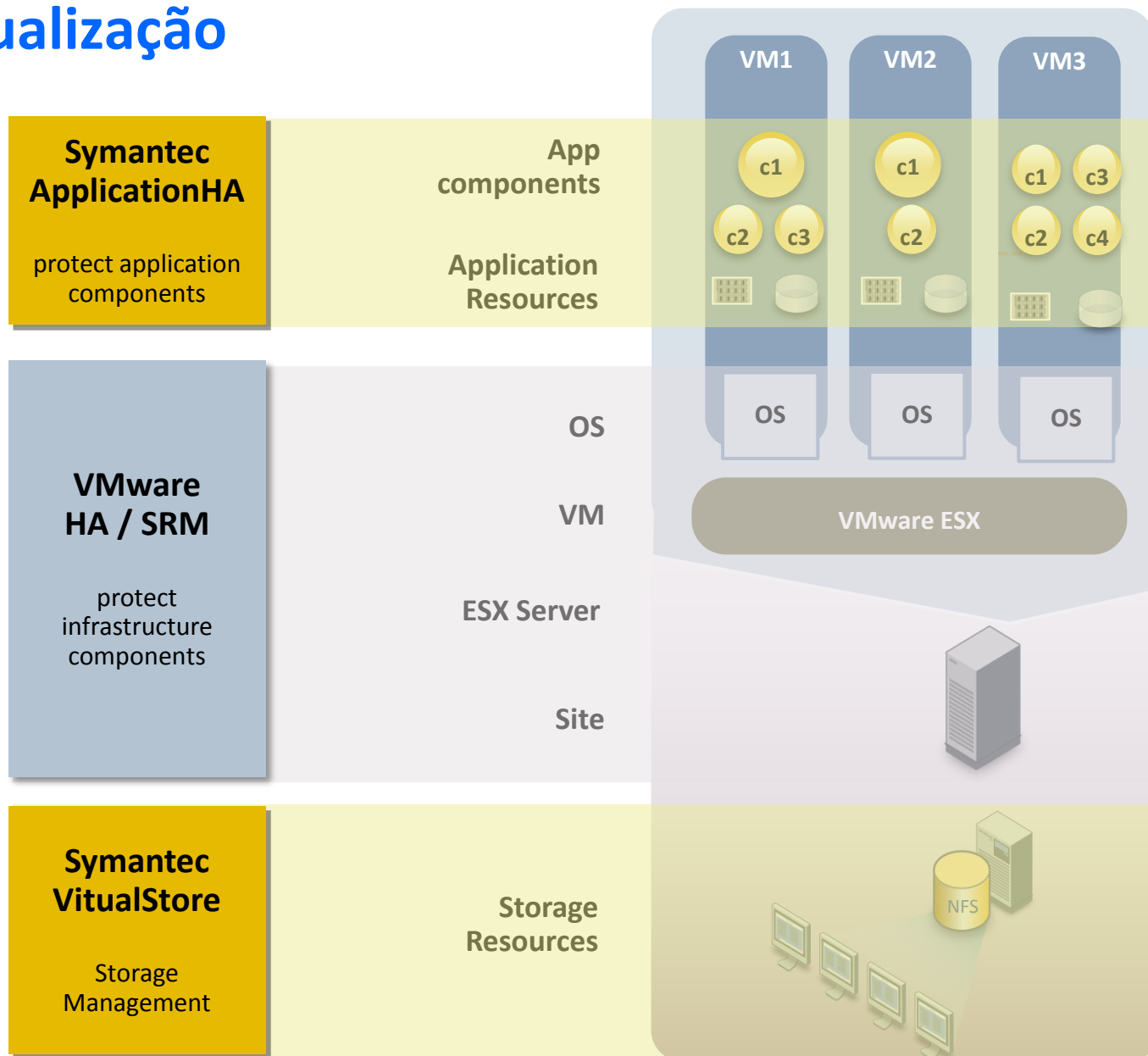
# GDOC (Geographically Dispersed Open Cluster)



IBM TCW (Technical Consulting Workshop)



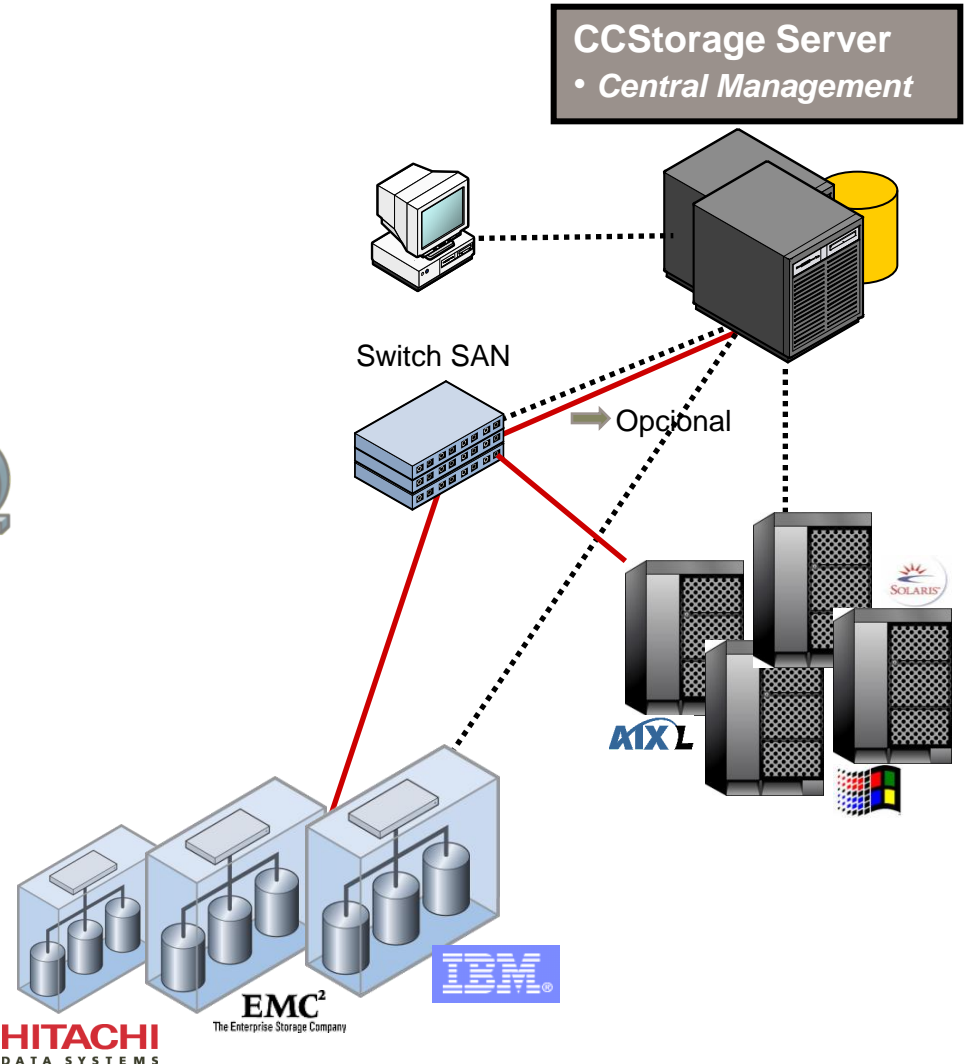
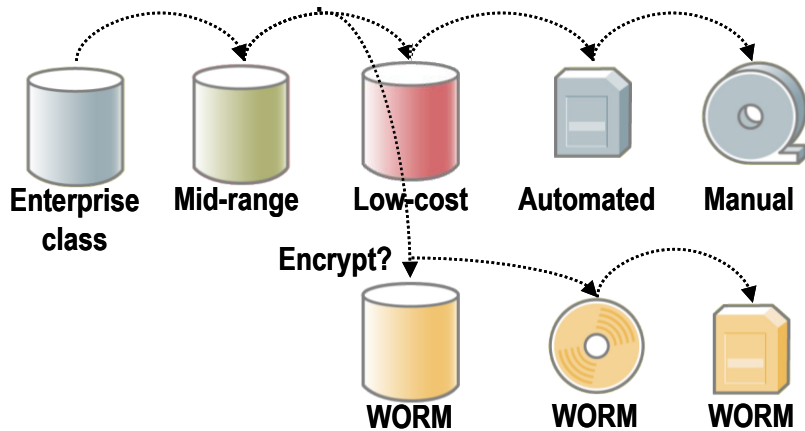
# Virtualização





# Gerenciamento de Storage

- Com a solução de SRM **Symantec CommandCentral Storage**, que é *agent less* e agnóstica, a IBM realiza serviços ILM, proporcionando redução de custos na aquisição de storage



# Por que IBM?



## Trusted Advisor

Ajudando Clientes a construir smarter cities, smarter grids, novos data centers, e muito mais.

## Líder em Segurança

Um Provedor líder de serviços e soluções de segurança nos mais diversos segmentos.

## Provedor de soluções de I/T

Um Provedor líder de soluções de software, hardware e serviços ao redor do mundo

## A Empresa

400,000 empregados em 130 países com 100 anos de existência





# Obrigado !

Marco Antonio Almeida - [marcao@br.ibm.com](mailto:marcao@br.ibm.com) - (55) – 11 – 9952-9934  
Adriano Barreto – [adrianob@br.ibm.com](mailto:adrianob@br.ibm.com) - (55) – 11 – 2132-3393

Copyright © 2011 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.

# Backup Slides

# IBM Managed Security Services – Fatos Relevantes

## EXPERIÊNCIA E SKILL

- Serviços existe desde 1995
- Constante investimento em inovação
- Conta com o input / skill do time da X-Force

## LIDERANÇA DE MERCADO

- Forrester Wave
- Gartner Magic Quadrant
- Frost & Sullivan

## PORTFOLIO INOVADOR

- Ofertas CPE & Cloud
- Portal do Cliente integrado e completo
- Vendor Agnóstico
- “Best in Class” SLAs



## ALCANCE GLOBAL

- 9 Security Operations Centers
- 325+ profissionais Dedicados

## BC/DRP & COMPLIANCE

- Fully Redundant Services
- Testes de BC/DRP realizados anualmente
- SAS-70, SysTrust, PCI, FFIEC, ITCS-104

## ALGUNS NÚMEROS

- Milhares de Clientes
- Dezenas de Milhares de Devices
- Bilhões de logs/eventos processados por dia

Experiência, Flexibilidade, Qualidade nos Serviços

# Uma solução completa construída em conjunto entre a Juniper (com a tecnologia do Junos Pulse) e a IBM com seu serviço de gerenciamento de segurança mundialmente reconhecido



JUNIPER  
NETWORKS



IBM

*...e Amplo e compreensivo suporte a diversos fabricantes / plataformas*



iPhone



Google Android



Win Mobile



Nokia Symbian



BlackBerry

# A visão de Cloud Computing da IBM

“Cloud” é um **novo modelo de consumo e entrega de serviços** baseado no acesso e gerenciamento através da internet.

Serviços em Cloud se caracterizam por :

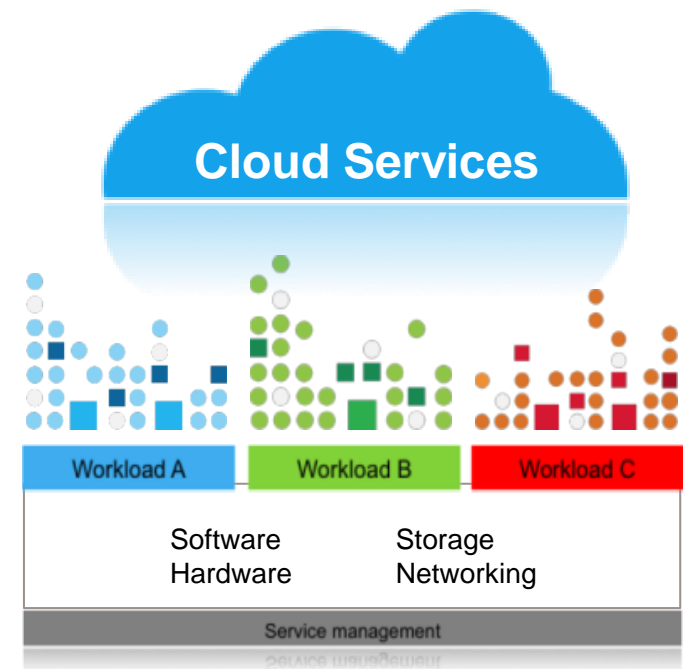
- **Virtualização** de recursos
- **Automação** do gerenciamento de serviços
- **Padronização** de workloads/demandas

Serviços em Cloud permitem :

- Self-service
- Independência de Localização (Mobilidade)
- Modelos de pagamento flexíveis
- Economias de escala

Cloud representa:

- A **industrialização** do **delivery** de serviços de IT



Apesar dos benefícios, muitos aspectos deixam as empresas relutantes em implementar serviços gerenciados na “nuvem”.

## Controle

Muitas empresas tem o receio de perder o controle / gerenciamento dos seus sistemas / informações .

## Compliance

A necessidade de cumprimento de leis e regulamentações pode ser um ponto crítico na implementação de serviços na nuvem.

## Proteção de Dados

As informações da minha empresa estarão protegidas ?? Os sistemas na “nuvem” terão o controle de acesso adequado ??

## Disponibilidade

Alta disponibilidade é uma preocupação. Aplicações de missão crítica não podem estar na “nuvem” se não houver uma garantia de “não interrupção” dos serviços

## Gerenciamento

Os Provedores de serviços na “nuvem” devem garantir o adequado nível de gerenciamento e fornecimento de informações ao Cliente.



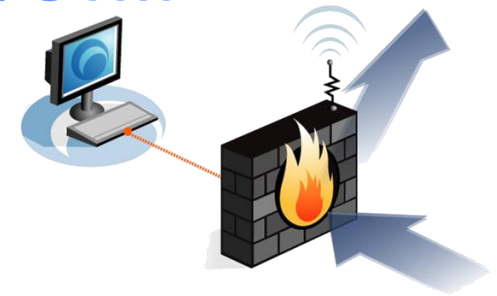
# Serviços Gerenciados para: Firewall, IPS & UTM

## Overview da Solução

Os serviços gerenciados IBM para Firewall, IPS e UTM são desenhados para diminuir o custo e overhead operacional associados com as tarefas de gerenciamento do dia a dia destas tecnologias de segurança. Este serviço combina: gerenciamento, monitoração, e manutenção de uma diversa quantidade de tecnologias de vendedores diferentes.

## Benefícios

- **Reduz Custo e trabalho operacional** no gerenciamento destas tecnologias multi vendor
- Fornece **Suporte 24x7** para as atividades de : **monitoração, resposta a incidentes , e gerenciamento**



## Características Principais

**Suporte as tecnologias líderes de mercado : solução agnóstica**

### SLA's líderes na indústria

Incluindo : resposta a incidente, gerenciamento de mudança , monitoramento dos appliances, criação de relatórios, etc.

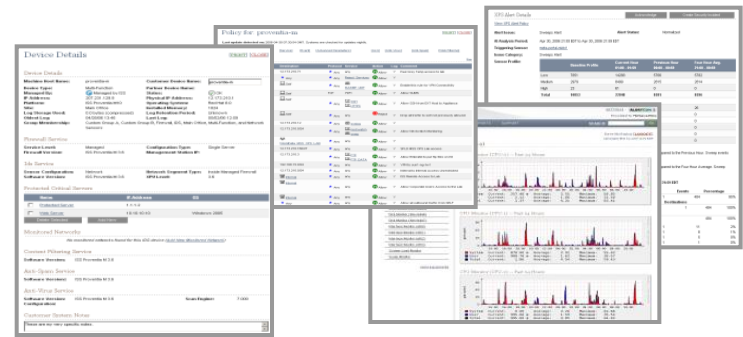
### Serviço integrado com o Portal do IBM Virtual SOC

Interface web da IBM que garante o gerenciamento real time e on demand, garantindo ao Cliente controle sobre relatórios, alertas , solicitação de atividades, configuração do ambiente, etc.

# Security Event and Log Management

## Overview da Solução

O serviço de “SELM” permite o armazenamento e compilação off-site de dados de eventos e arquivos de log de aplicações de rede, IPS's, Firewalls, servidores , tudo integrado em uma única interface



## Benefícios

- **Análise rápida de dados de logs/eventos de várias plataformas e tecnologias diferentes** através de uma interface única e integrada na Web.
- **Armazenamento Remoto** de dados críticos de log .
- **Economia de Storage** por parte de Cliente.

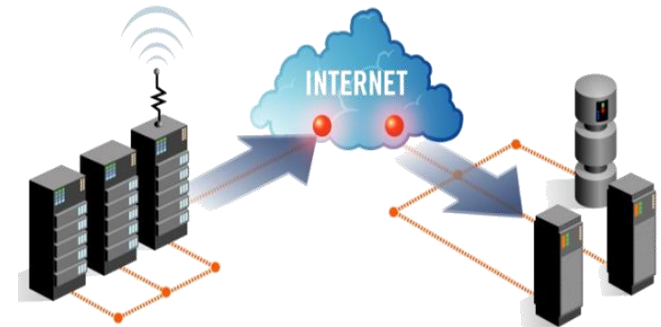
## Características Principais :

- Capacidade de análise integrada
- Eventos de Segurança podem ser investigados , escalados e armazenados usando a infra-estrutura da IBM
- Consolidação de Logs via ferramenta “on site agregator”
- Arquivamento remoto permite análise forense quando necessário

# Hosted Vulnerability Management

## Overview da Solução

O “HVM” combina um serviço de “scanning” / identificação de vulnerabilidades com reportes contendo as recomendações de mitigação dos riscos ou problemas encontrados. Relatórios customizáveis permitem facilmente demonstrar compliance e o status de vulnerabilidade dos sistemas pesquisados.



## Benefícios

- **Possibilidade de “scan”** a endereços IP na borda da rede assim como a sistemas internos **sem a necessidade de compra** de uma aplicação / SW de Scan.
- Após o Scan, relatórios customizados mostram as vulnerabilidades encontradas , assim como as sugestões de correção para as mesmas.

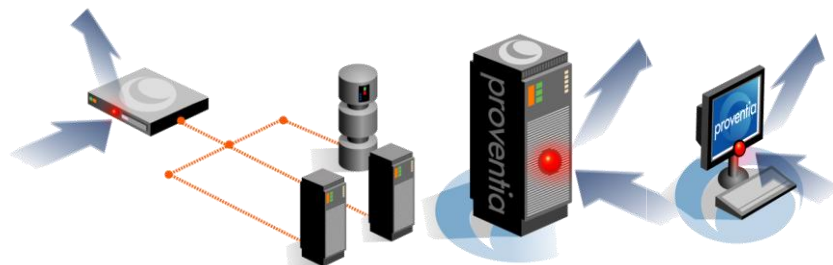
## Características Principais :

- Solução “Turnkey” para análise de vulnerabilidade.
- O Scan pode ser feito sob uma perspectiva interna ou externa a internet.
- Relatórios detalhados e customizáveis.
- Toda a análise e gerenciamento dos Scans está disponível no Portal Internet.

# IBM X-Force Hosted Threat Analysis Service

## Overview da Solução

Serviço de informação/inteligência que melhora o planejamento de estratégia de segurança e reduz riscos, fornecendo aos Clientes informações e recomendações baseadas na compilação de dados dos 9 SOC's da IBM e também nos dados gerados pelo time de Pesquisa e Desenvolvimento da the X-Force.



## Benefícios

- Fornecimento de **notificação prévia** de ameaças para ajudar o Cliente na prevenção e proteção as mesmas.
- **Melhora a tomada de decisão** e resposta a possíveis incidentes de segurança.

## Características Principais :

- Resumos diários sobre possíveis características e naturezas de ameaças.
- Recomendação de “patches e fixes” lançados pelos vendedores reconhecidos de mercado.
- Ajuda a otimizar investimentos em Segurança e na priorização de recursos para estes fins.

# IBM Mobile Device Security Services

NEW

Solução completa para aparelhos móveis – smartphones -  
desenhada para auxiliar os Clientes a implementar e gerenciar  
políticas de seguranças e proteção a estes ativos corporativos  
contra vários tipos de ameaças.



## Componentes da Solução:

- **Infraestrutura** de gerenciamento **na nuvem** gerenciada pela **Juniper e IBM**.
- A **licença de Software** para os aparelhos móveis está **incluída** na taxa mensal do serviço.
- **Gerenciamento e monitoração 24x7**.
- **Reportes mensais** e análise de uso, com notificação de riscos específicos e recomendações de melhoria nas políticas de segurança (best practices).

## Características principais:

- **Suporte a Multiplas plataformas** “best sellers” de mercado.
- **Conectividade segura, baseada na politica definida** Acesso a recursos corporativos baseado nas politicas definidas.
- **Serviço Suportado pelos 9 SOC's IBM**, usando o expertise da IBM em serviços gerenciados, reconhecidamente um dos maiores provedores do Mundo

## Benefícios aos Clientes:

- **Empresas podem proteger aparelhos móveis**, de diversos fabricantes diferentes através de uma solução única e integrada.
- **Redução no custo de implementação e gerenciamento de segurança para aparelhos móveis**.
- **Melhora o compliance com as politicas de segurança das empresas e ajuda a controlar o acesso a recursos e informações corporativos através do uso de aparelhos móveis**