4ª edição
IBM Security Forum

Os Desafios para a Segurança da Informação num Planeta mais Inteligente

A Estratégia da IBM para Segurança

Eduardo Abreu
IBM Security Team

Abril/2011

Estamos construindo um Planeta mais Inteligente

O planeta está ficando mais…

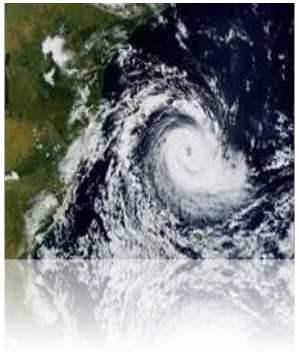
Smart Supply Chains

Smart Countries

Smart Retail

Smart Water Management

Smart Weather

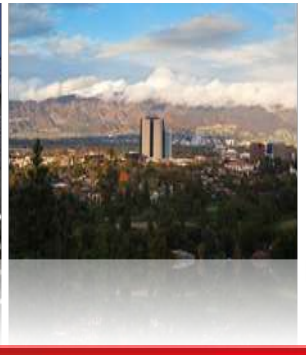


Smart Energy Grids

INSTRUMENTALIZADO **INTERCONECTADO** **INTELIGENTE**

Intelligent Oil Field Technologies

Smart Regions



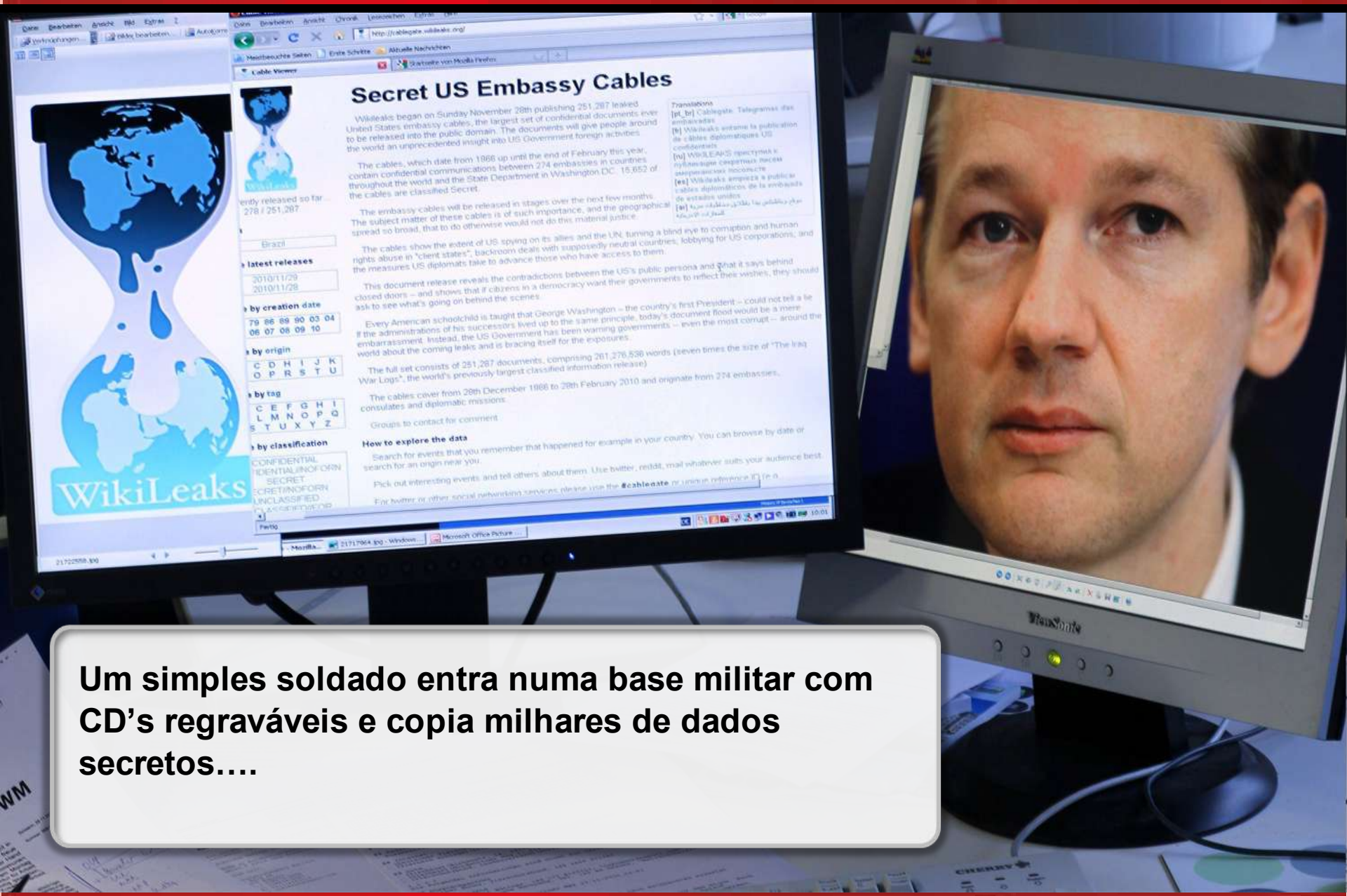
Smart Healthcare

Smart Traffic Systems

Smart Cities

Smart Food Systems

Mas será que a Segurança está avançando no mesmo passo?

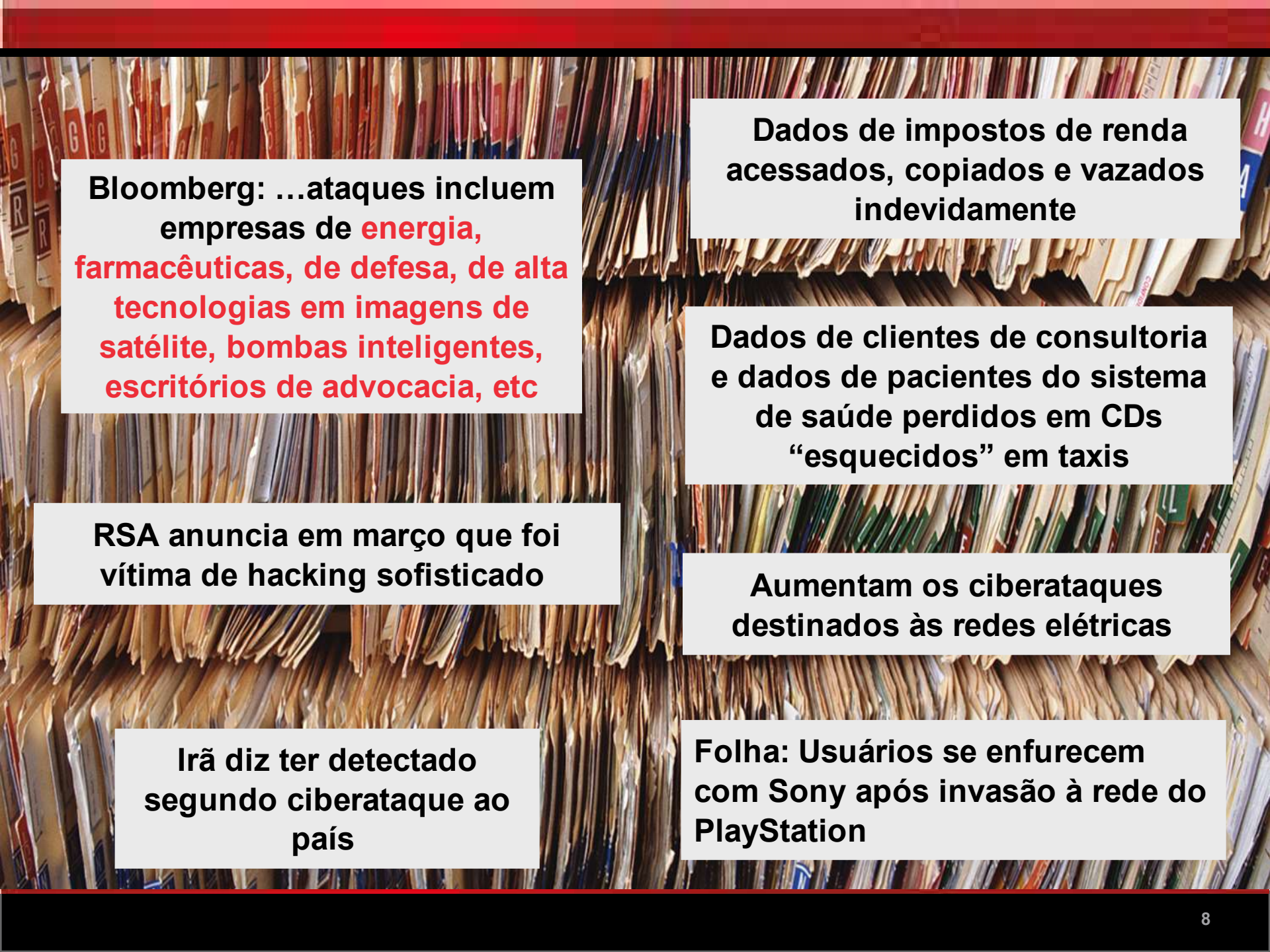


Um simples soldado entra numa base militar com CD's regraváveis e copia milhares de dados secretos….

Stuxnet: “Malware” orientado a sistemas de automação industrial que monitora centrífugas nucleares iranianas, arquitetado de forma sofisticada, levantando suspeitas diversas sobre a natureza da ação

- **Sofisticado:**
  - Inclui exploits para 4 vulnerabilidades (0-day) sem patches
  - Inclui componentess assinados certificados digitais roubados
  - Disseminados através de diversos vetores
  - Infectou máquinas de desenvolvimento c/rootkit que esconde tanto o “malware” como as mudanças que ele faz nos programas sendo desenvolvidos
- **Dirigido:**
  - Modifica códigos nos controladores lógicos programáveis - PLCs
  - Modificações só acontecem em determinadas circunstâncias (drivers de alguns fornecedores, operando em condições específicas de frequência, etc
- **Danos colaterais**
- – Infecção pode se espalhar de forma generalizada

NASDAQ: Portal usado por executivos de muitas empresas da Fortune 500 para compartilhar informações estratégicas e financeiras foi comprometido.


Bloomberg: …ataques incluem empresas de energia, farmacêuticas, de defesa, de alta tecnologias em imagens de satélite, bombas inteligentes, escritórios de advocacia, etc
Dados de impostos de renda acessados, copiados e vazados indevidamente
Dados de clientes de consultoria e dados de pacientes do sistema de saúde perdidos em CDs "esquecidos" em taxis
RSA anuncia em março que foi vítima de hacking sofisticado
Aumentam os ciberataques destinados às redes elétricas
Irã diz ter detectado segundo ciberataque ao país
Folha: Usuários se enfurecem com Sony após invasão à rede do PlayStation

Em que direção a Segurança está avançando?

4ª edição
IBM Security Forum

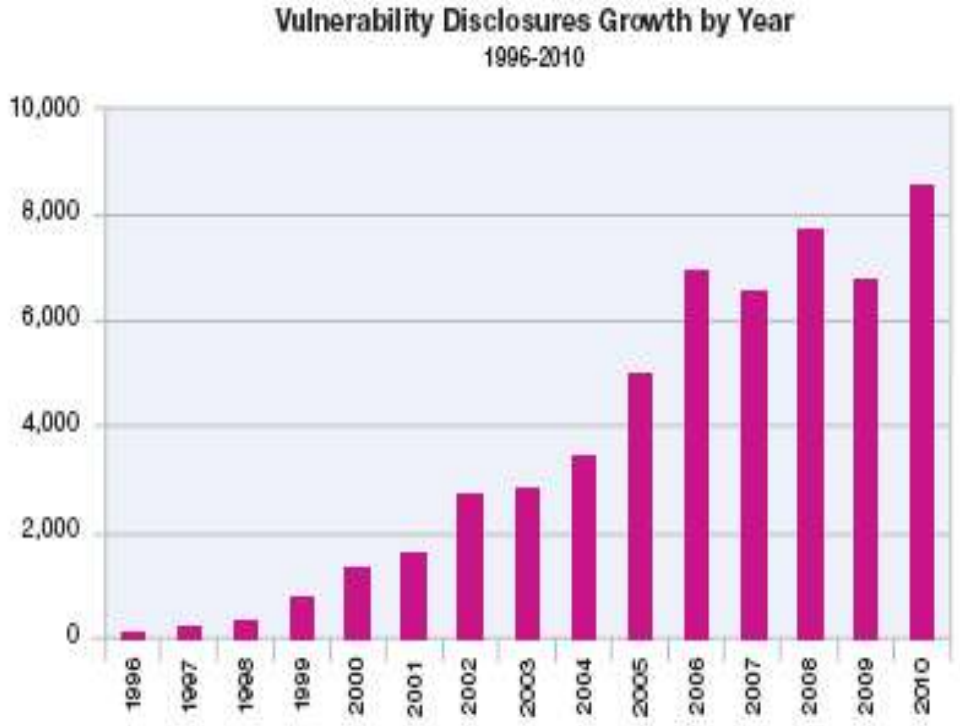
IBM X-Force® 2010 Trend and Risk Report

Annual Review of 2010

IBM

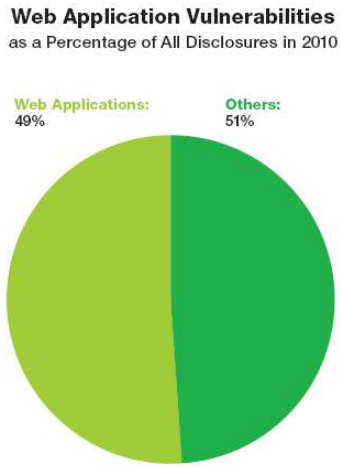
O maior número de vulnerabilidades jamais publicado

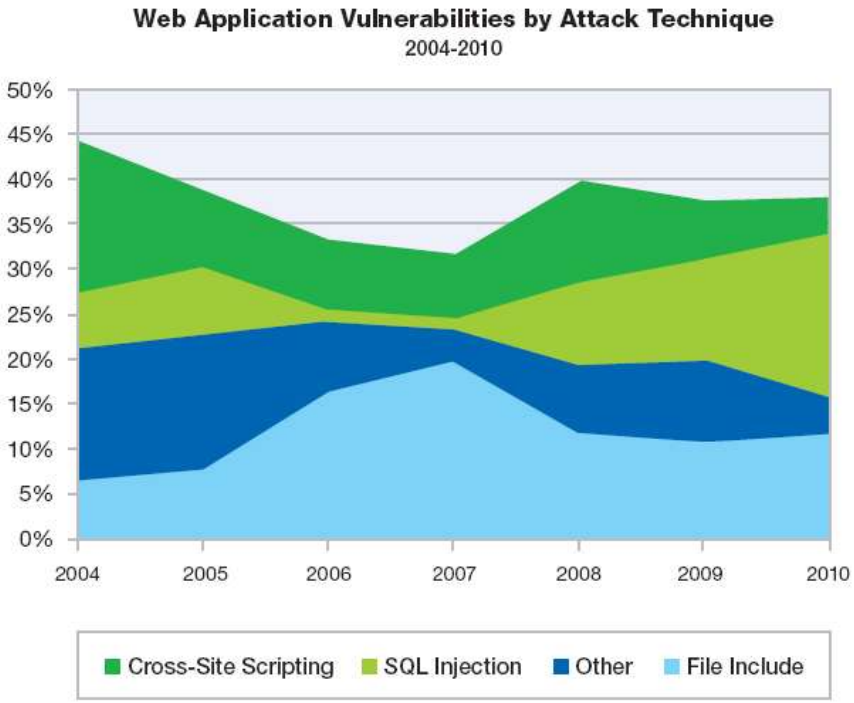
- Crescimento de **27%.**
- "Exploits" crescimento de **21%** em 2010 comparado com 2009
- Aproximadamente **14.9%** of das vulnerabilidades publicadas em 2010 tiveram "exploits'publicados
- A maior parte dos "exploits" publicados no mesmo dia da vulnerabilidade
- **44%** das vulnerabilidades publicadas em não tinham patches publicados até o final do ano

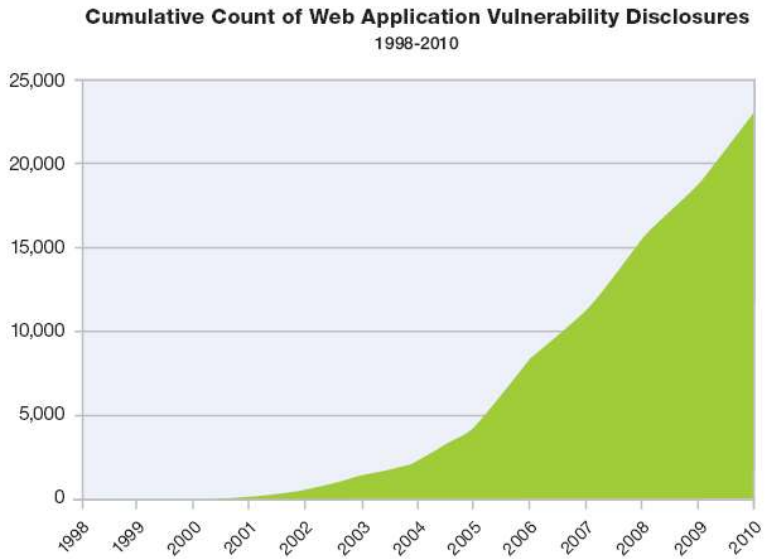


Vulnerabilidades das aplicações Web dominam o cenário

- **49%** das vulnerabilidades publicadas são relacionadas às aplicações Web
- Cross-Site Scripting & SQL injection são as vulnerabilidades predominantes

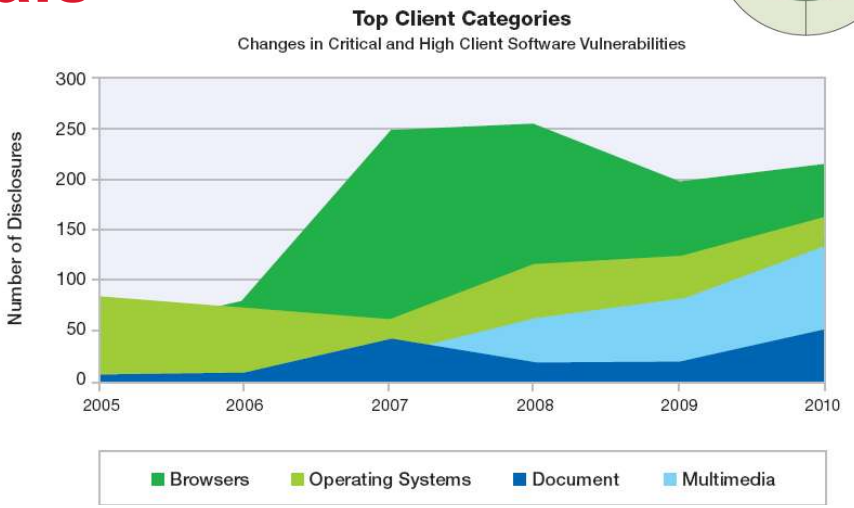


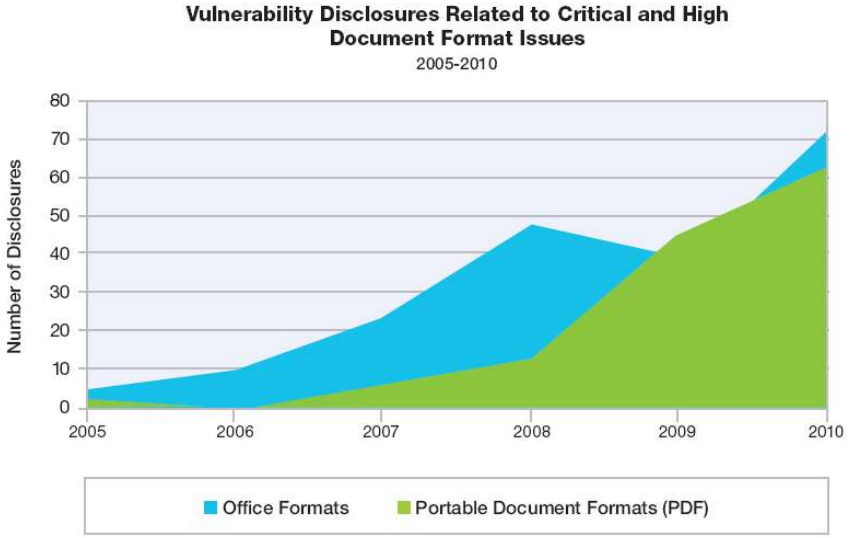


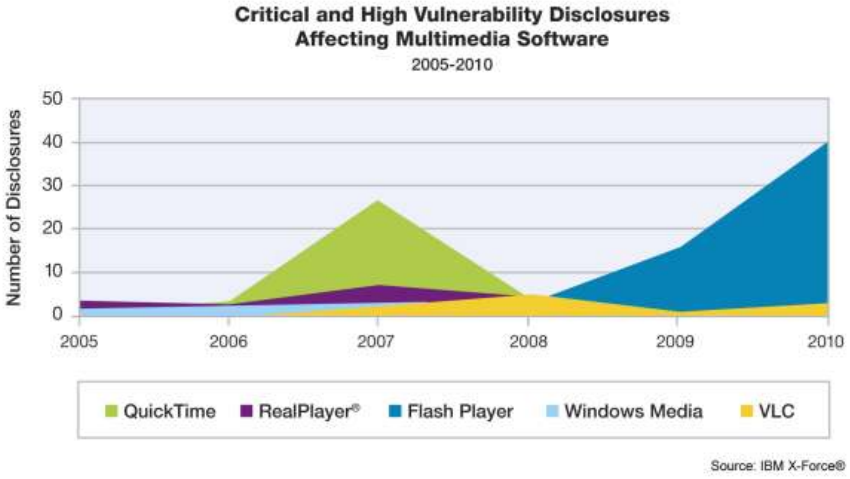


Vulnerabilidades nos clientes continuam a impactar os usuários finais

- Web browsers e seus plug-ins continuam liderando nesta categoria
- Em 2010 aumentaram cresceram as vulnerabilidades associadas aos leitores e editores de texto e aos multimedia players.

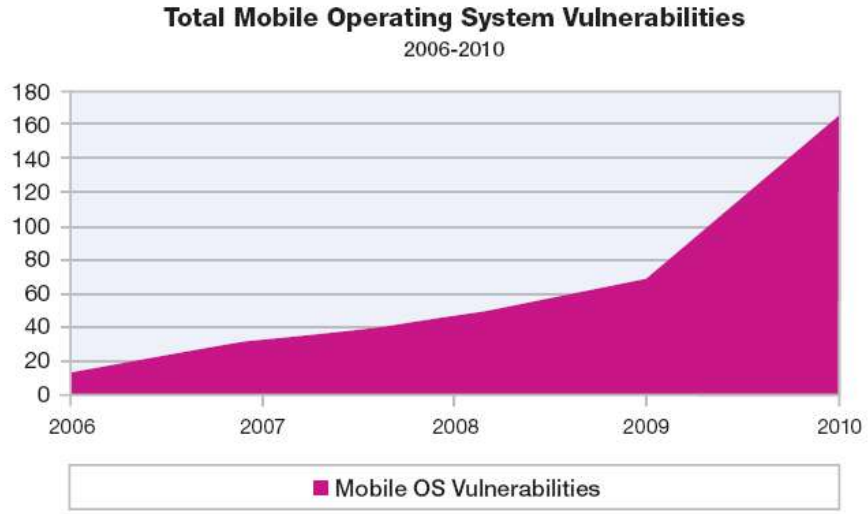


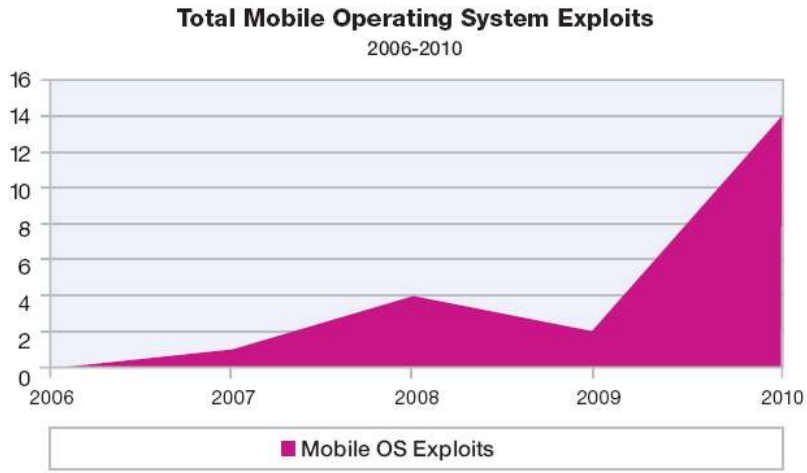




Proliferação de dispositivos móveis aumentam preocupação com Segurança

- Em 2010 cresceu o número de vulnerabilidades associadas aos dispositivos móveis e também os “exploits” destas vulnerabilidades.
  - Algumas motivações parecem estar associadas a liberar funcionalidades bloqueadas dos dispositivos
  - Outras aplicações maliciosas foram dissemidads para dar acesso acesso ao root dos dispositivos e roubar informações





Ameaças internas

Continuam a crescer, à medida que cresce o número de usuários, surgem novas formas de acesso às redes e cresce o número de pessoas que inadvertidamente caem nas mãos dos ciber-criminosos. As organizações devem encontrar novos meios para garantir que seus recursos não sejam comprometidos

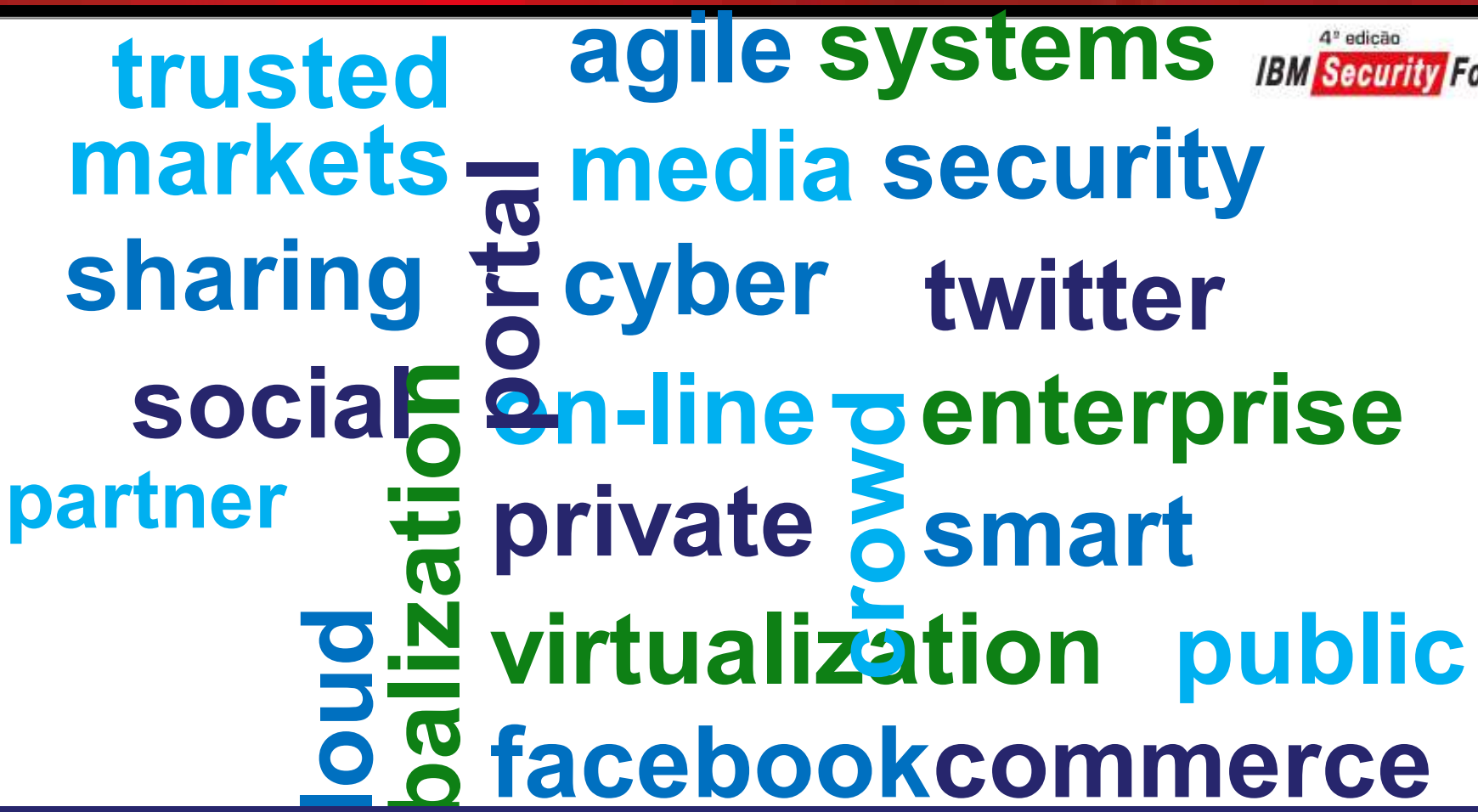


NORMAS E REGULAMENTAÇÕES

Maior enfase em conformidade gera maior complexidade para atender requisitos de garantia de privacidade, segurança e proteção de infra-estrutura e ativos críticos.

MOBILIDADE E “CLOUD COMPUTING”

Quanto maior a mobilidade da força de trabalho e maior a adoção da “Cloud Computing, gestão efetiva e segurança crescem em prioridade. Foco nos dados sensíveis, escolha adequada dos dispositivos e na gestão dos end-points é cada vez mais crítico.



4ª edição IBM Security Forum

INOVAÇÃO

Segurança deixa de ser um fator inibidor e passa a ser elemento viabilizador da adoção de novas tecnologias como "cloud computing", redes sociais e virtualização

E o que a IBM fazendo?

Keeping the bad guys out

4ª edição
IBM Security Forum

Novos modelos de entrega de produtos e serviços

Seguro = Gerenciado

Gerenciamento de Sistemas

Agente de Gestão comum

Console Unificada de Gestão

Infra-estrutura comum

Gerenciamento da Segurança

Tivoli Endpoint Manager

ENDPOINTS DIVERSOS
LAPTOP / SERVER

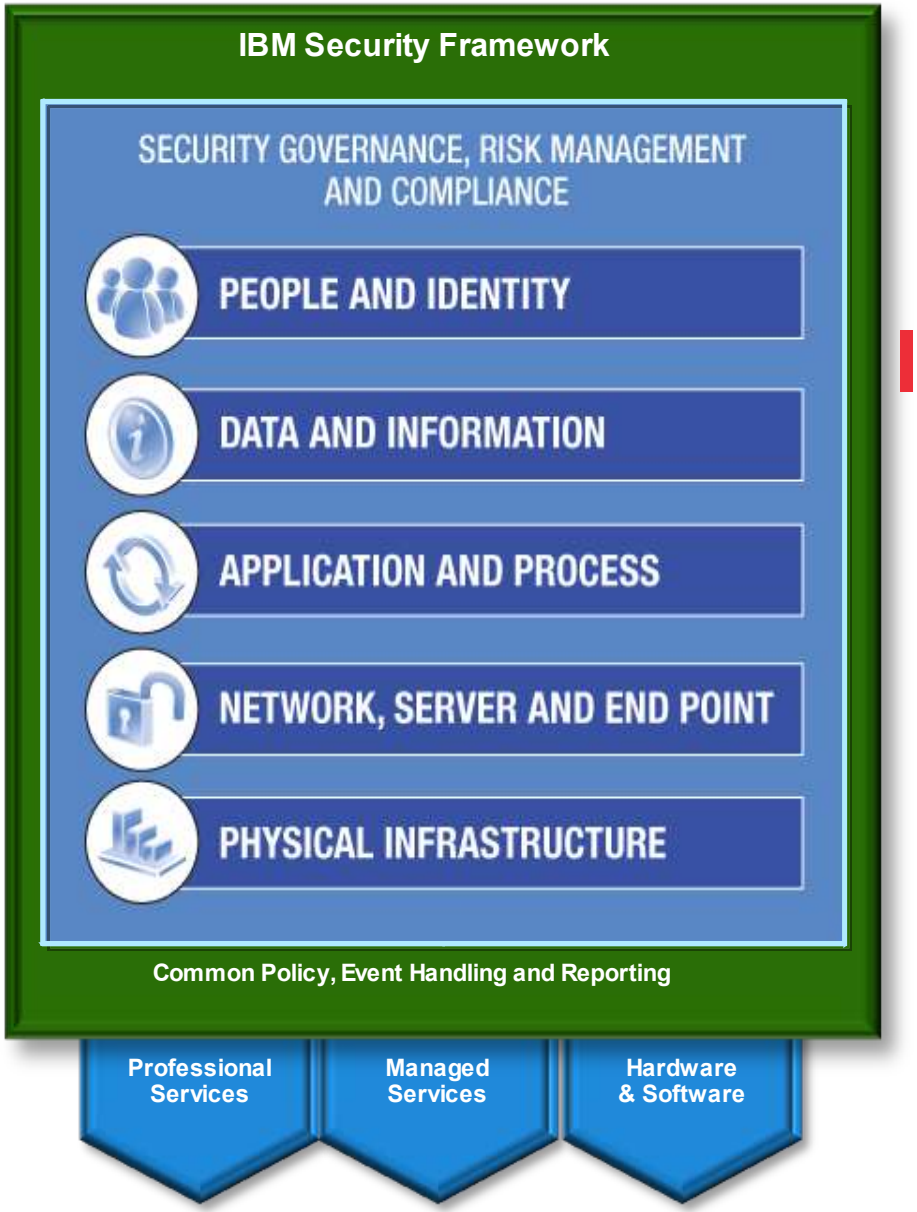
ENDPOINT MÓVEL

ENDPOINT PROPÓSITO ESPECÍFICO

Segurança Operacional

identidade rede email/web

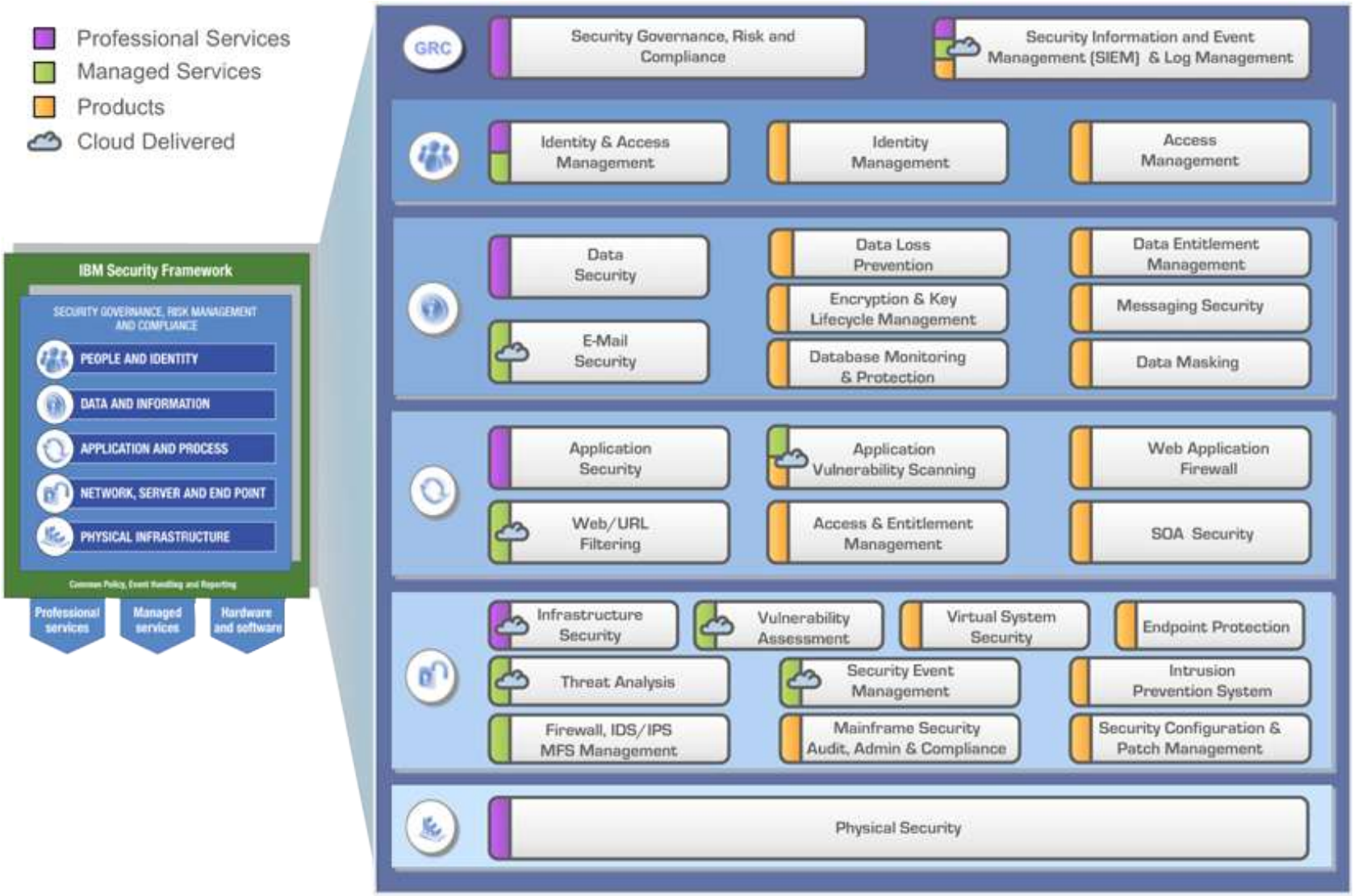
aplicação endpoint banco de dados



IBM Security Solutions

- **Protegendo seu futuro**
- **Viabilizando a Inovação**

IBM Security Framework



Obrigado !

Eduardo Abreu
IBM Security Team
eabreu@br.ibm.com
Fone:+55.11.21322435
Cel: +55.11.69057994