IBM Security Forum

Soluções para um ambiente seguro

Managed Security Services
Reduzindo custos operacionais de segurança de forma garantida e eficaz

Fernando Guimarães – MSS Global Architect
feguima@br.ibm.com

AGENDA

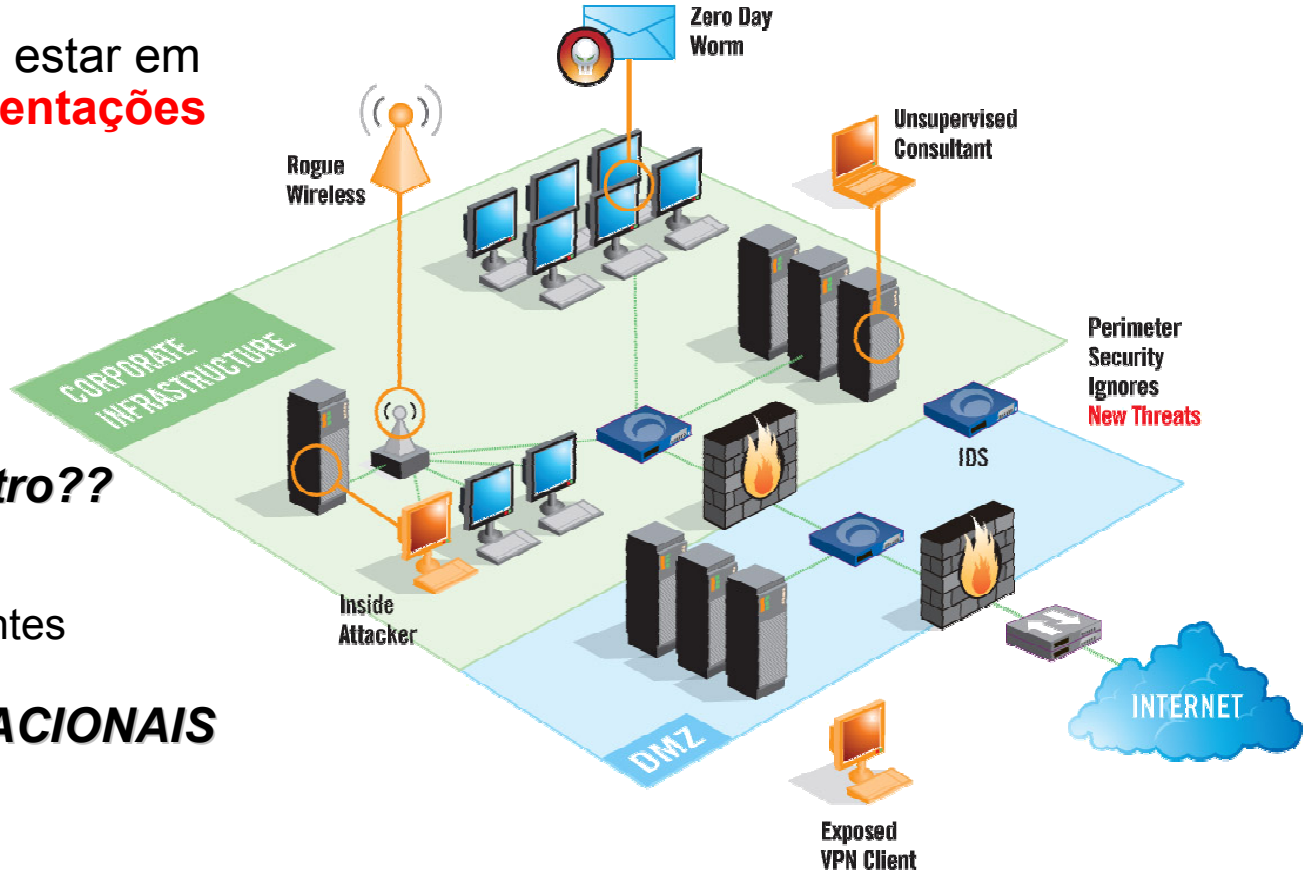
- Os Desafios dos Gestores de Segurança da Informação
- Os Serviços Oferecidos pela IBM ISS
- Como o MSS da IBM ISS pode lhe ajudar
- Portal Virtual-SOC

Os Desafios dos Gestores de Segurança da Informação

O Ambiente Atual de Segurança da Informação

- Ambiente **complexo** = **Altos custos** de gerenciamento/monitoração

- Riscos crescentes por não estar em conformidade com **regulamentações**



Onde foi parar o perímetro??

- **VPN's**, Wireless
- Terceiros, parceiros, clientes

MUDANÇAS ORGANIZACIONAIS

- Novos negócios, novas aplicações
- **Fusões** e aquisições

Muita coisa para tratar…

Ambiente Multi-Vendor

- ISS, CheckPoint, Cisco, Juniper, Symantec, McAfee, TrendMicro, 3com and more…

Operações Distribuídas

- Recursos distribuídos, escritórios remotos, equipes remotas.

Sobrecarga de Informações…Logs e Eventos de Segurança

- Firewalls & IDS/IPS
  - Facilmente mais de 10GB de dados por semana
  - Podem gerar centenas de alertas em 1 único dia

Tenho que Gerenciar e Monitorar isso Tudo!

Custos Altos

- Requer cobertura 24x7x365 (6 – 9 técnicos por posto)
- Requer ferramentas sofisticadas (**e caras!!)** para análise precisa das ameaças
- Requer boas instalações físicas e sistemas de suporte redundantes

Requer Equipe com Skills sofisticados e constantemente treinada

- Analistas capacitados para detecção e investigação de incidentes
- Analistas preparados para responder e resolver emergências
- Treinamento e política de retenção continua

Inteligência

- Conhecimento das últimas ameaças, virus, worms, etc...
- Compreensão dos mais sofisticados métodos de ataque
- PESQUISA, PESQUISA, PESQUISA...

Você Conhece esta Empresa ?

- **Não instalou** todos os produtos de segurança adquiridos no último ano.
- Possui **recursos limitados** para operar seu ambiente de segurança.
- Não possui equipe e/ou **capacitação** para gerenciar a solução de segurança recém adquirida.
- Quer **focar sua equipe** de segurança de TI em projetos/atividades estratégicas.
- Está sendo pressionada pela alta gerência para:
  - **Mostrar rapidamente o valor** dos investimentos feitos em segurança.
  - **Redução** imediata dos **custos** de operação de TI
- Precisa aderir às **regulamentações**.

Os Serviços de Gerenciamento de Segurança “MSS” da IBM ISS

Virtual Security Operations Center (VSOC)

Abrangência e Expertise Global

Visão Integrada e Centralizada

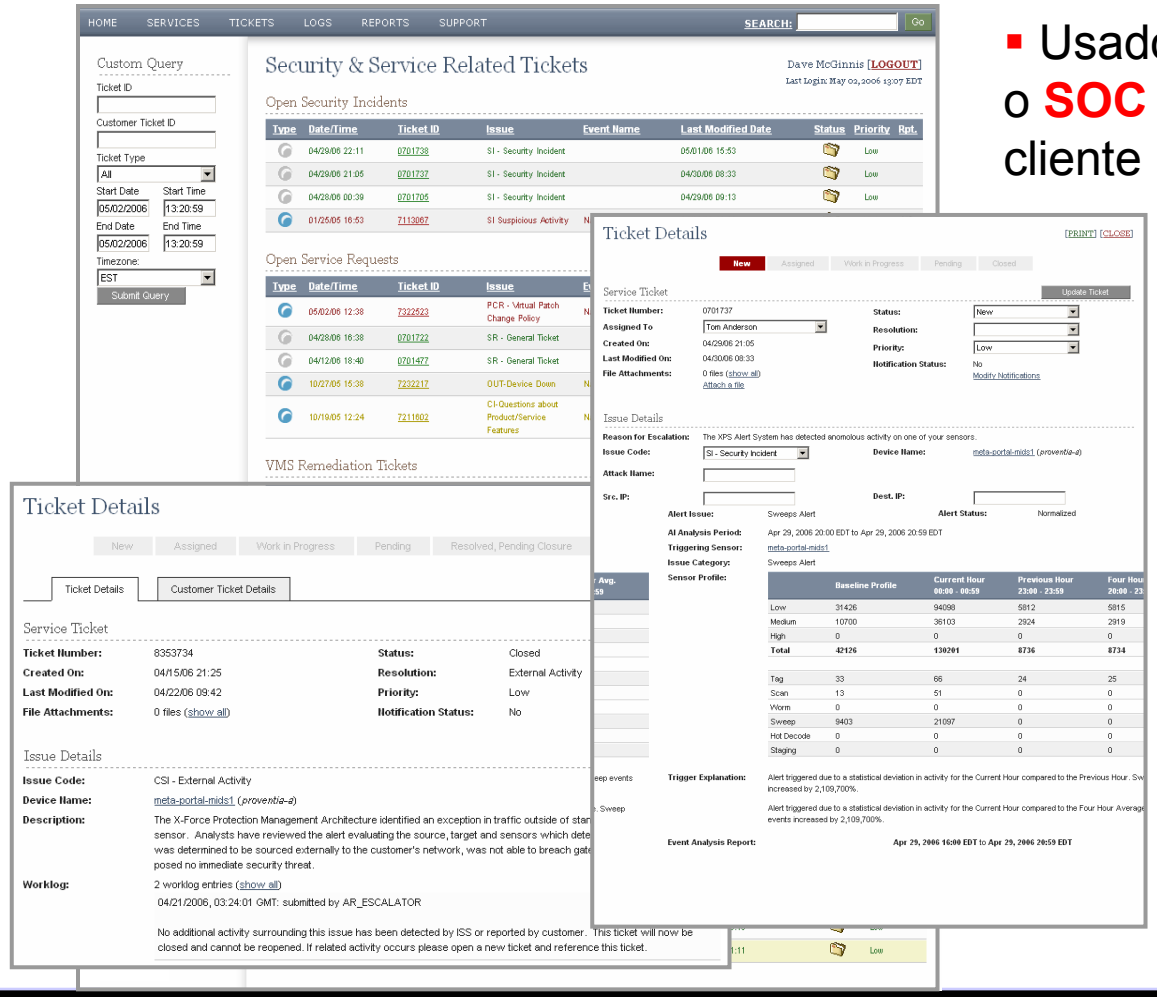
Portal Virtual-SOC

Portal Virtual SOC

- Visão **Centralizada**
- Visão **Consolidada**
- **100% web-based**: nenhum equipamento no cliente

Portal Ticket Manager

- Sistema de **Trouble-ticket** integrado
- Usado tanto para comunicação com o **SOC** quanto para uso **interno** do cliente



Informação na ponta dos dedos

Event Name	Priority	%	Count	Sources	Destinations	First Event	Last Event
IPM_Blocked_TCP_Connection		<1%	2,210	2	19	05/03/06 01:30:49 GMT	05/03/06 02:21:50 GMT
Nmap UDP Port Sweep 4003:0		<1%	760	1	26	05/03/06 01:25:51 GMT	05/03/06 01:34:04 GMT
SQL_SSRP_Slammer_Worm		<1%	252	65	62	05/03/06 00:02:54 GMT	05/03/06 14:32:55 GMT
IPM_Invalid_Protocol		<1%	234	1	1	05/03/06 01:01:32 GMT	05/03/06 01:20:25 GMT
UDP Port Sweep 4001:0		<1%	124	1	24	05/03/06 01:25:59 GMT	05/03/06 01:38:45 GMT
Tftp Passwd File 5509:0		<1%	75	1	23	05/03/06 01:29:21 GMT	05/03/06 01:37:43 GMT
SQL_SSRP_StackBo		<1%	53	33	39	05/03/06 00:12:24 GMT	05/03/06 14:28:40 GMT
SSH_Deattack_IO		<1%	48	1	26	05/03/06 01:35:44 GMT	05/03/06 02:22:52 GMT
Email_Pipe		<1%	43	1	1	05/03/06 01:29:17 GMT	05/03/06 01:33:10 GMT
TFTP_Passwd_File		<1%	34	1	9	05/03/06 01:36:10 GMT	05/03/06 01:42:11 GMT
TFTP_Traversal		<1%	34	1	9	05/03/06 01:36:10 GMT	05/03/06 01:42:11 GMT
SSH_Brute_Force		<1%	28	2	9	05/03/06 00:01:17 GMT	05/03/06 01:40:42 GMT
Cisco TFTPD Directory Traversal 5510:0		<1%	23	1	23	05/03/06 01:29:21 GMT	05/03/06 01:37:31 GMT
Syphillis_Scan_Request		<1%	15	1	14	05/03/06 01:39:35 GMT	05/03/06 01:55:40 GMT
Win_MessengerPopup_Bo		<1%	15	1	14	05/03/06 01:39:02 GMT	05/03/06 01:48:55 GMT
Telnet_Linker_Bug		<1%	14	1	2	05/03/06 01:29:51 GMT	05/03/06 01:29:52 GMT
TCP Hijack 3250:0		<1%	11	4	5	05/03/06 00:51:12 GMT	05/03/06 14:03:09 GMT
Dtspcd_Overflow		<1%	10	1	1	05/03/06 01:35:50 GMT	05/03/06 01:35:51 GMT
FW1_Auth_As_Local		<1%	8	1	6	05/03/06 01:39:28 GMT	05/03/06 02:21:28 GMT
MSRPC_RemoteActivate_Bo		<1%	8	1	1	05/03/06 01:34:34 GMT	05/03/06 01:34:34 GMT
LPRng_Format_String		<1%	5	1	1	05/03/06 01:34:44 GMT	05/03/06 01:34:45 GMT
statd dot dot 6188:0		<1%	3	1	3	05/03/06 01:31:36 GMT	05/03/06 01:36:31 GMT
SMB_Samba_Transaction2_bo		<1%	1	1	1	05/03/06 01:38:38 GMT	05/03/06 01:38:38 GMT

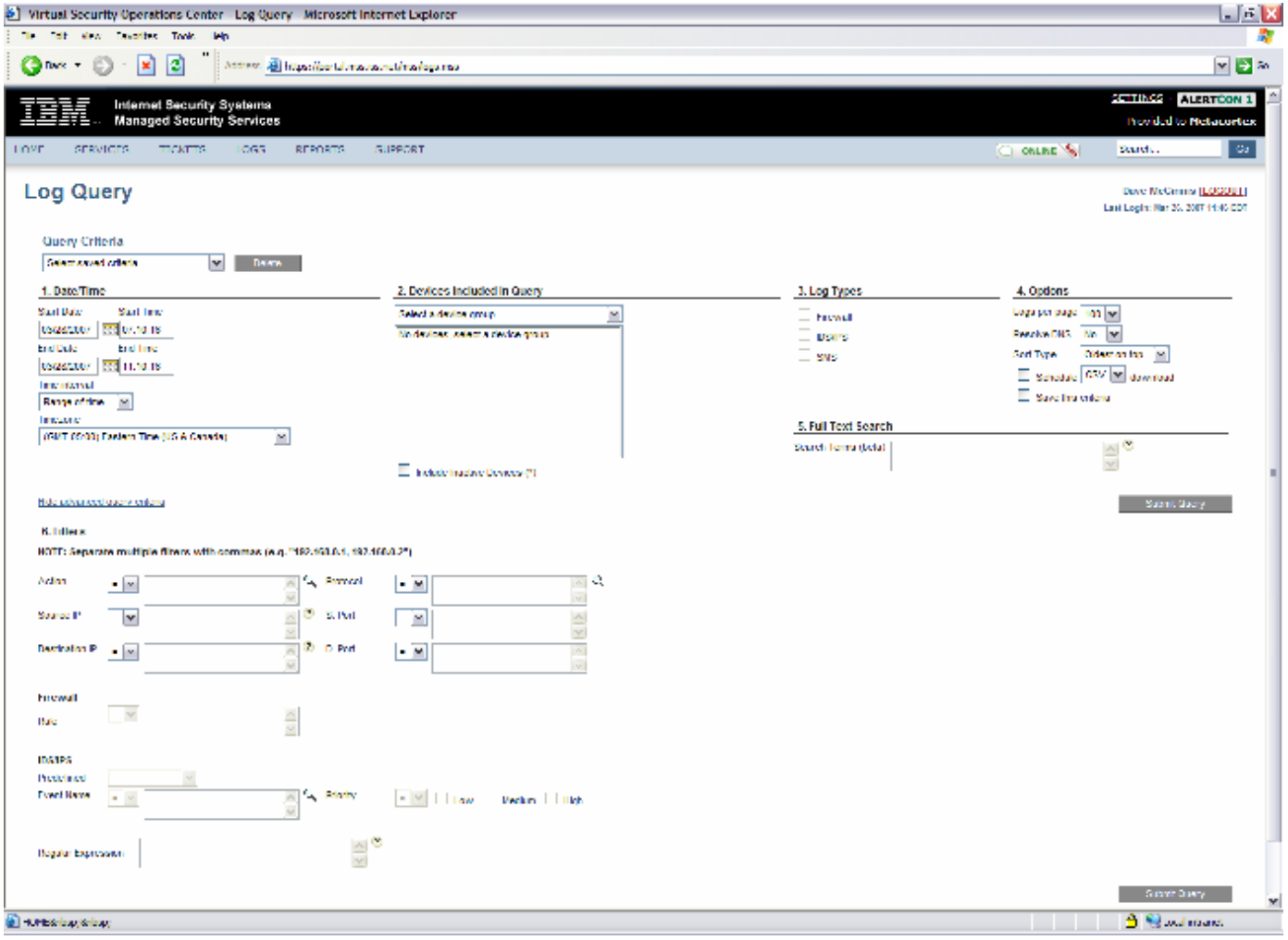
- Visualização de eventos em

REAL-TIME

Consultas históricas dos logs armazenados

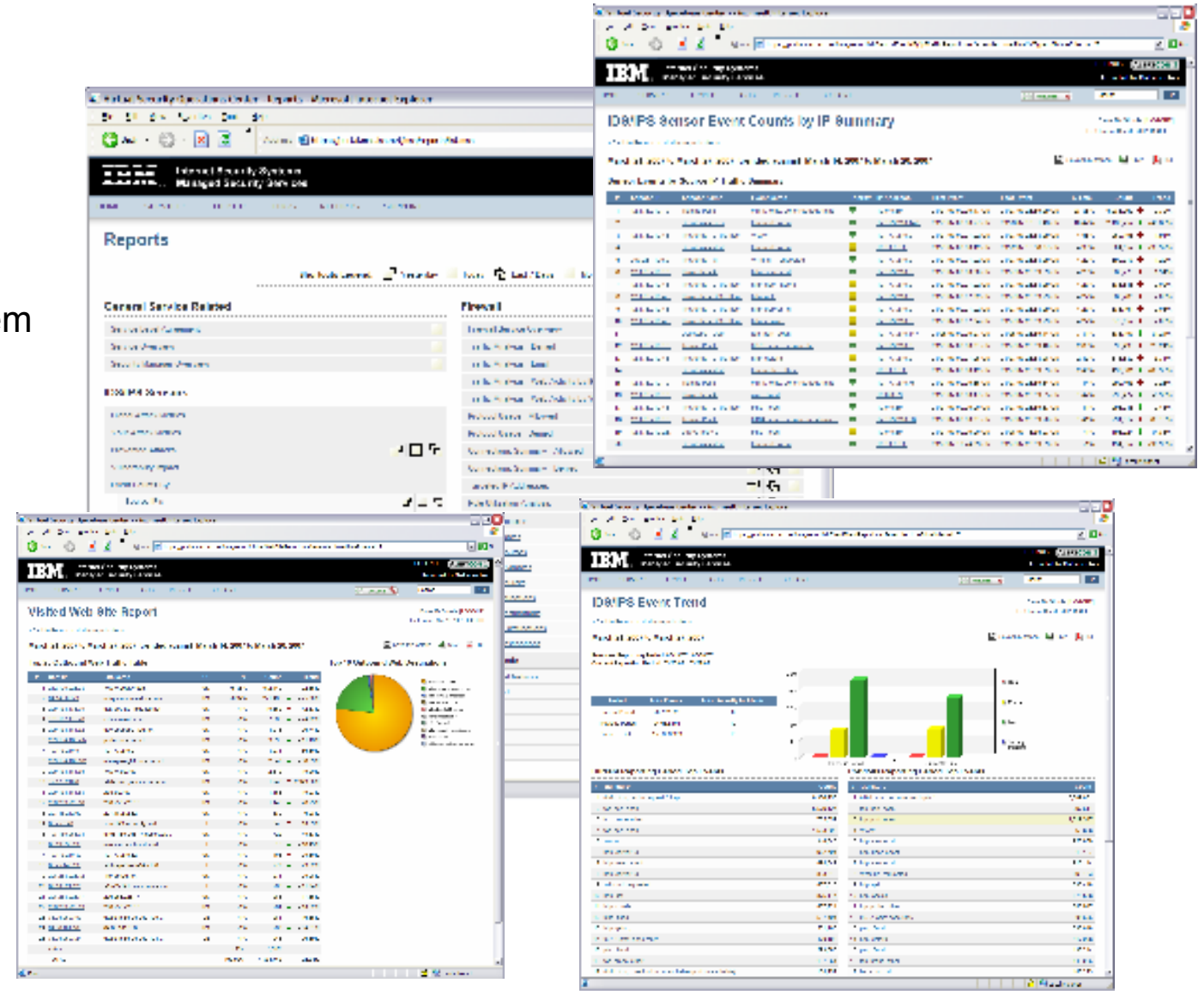
- Armazenamento por até

07 anos !!



Relatórios

- Mais de 20 tipos de **relatórios**
- Podem ser gerados em HTML, CSV e PDF

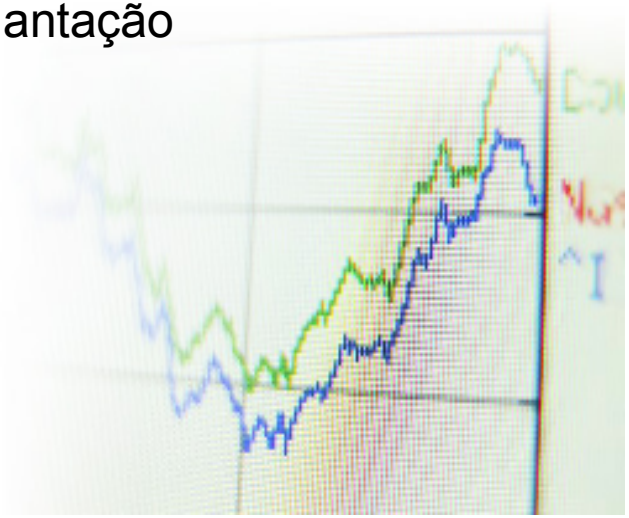


Como o MSS da IBM ISS pode lhe ajudar

Como podemos ajudá-lo

Resultados para o Negócio

- **Integrando** seu ambiente *multi-vendor* e provendo uma **visão centralizada** de suas condições de segurança em tempo-real.
- Auxiliando na **conformidade** com regulamentações
  - **Cobre 6 das 12 categorias PCI: Install firewalls, protect stored data, encrypt data, restrict data access, track and monitor access, test system regularly.**
- Mostrando rapidamente o retorno do investimento – **baixo custo** de implantação / **curtíssimo tempo** de implantação
- Protegendo sua ***marca/reputação***



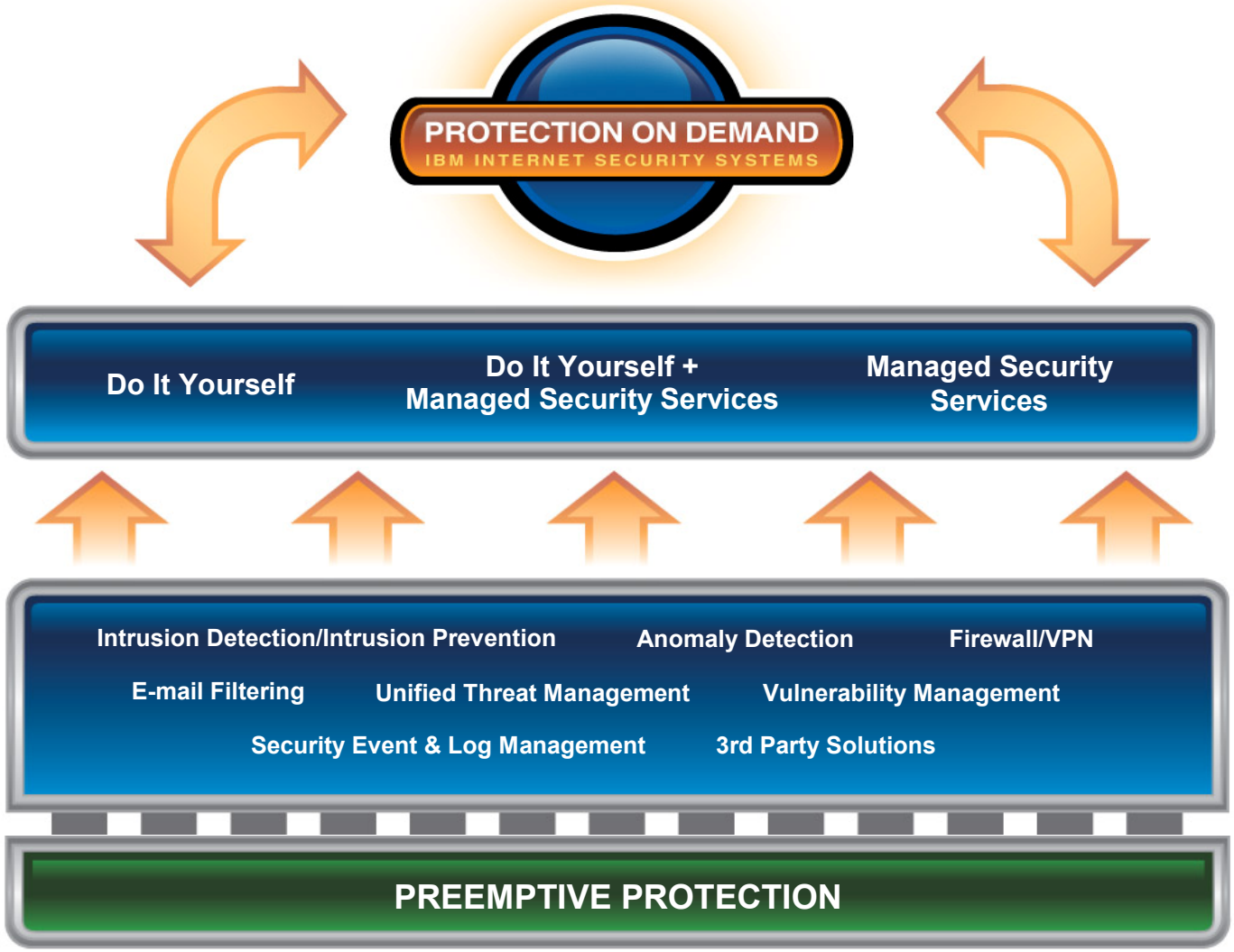
Como podemos ajudá-lo

Redução de Custos

- Evitando ***investimento*** em recursos e tecnologias adicionais
- Reduzindo seu ***custos*** operacionais
- Reduzindo ***perdas*** por incidentes de segurança

Proteção *On Demand*

- **Flexibilidade**
- **Modularidade**
- **Otimização dos custos** de contratação



Obrigado!

IBM Security Forum

Soluções para um ambiente seguro

Fernando Guimarães

feguima@br.ibm.com

Exemplos PCI

- PCI 1.1.1 - A formal process for approving and testing all external network connections and changes to the firewall configuration – Managed Firewall Service
- PCI 6.2 - Establish a process to identify newly discovered security vulnerabilities. Vulnerability Management Service, X-Force Theat Analysis Service
- Implement automated audit trails for all system components to reconstruct:
  - PCI 10.2.4 - Invalid logical access attempts. Security Event & Log Management Service (SELM)
  - PCI 10.2.7 - Creation and deletion of system-level objects. SELM Service