Segurança Conectada para o Mundo

Evandro Rodrigues | Pre-Sales System Engineer

Cibercriminosos já estão ganhando mais dinheiro

Cenário de Ameaças
(IoT, Mobile, SaaS, Virtualization)

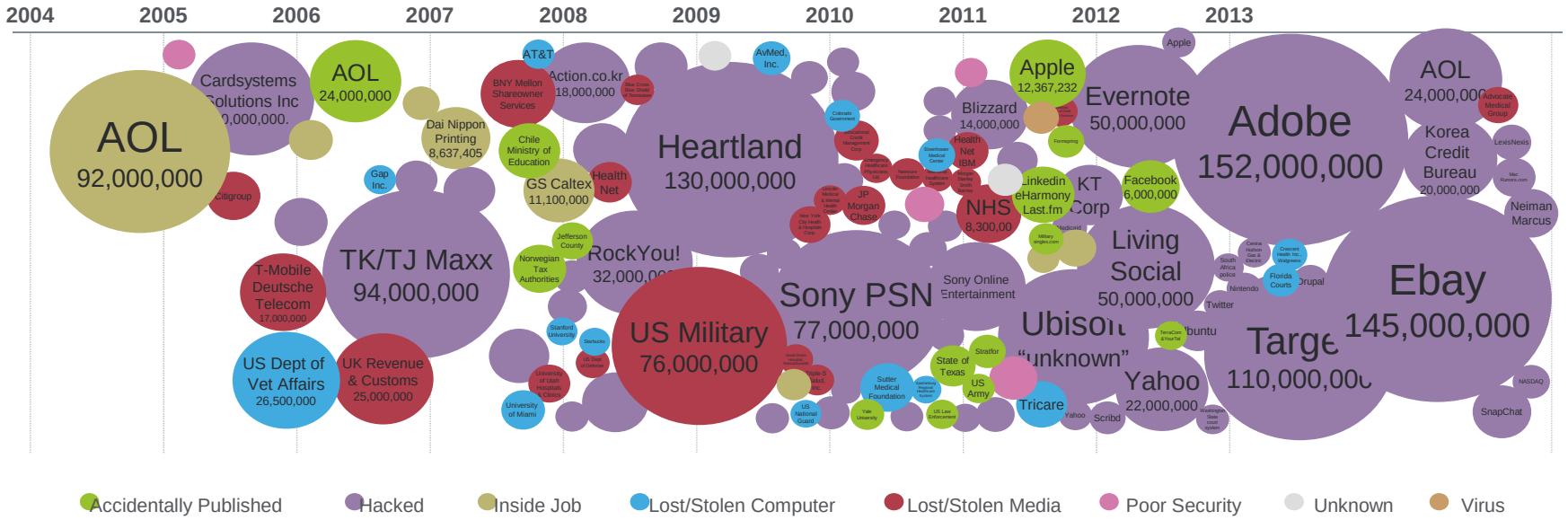
Cenário de Ameaças

387	Novas ameaças por minuto ou mais de 6 novas por segundo
87%	Aumento novas URLs suspeitas em 2014
14%	Aumento do volume de malware em dispositivos móveis em 2014, mais de 20M
347%	Crescimento de malwares desde 2012
+16,000,000	Novas URLs suspeitas em Q4 2014
+8,952,000	Novos assinaturas de códigos maliciosos em 2014
+352,000,000	Amostras de malware únicas no McAfee Labs “Zoo”, Q4 2014

Source: McAfee Labs Threats Report Summary, Feb 2015

Cenário das Ameaças - Impacto

As Maiores Violações de Dados, Global



Source: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Ciber-Segurança Automotiva

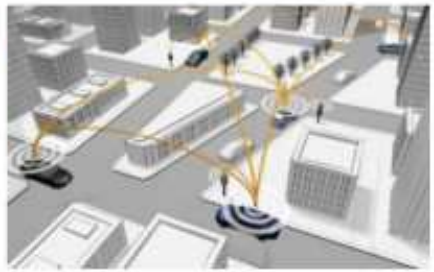
Segurança/Privacidade Pessoal
Área de Redes Pessoais no Carro
Proteja usuário de forma holística através cenário digital

Funções CE e Serviços Web
Pentram no Ambiente
Automotivo

Funções
Migram para
Nuvem

Carro Confiabilidade Integral
Segurança Integrada: Hardware, Software, Serviços

Proteger o Veículo Conectado
Segurança e integridade do Veículo



Carros 2x
Comunicação

Carros mudam de um mostrador no painel para um terminal de Internet das Coisas e Serviços

Ciber-Segurança Automotiva: Ataques Reais*

Emparelhamento Bluetooth

Smartphone explora Vulnerabilidade Bluetooth

Explorar Vulnerabilidade Parser arquivo de mídia (WMA)

Explorar vulnerabilidades no código modem de voz

Sequestro Do dispositivo Wi-Fi

Os Ataques Demonstraram permitir:

- **Controle total sobre os sistemas criticos do veiculo, comando de freio;**
- **Roubo: destravar as portas e ligar o motor sem chaves;**
- **Vigilância: rastrear o carro, gravar e transmitir dados de um microfone interno**

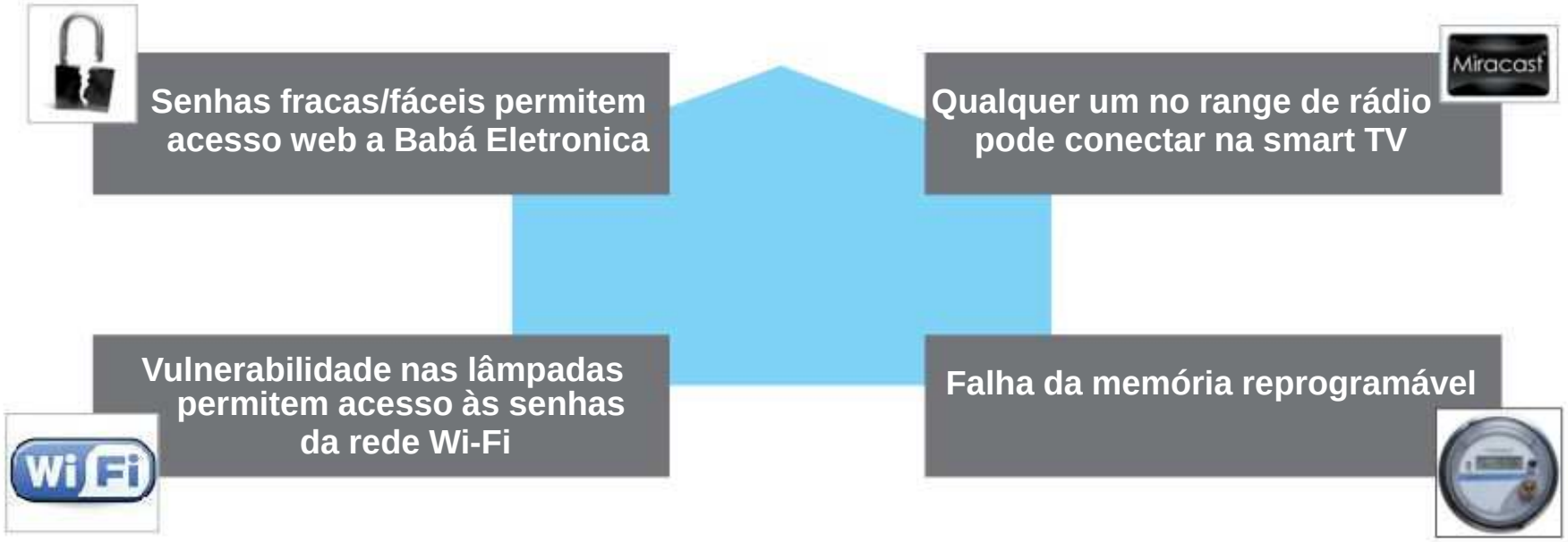
* Koscher et al: “Experimental Analysis of a Modern Automobile,” S&P 2010

Rouf et al: “Security and Privacy Vulnerabilities of In-Car Wireless Networks, USENIX Security,” Aug. 2011

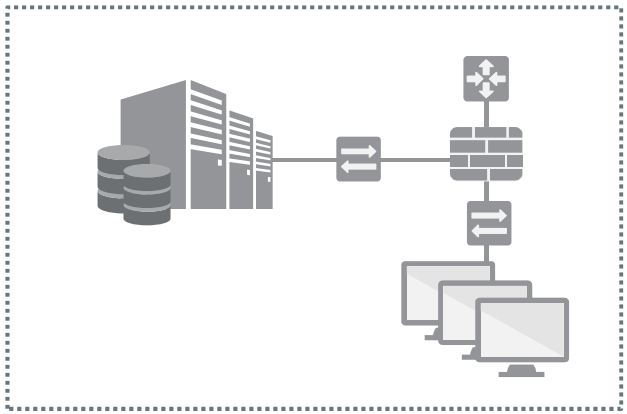
Checkoway et al: “Comprehensive Experimental Analyses of Automotive Attack Surface,” USENIX Security, Aug. 2011

Casas Inteligentes

Casas Inteligentes: Ataques Reais



SaaS – Aplicações indo para a nuvem

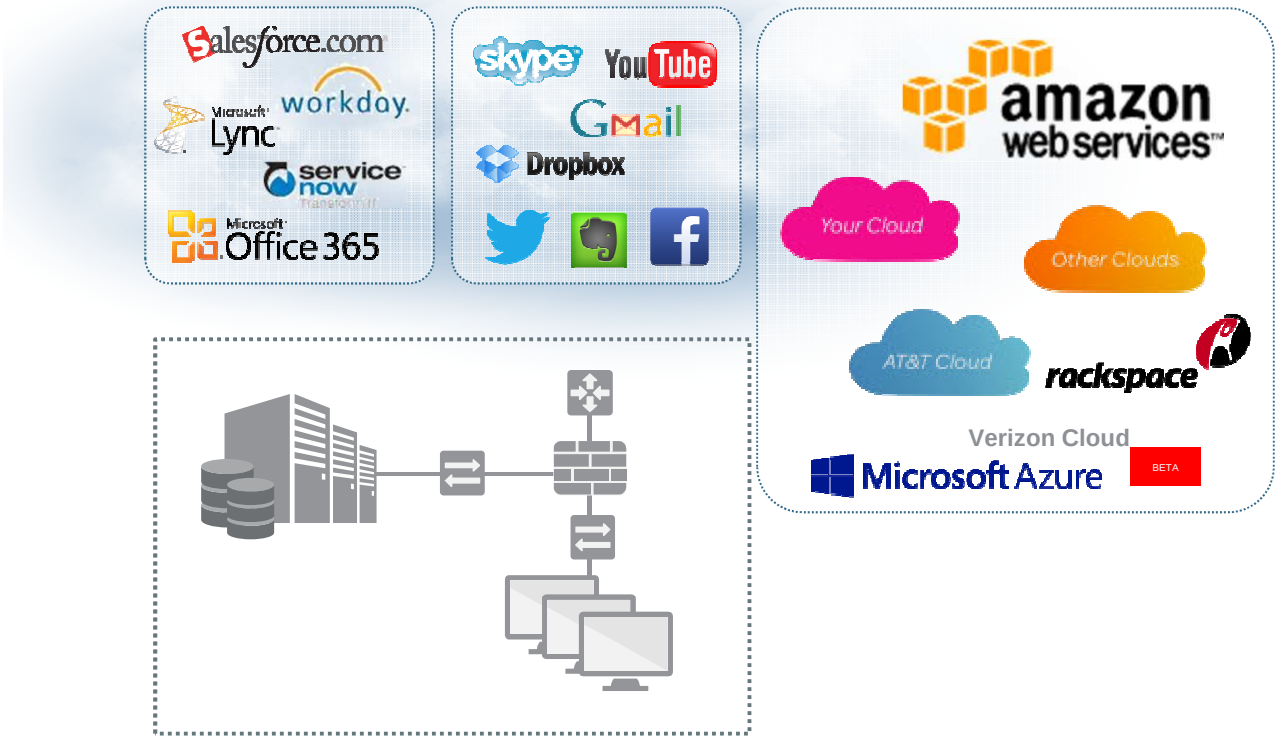


Crescimento SaaS

Mais Pessoas e dispositivos conectados a mais aplicações fora da rede corporativa. Isso significa mais oportunidades de fuga de dados.

Cloud + Virtualização

Serviços em nuvens públicas e privadas



Casos de (in)Sucesso

Casos de (in)Sucesso

Home Depot

- 56 milhões de registros de cartões de crédito
  - Maior perda de dados no varejo até hoje
- Período de 18 meses
- Provável nova variante do “Black PoS”que atingiu a target

http://blog.nuix.com/2014/09/08/blackpos-v2-new-variant-or-different-family/

http://www.forbes.com/sites/katevinton/2014/09/23/data-breach-bulletin-home-depot-ebay-ck-systems-call-of-duty-destiny/

Casos de (in)Sucesso

Sony

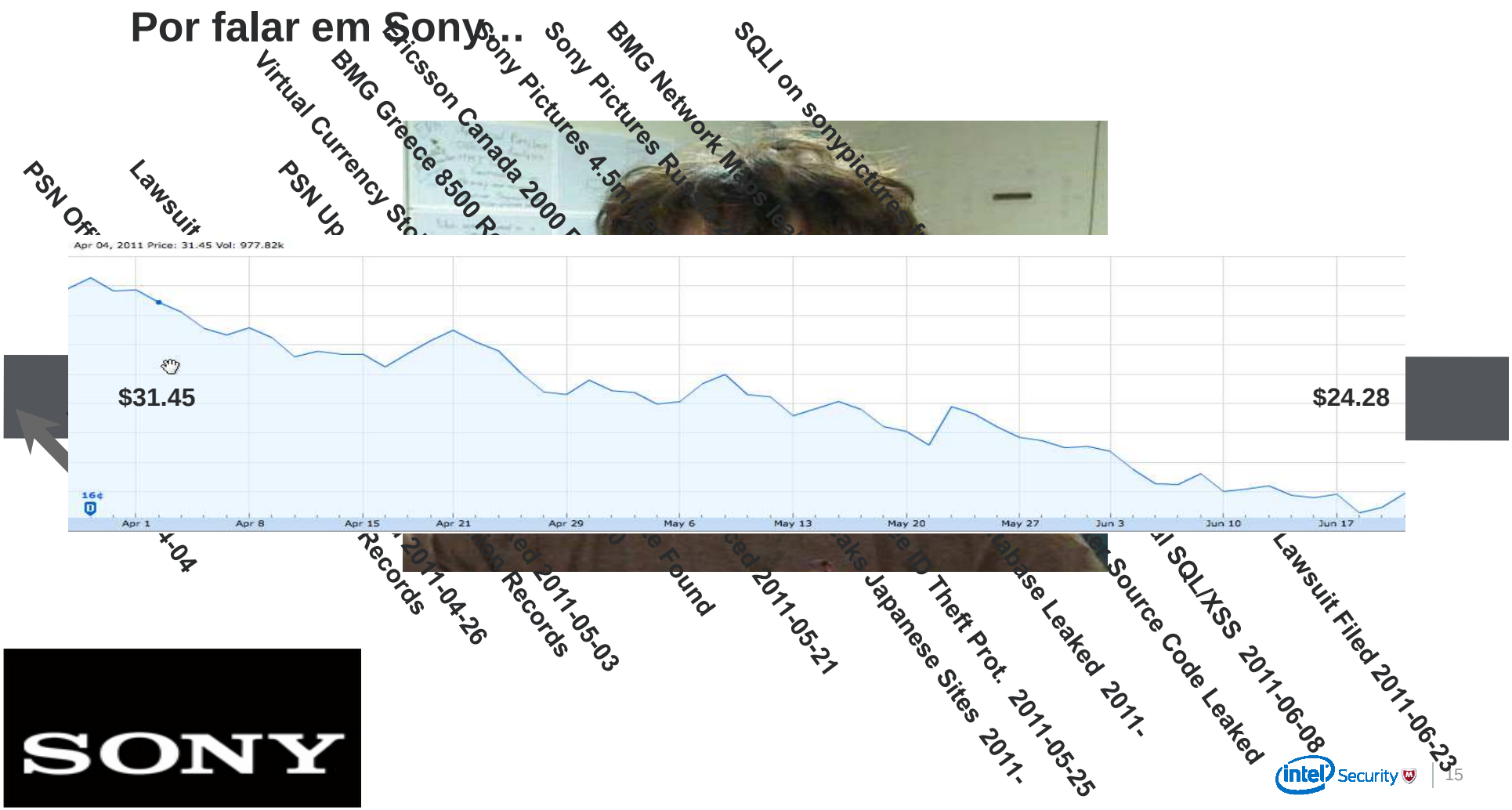
No que pareceu ser uma resposta ao filme “The Interview” um grupo de hackers chamado “Guardians of Peace” atacou a Sony

- 27 de Nov o filme vazou em redes Torrent e P2P
- 2 de Dezembro vazaram salários de 17 executivos
- 47.000 números de SSID com cartões de crédito e Passaportes
- Mais de 100Terabytes de dados roubados

http://deadline.com/2014/12/sony-hack-timeline-any-pascal-the-interview-north-korea-1201325501/

http://www.businessinsider.com/sony-cyber-hack-timeline-2014-12

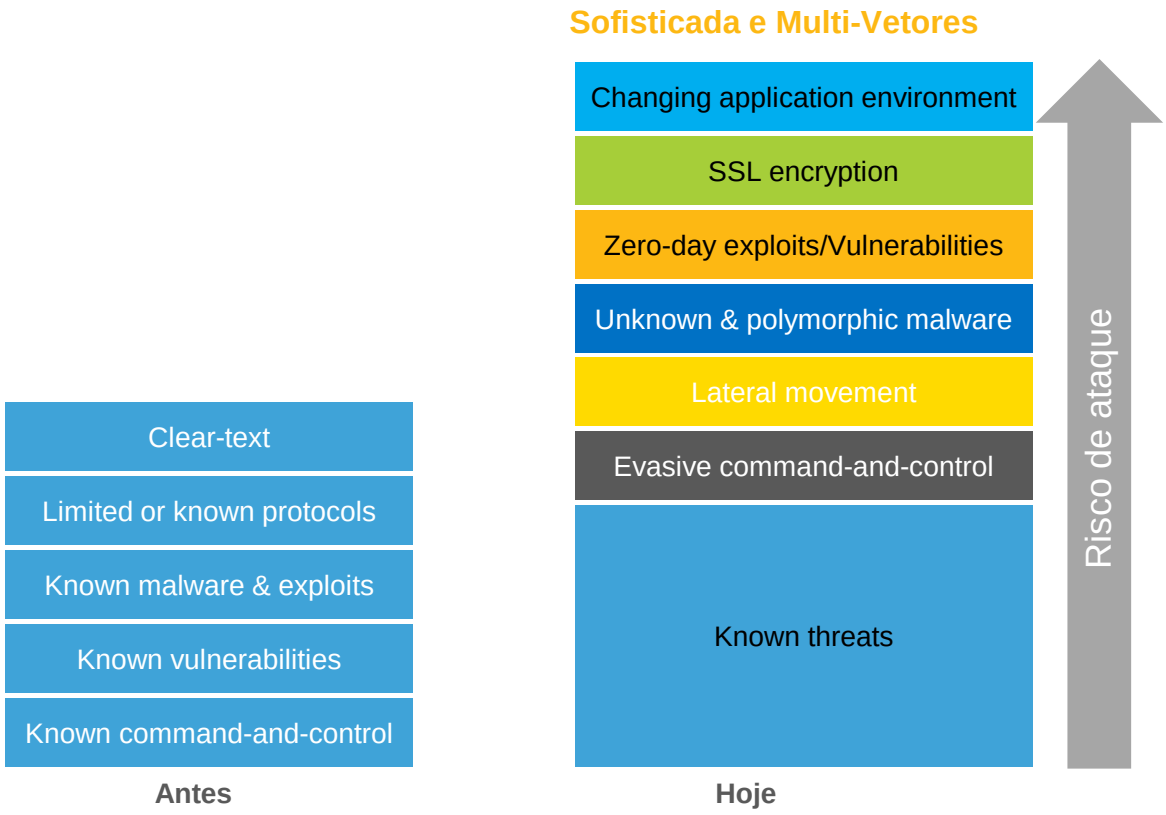
Por falar em Sony...



Hacktivismo

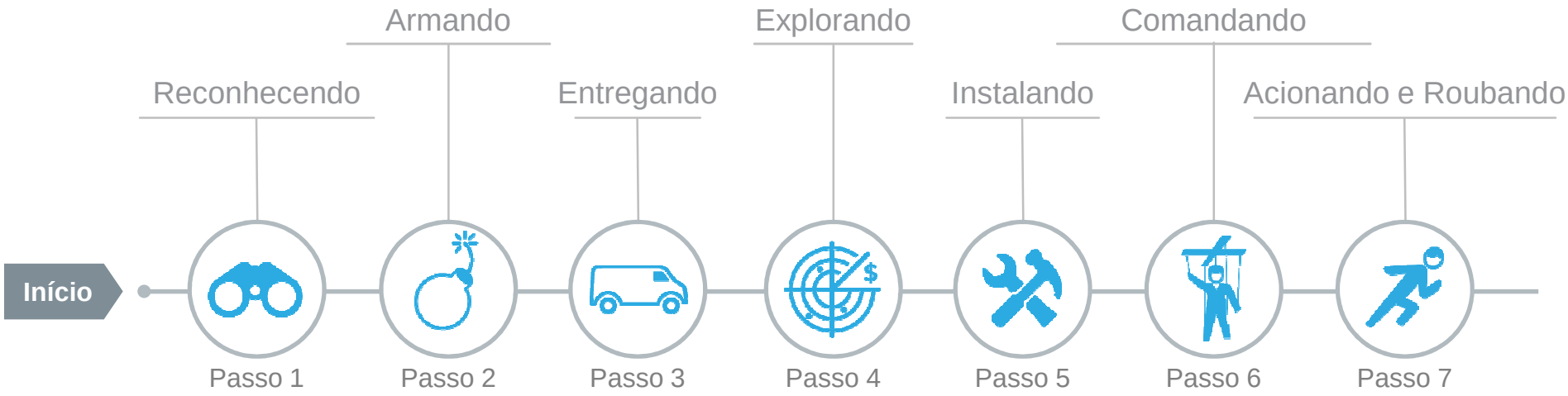
Ameaça como Commodities?

Ferramentas avançadas disponíveis a todos



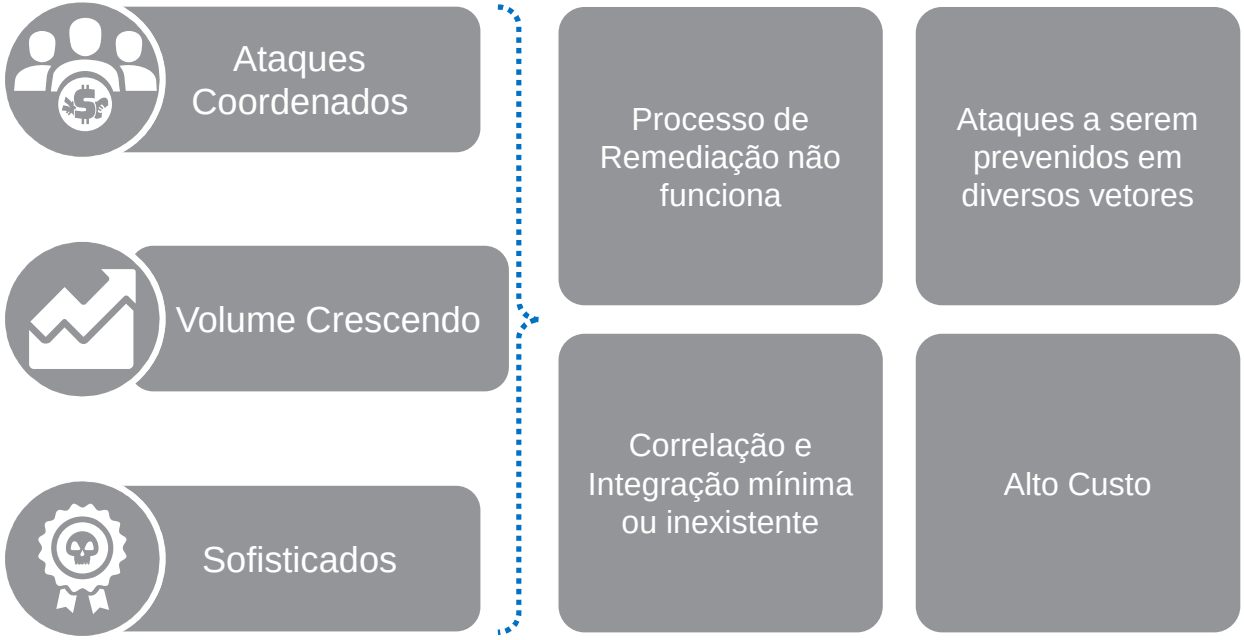
Quem é mais atacado?!

Supply Chain do ataque

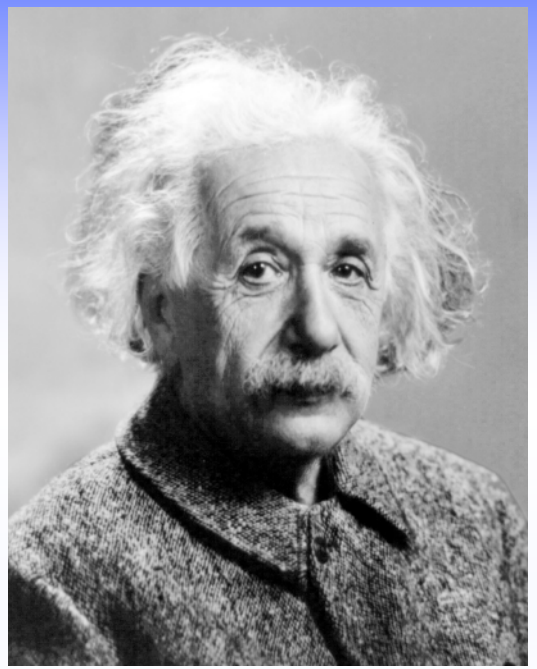


Como se Proteger?
(IPS, Firewall, AV, IDS, Sandbox, WAF)

O Estado Atual de Segurança Corporativa



Desafios do CSO



Albert Einstein

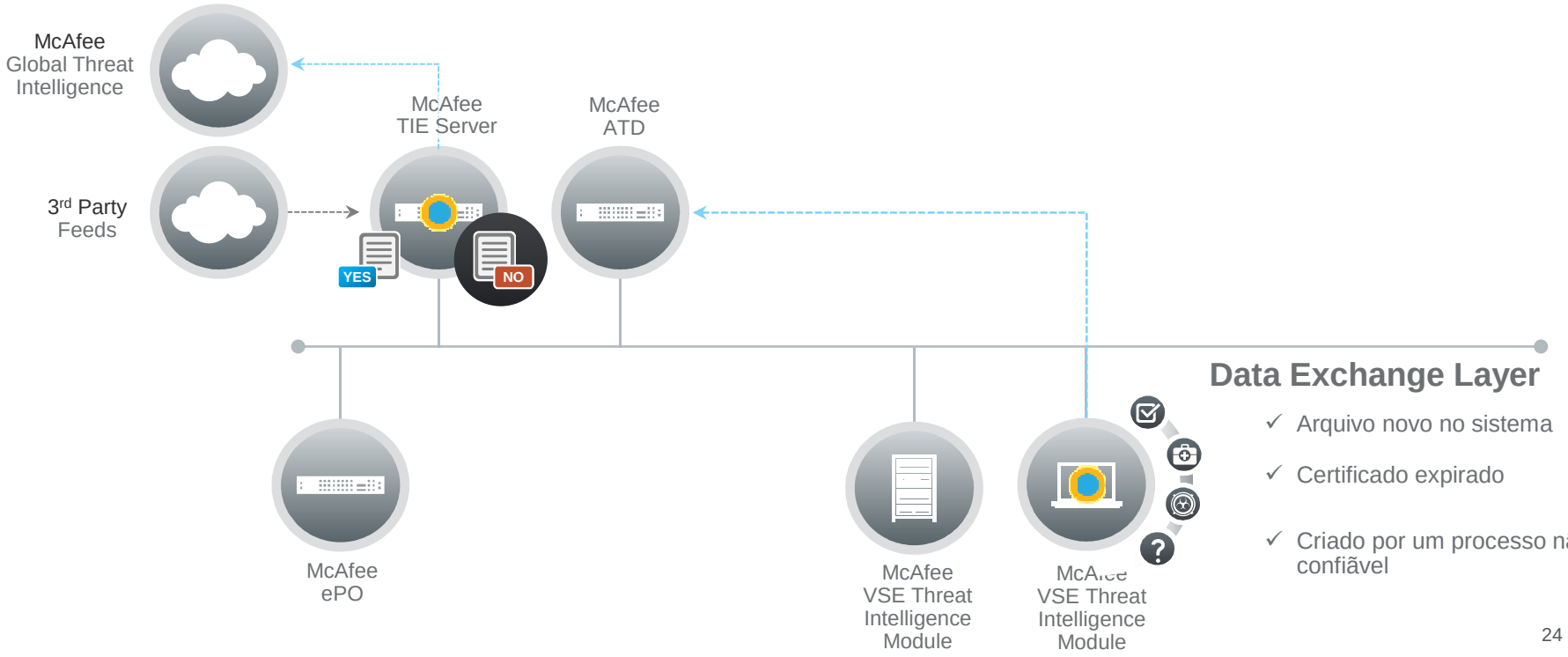
“INSANIDADE:
fazer a mesma coisa
continuamente esperando
resultados diferentes.”

“Não podemos solucionar
nossos problemas com o
mesmo pensamento que
tínhamos quando os criamos.”

intel Security

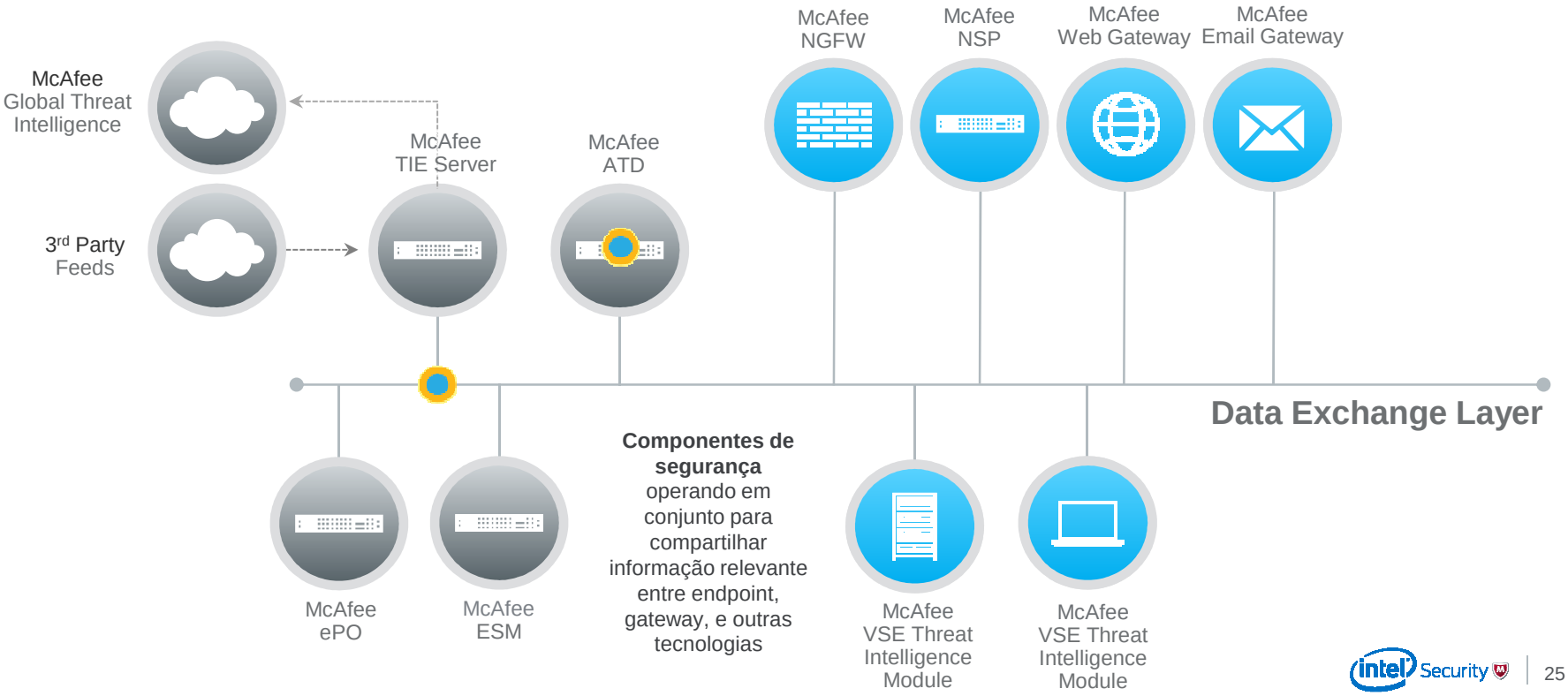
Segurança Conectada

Segurança Conectada – em Ação

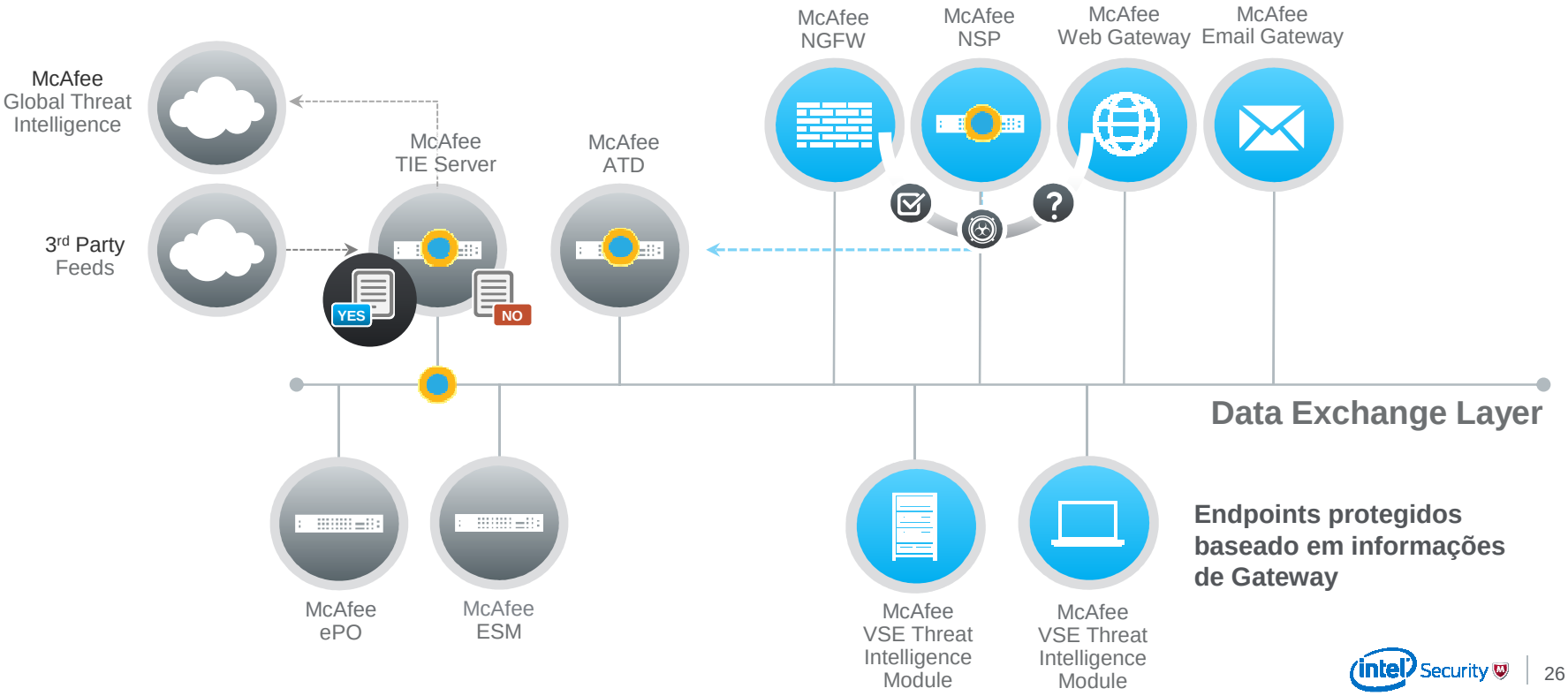


Segurança Conectada – em Ação

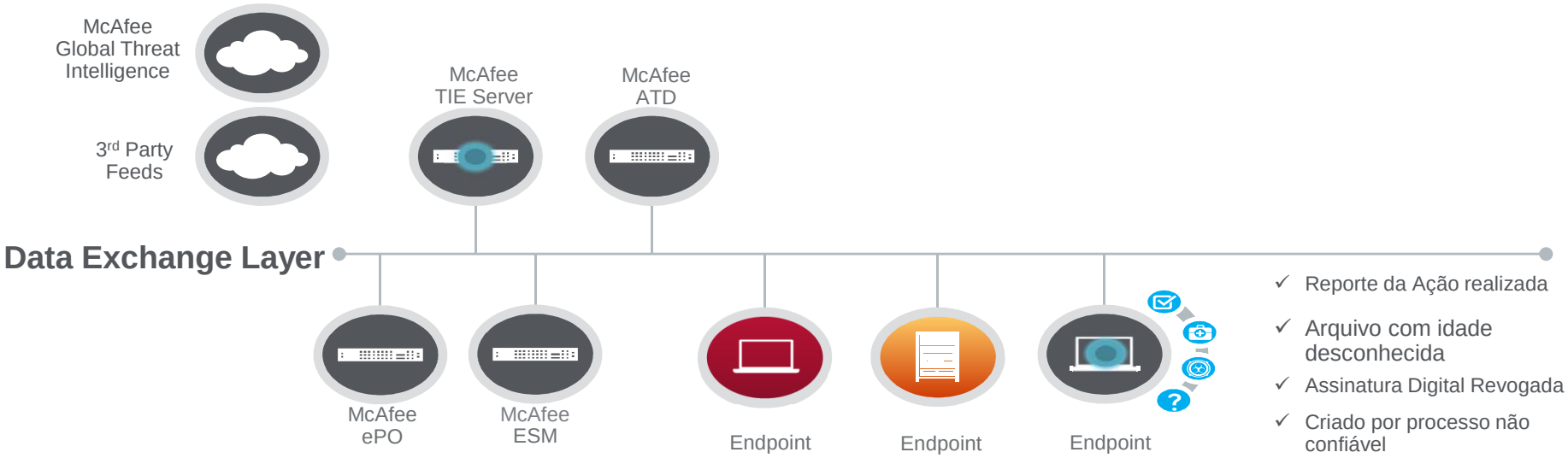
Gateway gerando bloqueios baseado em informações vindas do Endpoint



Segurança Conectada – em Ação



Segurança Conectada – em Ação



27


intel
Security