



---

# Segurança Conectada para o Mundo

---

Evandro Rodrigues | Pre-Sales System Engineer



Cibercriminosos já estão ganhando mais dinheiro

do que o 28º maior país do mundo





---

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

---



## Cenário de Ameaças

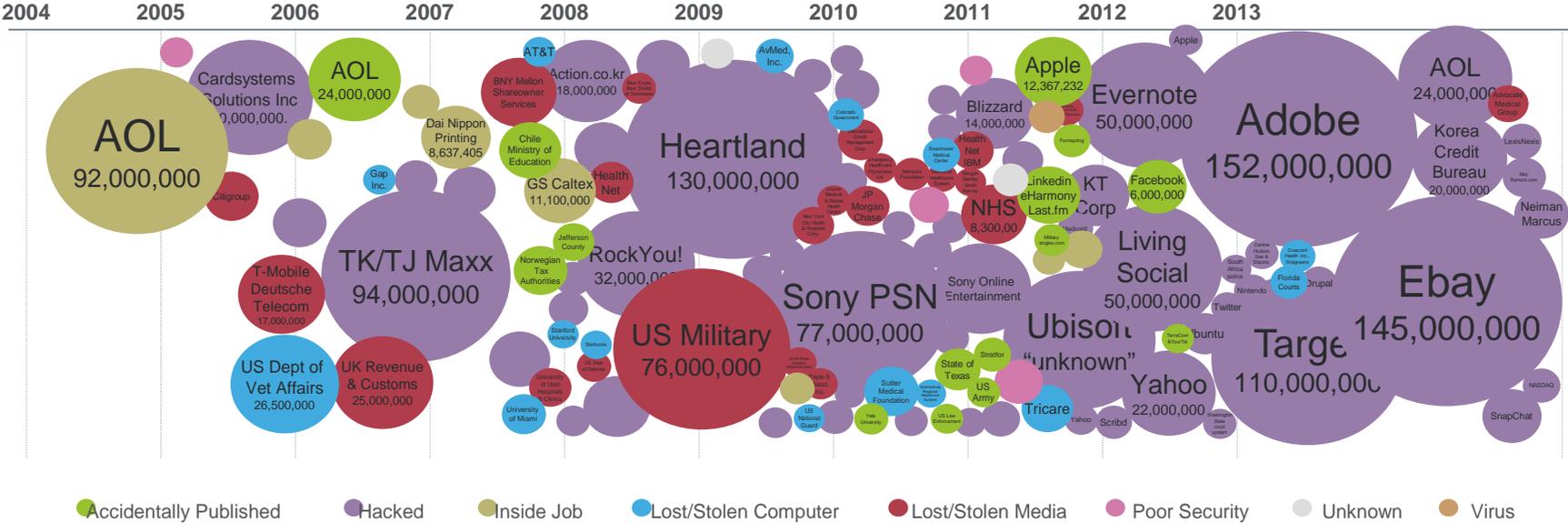
<b>387</b>	Novas ameaças por minuto ou mais de 6 novas por segundo
<b>87%</b>	Aumento novas URLs suspeitas em 2014
<b>14%</b>	Aumento do volume de malware em dispositivos móveis em 2014, mais de 20M
<b>347%</b>	Crescimento de malwares desde 2012
<b>+16,000,000</b>	Novas URLs suspeitas em Q4 2014
<b>+8,952,000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

Source: McAfee Labs Threats Report Summary, Feb 2015

McAfee Confidential

# Cenário das Ameaças - Impacto

## As Maiores Violações de Dados, Global



Source: <http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>  
McAfee Confidential

# Ciber-Securança Automotiva



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



Funções CE e Serviços Web  
Penetram no Ambiente  
Automotivo

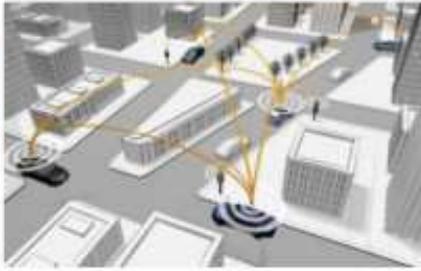


Funções  
Migram para  
Nuvem



**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-Securança 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 críticos do veículo, 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

## Privacidade e Integridade dos Dados

Novos Serviços:

- Tratamento médico em casa
- Gerenciamento de Energia

Acesso e Ações Autorizados,  
Proteção de Dados



## Conteúdo e Entretenimento

Transmissão de Conteúdo Interativo e comunicações.

Controle Parental, Controle de Restrição de Dispositivo, Incluindo Camera, Audio



## Rede Local Doméstica

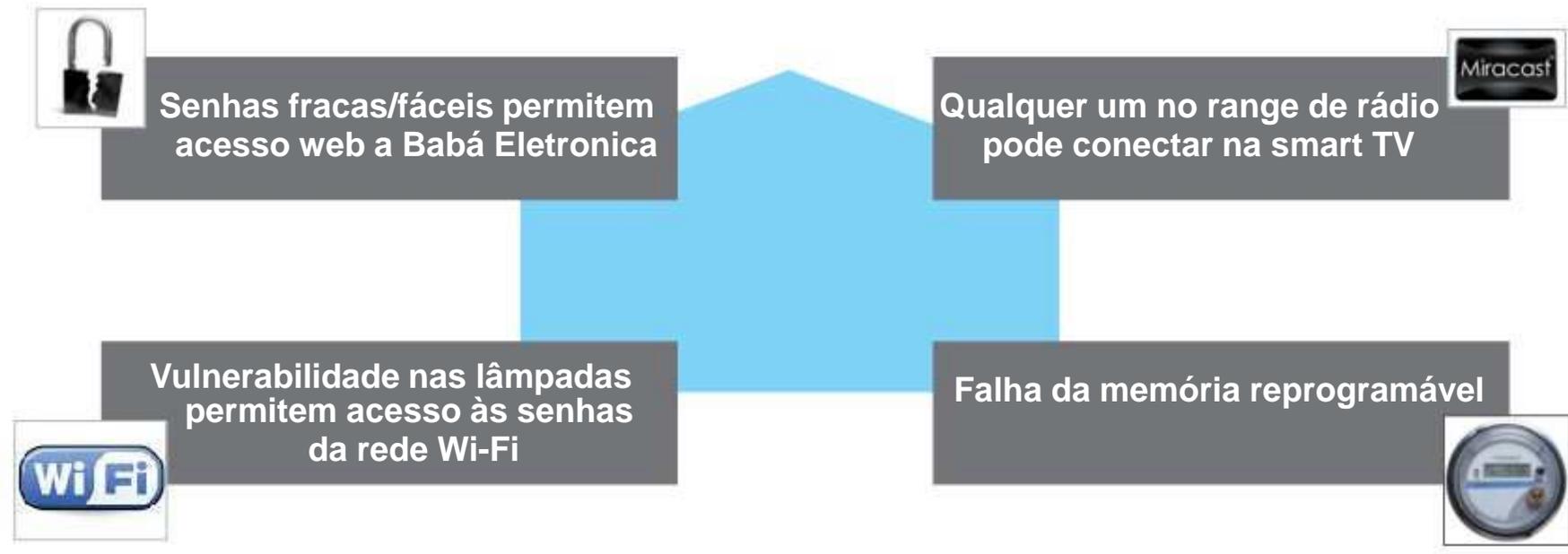
### Segurança dos Dispositivos Conectados:

Rede Local, Gateway, Dispositivos Inteligentes

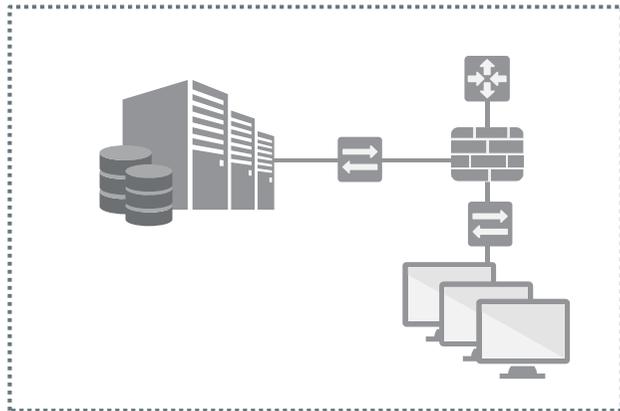
Proteção para Rede e Dispositivos



# Casas Inteligentes: Ataques Reais



# SaaS – Aplicações indo para a nuvem

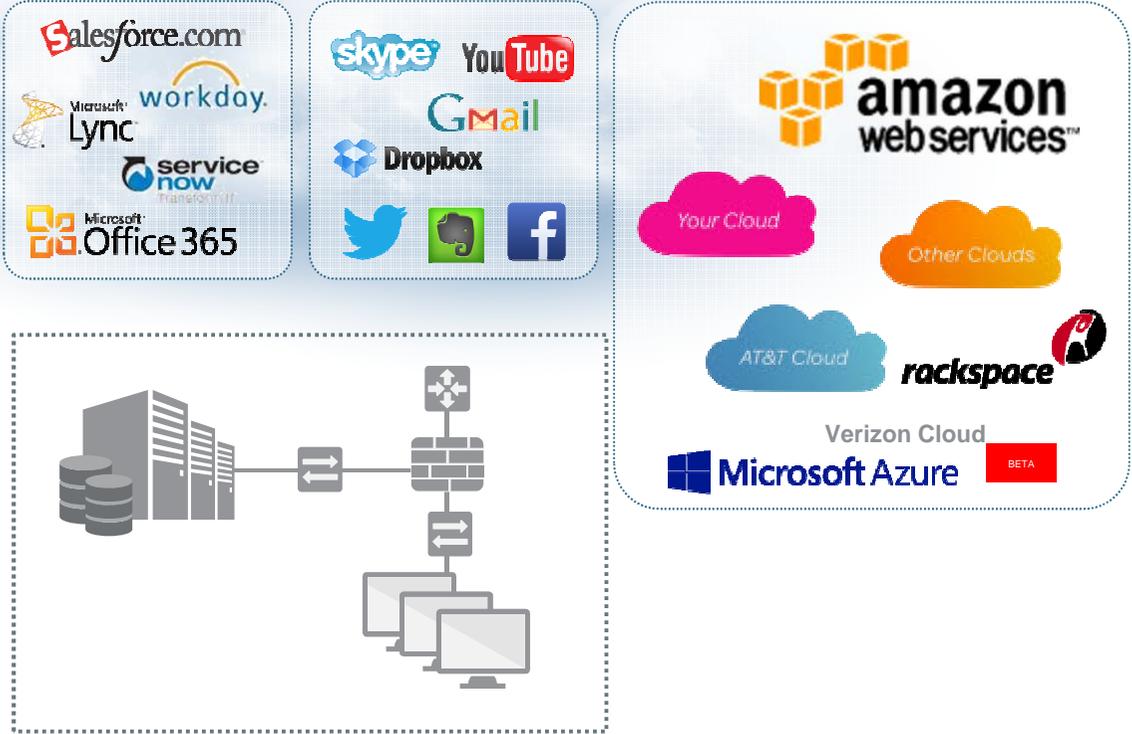


## Crescimento SaaS

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/>

McAfee Confidential



# 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>

McAfee Confidential



# Por falar em Sony...

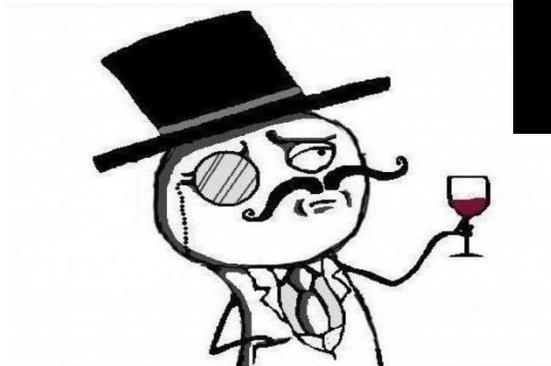
PSN Off  
Lawsuit  
Virtual Currency Str  
PSN Up  
Ericsson Canada 2000 R  
BMG Greece 8500 R  
Sony Pictures 4.5m  
BMG Network Maps Le  
SQLI on sonypictures

Apr 04, 2011 Price: 31.45 Vol: 977.82k



4-04  
Records  
2011-04-26  
Records  
2011-05-03  
Found  
2011-05-21  
Japanese Sites 2011-  
Database Leaked 2011-  
Source Code Leaked  
SQL/XSS 2011-06-08  
Lawsuit Filed 2011-06-23

# Hacktivismo

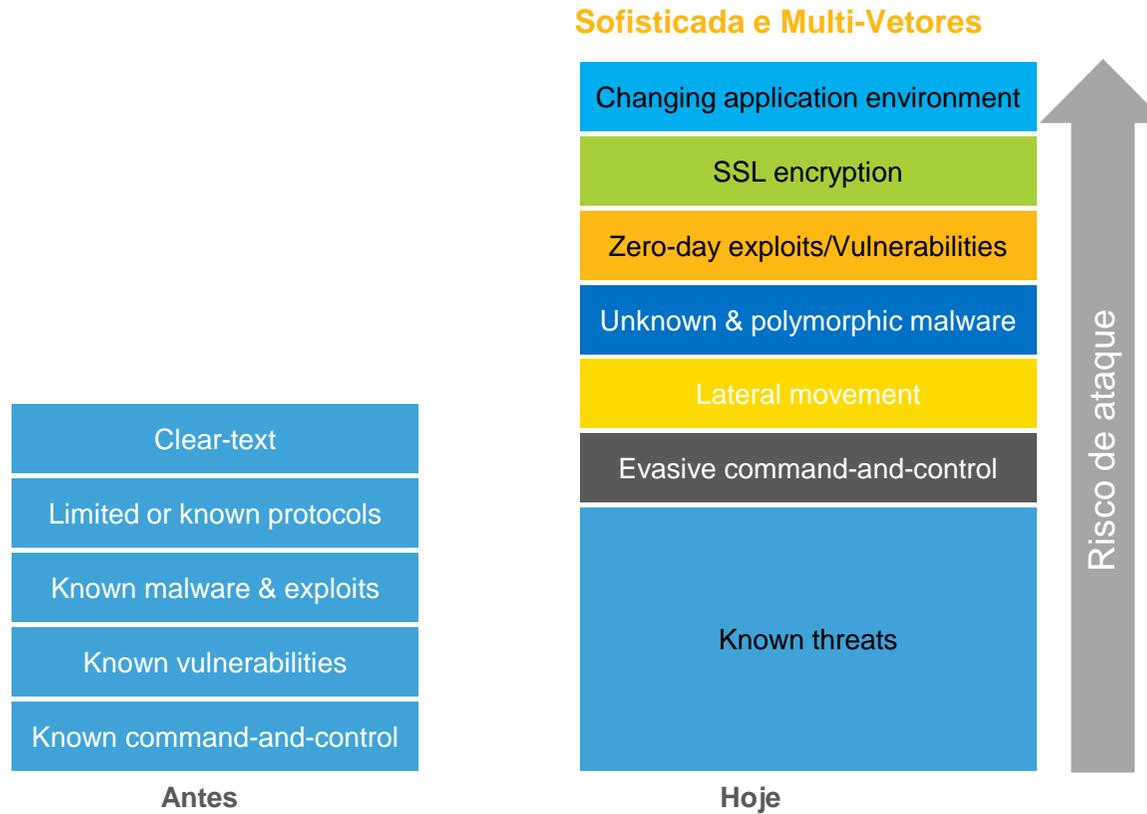


McAfee Confidential



# Ameaça como Commodities?

Ferramentas avançadas disponíveis a todos



# Quem é mais atacado?!

## 5 Most Attacked Industries

Attack rates can differ greatly between industries. **How does yours compare?**



Manufacturing

**26.5%**



Finance & Insurance

**20.9%**



Information & Communication

**18.7%**



Health & Social Services

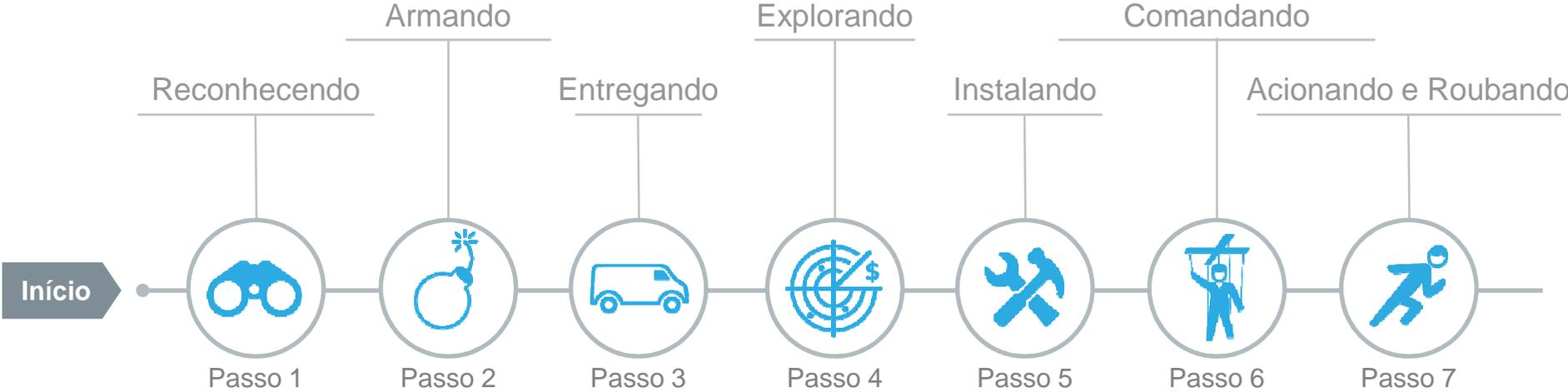
**7.3%**



Retail & Wholesale

**6.6%**

# Supply Chain do ataque





---

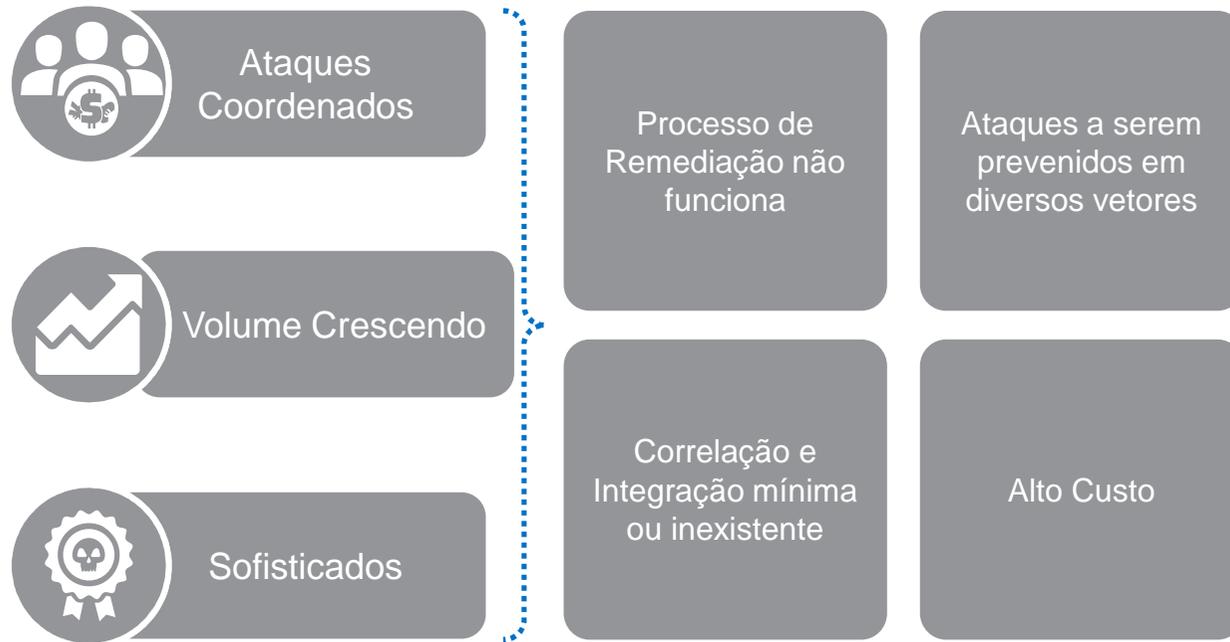
## Como se Proteger?

(IPS, Firewall, AV, IDS, Sandbox, WAF)

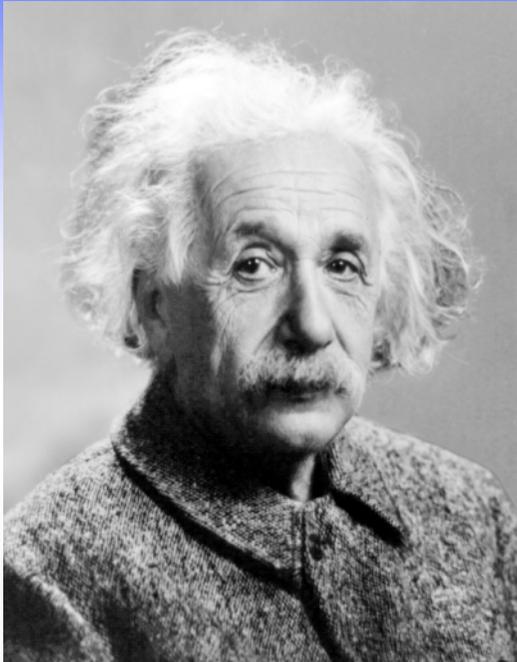
---



# 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.”

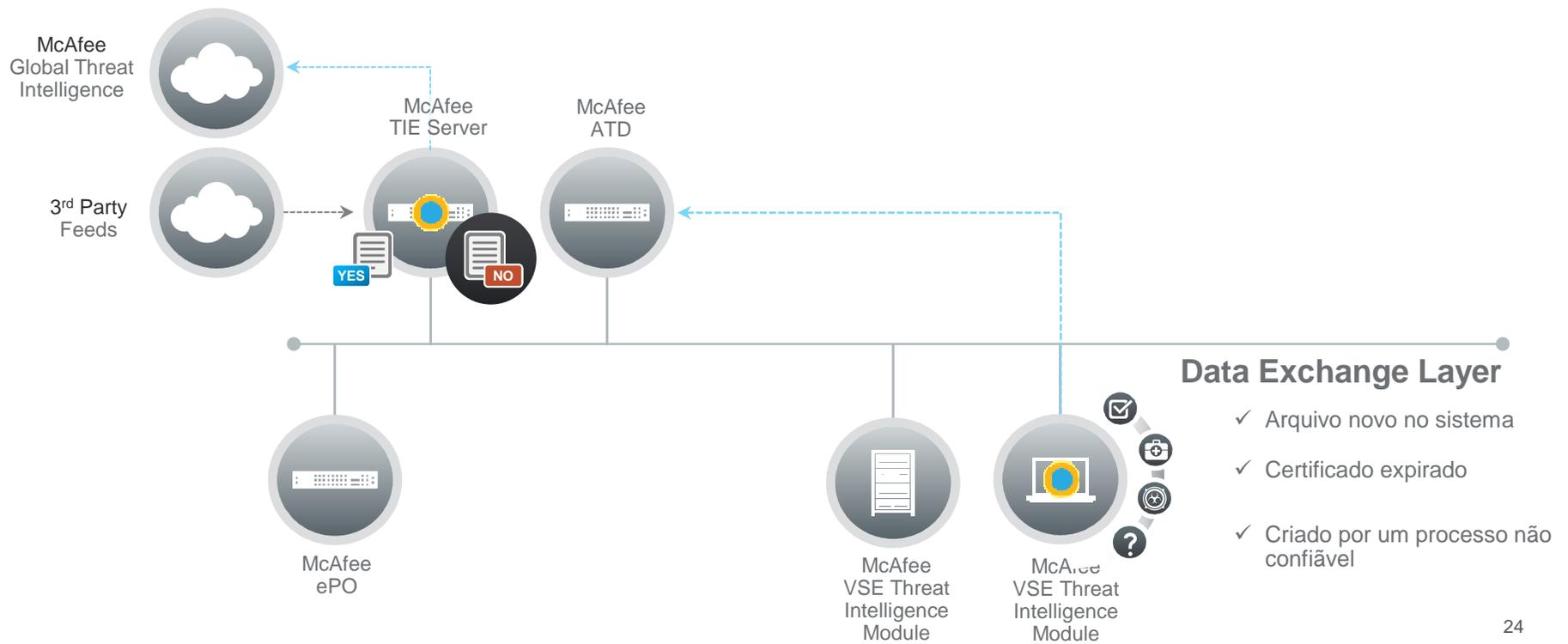


---

Segurança Conectada

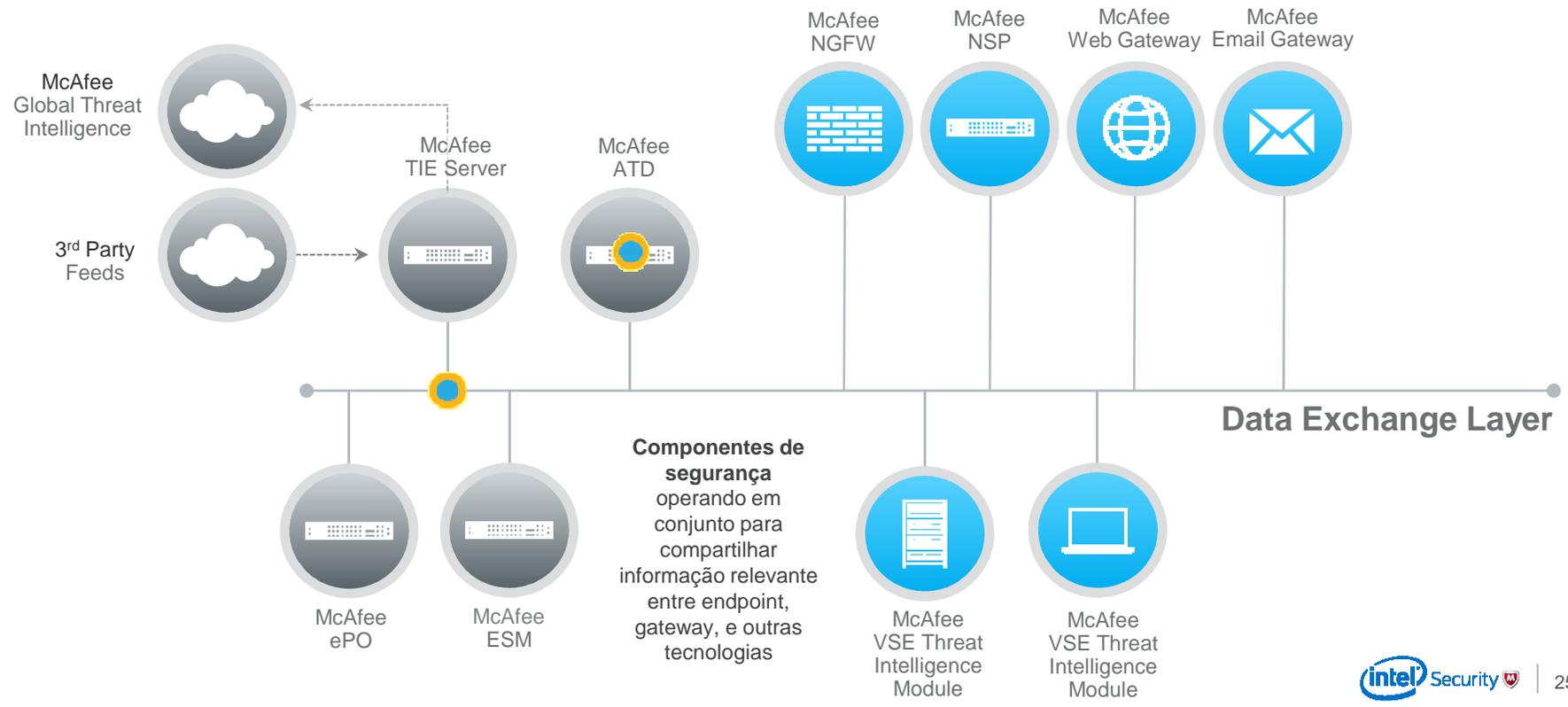


# Segurança Conectada – em Ação

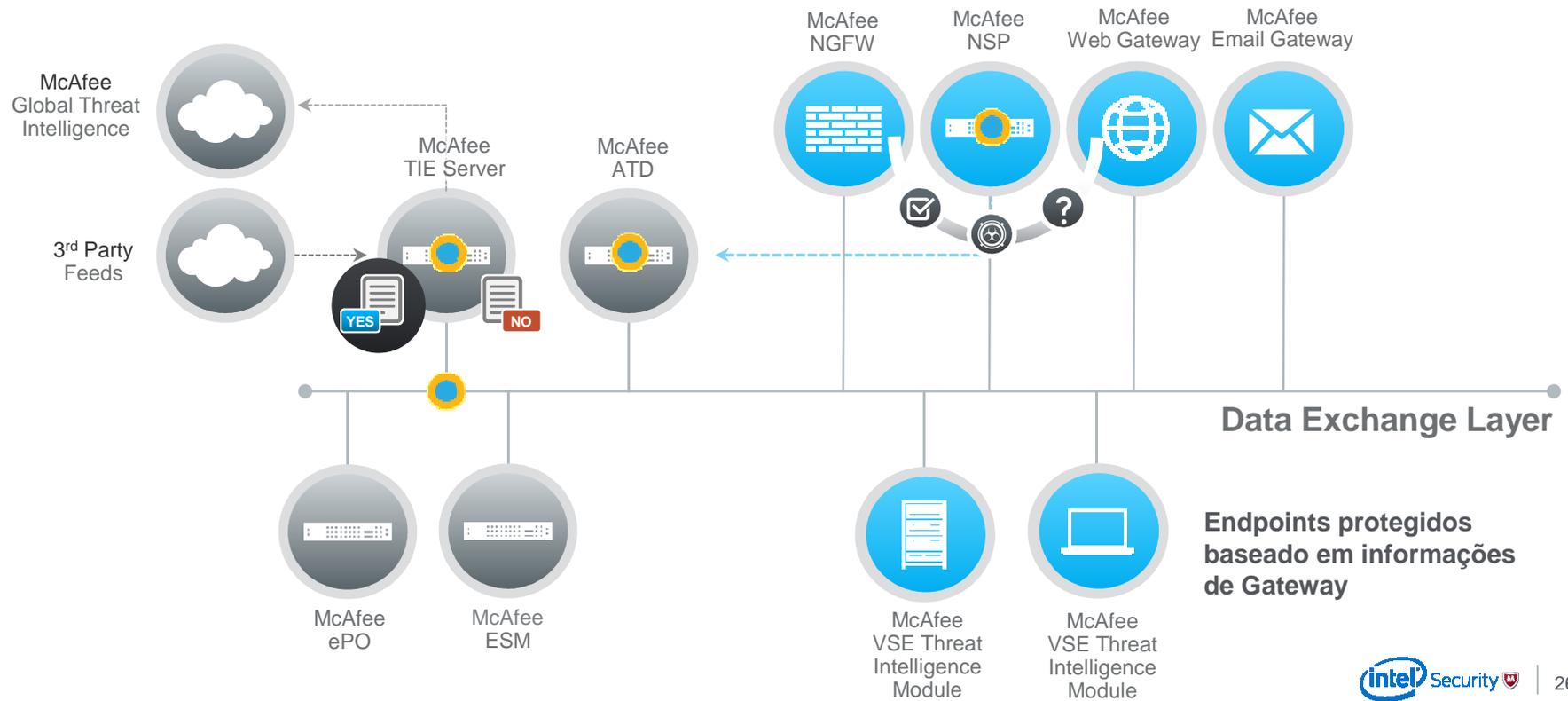


# Segurança Conectada – em Ação

Gateway gerando bloqueios baseado em informações vindas do Endpoint



# Segurança Conectada – em Ação



# Segurança Conectada – em Ação

