



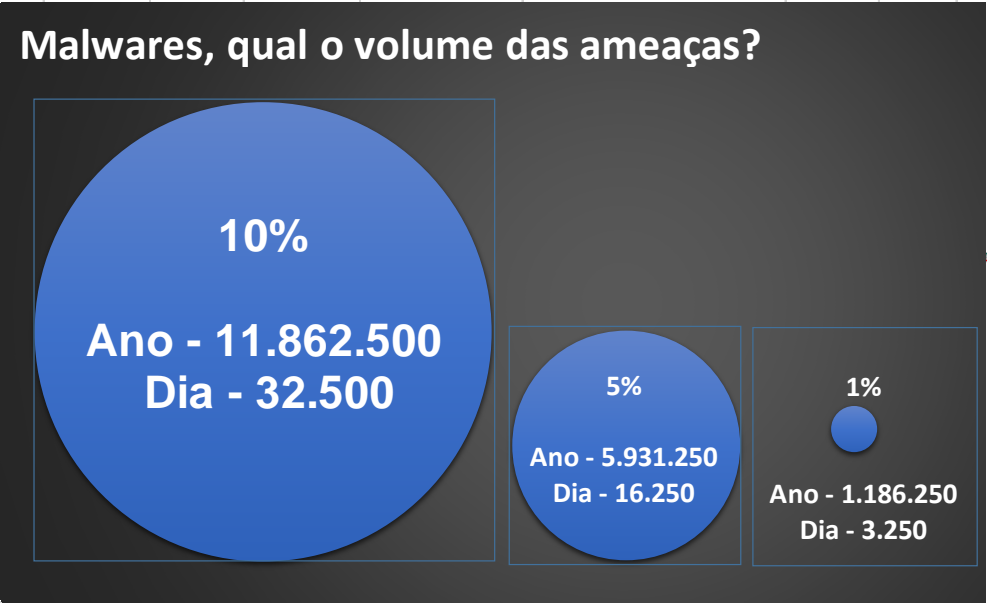
# HPE Security Meeting



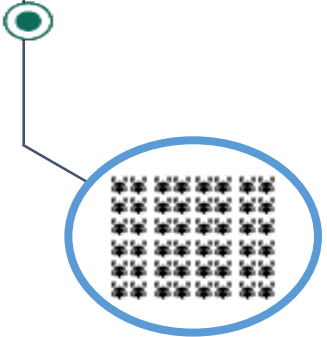
**Hewlett Packard  
Enterprise**

SOLUÇÕES QUE VALORIZAM  
E IMPULSIONAM SEU NEGÓCIO.  
[SOLONETWORK.COM.BR](http://SOLONETWORK.COM.BR)

# Quantos malwares são criados em um dia?



**2015**  
**325,000**  
 AMOSTRAS UNICAS POR DIA



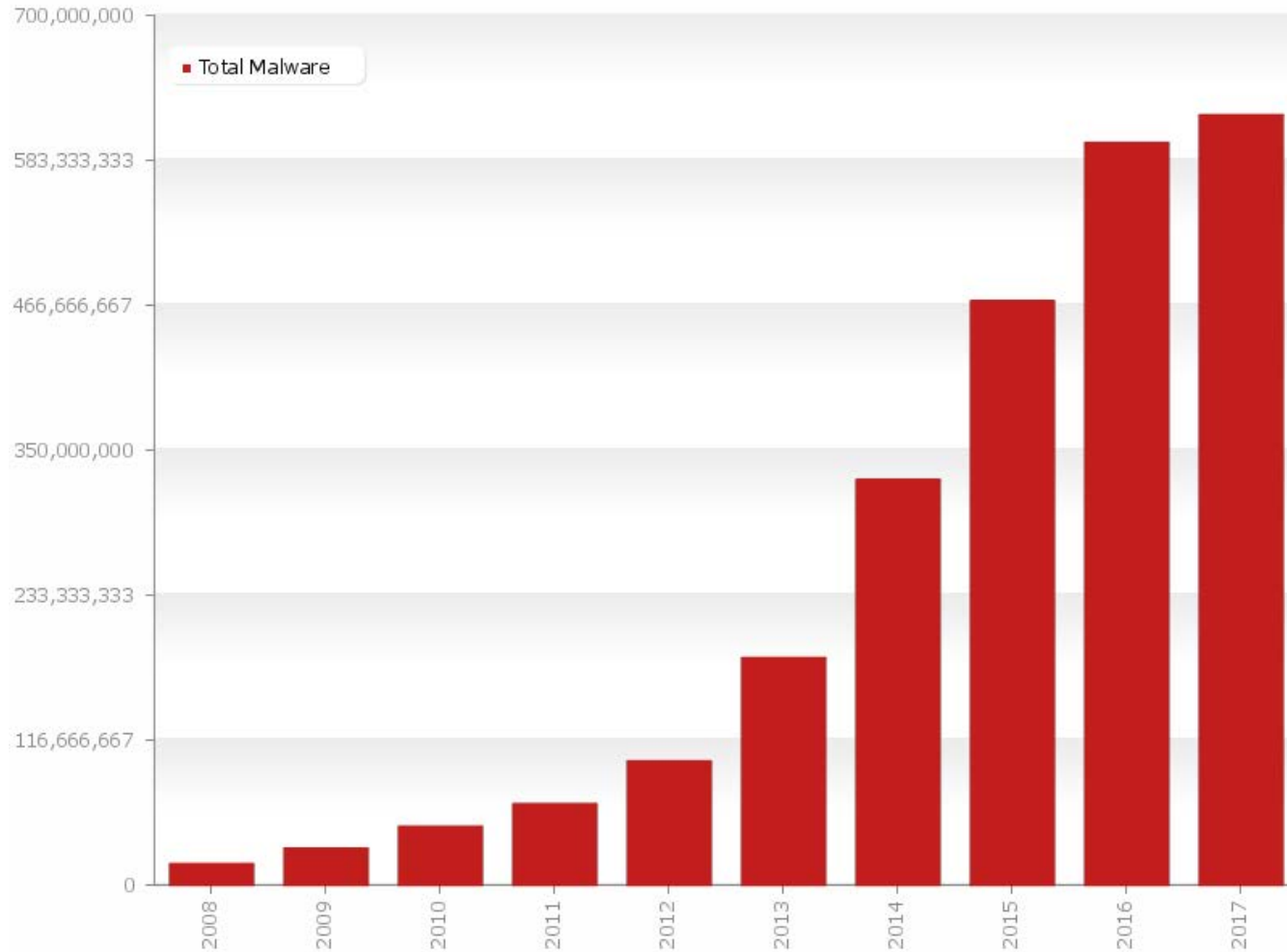
Produto	Taxa	Não Detectado
Kaspersky	99.9%	-
F-Secure	99.8%	114 975
BitDef. - McAfee	99.7%	229 950
Avast	99.4%	574 875
Eset - Baidu	98.6%	1 494 675
Sophos - AVG	98.1%	2 069 550
TrendMicro	95.1%	5 518 800
Microsoft	86.3%	15 636 600

AV-Comparatives  
 File Detection - March 2015

**Malwares, qual o volume das ameaças?**

Porcentagem	Ano	Dia
10%	11.862.500	32.500
5%	5.931.250	16.250
1%	1.186.250	3.250

# Quantos malwares são criados em um dia?



Last update: 03-20-2017 10:38

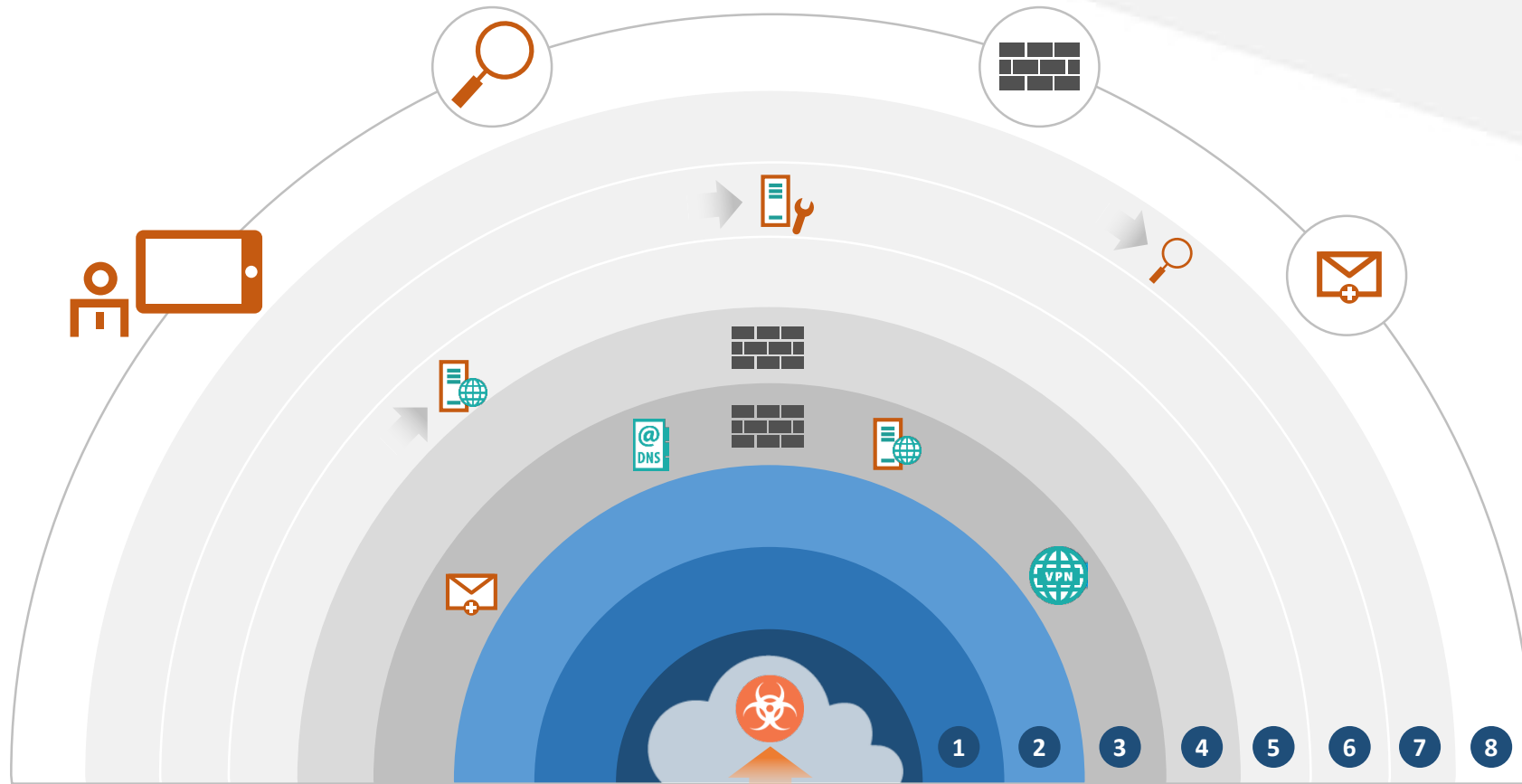
Copyright © AV-TEST GmbH, www.av-test.org

**AV-TEST**  
The Independent IT-Security Institute

Segundo o AV-TEST, o instituto registra mais de **390.000** novos programas maliciosos todos os dias.

[av-test.org/en/statistics/malware/](http://av-test.org/en/statistics/malware/)

# Segurança de perímetro não é suficiente

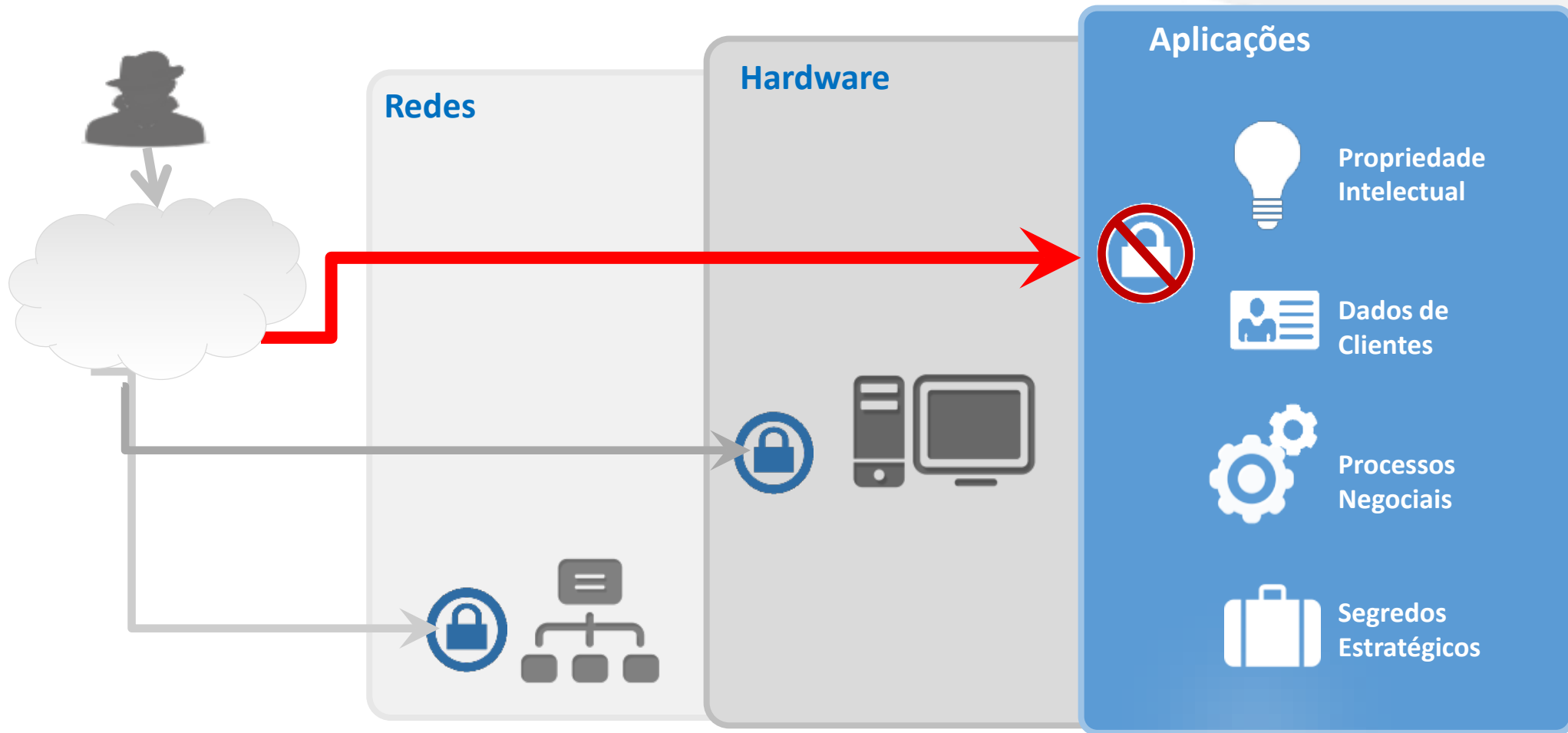


**Proporção de Investimento entre Perímetro e Aplicação é de 23-para-1**

- Gartner Maverick Research: Stop Protecting Your Apps; It's Time for Apps to Protect Themselves (2014)

# Proteção de Aplicações

## 84% das invasões acontecem pela Camada Aplicação



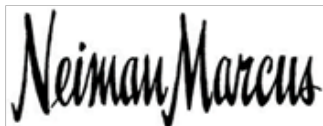
# Ciclo de vida de um ataque



# Grandes vazamentos de dados continuam a ocorrer... ...mesmo com grandes investimentos em segurança e conformidade



2015



2014



2013



2013



2011



2009



2017



2009 e 2015



2017

Segundo estudos da IBM X-Force, os custos de uma violação de dados per capita foi em média R\$175, chegando a casos de R\$233.



# Data Protection

SOLUÇÕES QUE VALORIZAM  
E IMPULSIONAM SEU NEGÓCIO.  
[SOLONETWORK.COM.BR](http://SOLONETWORK.COM.BR)



# Quais os nossos desafios

Impossível estar 100% protegido de todas as vulnerabilidades

Impossível manter tudo atrás dos Firewalls

Os dados devem ser constantemente compartilhados

Porque isso ocorre?

# Quais as opções disponíveis

Muda a estrutura dos dados e das aplicações

7412 2456 7890 0000

Dado totalmente criptografado é inútil se não for bem usado

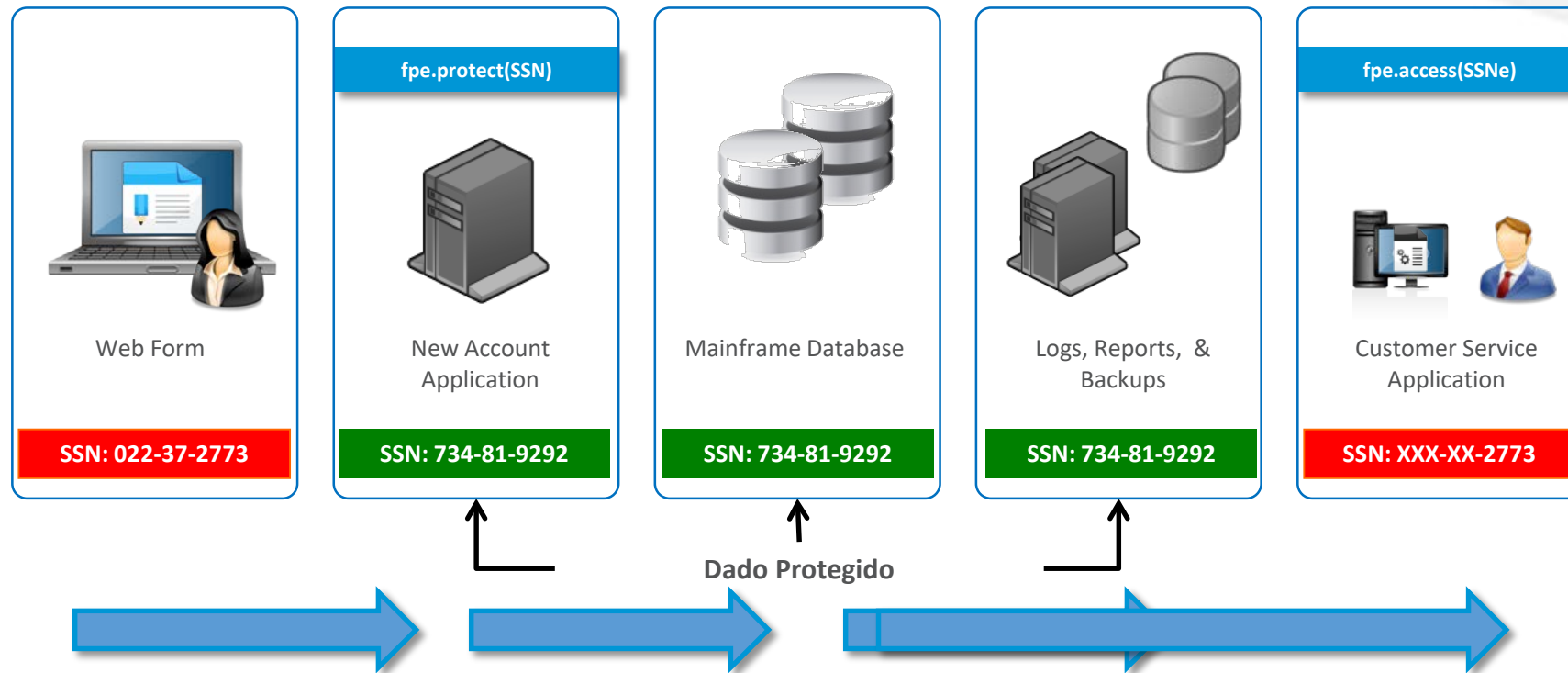
8juYE%Uks&dDFa2345^WFLER

Gerenciamento de chaves é um pesadelo

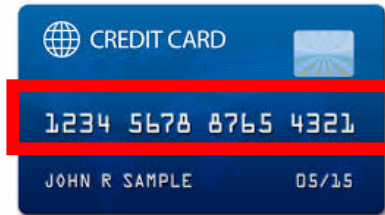
Necessidade de múltiplas soluções, muitas com brechas de segurança

# Mundo ideal

## Dados descaracterizados



# Modelos de proteção existentes



4361 4871 1917 5946

**FPE**

1234 56024342 4321

**Partial FPE**

1234 56116197 4321

**Stateless Token**

1234 56WX4WDL 4321

**eFPE**

1234 56BQDSJHKGZS

**Obviously  
Protected**

XXXXXXXXXXXX 4321

**Masked**

12

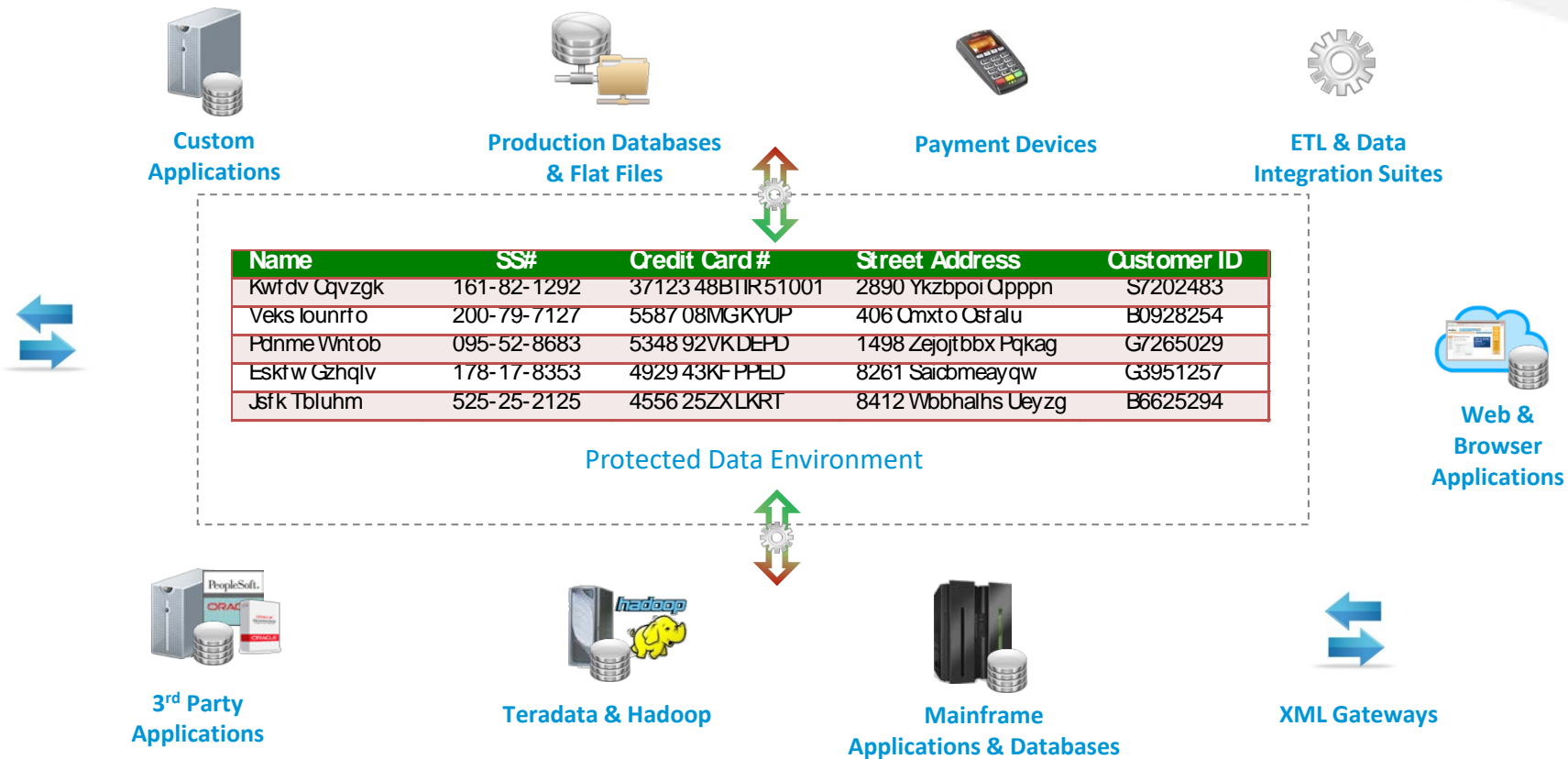
# Mescla dos modelos

Name	SS#	Credit Card #	Street Address	Customer ID
		5 1830	2893 Hamilton Drive	S9298273

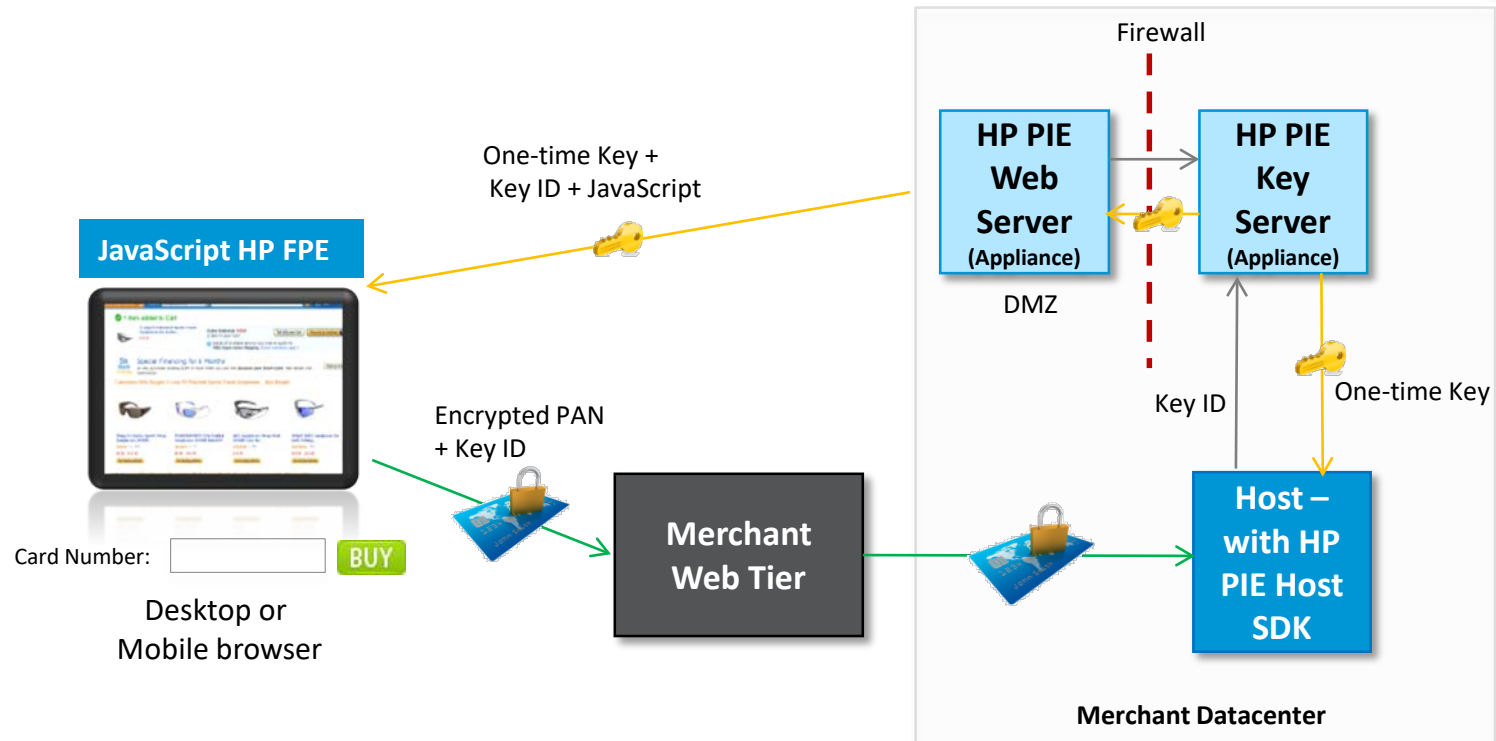


Name	SS#	Credit Card #	Street Address	Customer ID
Kwfdv Cqvzgj	161-82-1292	37123 48BTIR 51001	2890 Ykzbpoi Clpppn	S7202483
Veks lounfo	200-79-7127	5587 08MG KYUP 0139	406 Cmxt0 Osfalu	B0928254
Pdnme Wntob	095-52-8683	5348 92VK DEPD 2829	1498 Zejojtbbx Pqkag	G7265029
Eskfw Gzhqlv	178-17-8353	4929 43KF PPED 4379	8261 Saicbmeayqw Yotv	G3951257
Jsfk Tbluhm	525-25-2125	4556 25ZX LKRT 1830	8412 Wbbhalhs Ueyzg	B6625294

# Utilização dos dados



# E-Commerce como referência





# Desenvolvimento Seguro

SOLUÇÕES QUE VALORIZAM  
E IMPULSIONAM SEU NEGÓCIO.  
[SOLONETWORK.COM.BR](http://SOLONETWORK.COM.BR)



# Custos envolvidos



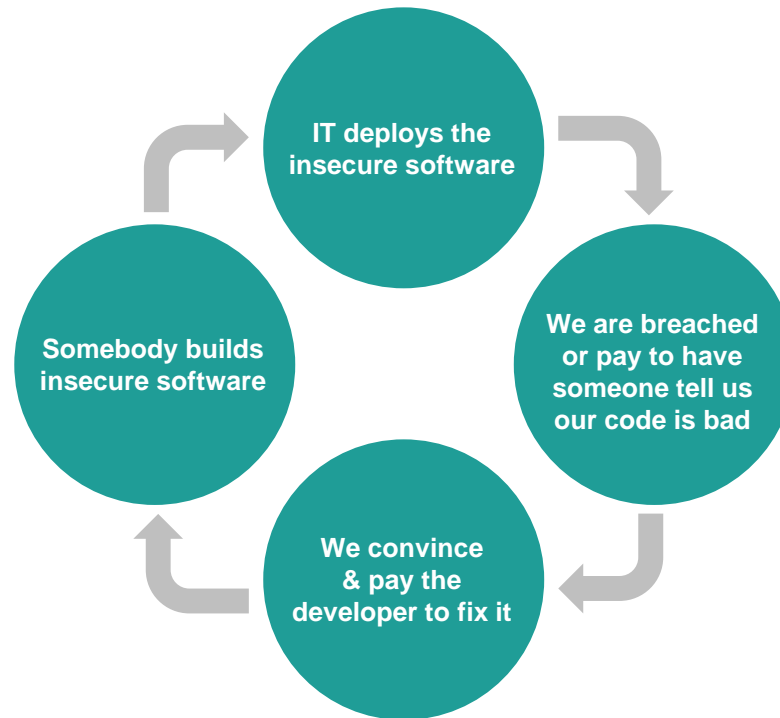
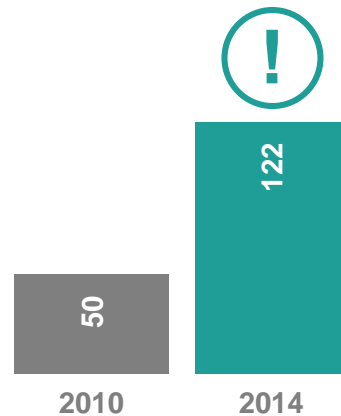
## Costs

Costs and incidence of attacks are high and growing.

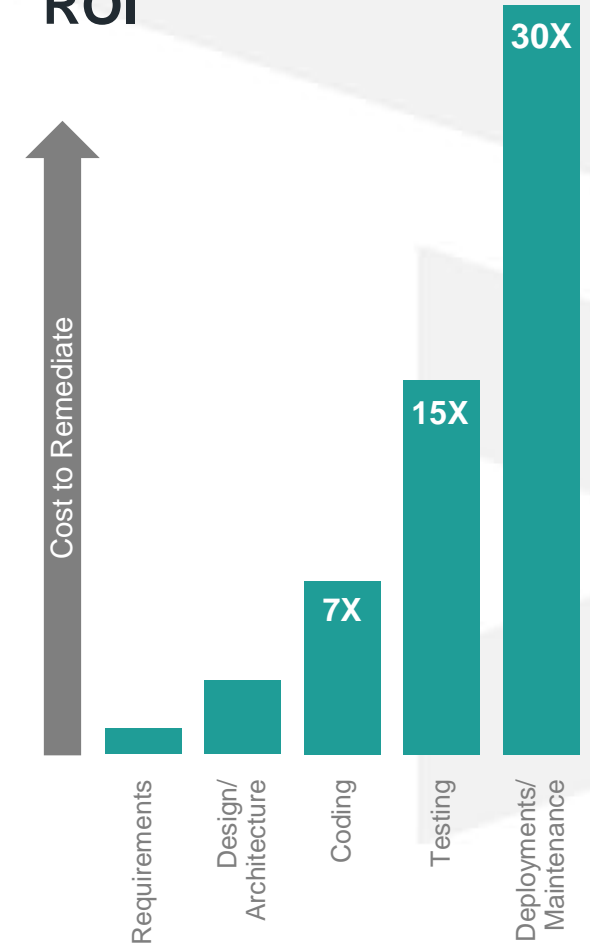
Average cost of cyber crime per company:  
95% increase in 4 years



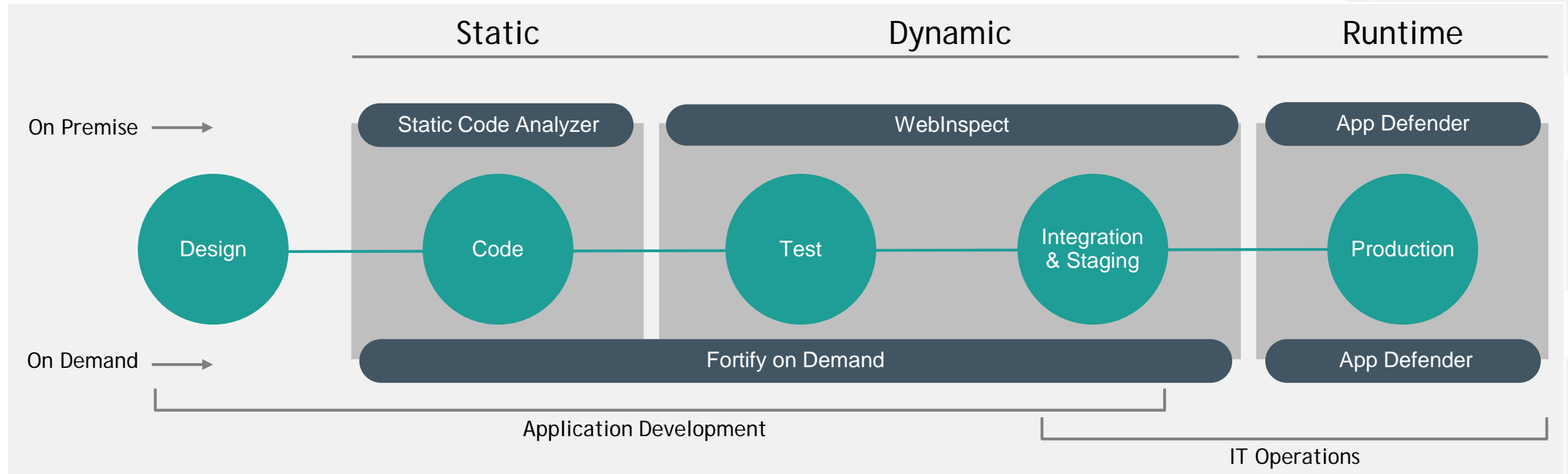
Number of successful attacks per year per company:  
144% increase in 4 years



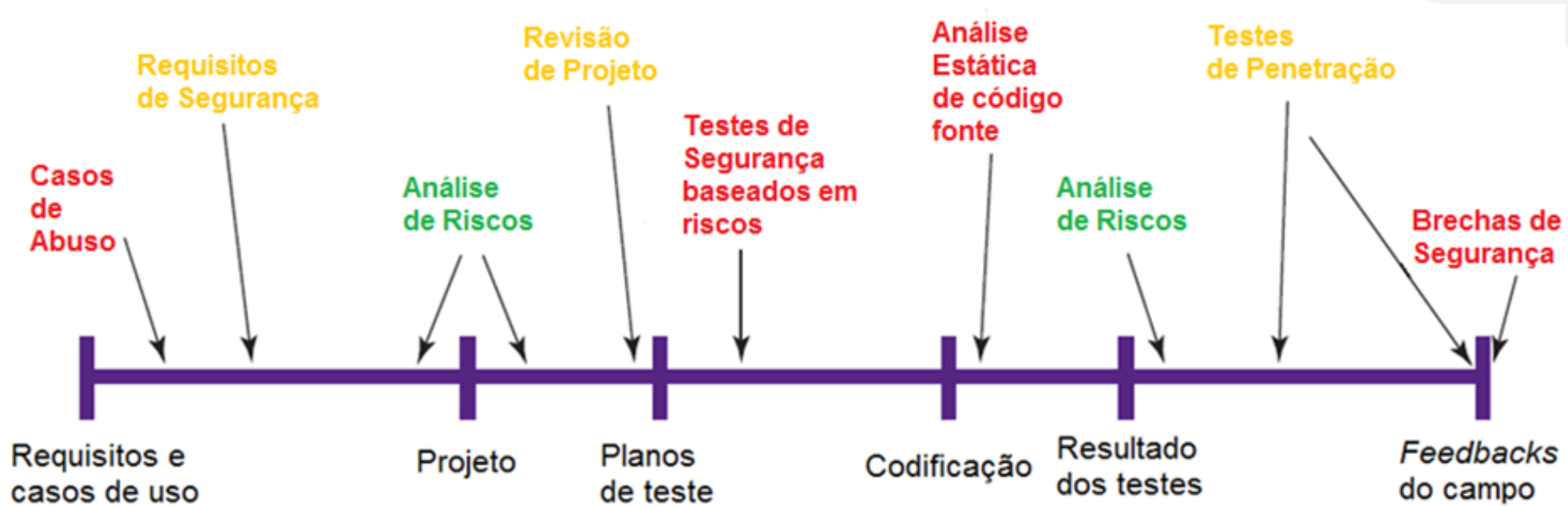
## ROI



# Diferentes necessidades em diferentes etapas



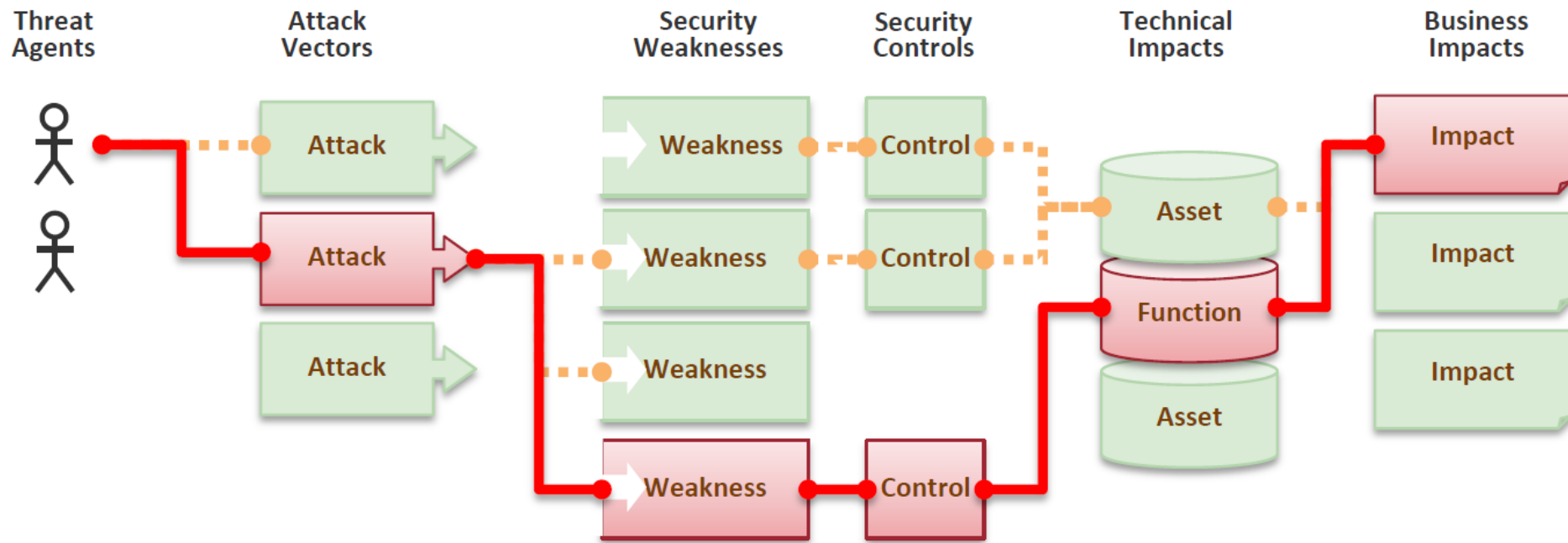
# S-SDLC: Secure Software Development Lifecycle



IEEE Security and Privacy – Software Security, Gary McGraw, 2004

# OWASP Top 10

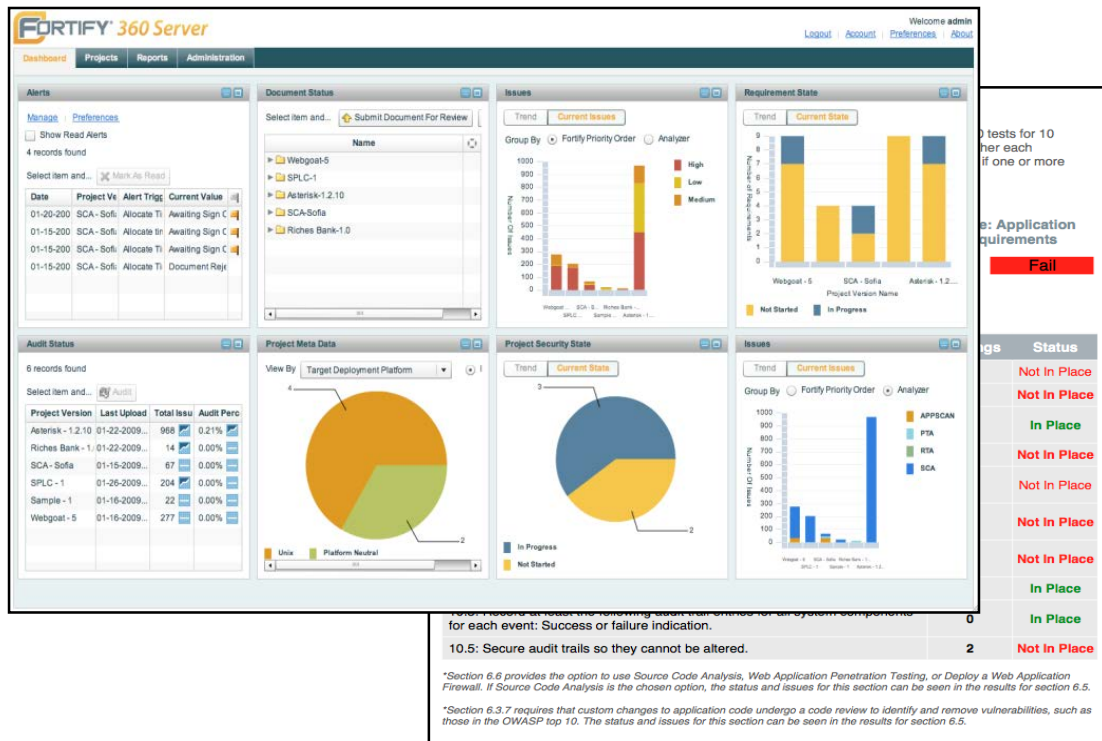
## Representação de Risco



- A1 – Injection
- A2 – Broken Authentication and Session Management
- A3 – Cross-Site Scripting (XSS)
- A4 – Insecure Direct Object References
- A5 – Security Misconfiguration
- A6 – Sensitive Data Exposure
- A7 – Missing Function Level Access Control
- A8 – Cross-Site Request Forgery (CSRF)
- A9 – Using Components with Known Vulnerabilities
- A10 – Unvalidated Redirects and Forwards

# Software Security Center Server

Administração, acompanhamento e remediação dos riscos de software



## Problemas que endereça:

Falta de visibilidade ponta a ponta do processo de segurança de aplicações entre as áreas envolvidas no processo de desenvolvimento de software.

## Características:

- Especificação, comunicação e acompanhamento das atividades de segurança realizadas ao longo do desenvolvimento de software;
- Plataforma de administração de segurança em desenvolvimento de software com enfoque orientado a processos e papéis;
- Centralização de resultados e possibilidade de exportação de relatórios em diferentes formatos para acompanhamento de métricas do S-SDLC;

## Benefícios:

- Contar com uma visão clara e precisa do risco de software desenvolvido para a organização;
- Redução do custo e do tempo para a remediação de vulnerabilidades;
- Acelera a redução de riscos e custos no desenvolvimento de software.



# Gestão de Segurança

SOLUÇÕES QUE VALORIZAM  
E IMPULSIONAM SEU NEGÓCIO.  
[SOLONETWORK.COM.BR](http://SOLONETWORK.COM.BR)

# Inteligência

## Coleta / Correlaciona

Eventos / Segundo



## Procura

Milhões de Dados

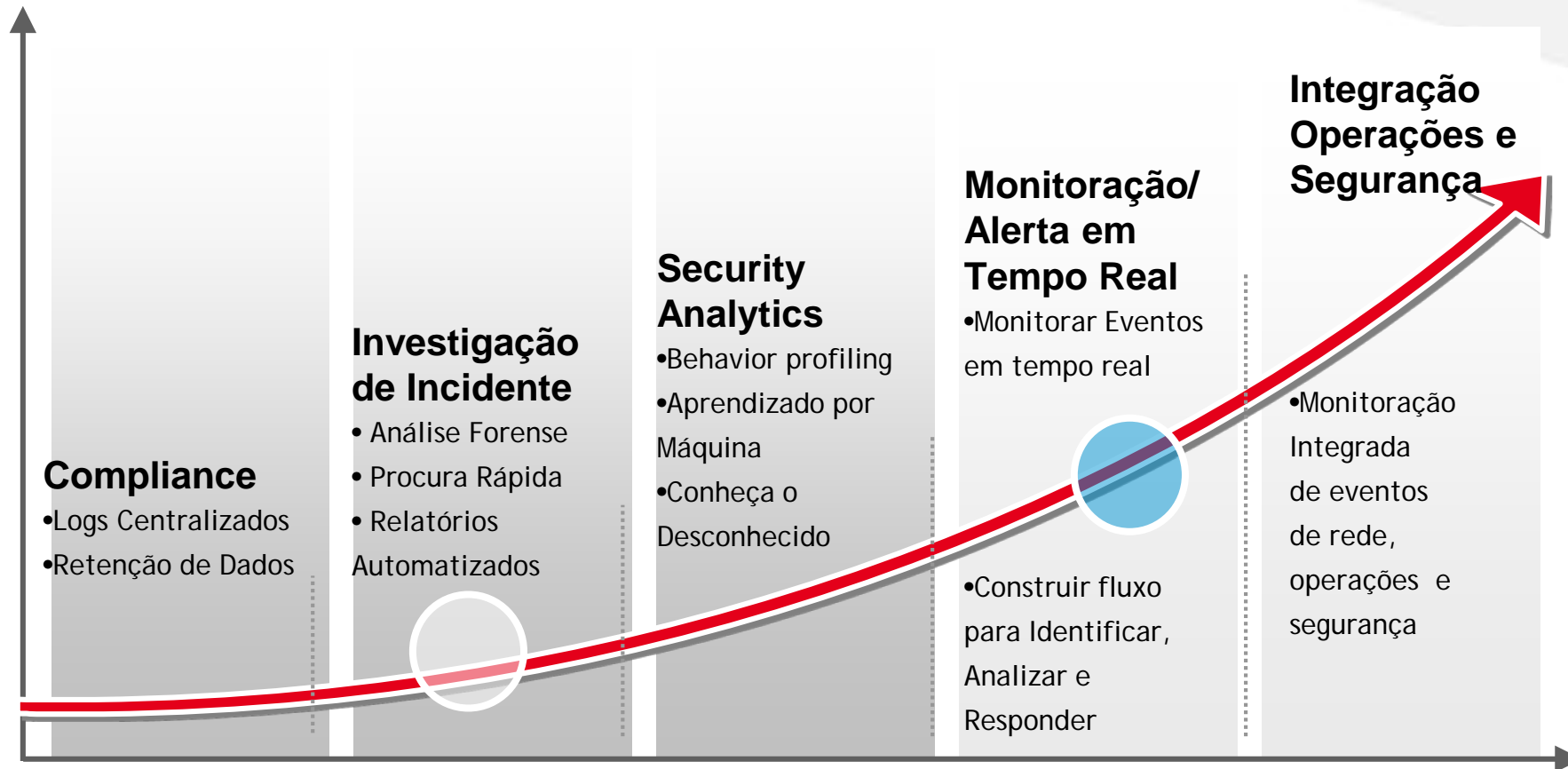


## Analiza

Evento Específico



# Inteligência

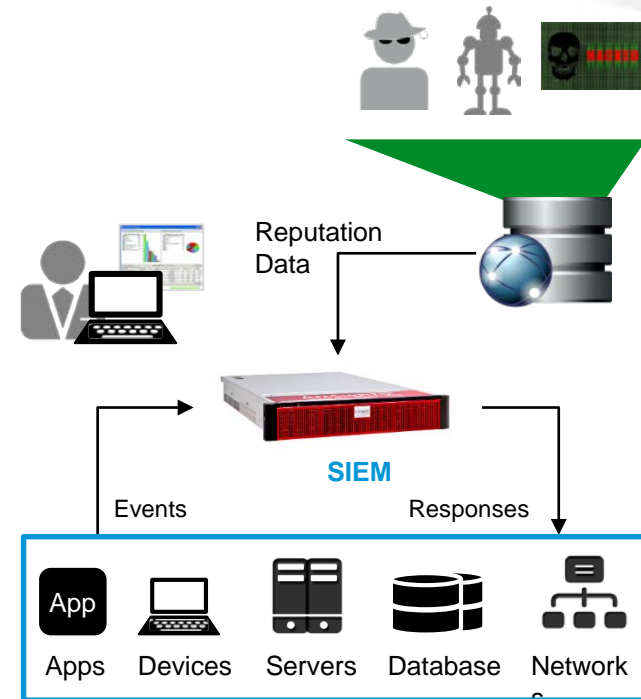




# Reputação

Gerência ativa “baseada em reputação” políticas de segurança para detectar e impedir a comunicação com os “hosts com alto risco”.

- Pesquisa e uma visão de comunidade de segurança global
- Inteligência alimentado o Siem para correlação em tempo real
- Detecta e prioriza as ameaças através da correlação de atividade suspeita



# Comportamento



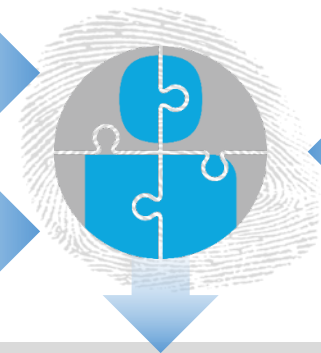
Directories



Applications

Users & roles

Accounts



Events

- Find the Bad Guys
- Faster Event Resolution
- Lowered monitoring and management costs
- ROI Impact



Database Queries



USB Files Saved



VPN Logins



Files Accessed



Emails Sent



Screen Prints



Web Surfing



Hosted Apps

# Medias sociais



**Joe Schmopped**

@hakdpint



Follow

Kobalt Systems is infringing upon their employees' rights by monitoring every action on the network. We should teach them a lesson: DDOS



Reply



Retweet



Favorite



More



**Joe Schmopped**

@hakdpint



Follow

Found a JS/iframe/vulnerable server at 10.10.10.120



Reply



Retweet



Favorite



More

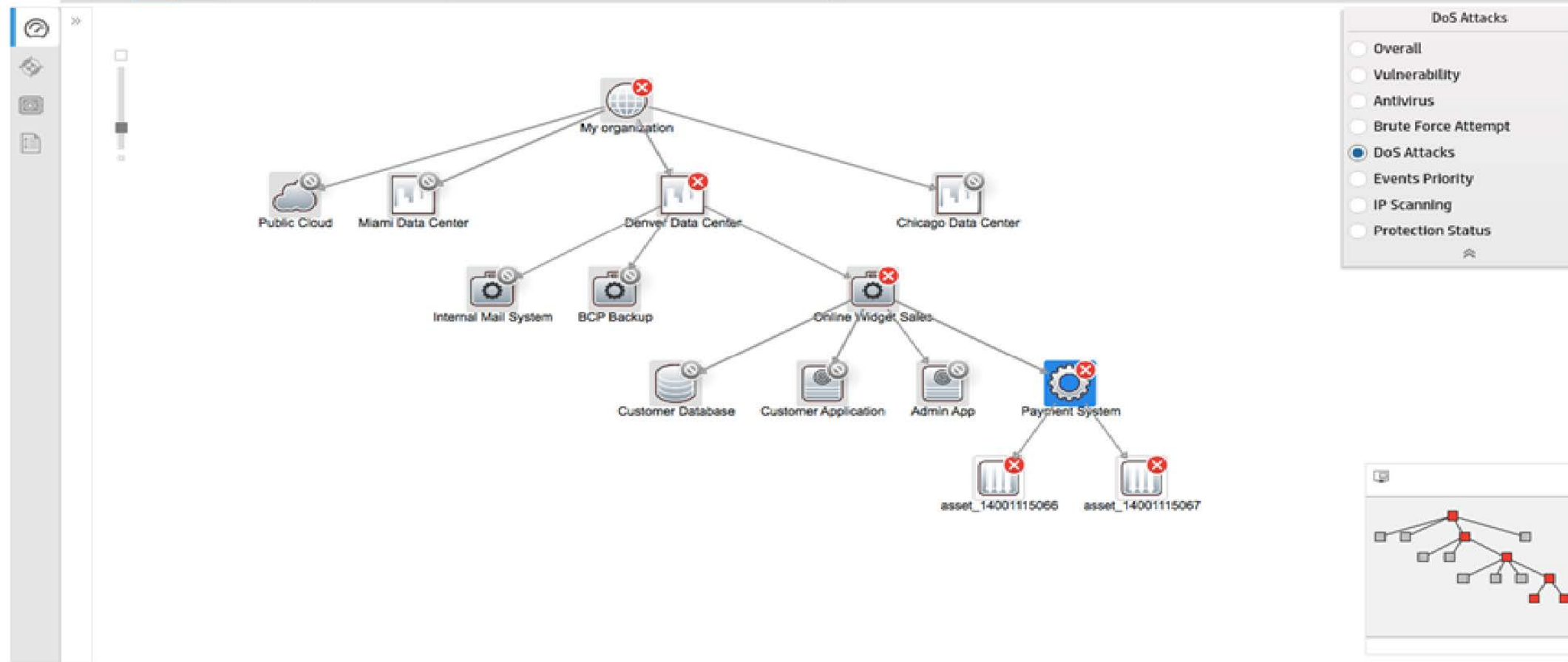
# Mapa de risco e serviços afetados

Risk Insight - Risk Indicators

Layout: [Icons]

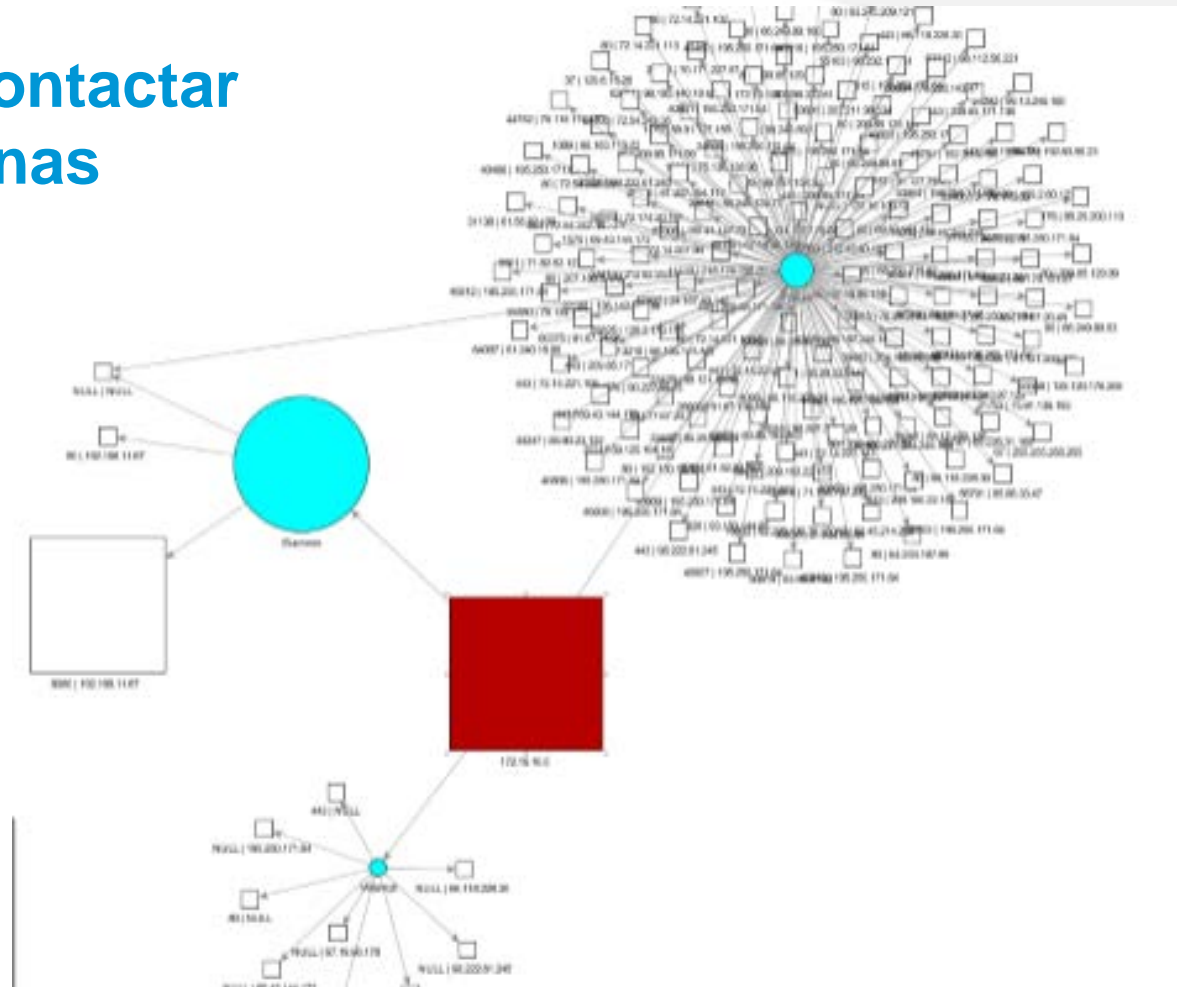
Save View

Filter by CPEs



# Padrões

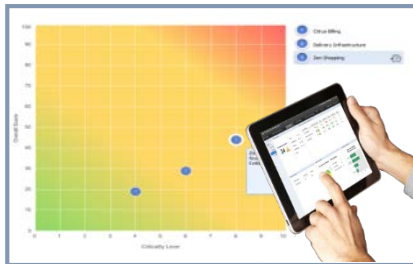
Uma máquina interna tenta contactar um número grande de maquinas externas desconhecidas



# Visão consolidada

Visão única de segurança, operações e conformidade de TI

## Mapa de Calor



- Priorização
- Risco alinhado com áreas de negócios

## Mapeamento dos Ativos



- Rápida identificação e isolamento de ameaças
- Score de inteligência e Vulnerabilidades

## Indicadores de Risco



- Consolidação de múltiplas fontes de risco
- Relatórios de risco e tendências

## Conformidade



- Monitoração continua
- Conformidade de maneira analítica



# Cybercrime Ransomware

SOLUÇÕES QUE VALORIZAM  
E IMPULSIONAM SEU NEGÓCIO.  
[SOLONETWORK.COM.BR](http://SOLONETWORK.COM.BR)

# O que é Cibercrime e temos leis contra ?

**Cibercrime, crimes eletrônicos** ou **crime digital** são termos utilizados para se referir a toda a atividade onde um computador ou uma rede de computadores é utilizada como uma ferramenta, uma base de ataque ou como meio de crime.

**Calúnia** (art. 138 do CP), **Difamação** (art. 139 do CP), **Injúria** (art. 140 do CP),

**Interceptação telemática ilegal**, CP art. 10 da lei 9296/96 (Lei federal Brasileira)

**Proteção a Propriedade intelectual** Lei 9.610/98 (Antipirataria )

**Dano ao patrimônio** - Previsto no art.163 do Código Penal

**Sabotagem informática** - art.163 do Código Penal (Dano ao patrimônio )

**Pornografia infantil** - o art. 241 do Estatuto da Criança e do Adolescentes

**Apropriação indébita** - O Código Penal artigo 168, reclusão de 3 a 6 anos e multa

**Estelionato** - Código Penal artigo 171

**Invasão de dispositivos informáticos** - Código Penal, Lei 12.737/2012, (Lei Carolina Dieckmann)



# ▶ RANSOMWARE & CYBER EXTORTION: COMPUTERS UNDER SIEGE



# Como acontece a contaminação?



# Quais os resultados da contaminação?



# Pagar o resgate ou não?

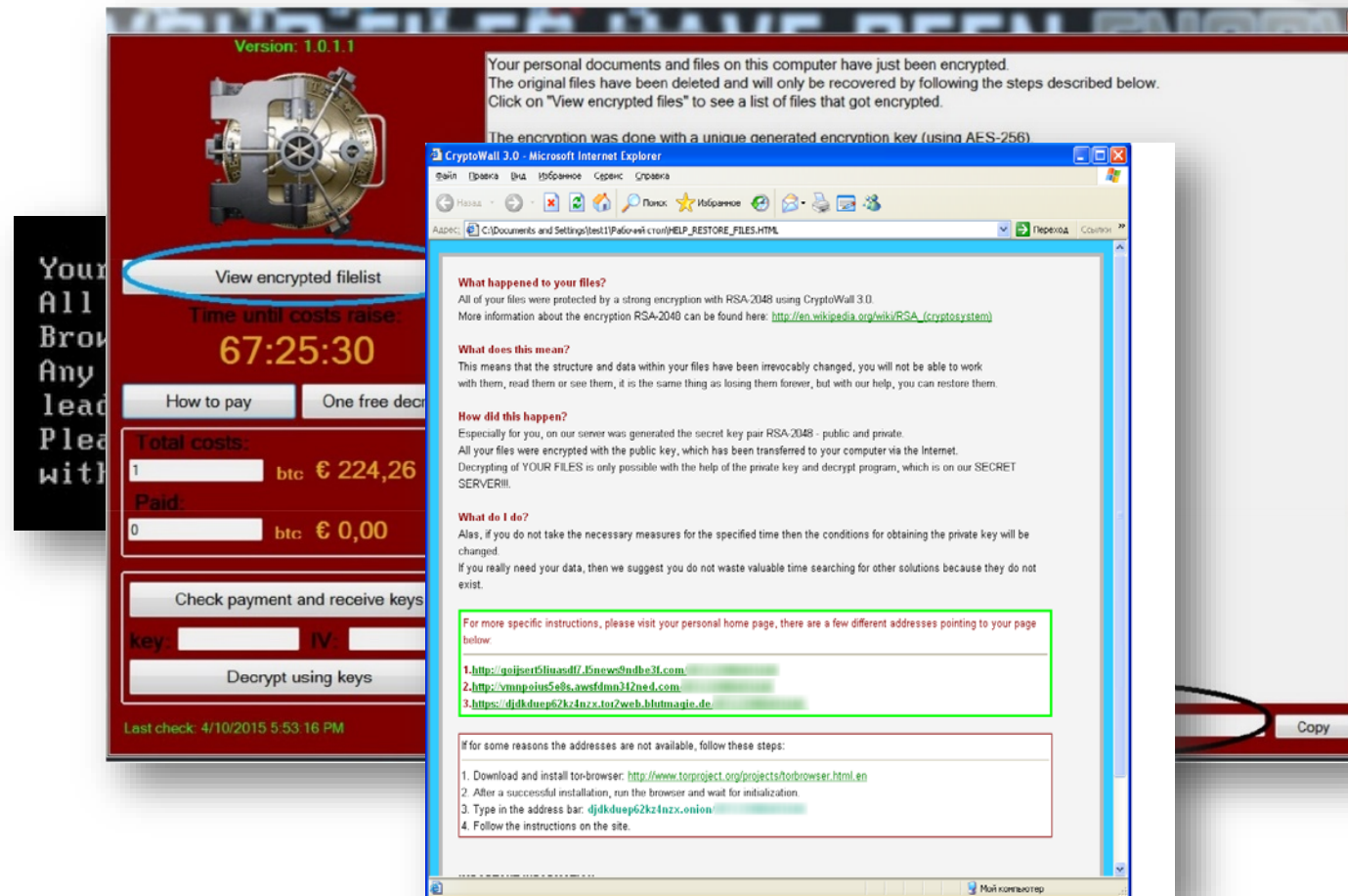


## O RESGATE

- Depois do bloqueio, os criminosos entram em contato com a vítima, por SMS ou por e-mail,
- Solicitam uma quantia em **BITCOIN** em troca do código de desbloqueio.
- Muitas vezes o resgate pago é em vão, a senha é falsa e não dá acesso aos arquivos.
- Além de perder dinheiro, perde todos os dados!

# EXISTE APENAS UM TIPO DE RANSOMWARE?

- CryptoLocker,
- CryptoWall,
- CoinVault,
- TorLocker,
- CoinVault,
- TeslaCrypt,
- CTB-Locker,
- Etc...



# Quem está utilizando o cibercrime?



## Crime organizado:

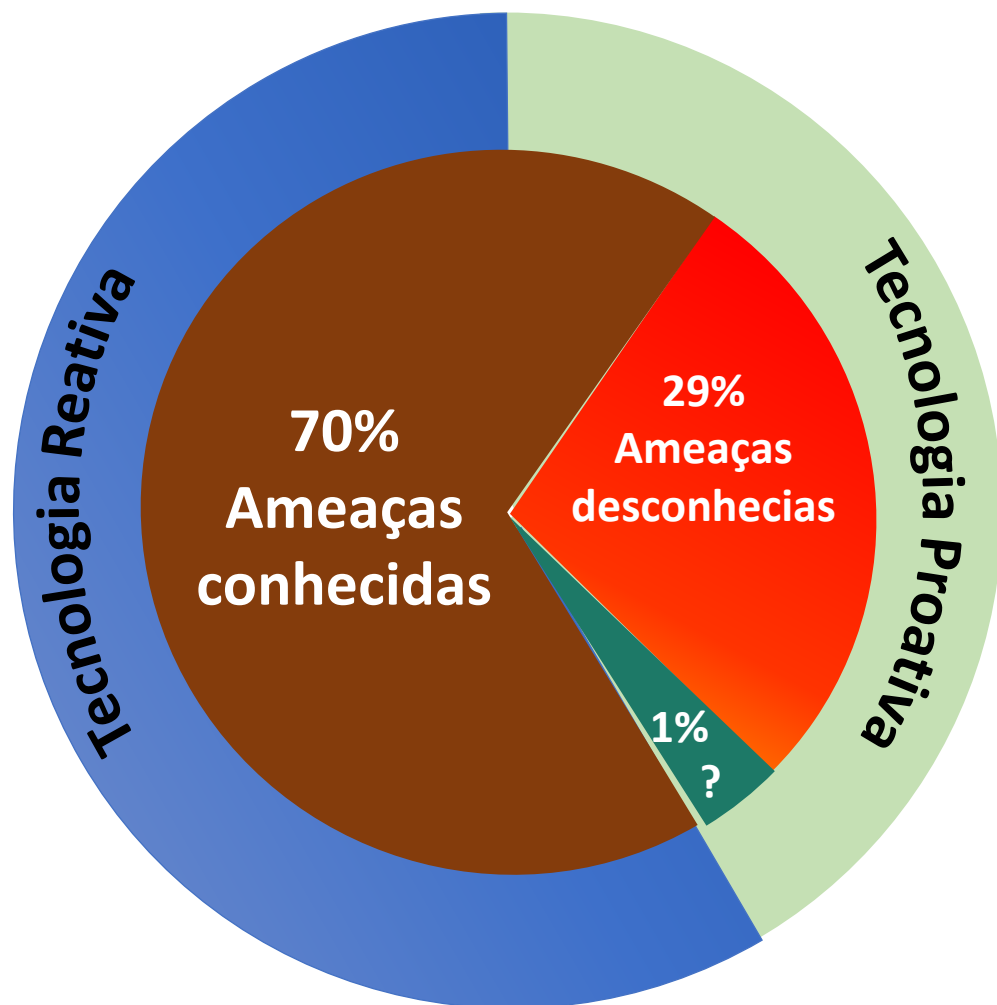
- *As evidências apontam que estamos entrando na “quarta grande era” do crime organizado, a “Idade de crime digital” – com os mundos online e offline convergindo;*
- *80% do crime digital se origina em alguma forma de atividade organizada;*
- *O crime digital não é privilégio da juventude, 43% dos criminosos são maiores de 35 anos;*
- *Terroristas entraram no cibercrime para financiar atividades terroristas.*

# Como se proteger contra o Ransomware?

- Antivírus com capacidade comprovada de defesa contra Ransomware.
- Cuidados com e-mails, softwares não originais e dispositivos móveis
- Mantenha seus softwares atualizados.
- Mantenha o Windows Update ativado.
- Cuidado com páginas que solicitam ou exigem o download de um programa
- Avisos de atualização não aparecem dentro da janela do navegador.
- Ter um backup atualizado para restaurar seus arquivos caso o pior aconteça.



# ANTIVÍRUS NÃO! CONSOLE DE SEGURANÇA SIM!



## FERRAMENTAS REATIVAS:

- HIPS & Firewall
- URL Filtering
- Anti-spam
- Anti-fishing
- Blacklist

- Ameaças simples
- Ameaças conhecidas
- Vulnerabilidades antigas

## FERRAMENTAS PRÓATIVAS:

- Heurística
- Whitelisting
- App Control
- Web Control
- System Watcher

- Reputação de sites e aplicações
- Sequestro de dados
- Botnets
- Controle de dispositivos
- Vulnerabilidades complexas
- Análise de comportamento

## FERRAMENTAS AVANÇADAS:

- BSS
- AEP
- AntiAPT
- System Watcher

- Ciber TERRORISMO
- ESPIONAGEM
- Zero-days







# Marco Civil da Internet

SOLUÇÕES QUE VALORIZAM  
E IMPULSIONAM SEU NEGÓCIO.  
[SOLONETWORK.COM.BR](http://SOLONETWORK.COM.BR)

# Marco Civil da Internet

- Em vigor desde junho de 2014;
- Constituição da Internet no Brasil
- Lei de Azeredo no. 84/1999
- Iniciado em 2010 – <http://culturadigital.br/marcocivil>
- Liberdade de expressão online, proteção de privacidade, divisão de responsabilidades



# Marco Civil da Internet

- Responsabilidade dos provedores
- Desenvolvimento e acesso à internet
- Privacidade
- Neutralidade da Rede
- Demais direitos
- Propostas de alterações do Marco Civil

# Marco Civil da Internet

## O Marco Civil da Internet em suas versões

Primeiro texto teve participação dos internautas e foi modificado até a aprovação

TEMAS	2011 TEXTO ORIGINAL	2012 PROPOSTA DO RELATOR	2014 PROPOSTA APROVADA
<b>INTERNET LIVRE (NEUTRALIDADE DE REDE)</b> 	Os provedores de internet devem dar tratamento igualitário de acesso e velocidade a todos os sites, a não ser por aspectos técnicos	A neutralidade poderá ser rompida para priorizar emergências (segurança pública etc). Regulamentação será por decreto presidencial, após consulta ao Comitê Gestor da Internet	Além do CGI, a Anatel deverá ser consultada. A regulamentação das exceções serão feitas por determinação constitucional de "fiel execução da lei"
<b>PRIVACIDADE</b> 	Os provedores devem guardar o registro de acesso geral à internet por um ano, mas não podem manter os registros específicos a sites	Permanece igual	Sites na internet com fins lucrativos, como Facebook e Google, devem manter o registro de acesso por 6 meses. Não podem guardar dados pessoais que extrapolem o serviço

# Marco Civil da Internet

## O Marco Civil da Internet em suas versões


Primeiro texto teve participação dos internautas e foi modificado até a aprovação

<b>TEMAS</b>	<b>2011</b> TEXTO ORIGINAL	<b>2012</b> PROPOSTA DO RELATOR	<b>2014</b> PROPOSTA APROVADA
<b>DADOS PESSOAIS E COMUNICAÇÕES NA INTERNET</b> 	Os registros de acesso à internet devem privar pela intimidade, vida privada e honra. Poderão ser fornecidos somente após ordem judicial	Permanece igual	Dados pessoais e conteúdo de comunicações privadas são incluídas no texto, o que permite a autoridades terem acesso a eles via ação judicial
<b>LIBERDADE DE EXPRESSÃO X CONTEÚDO ILEGAL/OFENSIVO</b> 	Provedores não são punidos por publicações de terceiros. Já sites e aplicações são responsabilizados se não acatarem a Justiça	A viabilidade técnica para serviços retirarem publicações após ordem judicial conta. O conteúdo pode ser substituído pela ordem judicial sobre a retirada	Se o conteúdo tiver imagens de nudez ou de atos sexuais do ofendido, o serviço deverá retirá-lo após notificação, sem necessidade de ação judicial

# Marco Civil da Internet

## O Marco Civil da Internet em suas versões

Primeiro texto teve participação dos internautas e foi modificado até a aprovação

<b>TEMAS</b>	<b>2011</b> TEXTO ORIGINAL	<b>2012</b> PROPOSTA DO RELATOR	<b>2014</b> PROPOSTA APROVADA
<b>MONITORAMENTO NA WEB</b> 	Não previa qualquer forma de coleta de dados pessoais na internet	Dados dos usuários poderão ser utilizados para as finalidades que fundamentam a oferta de um serviço e seu uso deverá ser especificado. Usuário pode pedir sua exclusão	A utilização deverá ser explicitada já no contrato. Serão nulos os contratos que não permitam ações na Justiça brasileira. Código do consumidor passam a valer nessa relação

 .com.br

Infográfico elaborado em 25/3/2014

SOLO NETWORK

# Parceria com Fabricantes



Microsoft Gold Partner



Dell Preferred Partner



HP Silver Partner



Kaspersky Platinum Partner



Adobe Platinum Reseller



APC Platinum Partner



Autodesk Partner



WatchGuard Partner



**solo**  
NETWORK

SOLUÇÕES QUE VALORIZAM  
E IMPULSIONAM SEU NEGÓCIO.  
[SOLONETWORK.COM.BR](http://SOLONETWORK.COM.BR)

# OBRIGADO!

Paulo Vendramini

[Paulo.Vendramini@solonetwork.com.br](mailto:Paulo.Vendramini@solonetwork.com.br)

+55 41 8887-4828

+55 11 99953-4444

CENTRAL DE ATENDIMENTO NACIONAL  
**0800 604 9596**

Curitiba  
(41) 4062-6971

São Paulo  
(11) 4062-6971

Rio de Janeiro  
(21) 4062-6971

Belo Horizonte  
(31) 4062-6971

Florianópolis  
(48) 4062-6971

Porto Alegre  
(51) 4062-6971

Brasília  
(61) 4062-6971

Campo Grande  
(67) 4062-6971