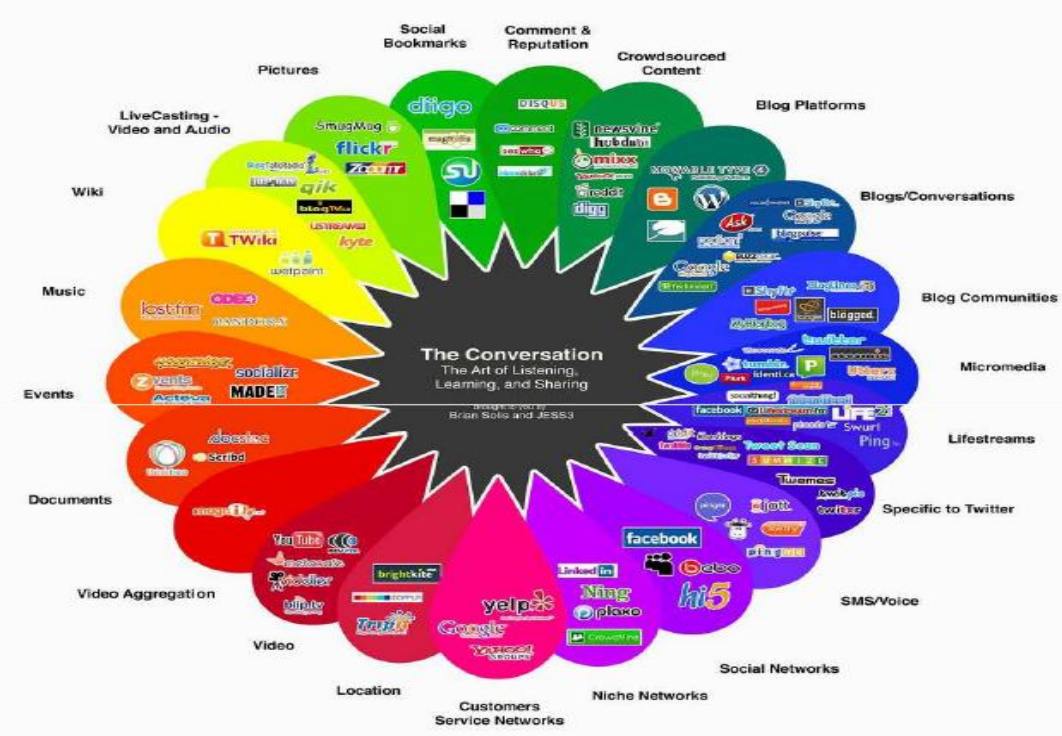
Cássio de Alcântara
Regional Sales Manager

Redes Sociais, nova fronteira de negócios ou um novo problema para as empresas?

websense

Quais são a novas fronteiras?



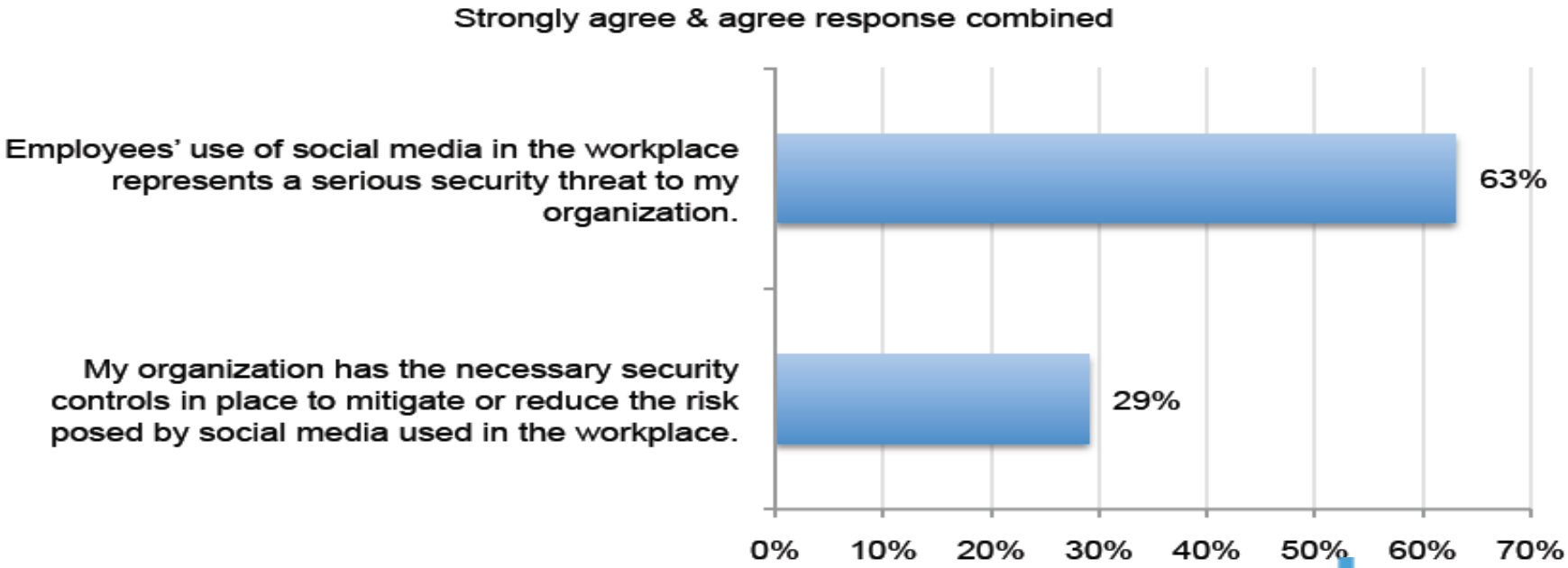
Quais são a novas ferramentas?

facebook Orkut YouTube vimeo foursquare Pinterest

g+ LinkedIn twitter flickr slideshare WIKIPEDIA


LIKE
search
E-mail
Add friends

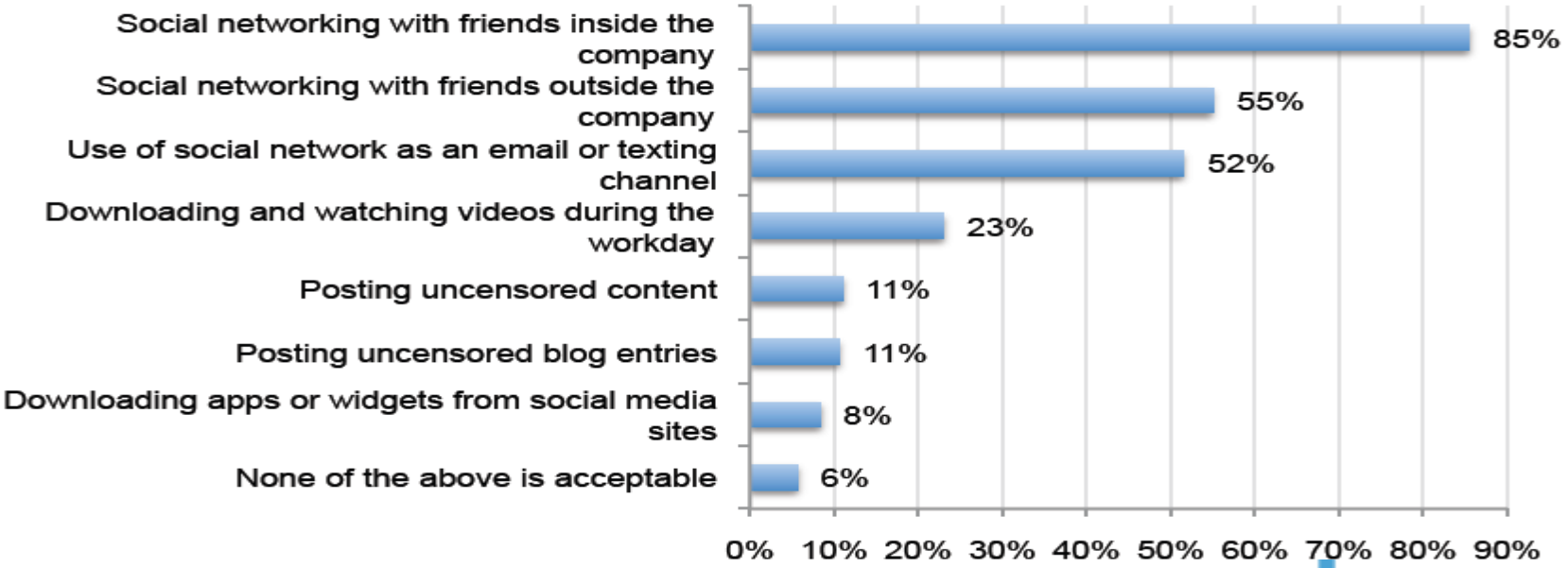
Voce vê o uso de redes sociais como um risco para a sua organização?



websense

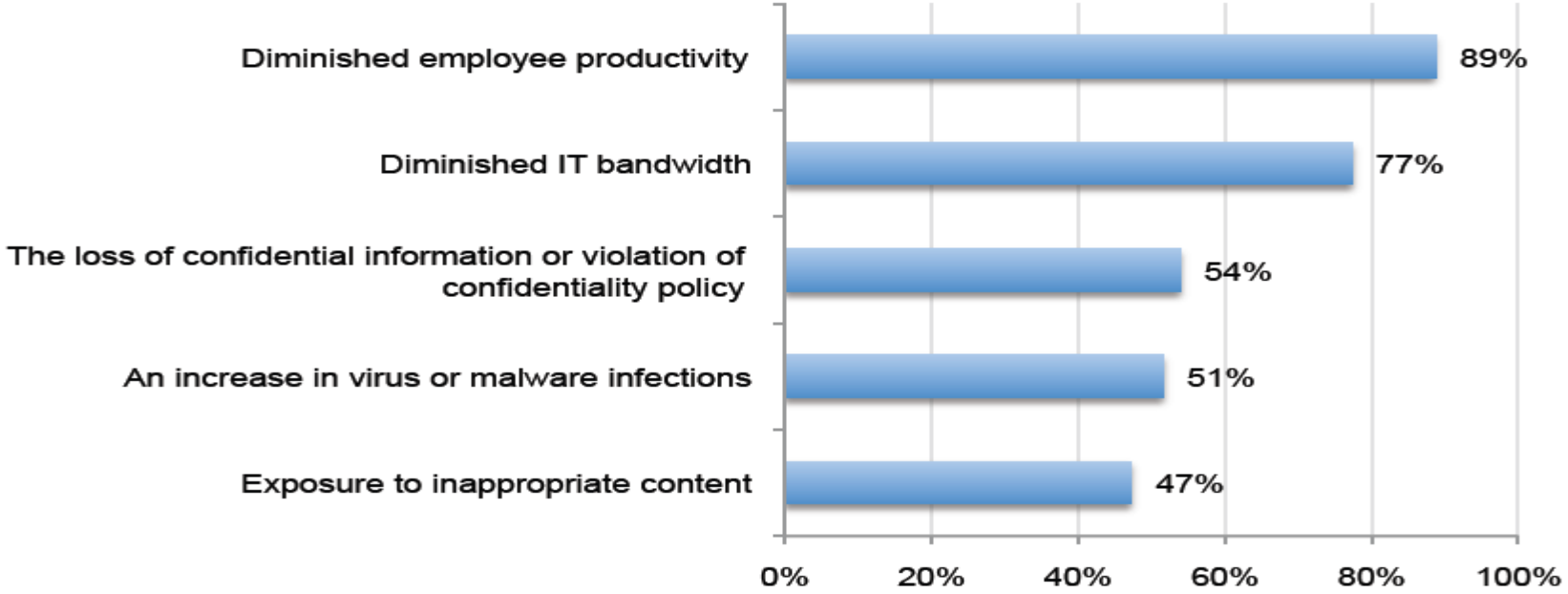
O que voce considera aceitável para o uso de redes sociais no trabalho?

Bar Chart 2: What is considered the acceptable use of social media in the workplace



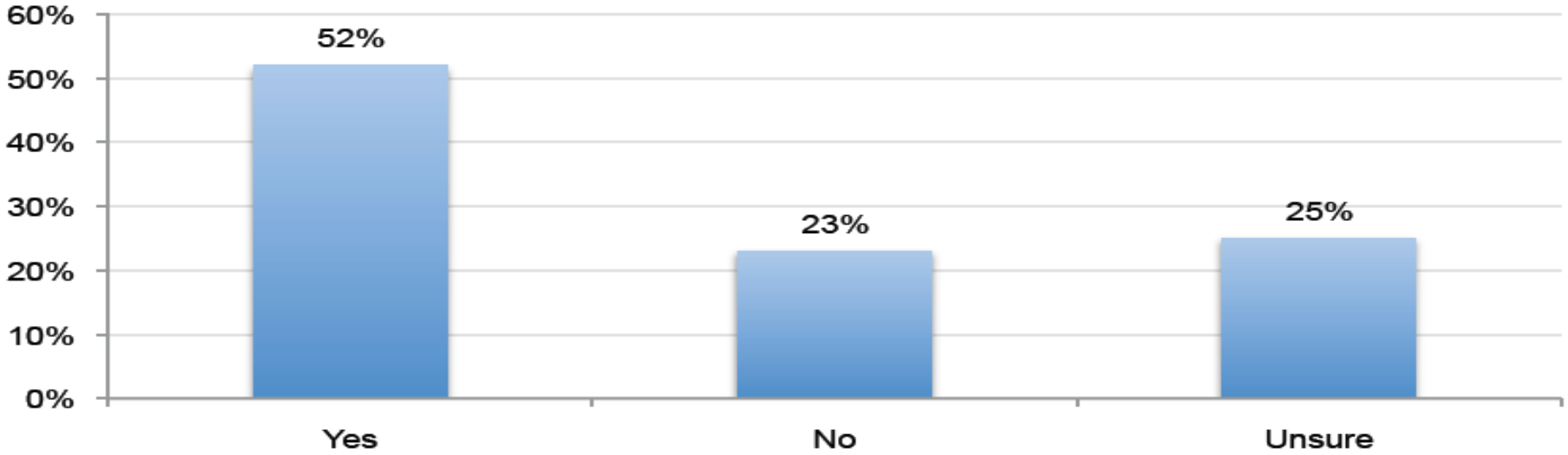
websense

Quais as consequências da utilização de redes sociais no trabalho?



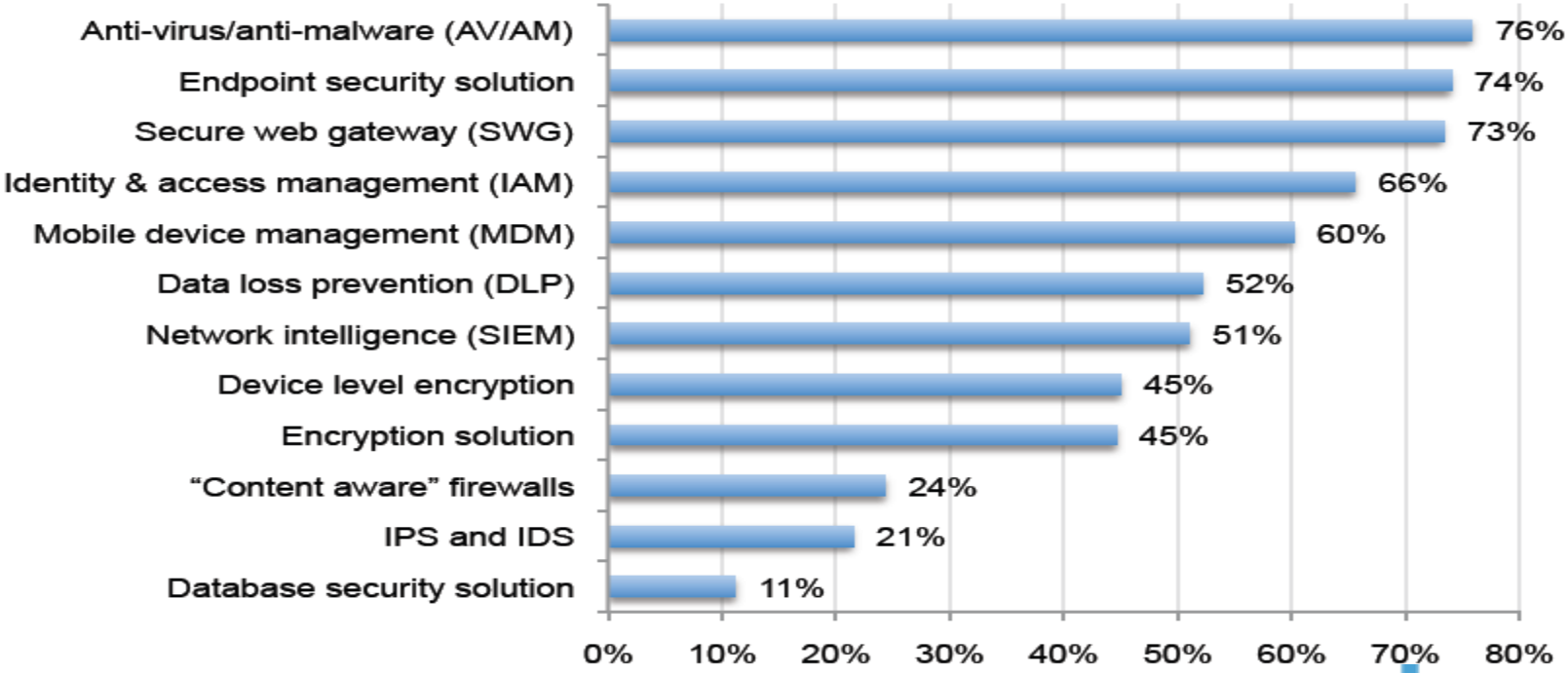
websense

Sua organização teve um aumento no número de incidentes com malwares após a permissão do uso de redes sociais?



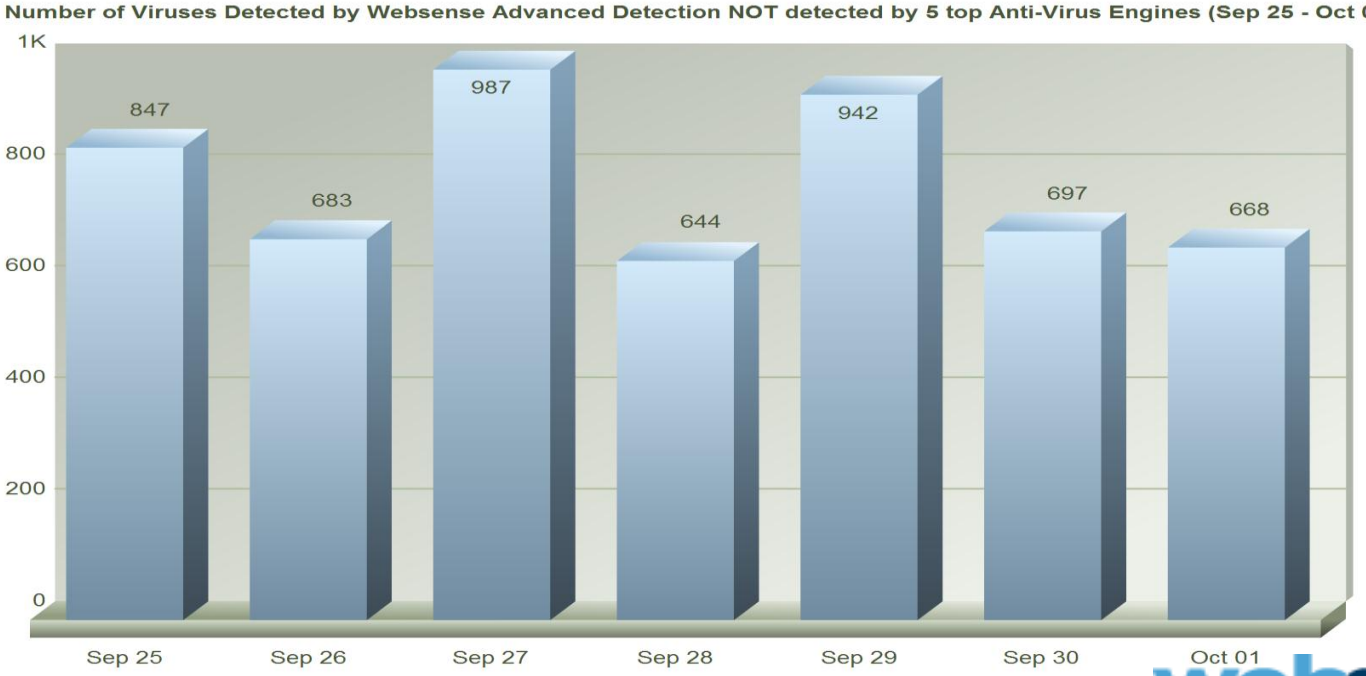
websense

Qual medida sua organização considera mais eficaz na redução dos riscos de segurança na utilização de redes sociais?



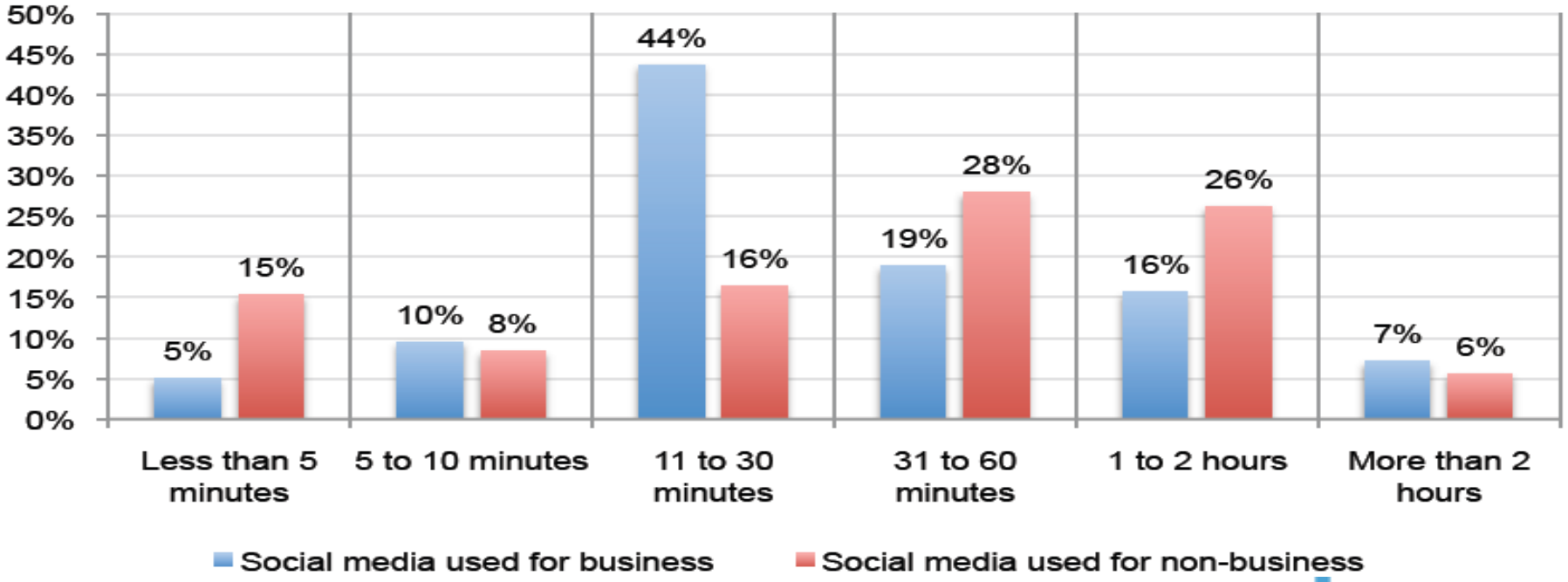
websense

Quantidade de ameaças descobertas por dia que um anti virus não identifica!



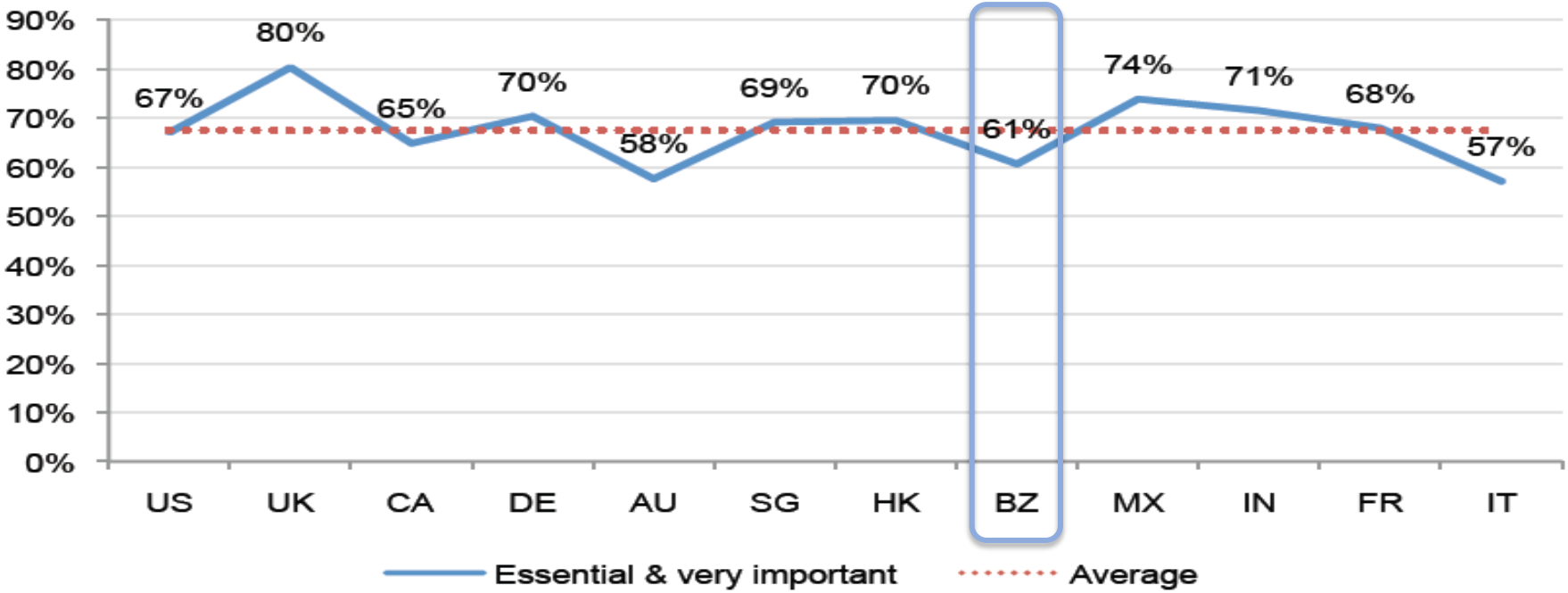
websense

Quanto tempo em média seus usuários passam em redes sociais durante do dia?



websense

Quão importante é a mídia social em termos de objetivos empresariais em sua organização?



websense

Pergunta

Libero ou não o acesso?


Já está liberado!

Solução

Oferecer a cada usuário exatamente o ferramental que ele necessita para a partir de uma

Quatro níveis básicos

Vê somente conteúdo restrito estático

Visibilidade com Pesquisa em controle de conteúdo rede social.

Visibilidade com Pesquisa em controle de conteúdo rede social com e interatividade interatividade.

Visibilidade com Pesquisa em controle de conteúdo, rede social com Interatividade e comunicação.

Quatro níveis básicos

Terceirizados

Usuário Comum

Marketing

Call Center

websense®
TRITON™
SEE MORE • SECURE MORE • DO MORE™

Idéias surgem de idéias. A internet é o maior celeiro

Apresentando Websense TRITON v7.7

Novas Defesas de Segurança

Graziani Pengue

TRITON™

- Web security
- Email security
- Data security
- Mobile security

Novo Jogo na Defesa

websense

“ Signature based tools (anti-virus, firewalls, and intrusion prevention) are **only effective against 30-50% of current security threats**. Moreover, customers expect the effectiveness of signature-based security to continue to decline rapidly.”

IDC Threat Intelligence Update, 14-Feb-2012

Sete Etapas - Ameaças Avançadas

websense

Sete Etapas - Ameaças Avançadas

websense

Recon

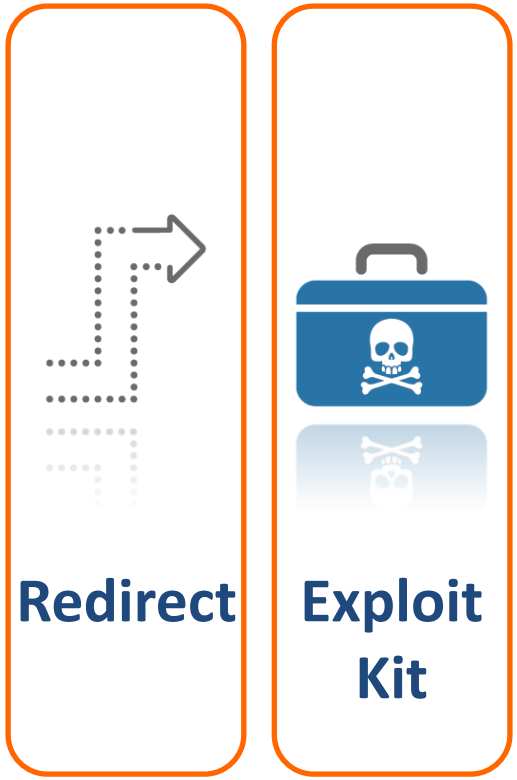
Lure

CONSCIÊNCIA

- Web e Email
- Facebook, Blogs, Tweets
- Spear-phishing
- Confiável
- Alvo
- Dinâmico
- Temporário

Sete Etapas - Ameaças Avançadas

websense



ANÁLISE EM TEMPO REAL

- Cód do Browser e Scripts
- Análise de Link
- Análise Exploit
- Pontuação Composta
- Preditivo

Sete Etapas - Ameaças Avançadas

websense

DEFENSAS INLINE

- Análise de App
- PDFs Maliciosos
- Múltiplos AVs
- Compressão de Arquivo
- DNS Dinâmico
- Comms CnC

Dropper File

Call Home

Sete Etapas - Ameaças Avançadas

websense

CONTENÇÃO

- Defensas contra Roubo de Dados
- DLP
- Captura de Dado
- Geo-location
- Análise Forense e Relatório

Data Theft

Técnicas de Ataques Avançados

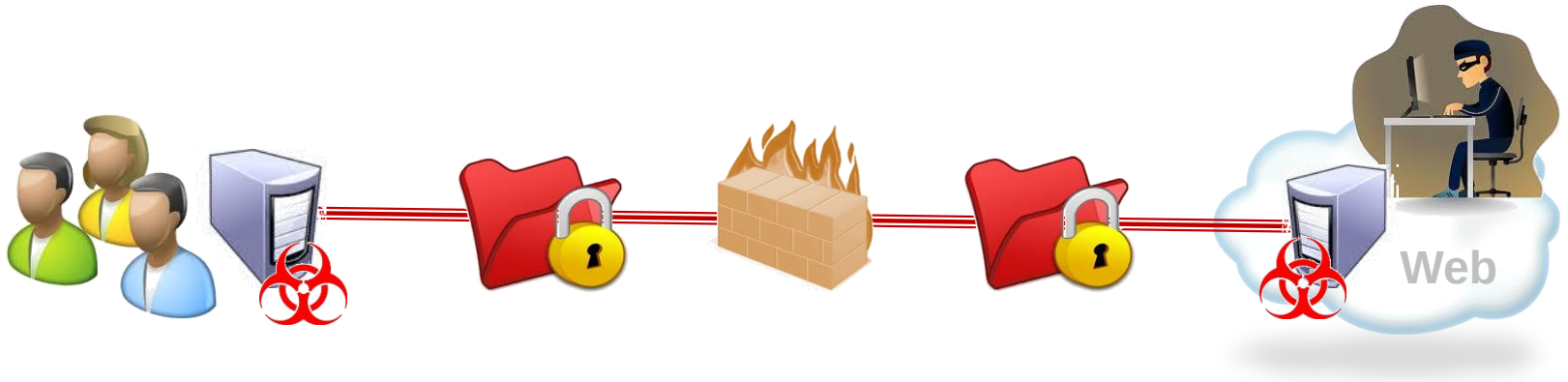
Como Evitar Detecção?

TRITON™

- **Web security**
- **Email security**
- **Data security**
- **Mobile security**

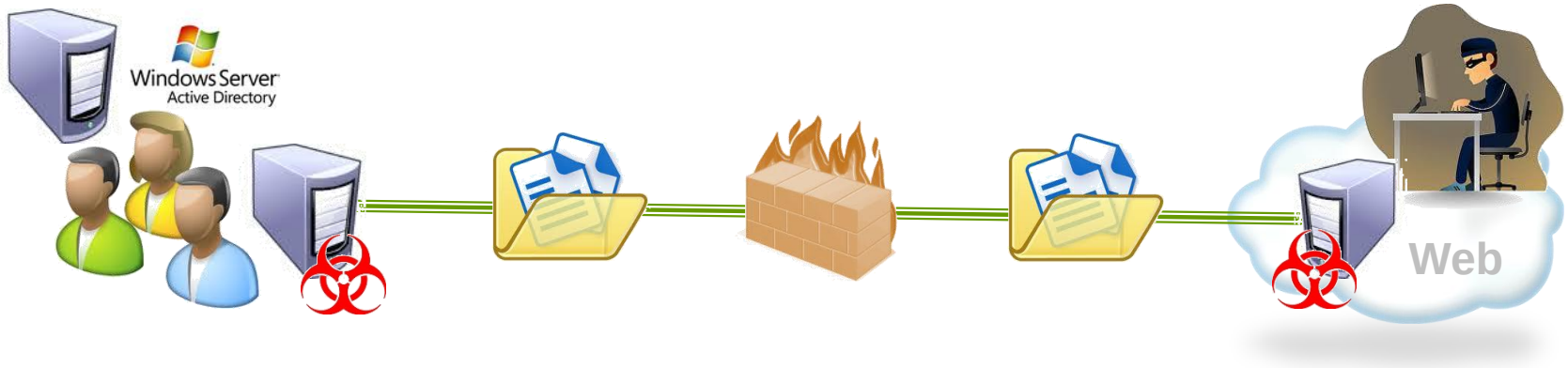
Uploads Criptografados

- Criptografia Proprietária
- Roubo de Dados
- Criado por Toolkit Crimeware
- “Ponto Cego” para as Defesas



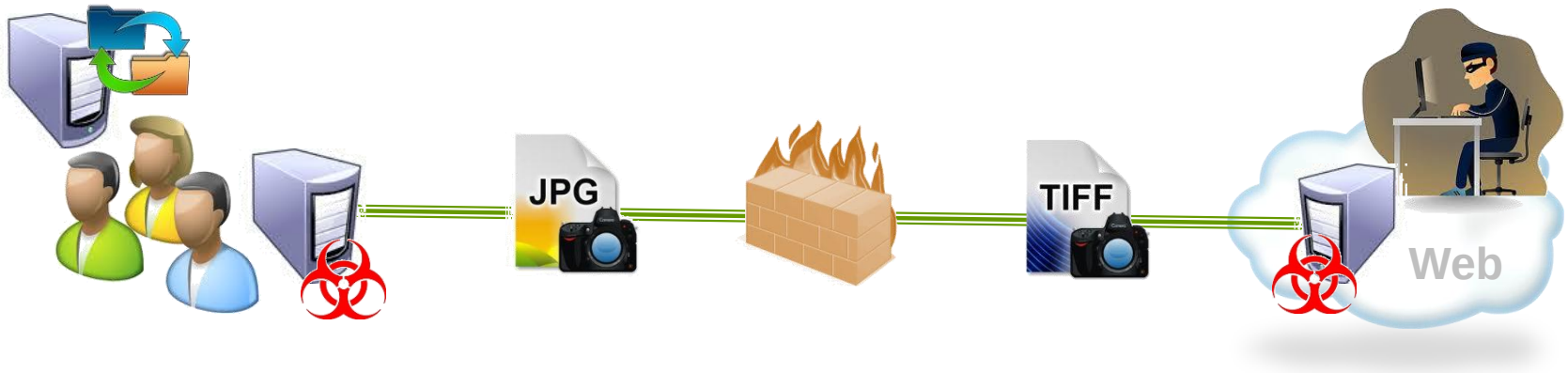
Roubo de Arquivos com Senha

- Arquivos contendo senhas
- Active Directory/Banco de Dados SAM
- Aumento do Alcance/Controle dentro do Alvo
- Privilégios Administrativos após Infiltrado



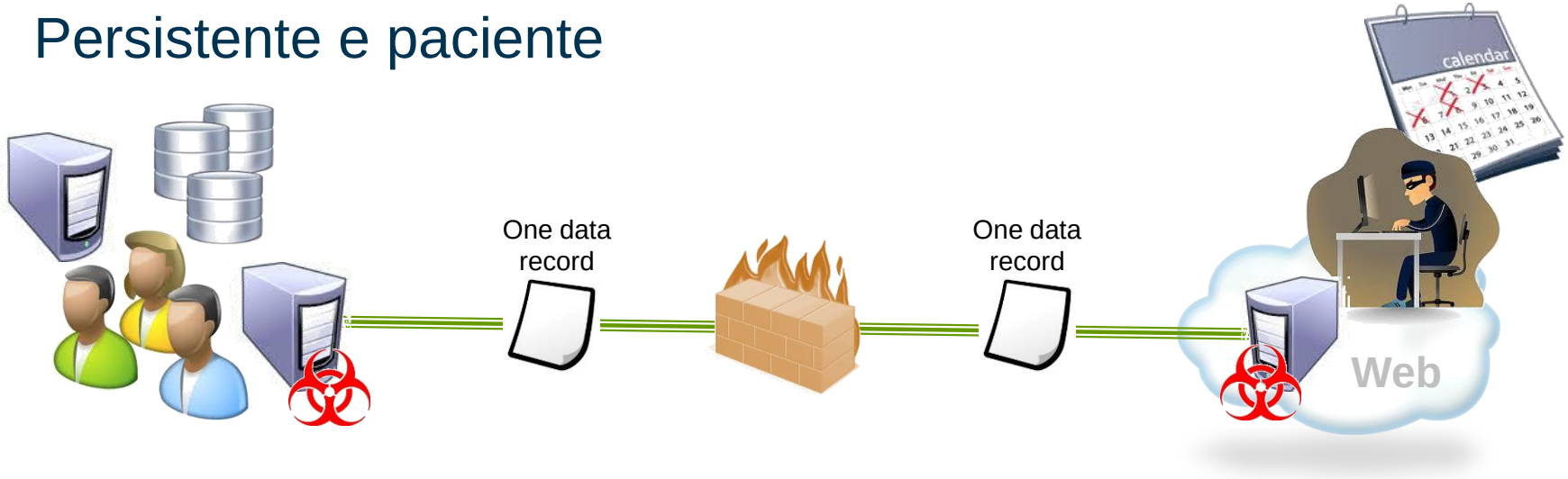
Roubo de Dados sem ser Texto

- Arquivos de Imagem
- Informação Confidencial
- Fotos de Smartphones
- “Ponto Cego” para as Defesas



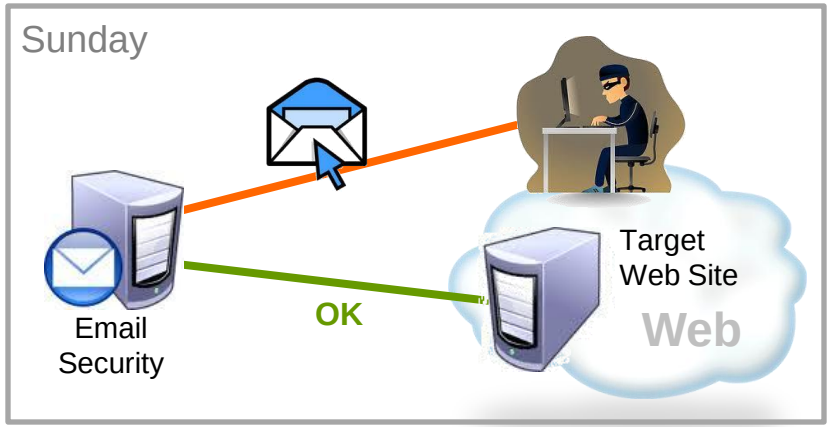
Vazamento de Dados “Pausado”

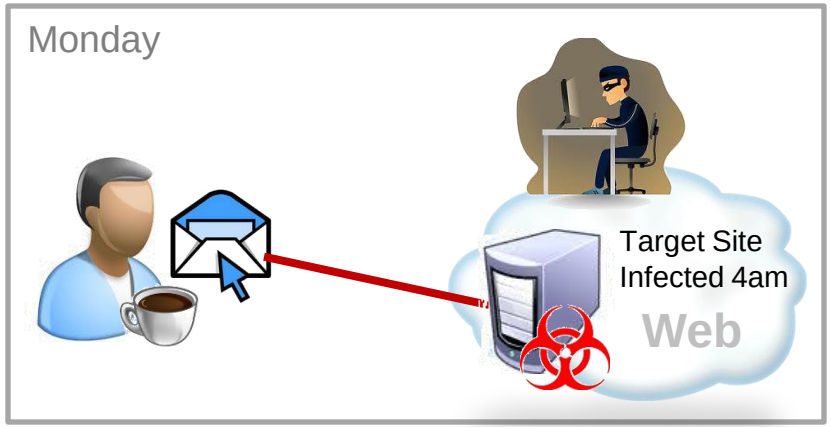
- Fica abaixo do “Radar”
- Pouco registros por requisição
- Roubo de Dados em pequenos pedaços
- Persistente e paciente



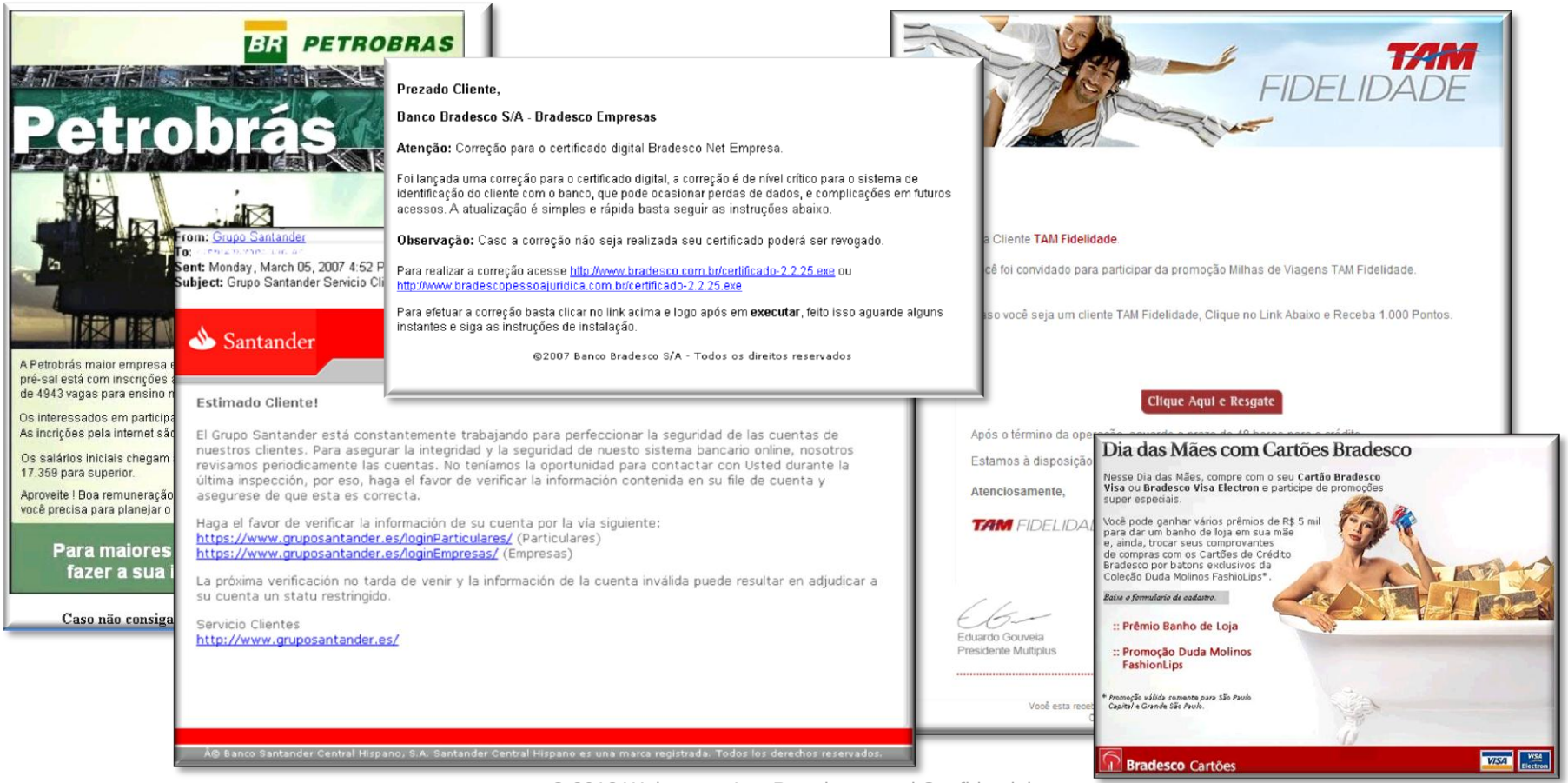
Evasão de Segurança de Email

- Técnica de “Spear-phishing”
- Isca dentro de links em emails
- Infecção acontece depois da entrega
- Segurança de email apenas vê um email limpo





Exemplos Recentes



Exemplo Websense - 15/10/12

From: No Reply-SPIFF Announcement [mailto:Sales-SPIFFs@applerts.net]
Sent: Monday, October 15, 2012 8:10 PM
To: Smith, Louis
Subject: Q4 SPIFF

Louis Smith,

We are excited to annnounce a Q4 SPIFF for WSGA and DLP. Please login to review and discuss it.

Keep up the good work and lets make Q4 your MONEY making QT.

Your Management Team.

websense

Note: This is an automated email. Please do not reply.

Click here to report this email as spam.

Necessidades dos Clientes

Resolvendo Problemas

TRITON™

- **Web security**
- **Email security**
- **Data security**
- **Mobile security**

Novas Necessidades de Segurança

- Proteção contra Ameaças Avançadas
- Contenção de Roubo de Dados
- Dashboard de Ameaças com Alertas
- Relatório Forense com Integração SIEM
- “Sandboxing” para Análise de Malware
- Performance com Defesa e Precisão

Plataforma de Segurança

websense®
TRITON™

- Arquitetura Unificada
- Inteligência de Segurança Unificada
- Console Unificada
- Políticas e Relatórios Unificados

websense® TRITON

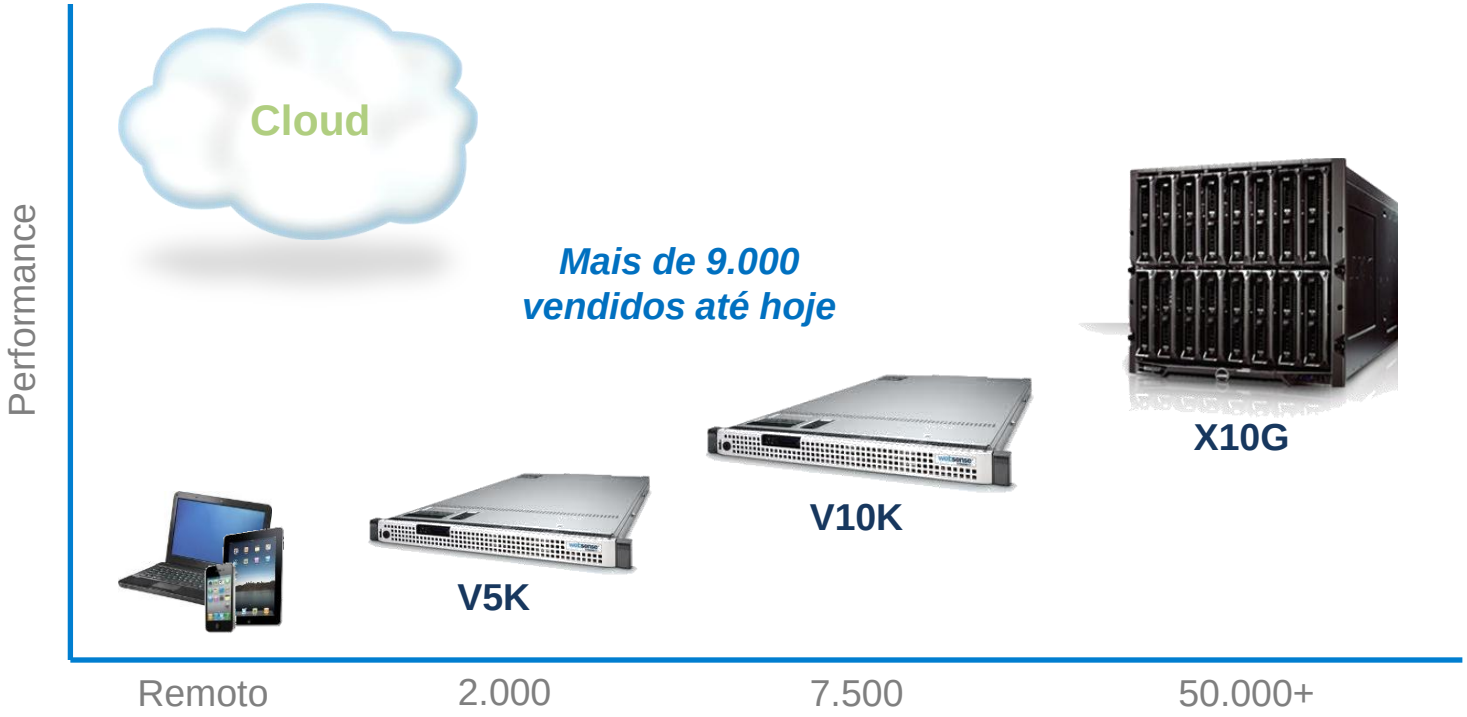
Unified Architecture/Security Intelligence/Console/Policy/Reporting

websense®
THREATSEEKER NETWORK
Unites over 850M research points.
Analyzes 3-5B requests per day.

websense®
ACE
ADVANCED CLASSIFICATION ENGINE

websense®
SECURITY LABS

Appliances



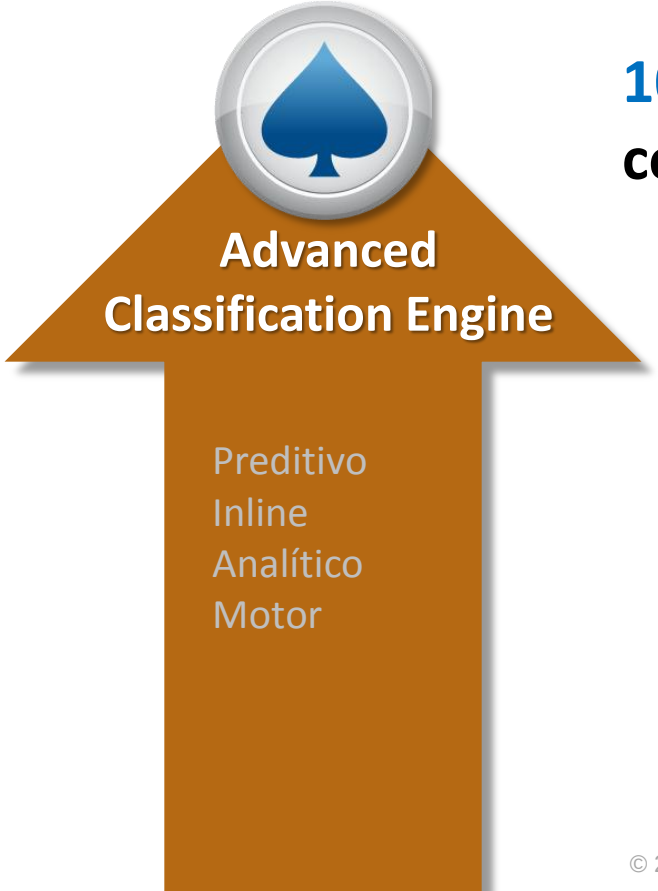
Novas Funcionalidades

Avançando com a Arquitetura TRITON

TRITON™

- **Web security**
- **Email security**
- **Data security**
- **Mobile security**

Novas Defesas ACE



10 Novas Defensas no ACE para proteção contra Ameaças Avançadas e Roubo de Dados

Advanced Malware Payloads ←
Potentially Exploited Documents ← **INBOUND**
Mobile Malware ←
Criminal Encrypted Uploads →
Files Containing Passwords →
Advanced Malware Command & Control →
Unauthorized Mobile Marketplaces → **OUTBOUND**
OCR (Optical Character Recognition) →
Drip (Stateful) DLP →
Geo-Location →

Proteção e Contenção

websense

Criminal Encrypted Uploads

Password File Data Theft

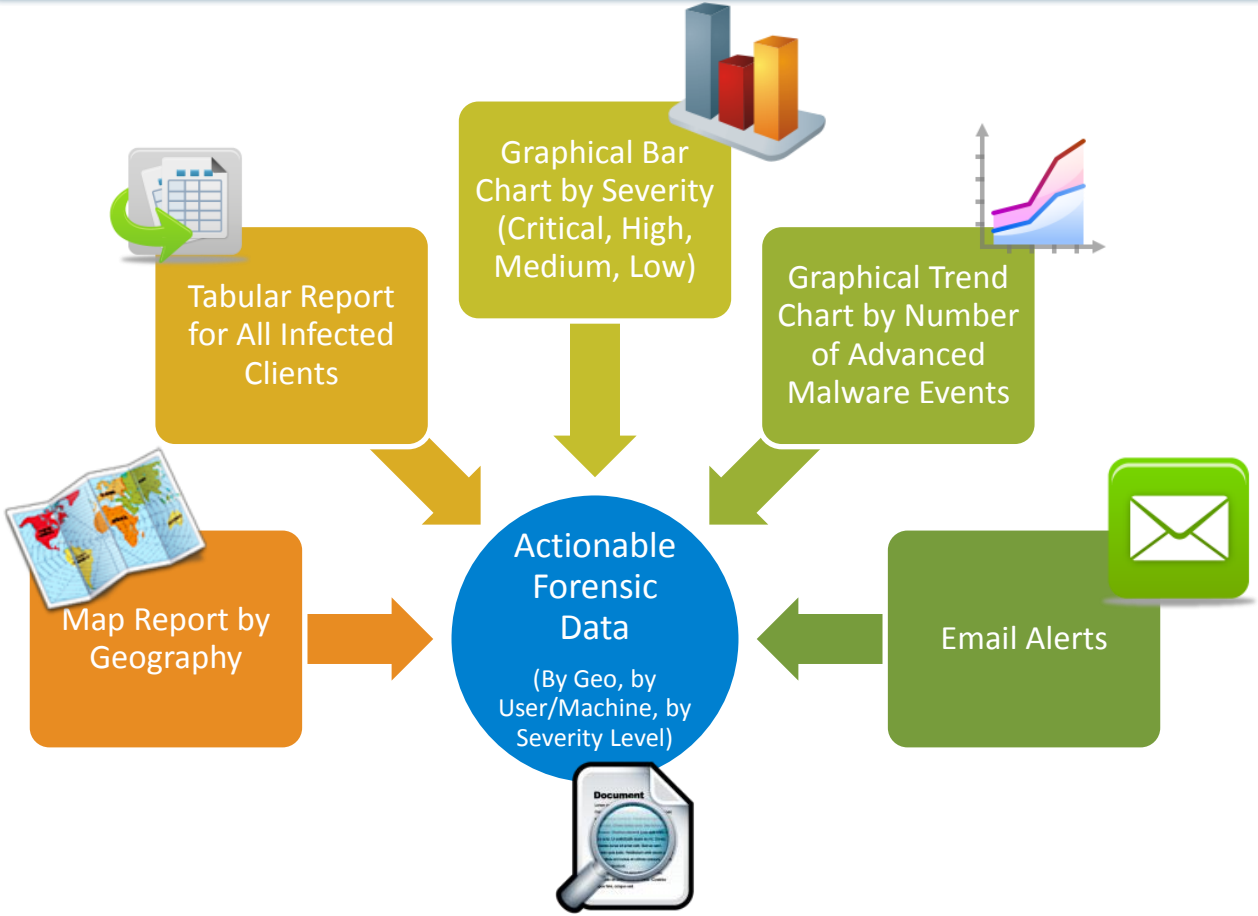
Image OCR/Text Analysis

One data record

Drip (Stateful) DLP

Cloud Sandboxing for Email

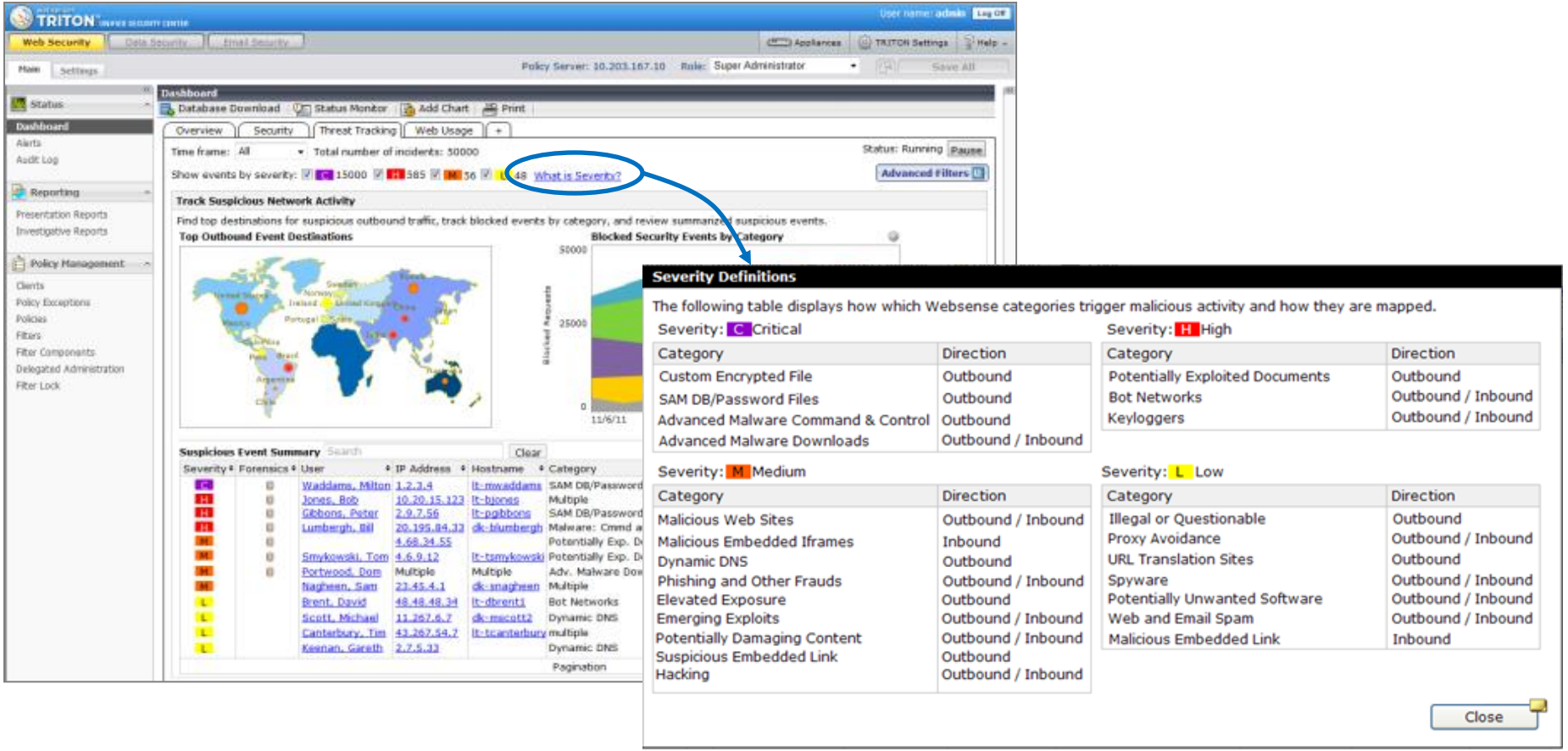
Advanced Malware Reporting Flow



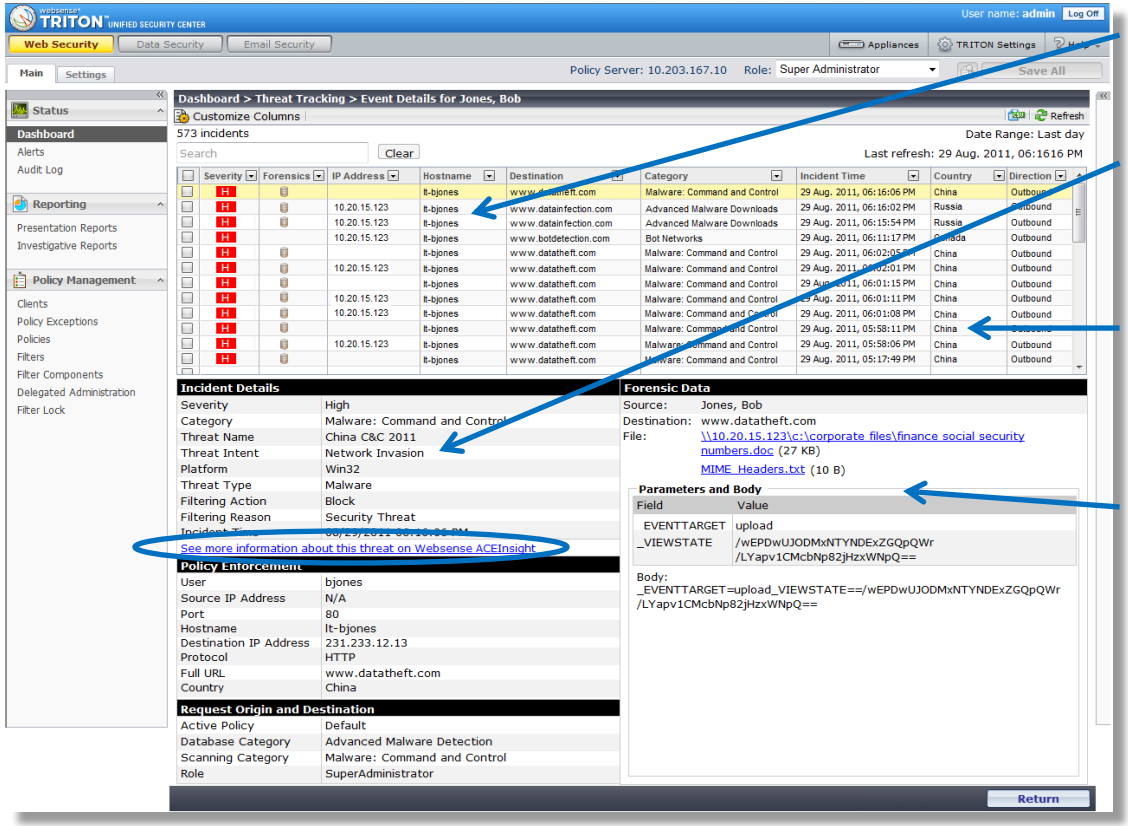
Desenvolvido para destacar incidentes que necessitam de ação

- Identifica cliente que necessita remediação
- Captura informação que tentaram roubar ou vazar
- Relatório para aumentarem consciência de ataques em progresso

Dashboard de Ameaças



Relatório Forense



- Sabe **QUEM** foi comprometido
- Sabe **COMO** o malware opera (intenção)
- Sabe para **ONDE** o dado foi enviado
- Sabe **O QUE** foi prevenido de ser roubado

Websense CSI: Serviço de “Sandbox” para Malware

websense

Analysis Report:

- HTTP traffic to server hosting malicious content
- Downloads malicious executable file(s)
- HTTP traffic shows characteristics of a malware family (ZeuS)
- Drops and runs executable file(s) in a directory of the user profile
- Drops and runs executable file(s) in a Windows system directory
- Injects and executes code in remote process
- Adds a registry key to automatically start an executable when the system starts
- HTTP traffic to server hosting potentially malicious content
- Writes to the filesystem in a Windows system directory
- Writes to the filesystem in a directory of the user profile often used by malware
- Executes the Windows command shell program

Analysis Result:

Malicious

Analysis Events:

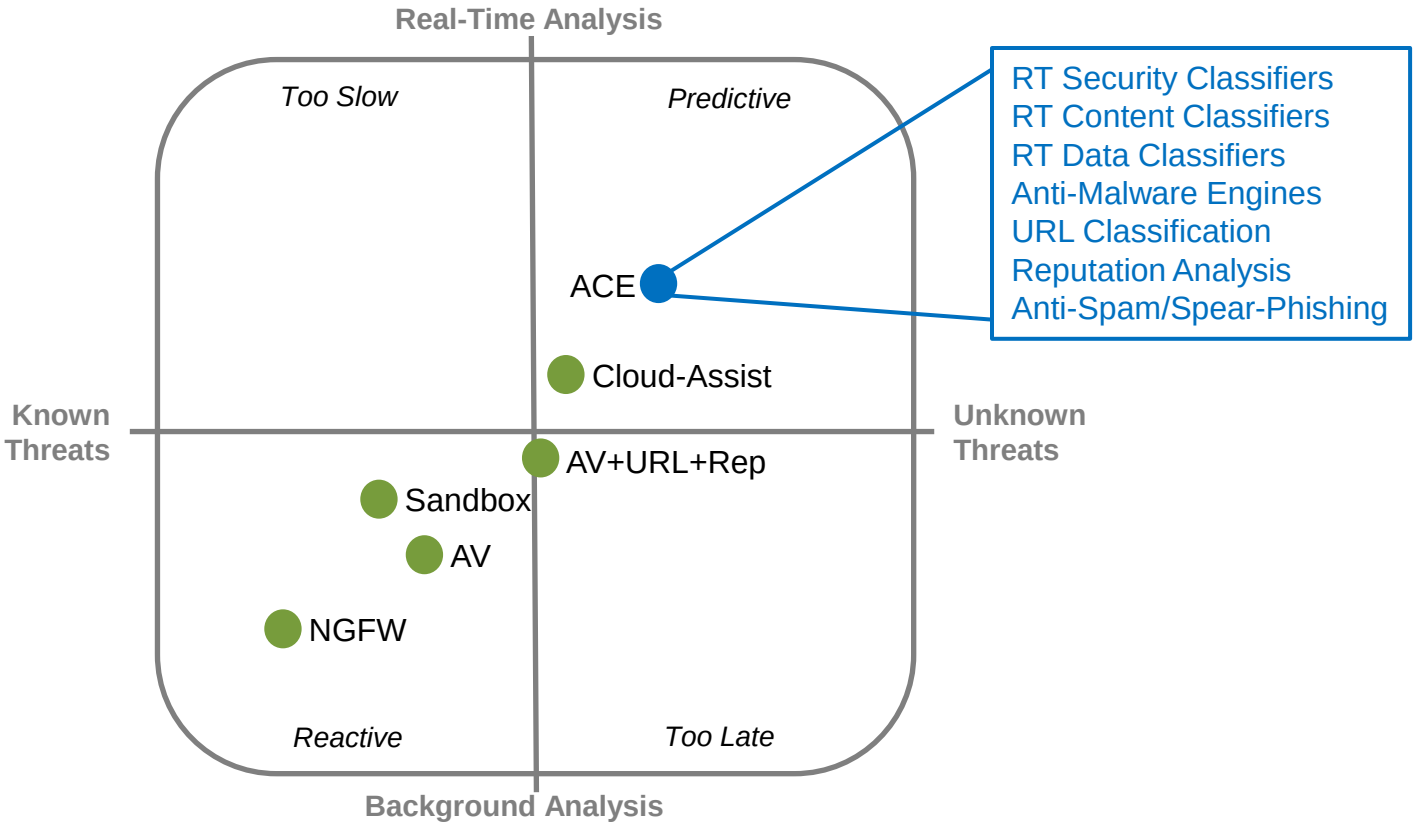
List of requested HTTP URLs:

URL	IP	Method	Status	MIME	Analysis	Cat
s2.streamscene.cc/mspeed.exe	94.23.40.65	GET	200	application/x-msdos-program application/x-dosexec		Potentially Damaging Con
tradingcenter.cc/NOT_ZUES/gate.php	217.23.4.77	POST	200	text/html; charset=UTF-8 application/octet-stream		Malicious Web Sites
www.google.com/webhp	74.125.226.80	GET	200	text/html; charset=UTF-8 text/html		Search Engines and Portal
tradingcenter.cc/NOT_ZUES/config.bin	217.23.4.77	GET	200	application/octet-stream application/octet-stream		Malicious Web Sites
tradingcenter.cc/NOT_ZUES/gate.php	217.23.4.77	POST	200	text/html; charset=UTF-8 application/octet-stream		Malicious Web Sites
tradingcenter.cc/snapbn/ip.php	217.23.4.77	GET	200	text/html; charset=UTF-8 text/plain		Malicious Web Sites
tradingcenter.cc/NOT_ZUES/gate.php	217.23.4.77	POST	200	text/html; charset=UTF-8 application/octet-stream		Malicious Web Sites

Sete Funcionalidades Pioneiras

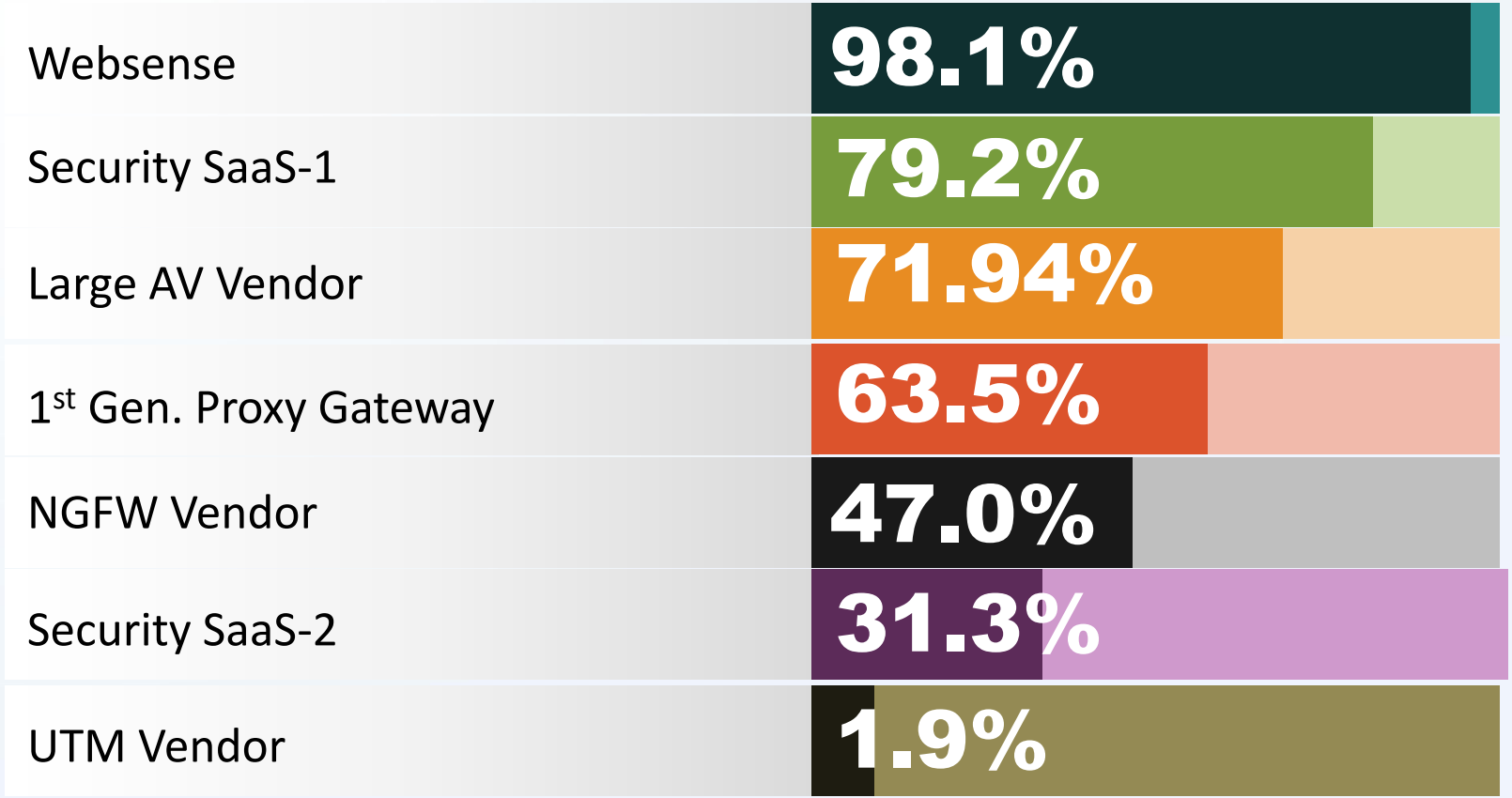
- Serviço de “Sandbox” Online
- “Sandboxing” na Nuvem para Links em Email
- Detecção de Criptografia Criminal
- Roubo de Arquivos com Senha
- OCR para Data-in-Motion
- Drip DLP
- Captura de Dados Forense

Eficiência das Defesas



Ataques Web Zero Day – Q1 2012

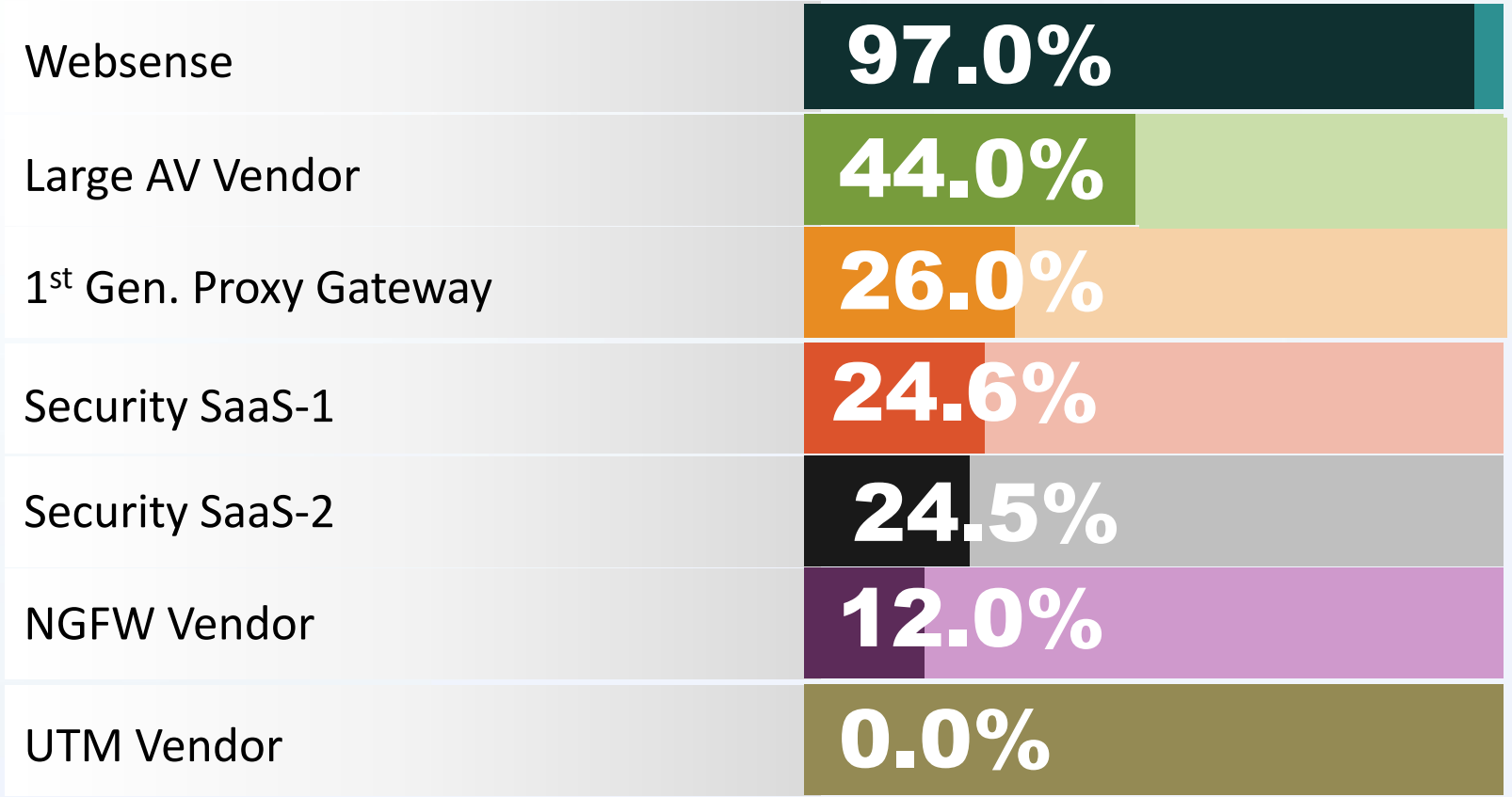
websense®



URLs containing malware, Q1 2012

Comunicação Command and Control – Q1 2012

websense®



URLs containing malware, Q1 2012

OBRIGADO!

Graziani Pengue
gpengue@websense.com

TRITON™

- Web security
- Email security
- Data security
- Mobile security