



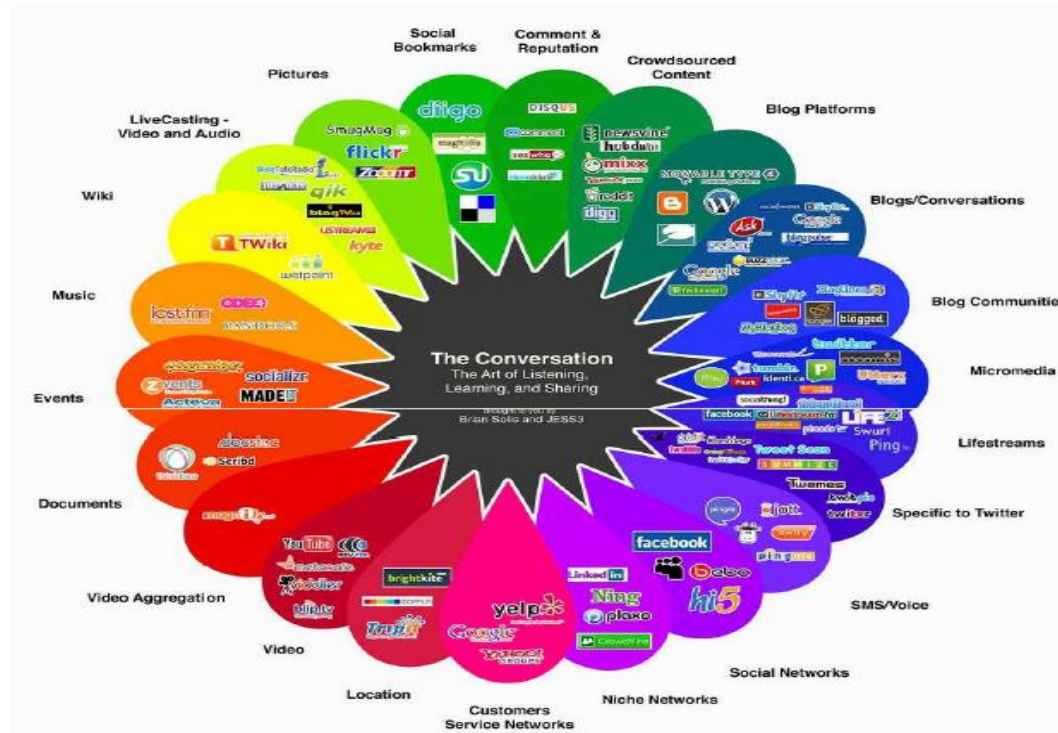
Cássio de Alcântara Regional Sales Manager



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

websense

Quais são as novas fronteiras?



Quais são as novas ferramentas?



Orkut

You Tube

vimeo

foursquare

Pinterest



Linked in

twitter

flickr



WIKIPEDIA



LIKE



e-mail



add friends

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



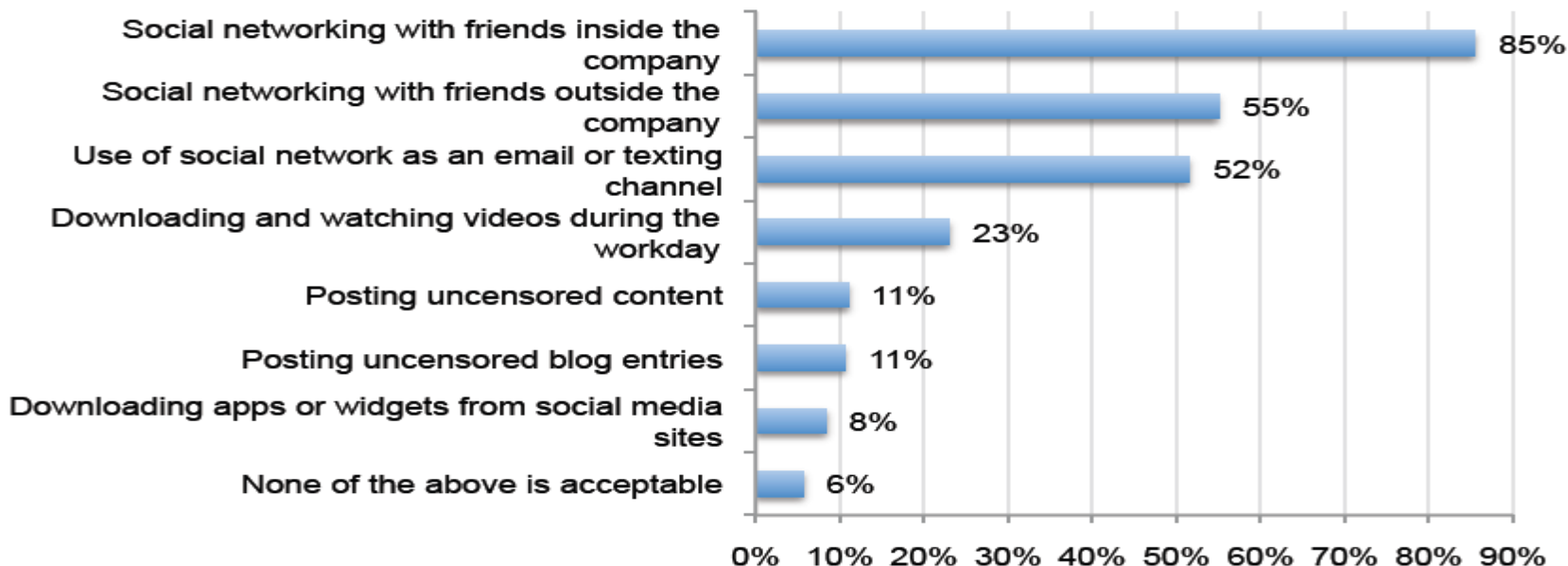
Strongly agree & agree response combined



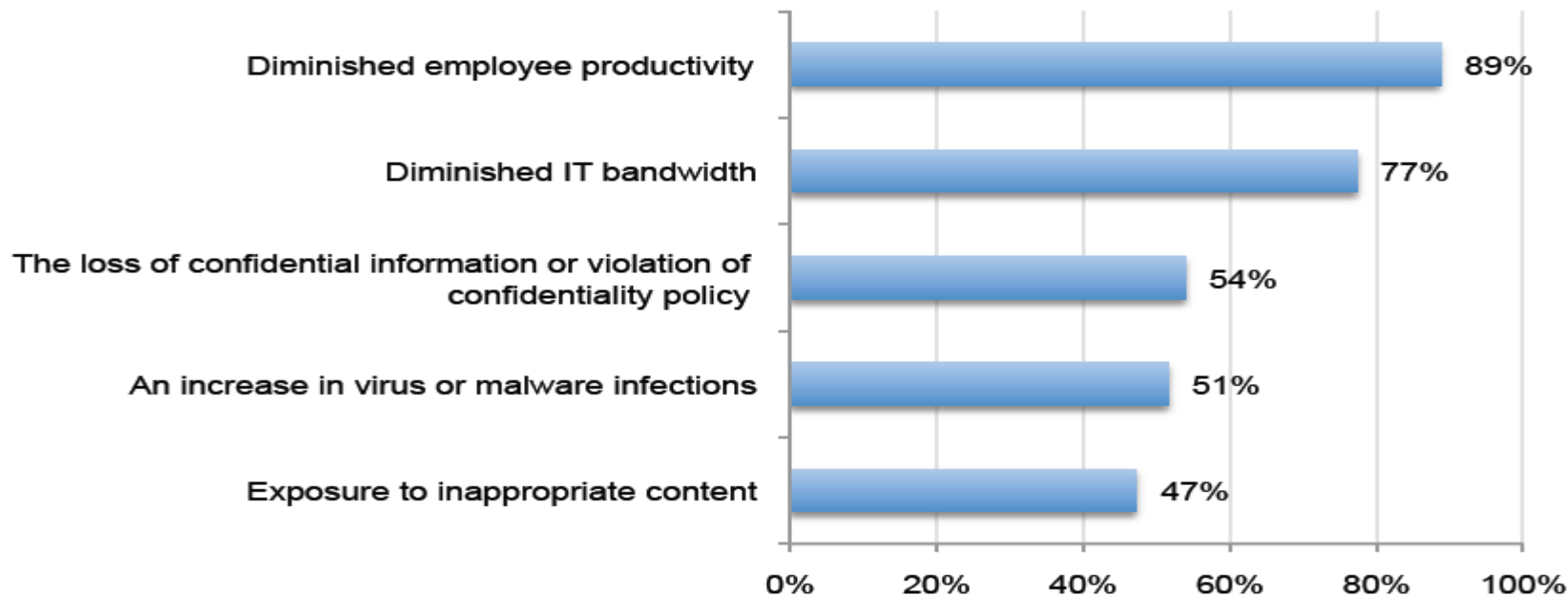
O que voce considera aceitável para o uso de redes sociais no trabalho?



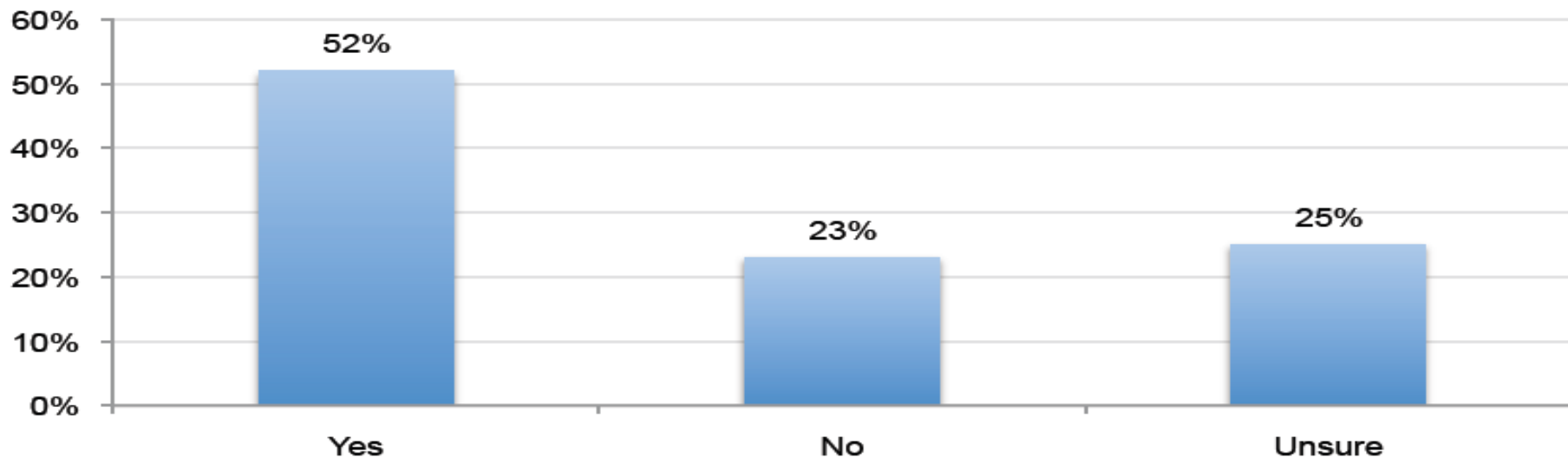
Bar Chart 2: What is considered the acceptable use of social media in the workplace



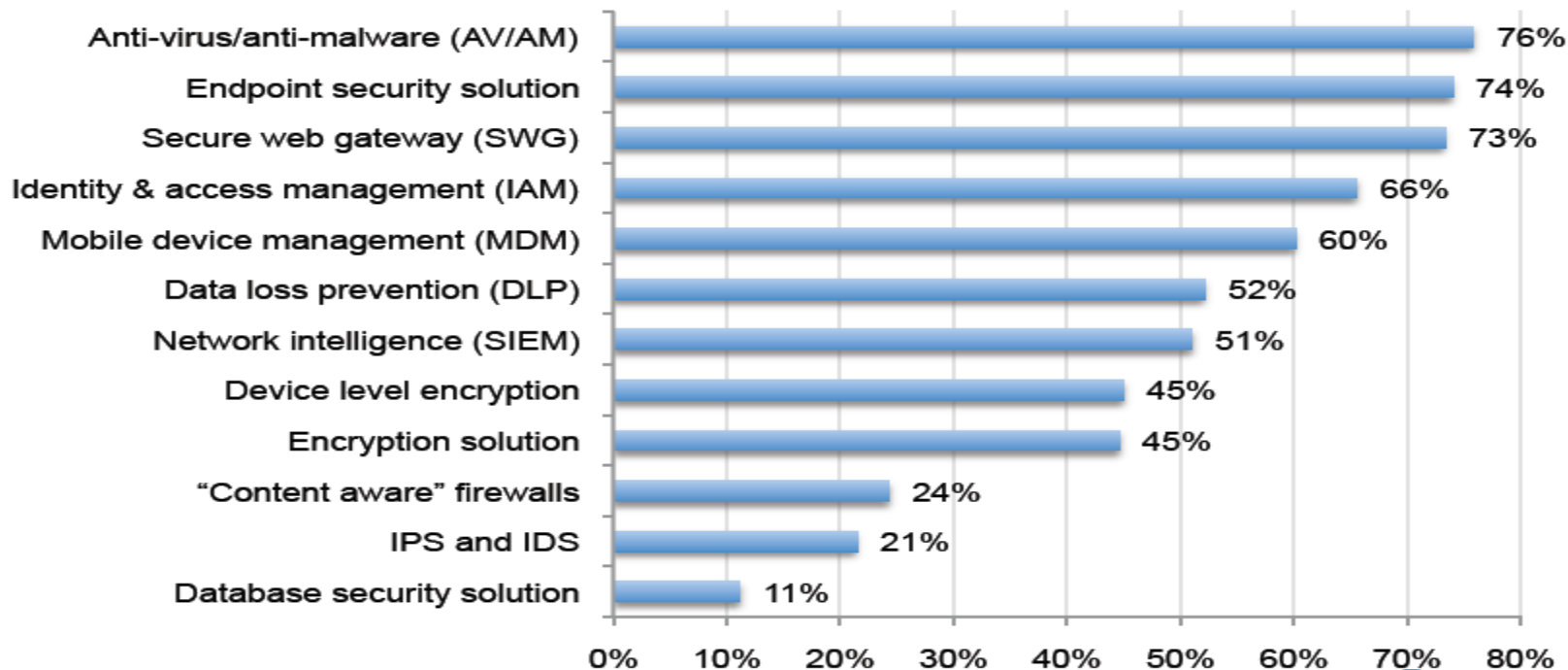
Quais as consequências da utilização de redes sociais no trabalho?



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



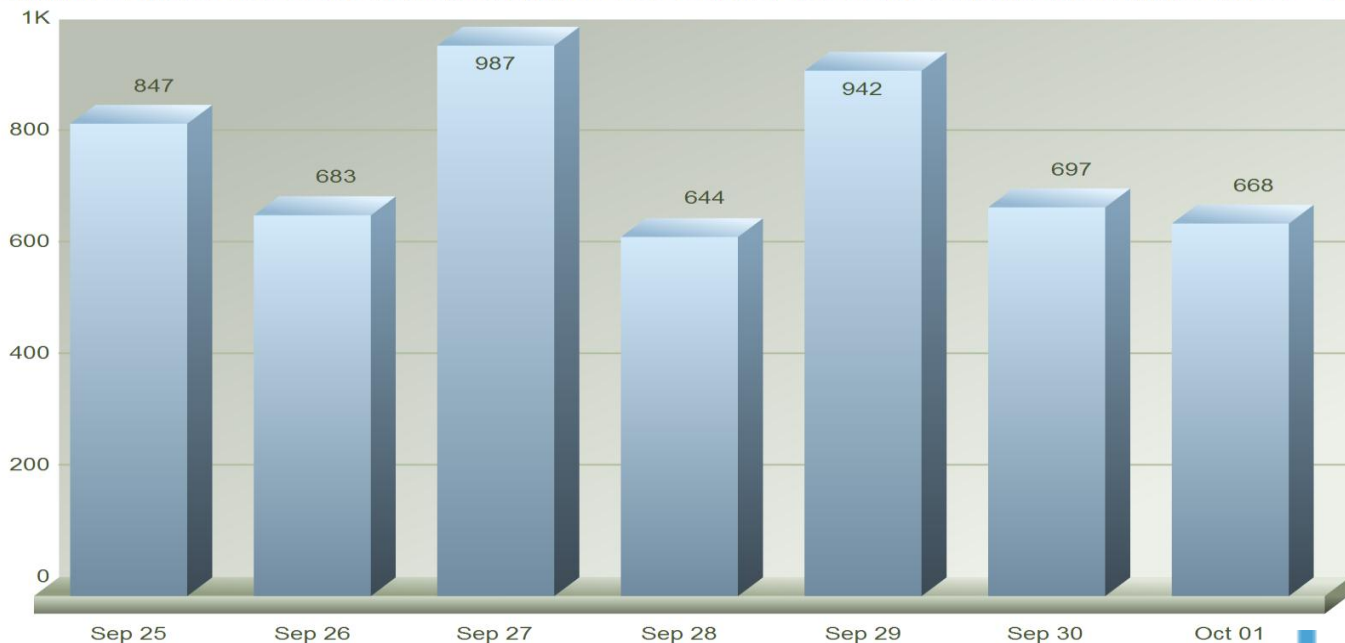
Qual medida sua organização considera mais eficaz na redução dos riscos de segurança na utilização de redes sociais?



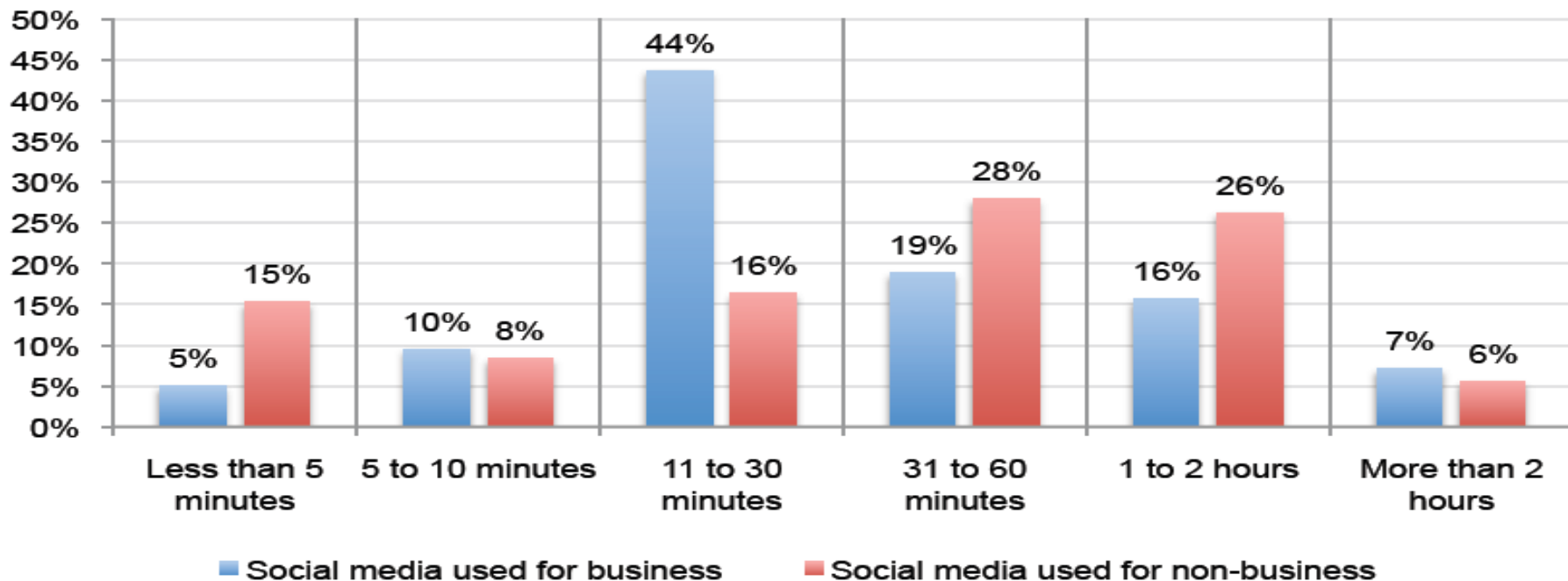
Quantidade de ameaças descobertas por dia que um anti virus não identifica!



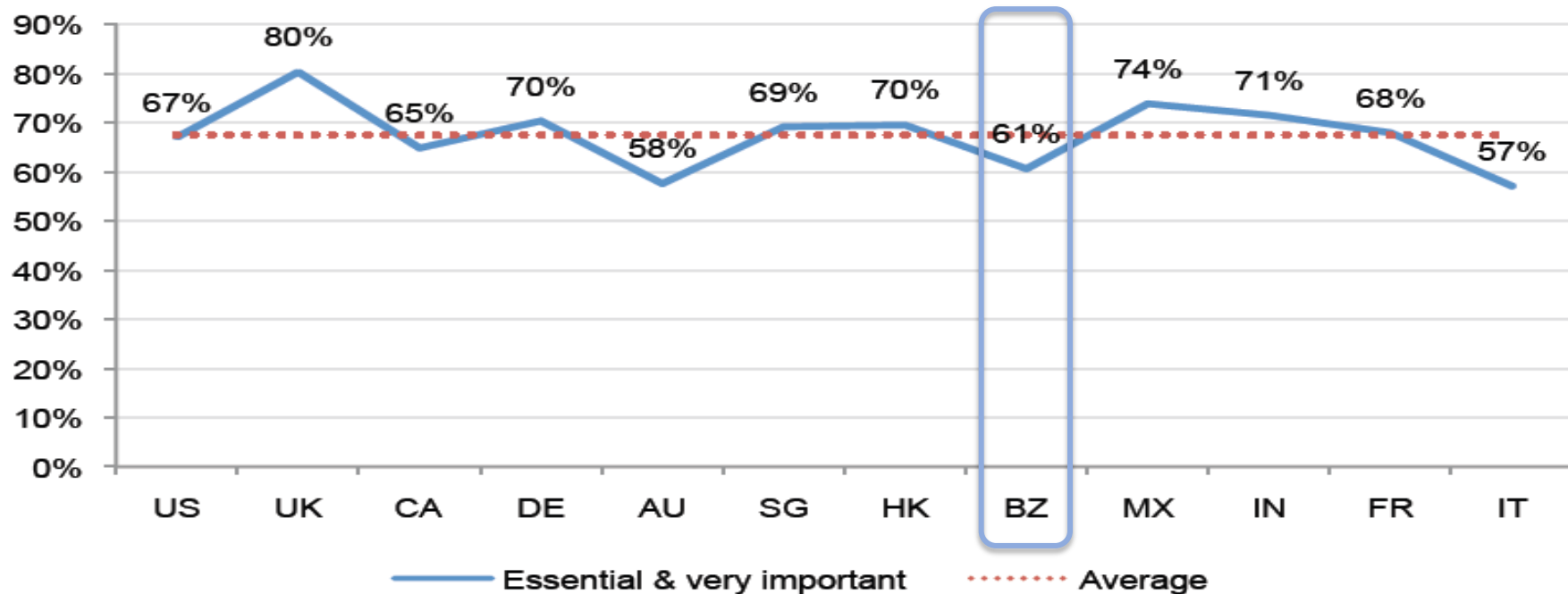
Number of Viruses Detected by Websense Advanced Detection NOT detected by 5 top Anti-Virus Engines (Sep 25 - Oct 01)



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



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



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,
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





“ 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®



Recon



Lure



Redirect



**Exploit
Kit**



**Dropper
File**



**Call
Home**



**Data
Theft**



Recon



Lure

CONSCIÊNCIA

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



Redirect



**Exploit
Kit**

ANÁLISE EM TEMPO REAL

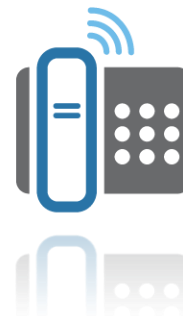
- Cód do Browser e Scripts
- Análise de Link
- Análise Exploit
- Pontuação Composta
- Preditivo

DEFENSAS INLINE

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



**Dropper
File**



**Call
Home**

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™

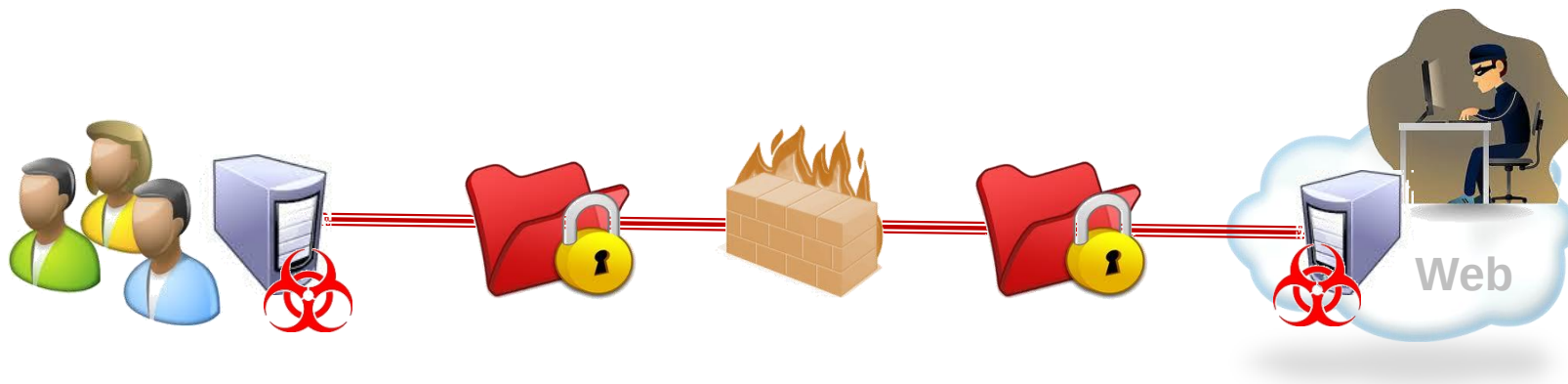
— Web security

— Email security

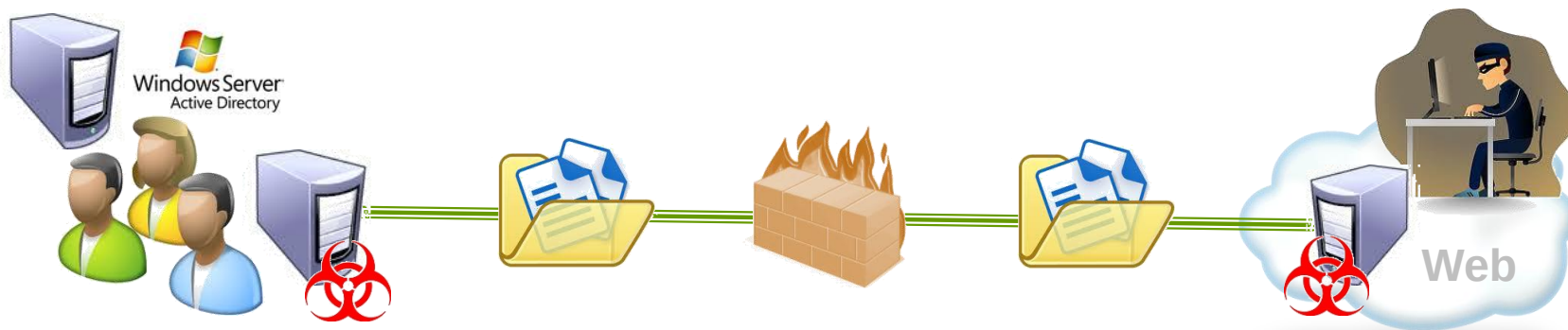
— Data security

— Mobile security

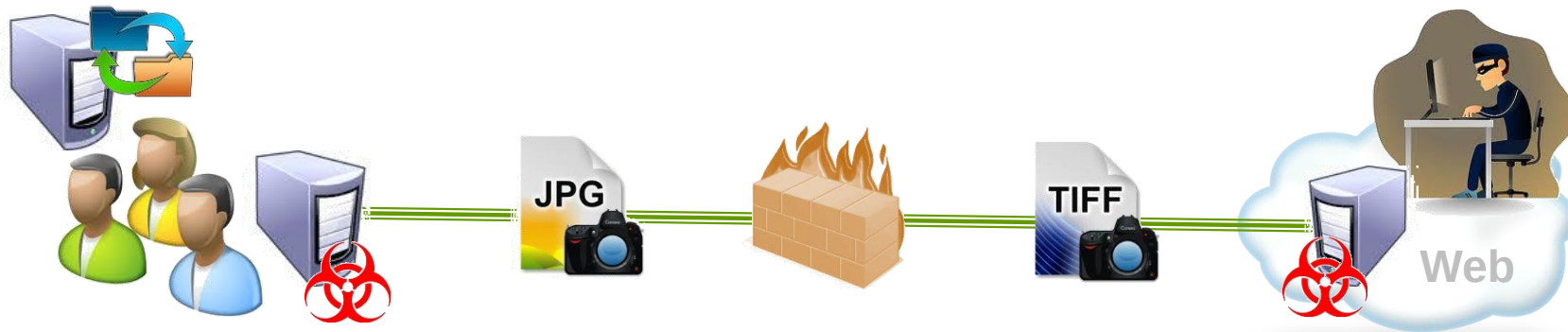
- Criptografia Proprietária
- Roubo de Dados
- Criado por Toolkit Crimeware
- “Ponto Cego” para as Defesas



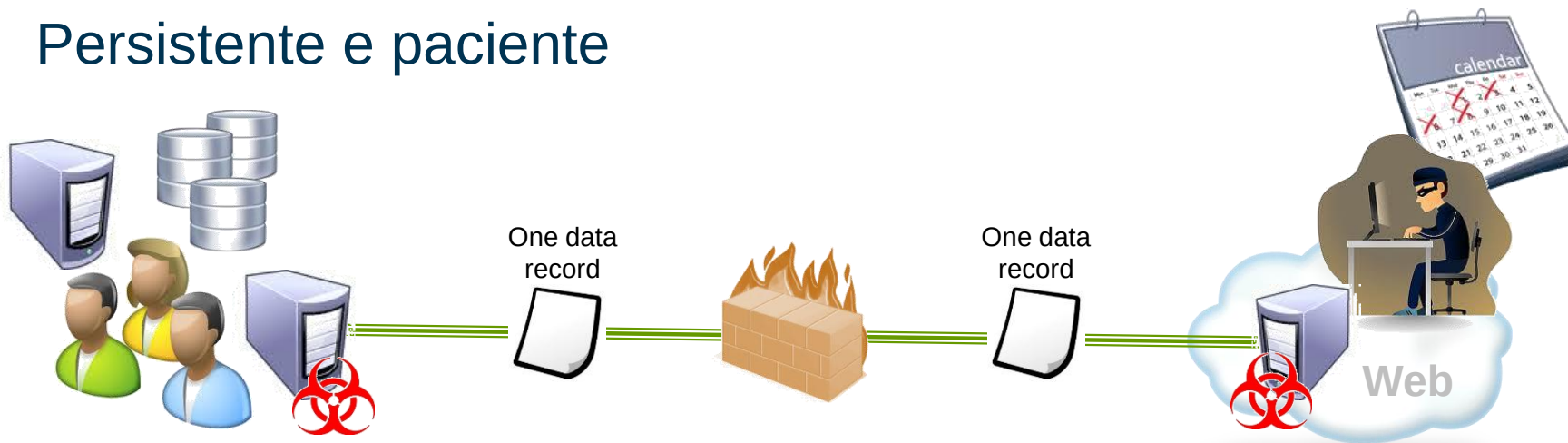
- Arquivos contendo senhas
- Active Directory/Banco de Dados SAM
- Aumento do Alcance/Controle dentro do Alvo
- Privilégios Administrativos após Infiltrado



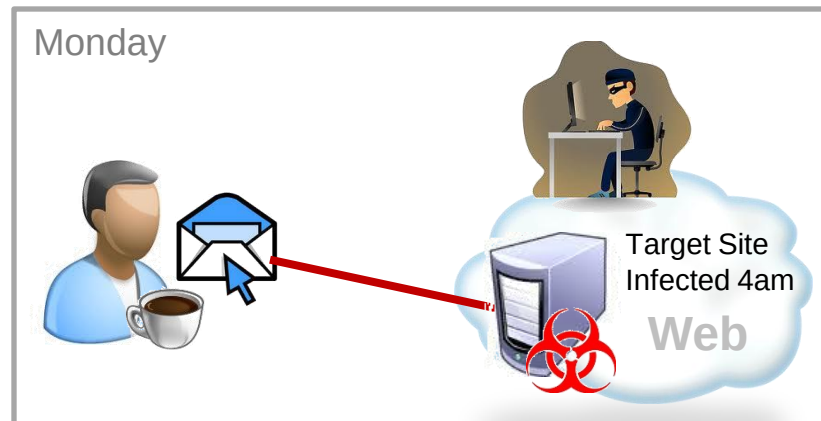
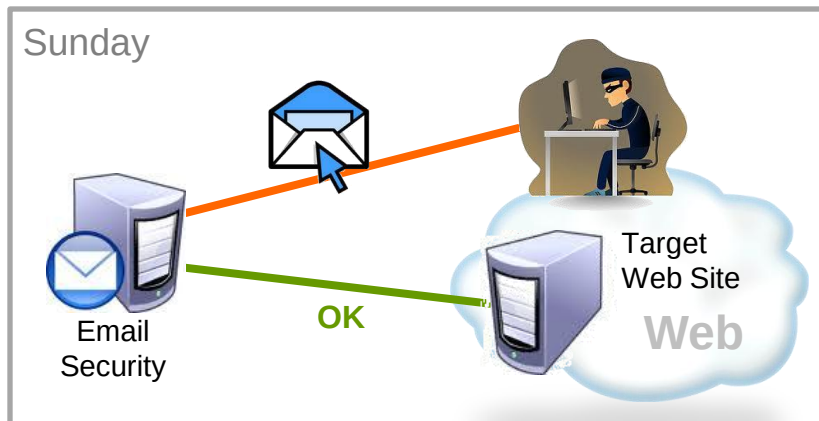
- Arquivos de Imagem
- Informação Confidencial
- Fotos de Smartphones
- “Ponto Cego” para as Defesas



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



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





BR PETROBRAS

Petrobrás

From: Grupo Santander
To: [REDACTED]
Sent: Monday, March 05, 2007 4:52 P
Subject: Grupo Santander Servicio Cl

A Petrobrás maior empresa de pré-sal está com inscrições de 4943 vagas para ensino m

Os interessados em participa

As inscrições pela internet são

Os salários iniciais chegam a 17.359 para superior.

Aproveite! Boa remuneração, você precisa para planejar o

Para maiores fazer a sua

Caso não consiga



Estimado Cliente!

El Grupo Santander está constantemente trabajando para perfeccionar la seguridad de las cuentas de nuestros clientes. Para asegurar la integridad y la seguridad de nuestro sistema bancario online, nosotros revisamos periódicamente las cuentas. No teníamos la oportunidad para contactar con Usted durante la última inspección, por eso, haga el favor de verificar la información contenida en su file de cuenta y asegurese de que esta es correcta.

Haga el favor de verificar la información de su cuenta por la vía siguiente:
<https://www.gruposantander.es/loginParticulares/> (Particulares)
<https://www.gruposantander.es/loginEmpresas/> (Empresas)

La próxima verificación no tarda de venir y la información de la cuenta inválida puede resultar en adjudicar a su cuenta un statu restringido.

Servicio Clientes
<http://www.gruposantander.es/>

A© Banco Santander Central Hispano, S.A. Santander Central Hispano es una marca registrada. Todos los derechos reservados.

Prezado Cliente,

Banco Bradesco S/A - Bradesco Empresas

Atenção: Correção para o certificado digital Bradesco Net Empresa.

Foi lançada uma correção para o certificado digital, a correção é de nível crítico para o sistema de identificação do cliente com o banco, que pode ocasionar perdas de dados, e complicações em futuros acessos. A atualização é simples e rápida basta seguir as instruções abaixo.

Observação: Caso a correção não seja realizada seu certificado poderá ser revogado.

Para realizar a correção acesse <http://www.bradesco.com.br/certificado-2.2.25.exe> ou <http://www.bradescopeessoa juridica.com.br/certificado-2.2.25.exe>

Para efetuar a correção basta clicar no link acima e logo após em **executar**, feito isso aguarde alguns instantes e siga as instruções de instalação.

©2007 Banco Bradesco S/A - Todos os direitos reservados



TAM FIDELIDADE

Cliente **TAM Fidelidade**

foi convidado para participar da promoção Milhas de Viagens TAM Fidelidade.

so você seja um cliente TAM Fidelidade, Clique no Link Abaixo e Receba 1.000 Pontos.

Clique Aqui e Resgate

Após o término da operação, o cliente receberá e passará de 10 horas para o sistema.

Estamos à disposição

Atenciosamente,

TAM FIDELIDADE

Eduardo Gouveia
Presidente Multiplus

Você está recad

Dia das Mães com Cartões Bradesco

Nesse Dia das Mães, compre com o seu **Cartão Bradesco Visa ou Bradesco Visa Electron** e participe de promoções super especiais.

Você pode ganhar vários prêmios de R\$ 5 mil para dar um banho de loja em sua mãe e, ainda, trocar seus comprovantes de compras com os Cartões de Crédito Bradesco por batons exclusivos da Coleção Duda Molinos FashionLips*.

Baixar o formulário de cadastro.

- Prêmio Banho de Loja
- Promoção Duda Molinos FashionLips

* Promoção válida somente para São Paulo, Capital e Grande São Paulo.

Bradesco Cartões

VISA Visa Electron

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 announce 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.



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

- 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



websense®
TRITON™

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



websense®
THREATSEEKER NETWORK

Unites over 850M research points.
Analyzes 3-5B requests per day.



websense®
ACE ADVANCED
CLASSIFICATION
ENGINE



websense®
SECURITY LABS



Novas Funcionalidades

Avançando com a Arquitetura TRITON

TRITON™

— Web security

— Email security

— Data security

— Mobile security



Advanced Classification Engine

Preditivo
Inline
Analítico
Motor

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

Advanced Malware Payloads ←

Potentially Exploited Documents ←

Mobile Malware ←

INBOUND

Criminal Encrypted Uploads →

Files Containing Passwords →

Advanced Malware Command & Control →

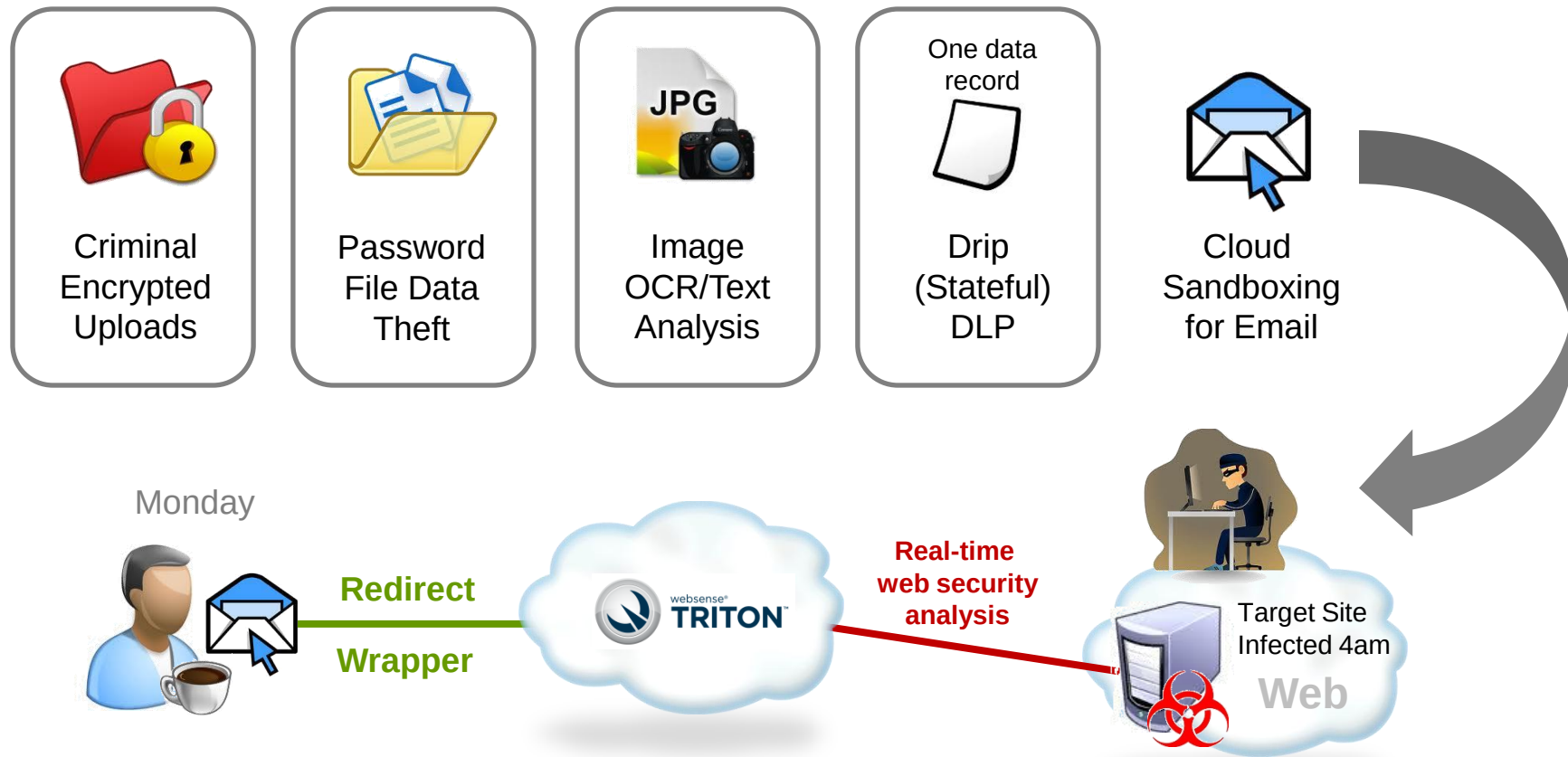
Unauthorized Mobile Marketplaces →

OUTBOUND

OCR (Optical Character Recognition) →

Drip (Stateful) DLP →

Geo-Location →

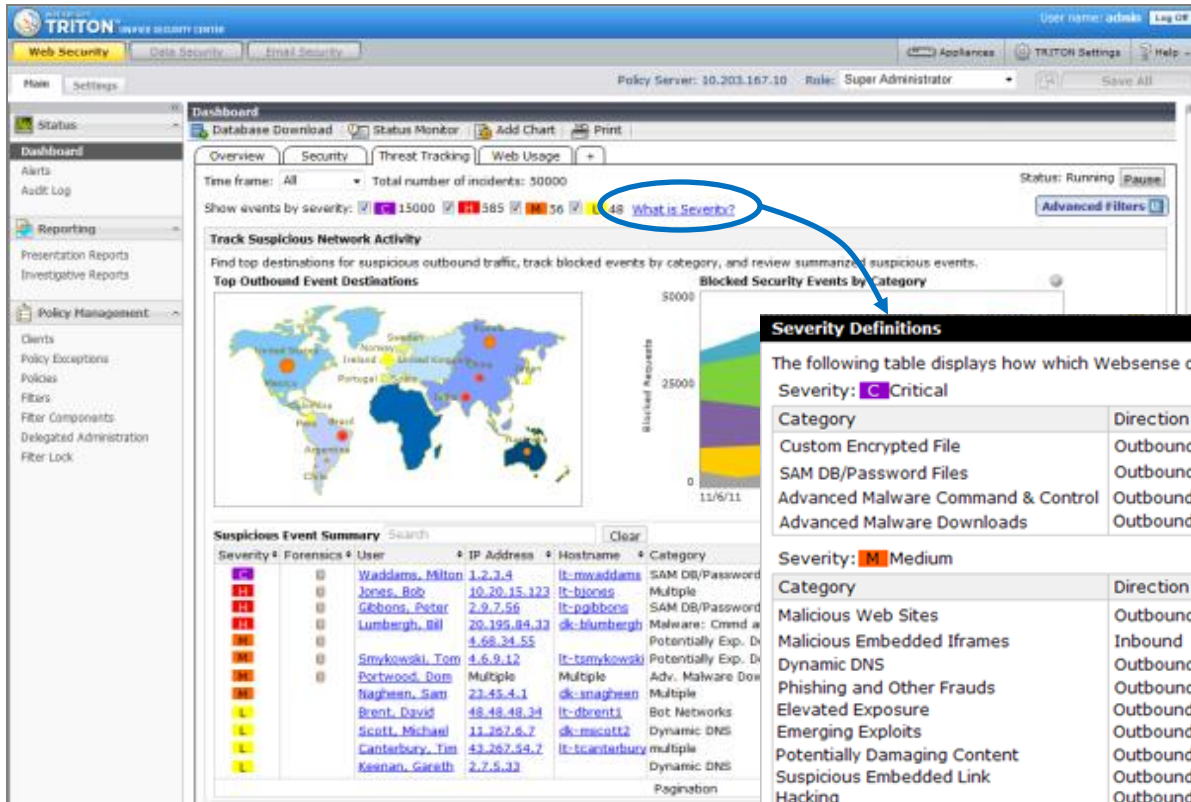




Desenvolvido para destacar incidentes que necessitam de ação

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

Dashboard de Ameaças



Severity Definitions

The following table displays how which Websense categories trigger malicious activity and how they are mapped.

Severity: **C** Critical

Category	Direction
Custom Encrypted File	Outbound
SAM DB/Password Files	Outbound
Advanced Malware Command & Control	Outbound
Advanced Malware Downloads	Outbound / Inbound

Severity: **H** High

Category	Direction
Potentially Exploited Documents	Outbound
Bot Networks	Outbound / Inbound
Keyloggers	Outbound / Inbound

Severity: **M** Medium

Category	Direction
Malicious Web Sites	Outbound / Inbound
Malicious Embedded Iframes	Inbound
Dynamic DNS	Outbound
Phishing and Other Frauds	Outbound / Inbound
Elevated Exposure	Outbound
Emerging Exploits	Outbound / Inbound
Potentially Damaging Content	Outbound / Inbound
Suspicious Embedded Link	Outbound
Hacking	Outbound / Inbound

Severity: **L** Low

Category	Direction
Illegal or Questionable	Outbound
Proxy Avoidance	Outbound / Inbound
URL Translation Sites	Outbound
Spyware	Outbound / Inbound
Potentially Unwanted Software	Outbound / Inbound
Web and Email Spam	Outbound / Inbound
Malicious Embedded Link	Inbound

Close

Dashboard > Threat Tracking > Event Details for Jones, Bob

573 incidents

Search [Clear]

Date Range: Last day
Last refresh: 29 Aug. 2011, 06:16:16 PM

Severity	Forensics	IP Address	Hostname	Destination	Category	Incident Time	Country	Direction
[H]	[H]	10.20.15.123	it-bjones	www.datatheft.com	Malware: Command and Control	29 Aug. 2011, 06:16:05 PM	China	Outbound
[H]	[H]	10.20.15.123	it-bjones	www.datatheft.com	Advanced Malware Downloads	29 Aug. 2011, 06:16:02 PM	Russia	Outbound
[H]	[H]	10.20.15.123	it-bjones	www.datatheft.com	Advanced Malware Downloads	29 Aug. 2011, 06:15:54 PM	Russia	Outbound
[H]	[H]	10.20.15.123	it-bjones	www.botdetection.com	Bot Networks	29 Aug. 2011, 06:11:17 PM	Canada	Outbound
[H]	[H]	10.20.15.123	it-bjones	www.datatheft.com	Malware: Command and Control	29 Aug. 2011, 06:02:05 PM	China	Outbound
[H]	[H]	10.20.15.123	it-bjones	www.datatheft.com	Malware: Command and Control	29 Aug. 2011, 06:02:01 PM	China	Outbound
[H]	[H]	10.20.15.123	it-bjones	www.datatheft.com	Malware: Command and Control	29 Aug. 2011, 06:01:15 PM	China	Outbound
[H]	[H]	10.20.15.123	it-bjones	www.datatheft.com	Malware: Command and Control	29 Aug. 2011, 06:01:11 PM	China	Outbound
[H]	[H]	10.20.15.123	it-bjones	www.datatheft.com	Malware: Command and Control	29 Aug. 2011, 05:58:11 PM	China	Outbound
[H]	[H]	10.20.15.123	it-bjones	www.datatheft.com	Malware: Command and Control	29 Aug. 2011, 05:58:06 PM	China	Outbound
[H]	[H]	10.20.15.123	it-bjones	www.datatheft.com	Malware: Command and Control	29 Aug. 2011, 05:17:49 PM	China	Outbound

Incident Details

Severity: High
Category: Malware: Command and Control
Threat Name: China C&C 2011
Threat Intent: Network Invasion
Platform: Win32
Threat Type: Malware
Filtering Action: Block
Filtering Reason: Security Threat
Incident Time: 29/08/2011 06:16:05 PM

[See more information about this threat on Websense ACEInsight](#)

Forensic Data

Source: Jones, Bob
Destination: www.datatheft.com
File: \\10.20.15.123\c:\corporate files\finance social security numbers.doc (27 KB)
MIME-Headers.txt (10 B)

Parameters and Body

Field	Value
EVENTTARGET	upload
_VIEWSTATE	/wEPdWUJODMxNTYNDExZGQpQWw
	/LYapv1CMcbNp82jHzxWNPq==

Body:
_EVENTTARGET=upload_VIEWSTATE==/wEPdWUJODMxNTYNDExZGQpQWw
/LYapv1CMcbNp82jHzxWNPq==

Policy Enforcement

User: bjones
Source IP Address: N/A
Port: 80
Hostname: It-bjones
Destination IP Address: 231.233.12.13
Protocol: HTTP
Full URL: www.datatheft.com
Country: China

Request Origin and Destination

Active Policy: Default
Database Category: Advanced Malware Detection
Scanning Category: Malware: Command and Control
Role: SuperAdministrator

Return

- 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

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:



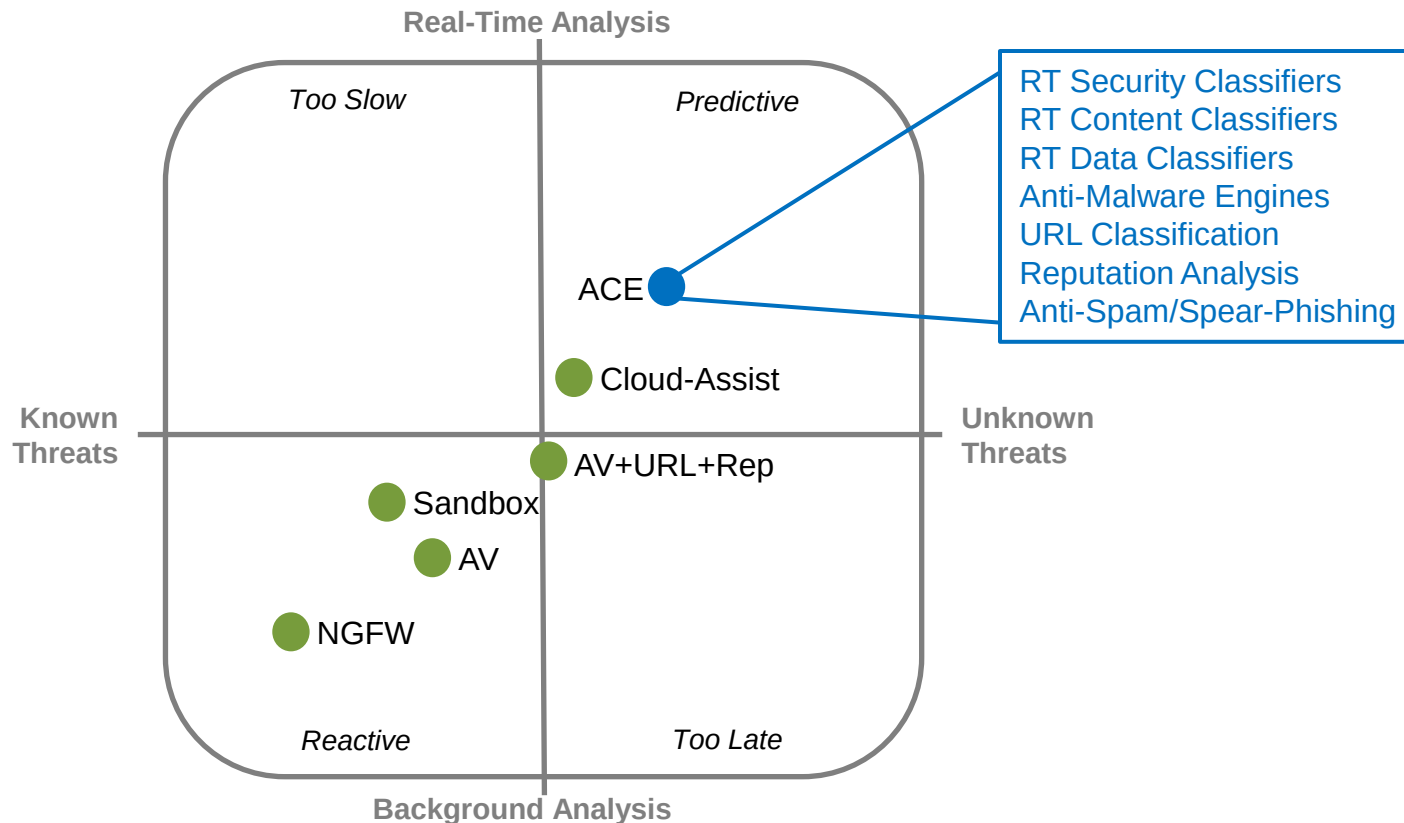
Analysis Events:

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

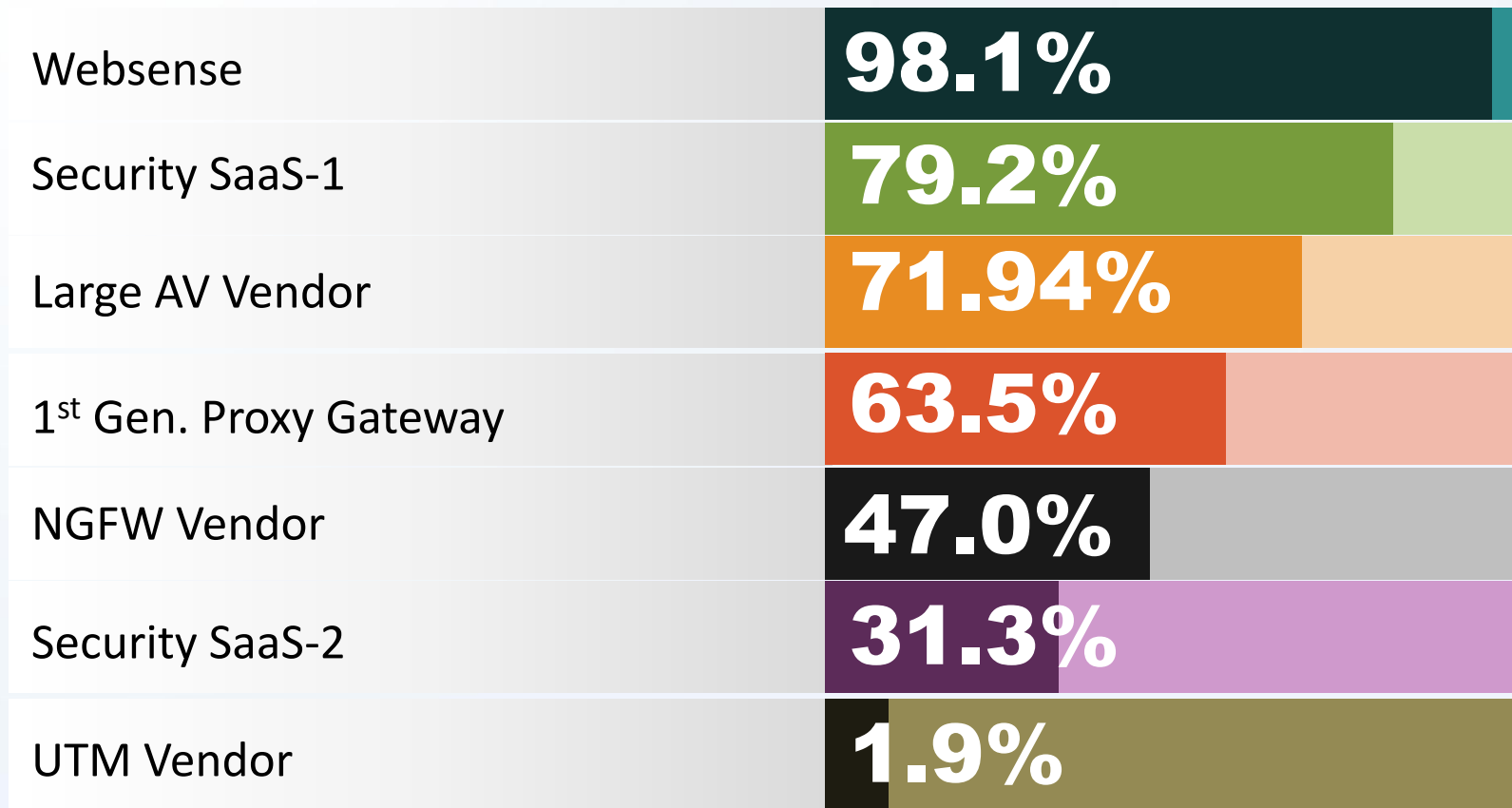


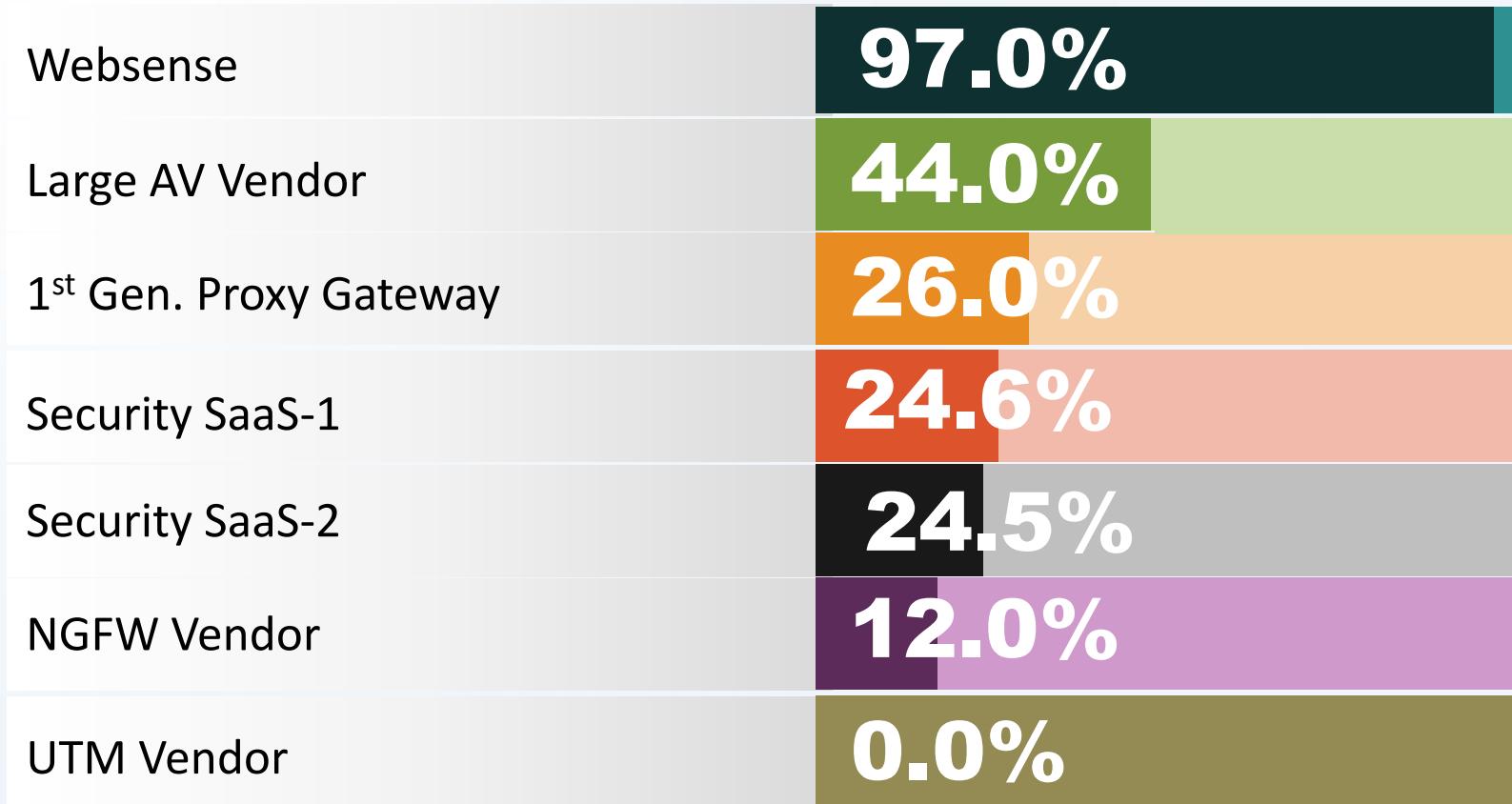
- Serviço de “Sandbox” Online
- “Sandboxing” na Nuvem para Links em Email
- Detecção de Criptografia Criminal
- Roubo de Arquivos com Senha
- OCR para Data-in-Motion
- Drip DLP
- Captura de Dados Forense



Ataques Web Zero Day – Q1 2012

websense®





OBRIGADO!

Graziani Pengue
gpengue@websense.com

TRITON™

Web security

Email security

Data security

Mobile security

