The TRITON Solution

Nordics, October 2012

TRITON™

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

Who Am I?

- John Enger (Senior Sales Engineer)
  - 14 year Industry Veteran
  - 7 Years with Websense
  - Scandinavian Ancestors!
  - Focused on Channel Partner Enablement

Agenda

- A Quick Recap
- The Websense TRITON Solution
- Ask the Panel (Q&A)

A Quick Recap…

TRITON™

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

Legacy Defences are full of holes!

“ 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

Managing many independent systems is HARD!

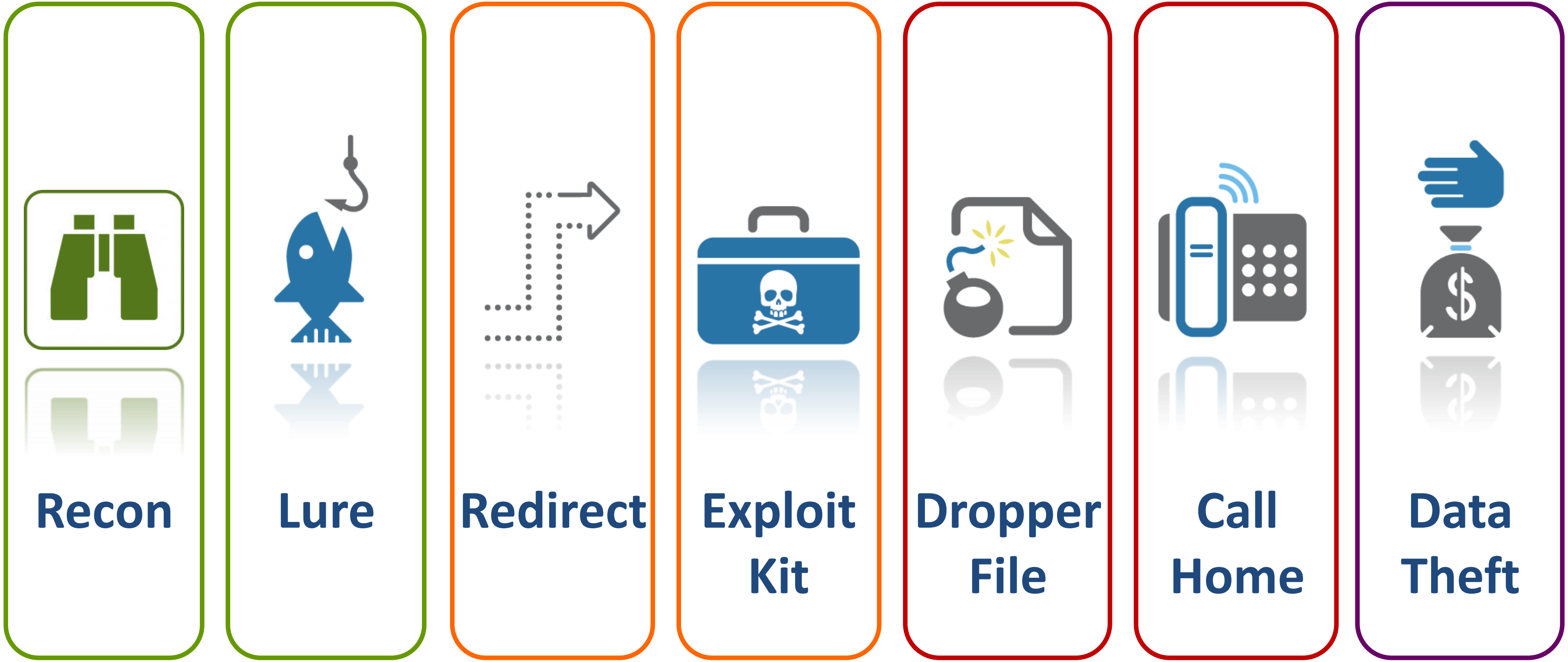
websense®

WE MUST REDUCE COMPLEXITY

The Enemy is in your Blind Spots

- SSL
- Spear Phishing
- AD, SAM, Password extraction
- Custom Encryption
- Malware

Seven Advanced Threat Stages



Recon

Lure

Redirect

Exploit Kit

Dropper File

Call Home

Data Theft

4 Reasons Why Current Defenses Fail

1 PRIMARILY BASED ON SIGNATURE & REPUTATION

History is not a reliable indicator of future behavior.

Signature creation cannot keep up with the dynamic creation of threats

2 LACK OF REAL-TIME INLINE CONTENT ANALYSIS

Collect samples for lab analysis using background processes

Producing new signatures (network/file) and reputations (URL/file)

3 FORWARD FACING ONLY, LACK OUTBOUND PROTECTION

Not data-aware, lack contextual analysis, minimal to no forensic visibility

4 MORE OF THE SAME IN NEW DEPLOYMENT OPTIONS

UTMs, NGFWs, IDSs, Network Threat Monitors

SSL severely impacts performance, or blind to it

The Websense TRITON Solution

TRITON™

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

Unified Platform

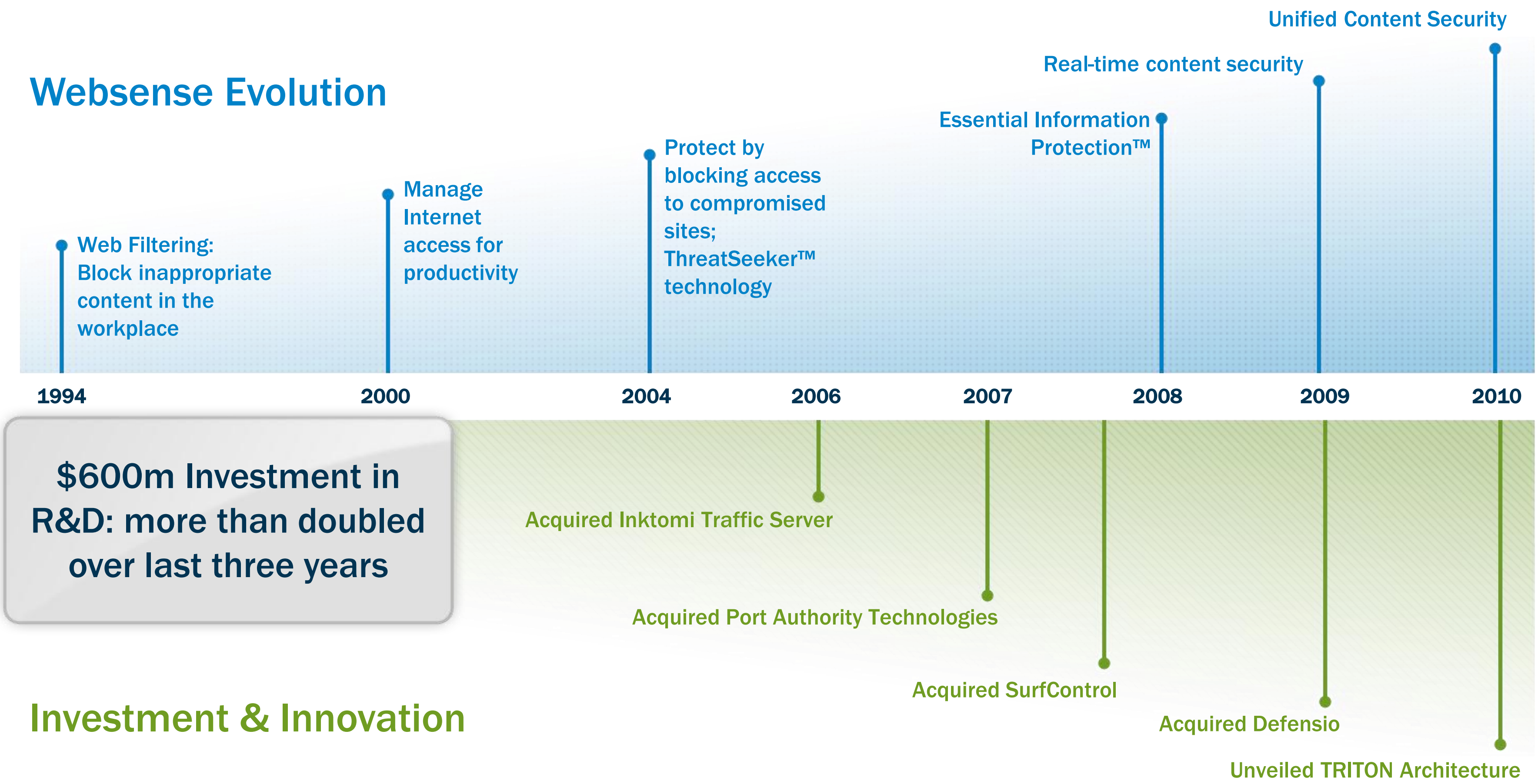
websense®

TRITON™

- Unified architecture
- Unified security intelligence
- Unified console
- Unified policy & reporting

Once Upon a Time…

Websense Evolution



1994 – Web Filtering: Block inappropriate content in the workplace

2000 – Manage Internet access for productivity

2004 – Protect by blocking access to compromised sites; ThreatSeeker™ technology

2008 – Essential Information Protection™

2009 – Real-time content security

2010 – Unified Content Security

2006 – Acquired Inktomi Traffic Server

2007 – Acquired Port Authority Technologies

Acquired SurfControl

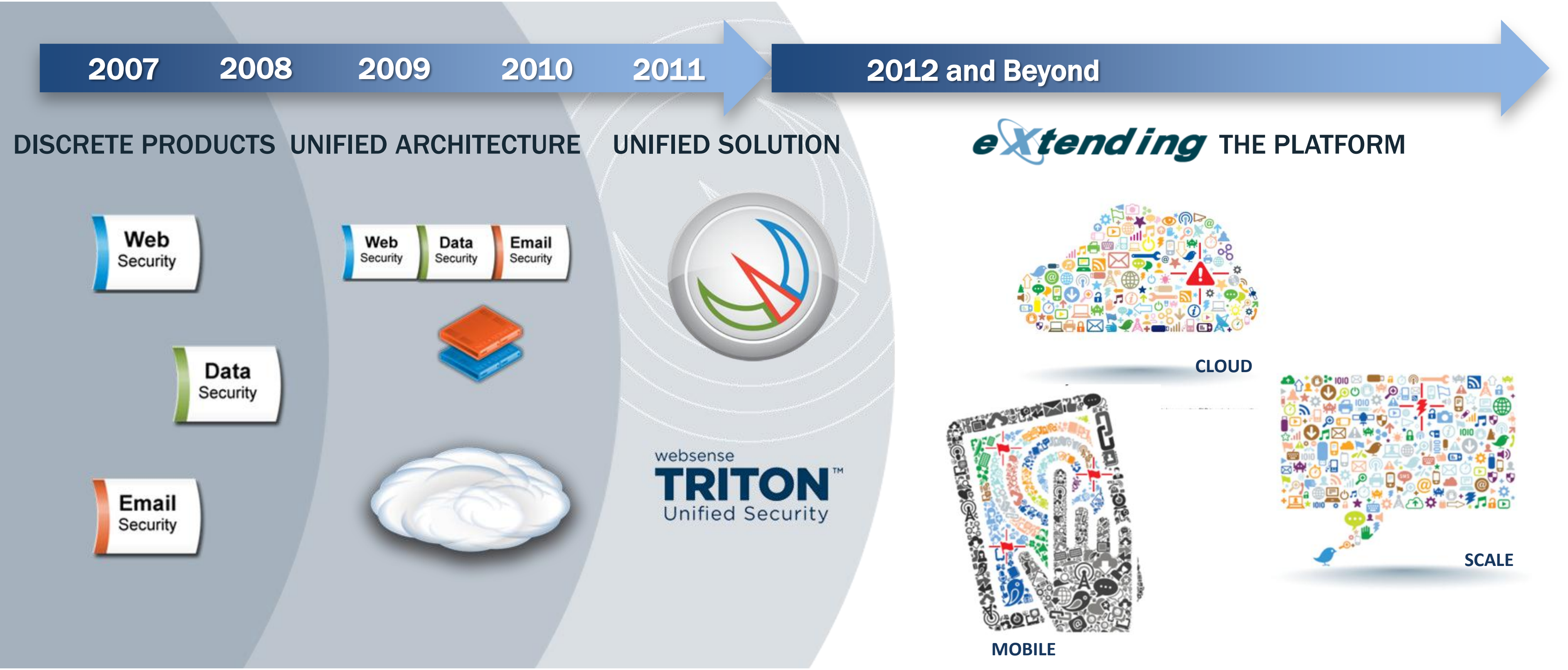
2009 – Acquired Defensio

2010 – Unveiled TRITON Architecture

$600m Investment in R&D: more than doubled over last three years

Investment & Innovation

Websense Evolution



2007 2008 2009 2010 2011

2012 and Beyond

DISCRETE PRODUCTS

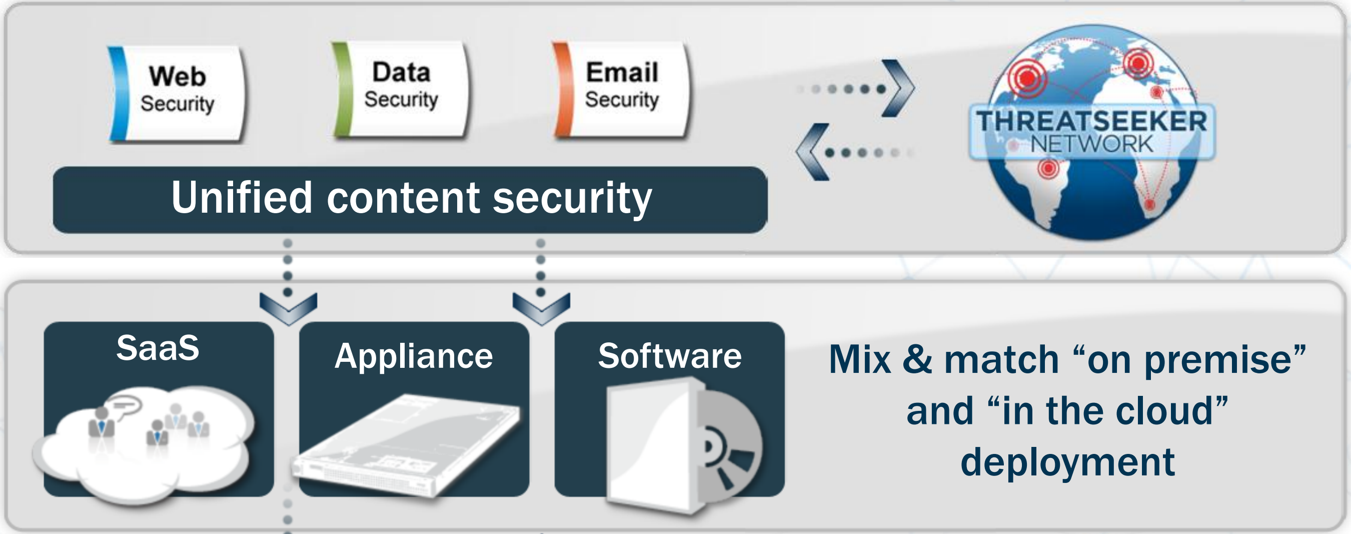
UNIFIED ARCHITECTURE

UNIFIED SOLUTION

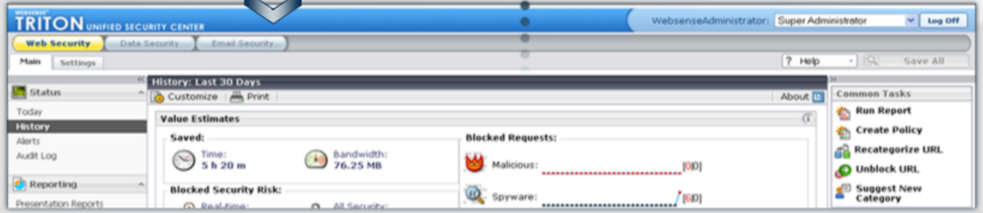
eXtending THE PLATFORM

TRITON Unified Security Architecture

websense



Mix & match "on premise" and "in the cloud" deployment



WebsenseAdministrator: Super Administrator

History: Last 30 Days

Value Estimates

Saved:

Time: 5 h 20 m

Bandwidth: 76.25 MB

Blocked Requests:

Malicious: [0|0]

Spyware: [6|0]

Blocked Security Risk:

Real-time:

All Security:

Maximize visibility and control

websense®
TRITON™

Unified Architecture/Security Intelligence/Console/Policy/Reporting

websense®
THREATSEEKER NETWORK

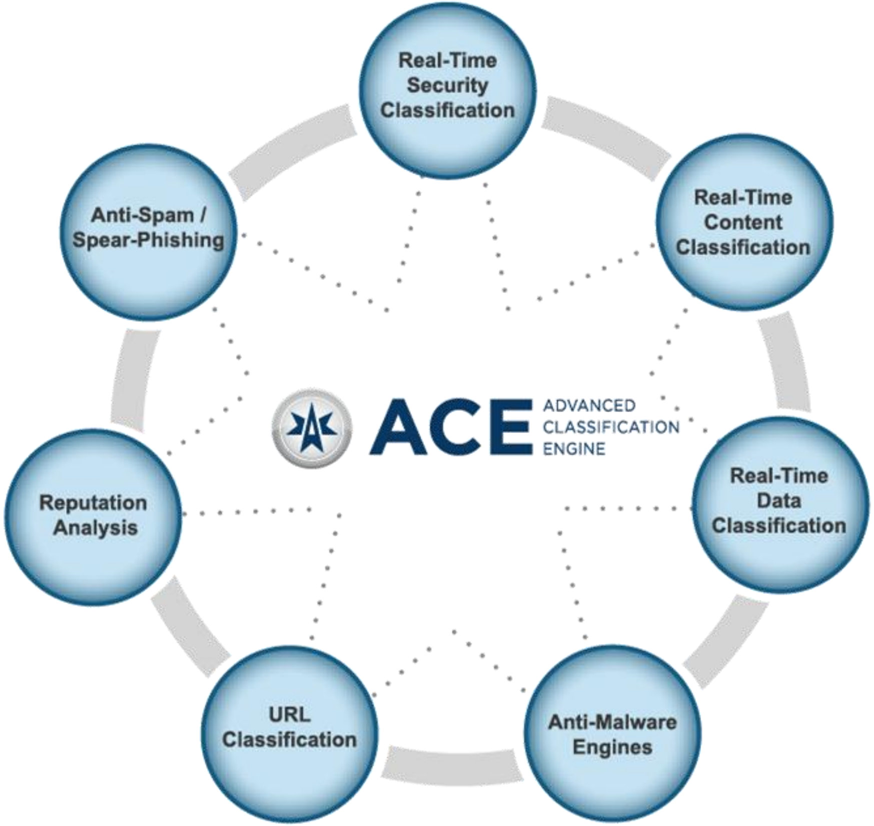
Unites over 850M research points.
Analyzes 3-5B requests per day.

websense®
ACE
ADVANCED
CLASSIFICATION
ENGINE

websense®
SECURITY LABS

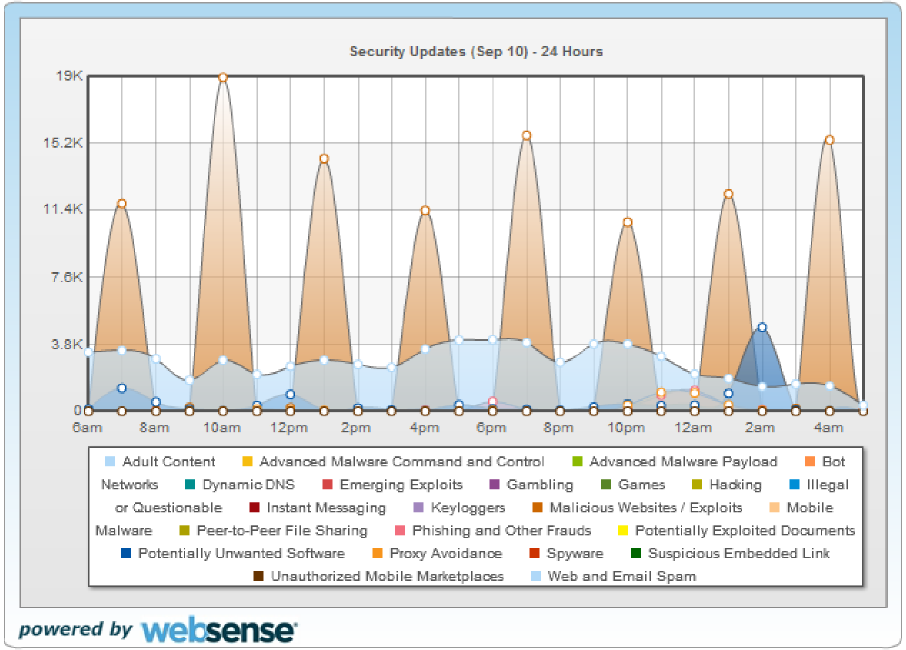
Real-time Threat & Content Analysis

- Real-time Threat Engines
  - Security, Data, Content
  - Over 10,000 Analytics
- Three Anti-Malware Engines
  - Commercial AV Engine
  - Heuristic Analysis Engine
  - Malicious PDF Engine
- Spear-Phishing, Reputation and Web Link defenses
- Composite Scoring Model


Real-Time Security Classification
Real-Time Content Classification
Real-Time Data Classification
Anti-Malware Engines
URL Classification
Reputation Analysis
Anti-Spam / Spear-Phishing
ACE ADVANCED CLASSIFICATION ENGINE

Defenses & Analytics

- ThreatSeeker Network Intelligence
  - Over 900M Endpoints, 3-5B Requests/day
  - Facebook Partnership
- Websense Security Labs
  - Global locations working 24/7
- Real-time Updates to ACE
- Predictive Defense
  - Composite scoring inputs
  - Determine defense analysis
  - Convicts via prediction

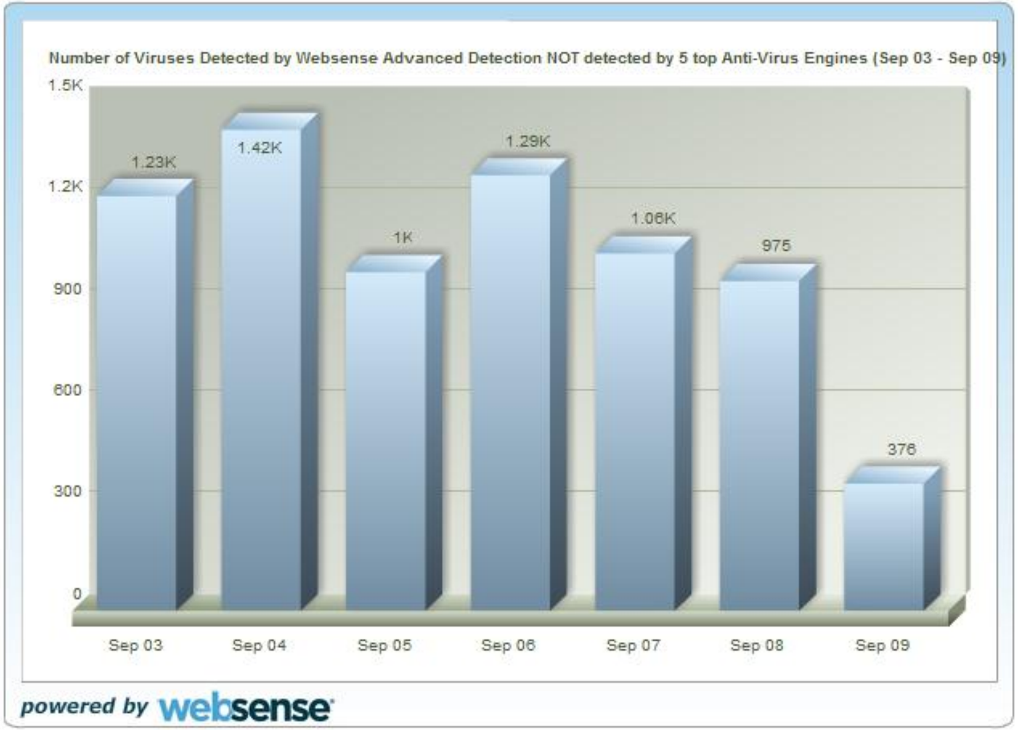


Effectiveness Proven Daily

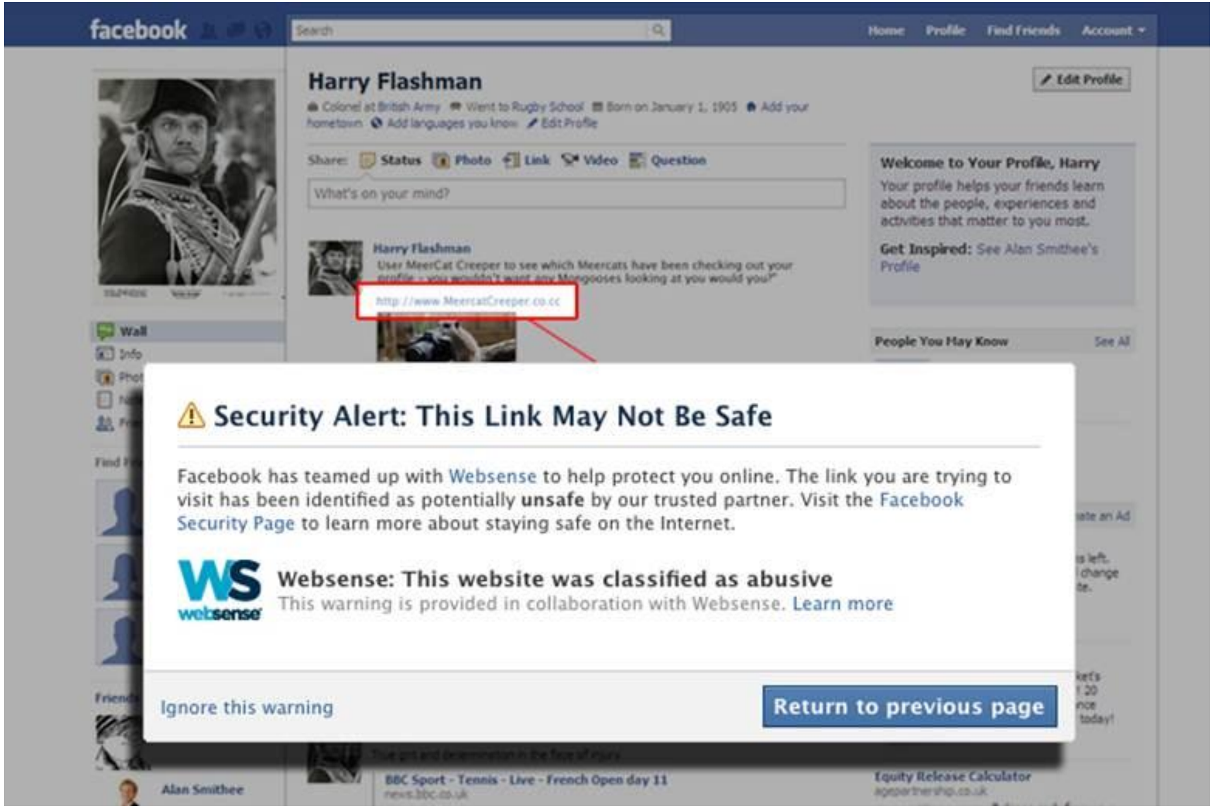
websense

- Five Top AV Engines
- Results Posted Daily
- Security Labs Site
  - AV Test Results
  - Real-time Updates
  - Requests Analyzed
  - Security Blog

websense® SECURITY LABS



Facebook Partnership



Harry Flashman

Colonel at British Army · Went to Rugby School · Born on January 1, 1905 · Add your hometown · Add languages you know · Edit Profile

Share: Status Photo Link Video Question

What's on your mind?

Harry Flashman
User MeerCat Creeper to see which Meercats have been checking out your profile – you wouldn't want any Mongooses looking at you would you?"

http://www.MeercatCreeper.co.cc

Welcome to Your Profile, Harry
Your profile helps your friends learn about the people, experiences and activities that matter to you most.

Get Inspired: See Alan Smithee's Profile

BBC Sport - Tennis - Live - French Open day 11
news.bbc.co.uk

Equity Release Calculator

⚠ Security Alert: This Link May Not Be Safe

Facebook has teamed up with Websense to help protect you online. The link you are trying to visit has been identified as potentially **unsafe** by our trusted partner. Visit the Facebook Security Page to learn more about staying safe on the Internet.

Websense: This website was classified as abusive
This warning is provided in collaboration with Websense. Learn more

Ignore this warning

Return to previous page

OUR FACEBOOK INTEGRATION

- Exclusive Partnership Protecting Facebook Users since October 2011
- All Facebook users protected
- Free Defensio Facebook App for Consumers
- Provides Websense with visibility into the Facebook private network
- **Unparalleled Intelligence Enhancing ThreatSeeker**

websense® TRITON™

Unified Architecture/Security Intelligence/Console/Policy/Reporting

WEB

The **most effective anti-malware protection** from **advanced threats** and **data theft.**

EMAIL

The **most advanced** email **defenses** against **blended & targeted** attacks (APTs).

DATA

Enterprise DLP with **proven risk reduction** in **5-6 weeks** with user and destination awareness.

CLOUD

The **best protection** for web and email for **any location** at the **lowest TCO** & **easiest deployment.**

MOBILE

Uniquely effective protection for mobile data from **theft , loss, malicious apps,** and **malware.**

websense® THREATSEEKER NETWORK

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

websense® ACE ADVANCED CLASSIFICATION ENGINE

websense® SECURITY LABS

websense®
TRITON™ Unified Architecture/Security Intelligence/Console/Policy/Reporting

WEB

- ✓ Advanced threats
- ✓ Modern malware
- ✓ TruWeb DLP
- ✓ Containment
- ✓ Forensic data
- ✓ Social media
- ✓ Cloud apps
- ✓ Viral videos
- ✓ Visibility
- ✓ Productivity
- ✓ Compliance
- ✓ TruHybrid

EMAIL

- ✓ Targeted attacks
- ✓ Blended threats
- ✓ URL sandboxing
- ✓ Anti-malware
- ✓ Anti-spam
- ✓ TruEmail DLP
- ✓ Cloud cleansing
- ✓ Encryption services
- ✓ Archiving
- ✓ Image analysis
- ✓ Compliance
- ✓ TruHybrid

DATA

- ✓ DLP methodology
- ✓ Risk reduction
- ✓ Data registration
- ✓ 1,100+ policies
- ✓ Data-in-motion
- ✓ Data-in-use
- ✓ Data-at-rest
- ✓ Scan/remediate
- ✓ User/dest. aware
- ✓ End-point agent
- ✓ Portable encrypt.
- ✓ Compliance

CLOUD

- ✓ Web & email
- ✓ Advanced threats
- ✓ Targeted attacks
- ✓ URL sandboxing
- ✓ Social media
- ✓ Cloud apps
- ✓ Viral videos
- ✓ Monitor & protect web presence
- ✓ Visibility/productivity
- ✓ Global ops centers
- ✓ ISO 27001

MOBILE

- ✓ Cloud service
- ✓ Malicious apps
- ✓ Mobile malware
- ✓ Mobile DLP (email)
- ✓ Web security
- ✓ App controls
- ✓ Device mgmt.
- ✓ BYOD programs
- ✓ Corporate devices
- ✓ Reporting/inventory
- ✓ Global ops centers
- ✓ ISO 27001

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

websense®
ACE ADVANCED CLASSIFICATION ENGINE

websense®
SECURITY LABS

TRITON Security in Action

Threat & Solution Examples

TRITON™

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

Example #1

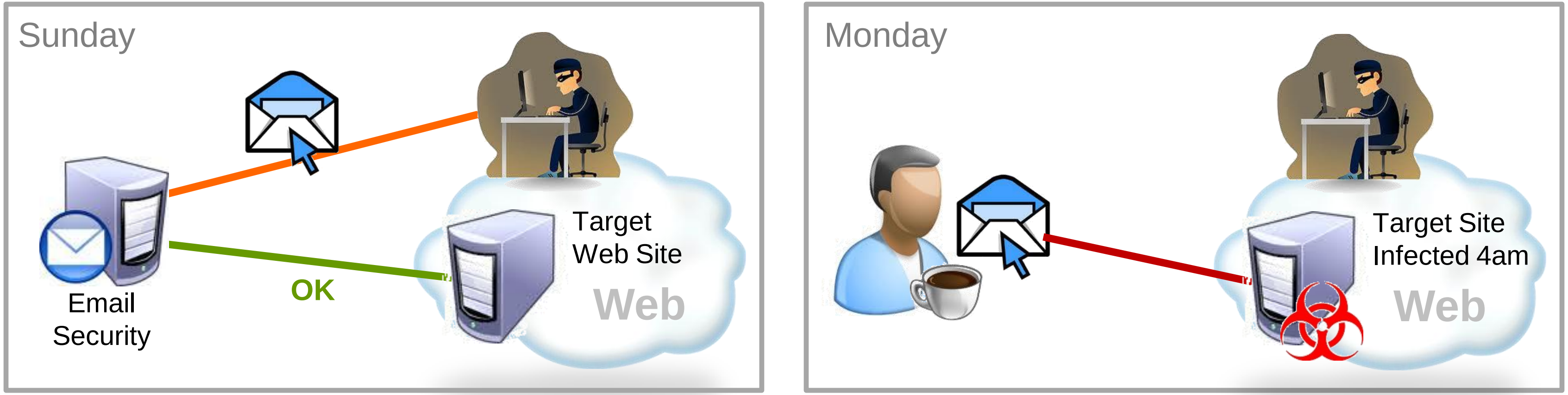
Email Security Evasion

TRITON™

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

Email Security Evasion

- Spear-phishing technique
  - Embedded web link in email lure
  - Time malware infection after delivery
  - Email security sees a clean link



© 2012 Websense, Inc.

Example #2

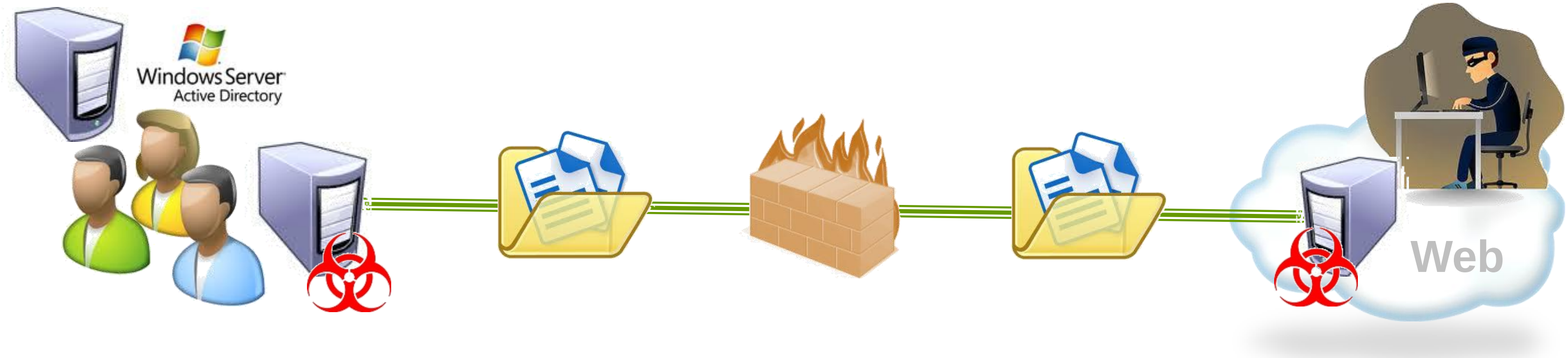
Network Invasion / Privilege Escalation

TRITON™

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

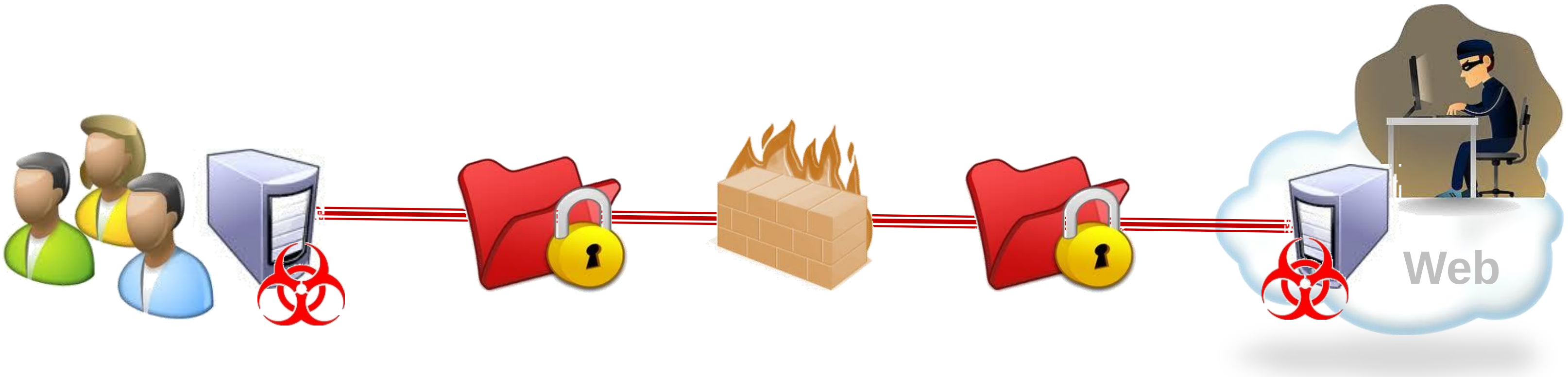
Password File Data Theft

- Password files
- Active Directory/SAM database
- Expand reach/control within target
- First priority once inside



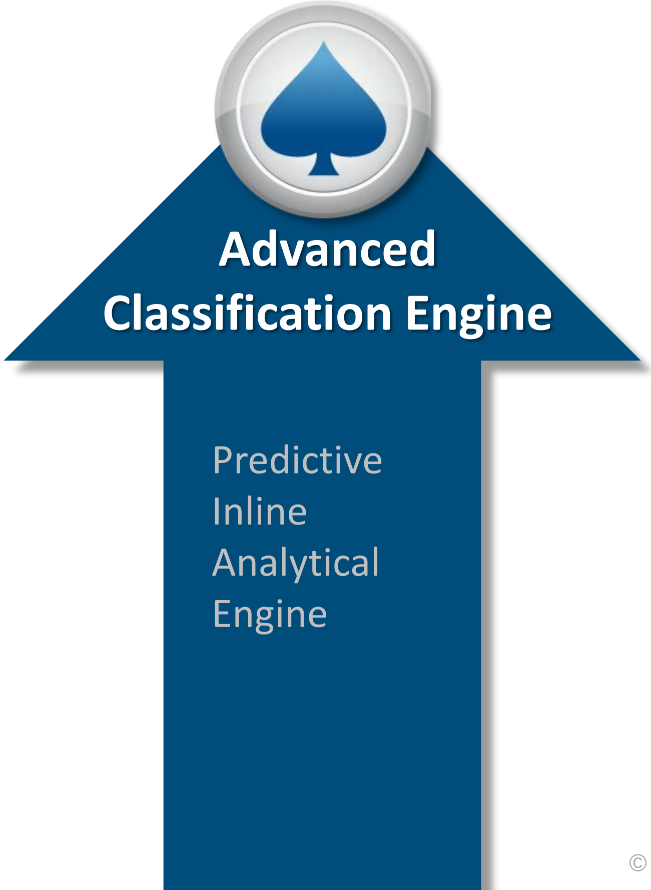
Criminal Encrypted Uploads

- Proprietary encryption
- Cloak comms & data theft
- Crimeware toolkit enabled
- Blind spot for defenses



ACE New Defenses

websense



Advanced Classification Engine

Predictive
Inline
Analytical
Engine

10 New Defenses in ACE to protect against Advanced Threats & Data Theft

New ACE Analytics/Defenses:

Advanced Malware Payloads ←
Potentially Exploited Documents ←
Mobile Malware ←

INBOUND WSG

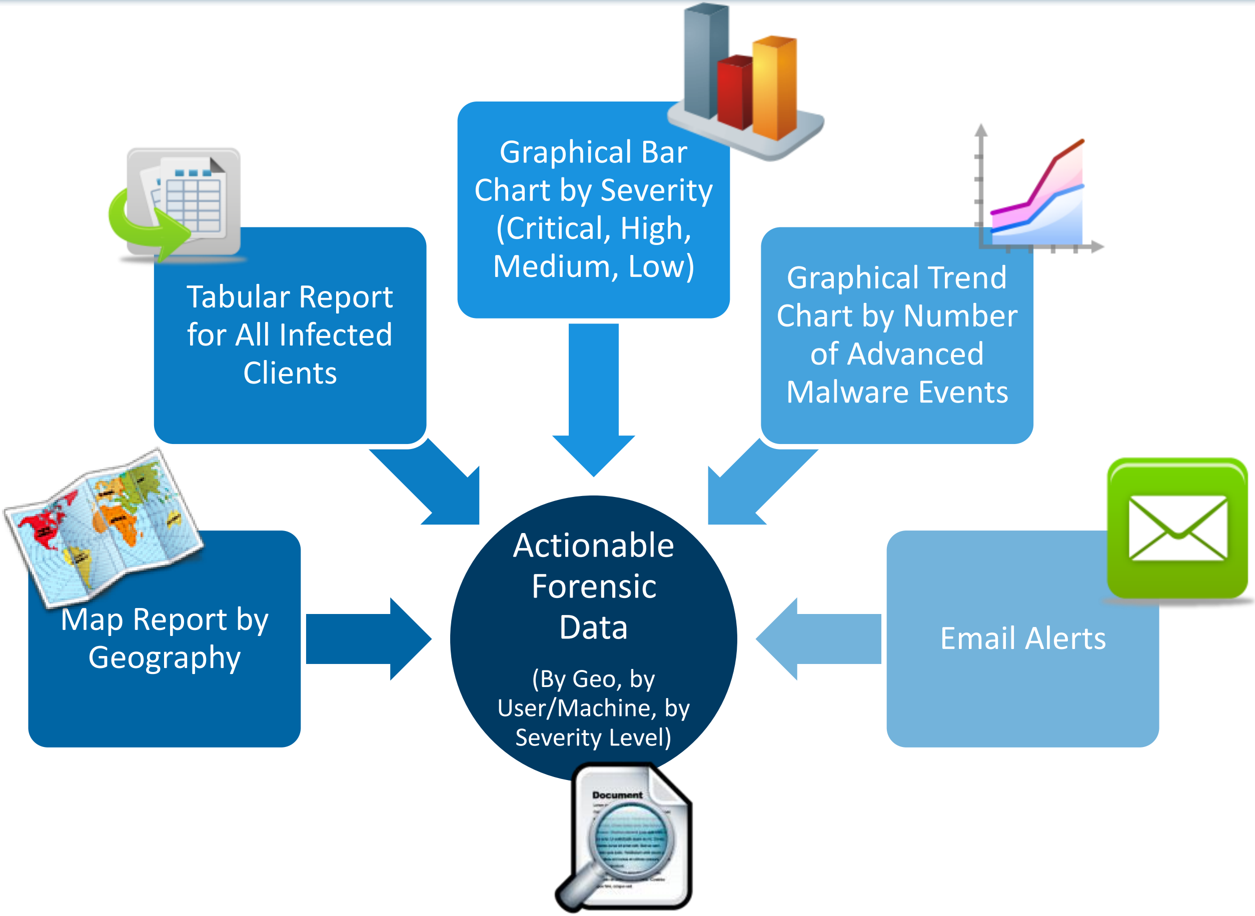
Criminal Encrypted Uploads →
Files Containing Passwords →
Advanced Malware Command & Control →
Unauthorized Mobile Marketplaces →

OUTBOUND WSG

OCR (Optical Character Recognition) →
Behavioral (Drip) DLP →
Geo-Location →

OUTBOUND WSGA

Advanced Malware Reporting Flow



Tabular Report for All Infected Clients

Graphical Bar Chart by Severity (Critical, High, Medium, Low)

Graphical Trend Chart by Number of Advanced Malware Events

Map Report by Geography

Actionable Forensic Data

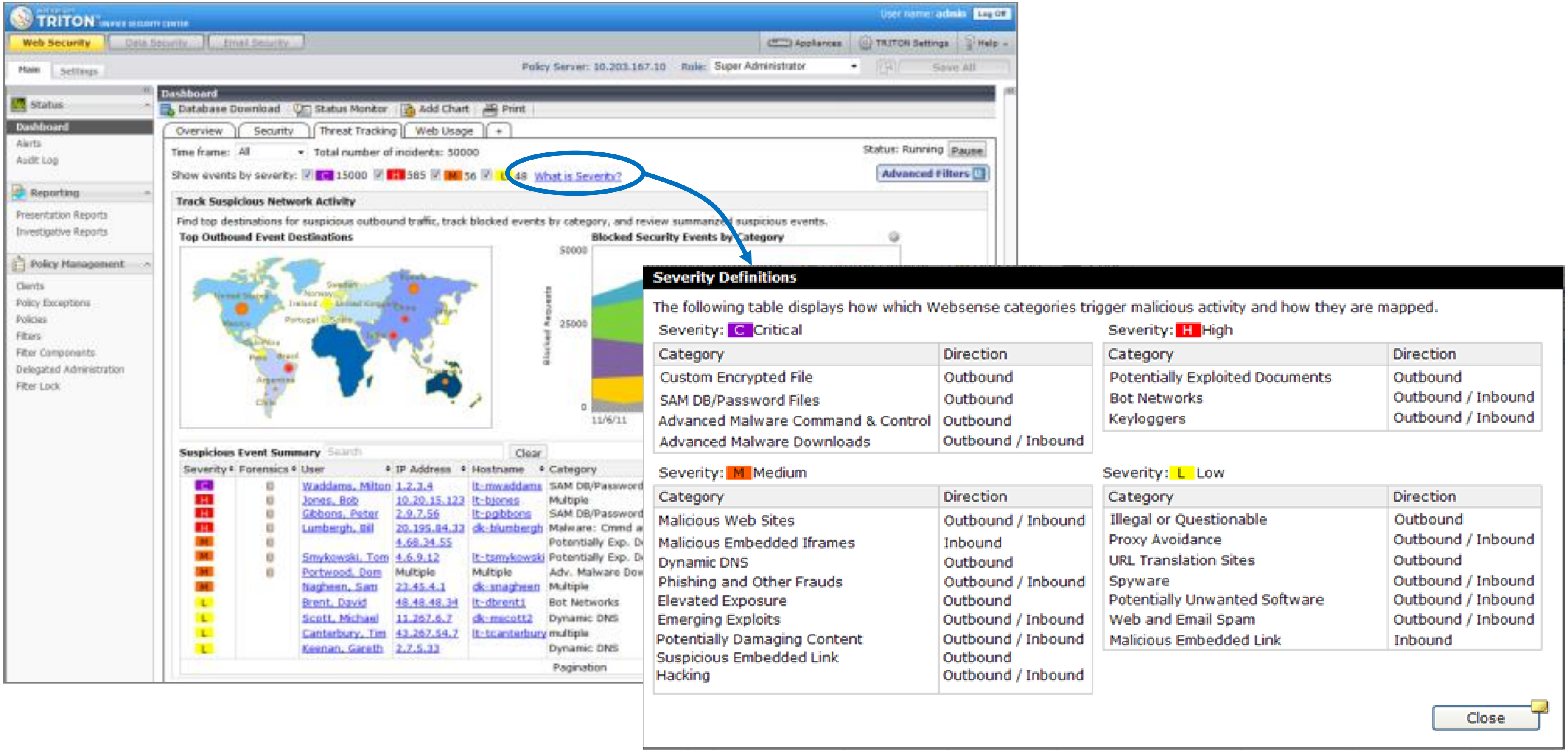
(By Geo, by User/Machine, by Severity Level)

Email Alerts

Designed to draw you to <u>actionable</u> data

- Identifies client to be remediated
- Captures data that was attempted to be stolen
- Reports to raise awareness of attacks in progress

Threat Dashboard



Policy Server: 10.203.167.10 Role: Super Administrator

Time frame: All Total number of incidents: 50000

Status: Running

Show events by severity: ☑ C 15000 ☑ H 585 ☑ M 56 ☑ L 48 What is Severity?

Track Suspicious Network Activity

Find top destinations for suspicious outbound traffic, track blocked events by category, and review summarized suspicious events.

Suspicious Event Summary Search

Severity	Forensics	User	IP Address	Hostname	Category
C	□	Waddams, Milton	1.2.3.4	lt-mwaddams	SAM DB/Password
H	□	Jones, Bob	10.20.15.123	lt-bjones	Multiple
H	□	Gibbons, Peter	2.9.7.56	lt-pgibbons	SAM DB/Password
H	□	Lumbergh, Bill	20.195.84.33	dk-blumbergh	Malware: Cmnd a
M	□		4.68.34.55		Potentially Exp. D
M	□	Smykowski, Tom	4.6.9.12	lt-tsmykowski	Potentially Exp. D
M	□	Portwood, Dom	Multiple	Multiple	Adv. Malware Dow
M		Nagheen, Sam	23.45.4.1	dk-snagheen	Multiple
L		Brent, David	48.48.48.34	lt-dbrent1	Bot Networks
L		Scott, Michael	11.267.6.7	dk-mscott2	Dynamic DNS
L		Canterbury, Tim	43.267.54.7	lt-tcanterbury	multiple
L		Keenan, Gareth	2.7.5.33		Dynamic DNS

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

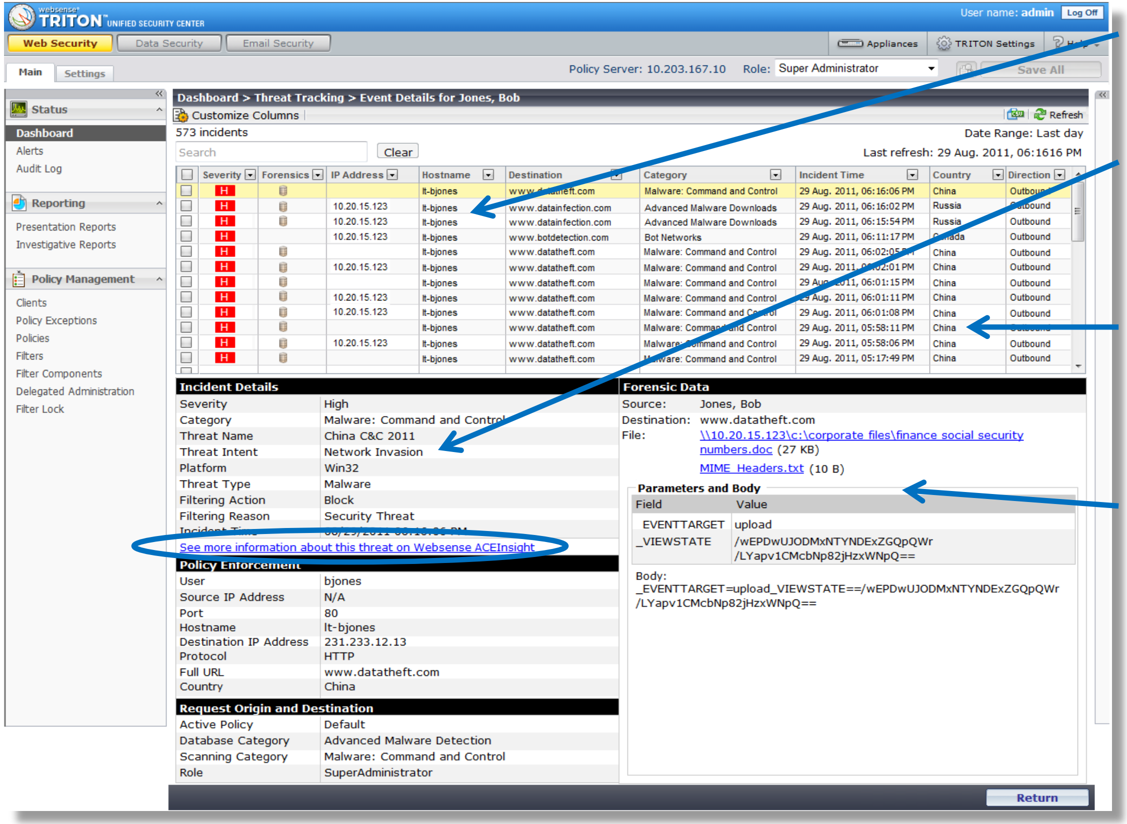
Severity: M Medium

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

Forensic Reporting



Policy Server: 10.203.167.10 Role: Super Administrator

Dashboard > Threat Tracking > Event Details for Jones, Bob

573 incidents

Date Range: Last day

Last refresh: 29 Aug. 2011, 06:1616 PM

□	Severity	Forensics	IP Address	Hostname	Destination	Category	Incident Time	Country	Direction
□	H	●		lt-bjones	www.datatheft.com	Malware: Command and Control	29 Aug. 2011, 06:16:06 PM	China	Outbound
□	H	●	10.20.15.123	lt-bjones	www.datainfection.com	Advanced Malware Downloads	29 Aug. 2011, 06:16:02 PM	Russia	Outbound
□	H	●	10.20.15.123	lt-bjones	www.datainfection.com	Advanced Malware Downloads	29 Aug. 2011, 06:15:54 PM	Russia	Outbound
□	H		10.20.15.123	lt-bjones	www.botdetection.com	Bot Networks	29 Aug. 2011, 06:11:17 PM	Canada	Outbound
□	H	●		lt-bjones	www.datatheft.com	Malware: Command and Control	29 Aug. 2011, 06:02:05 PM	China	Outbound
□	H	●	10.20.15.123	lt-bjones	www.datatheft.com	Malware: Command and Control	29 Aug. 2011, 06:02:01 PM	China	Outbound
□	H	●		lt-bjones	www.datatheft.com	Malware: Command and Control	29 Aug. 2011, 06:01:15 PM	China	Outbound
□	H	●	10.20.15.123	lt-bjones	www.datatheft.com	Malware: Command and Control	29 Aug. 2011, 06:01:11 PM	China	Outbound
□	H	●	10.20.15.123	lt-bjones	www.datatheft.com	Malware: Command and Control	29 Aug. 2011, 06:01:08 PM	China	Outbound
□	H	●		lt-bjones	www.datatheft.com	Malware: Command and Control	29 Aug. 2011, 05:58:11 PM	China	Outbound
□	H	●	10.20.15.123	lt-bjones	www.datatheft.com	Malware: Command and Control	29 Aug. 2011, 05:58:06 PM	China	Outbound
□	H	●		lt-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	08/29/2011 06:16:06 PM

See more information about this threat on Websense ACEInsight

Policy Enforcement

User	bjones
Source IP Address	N/A
Port	80
Hostname	lt-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

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)

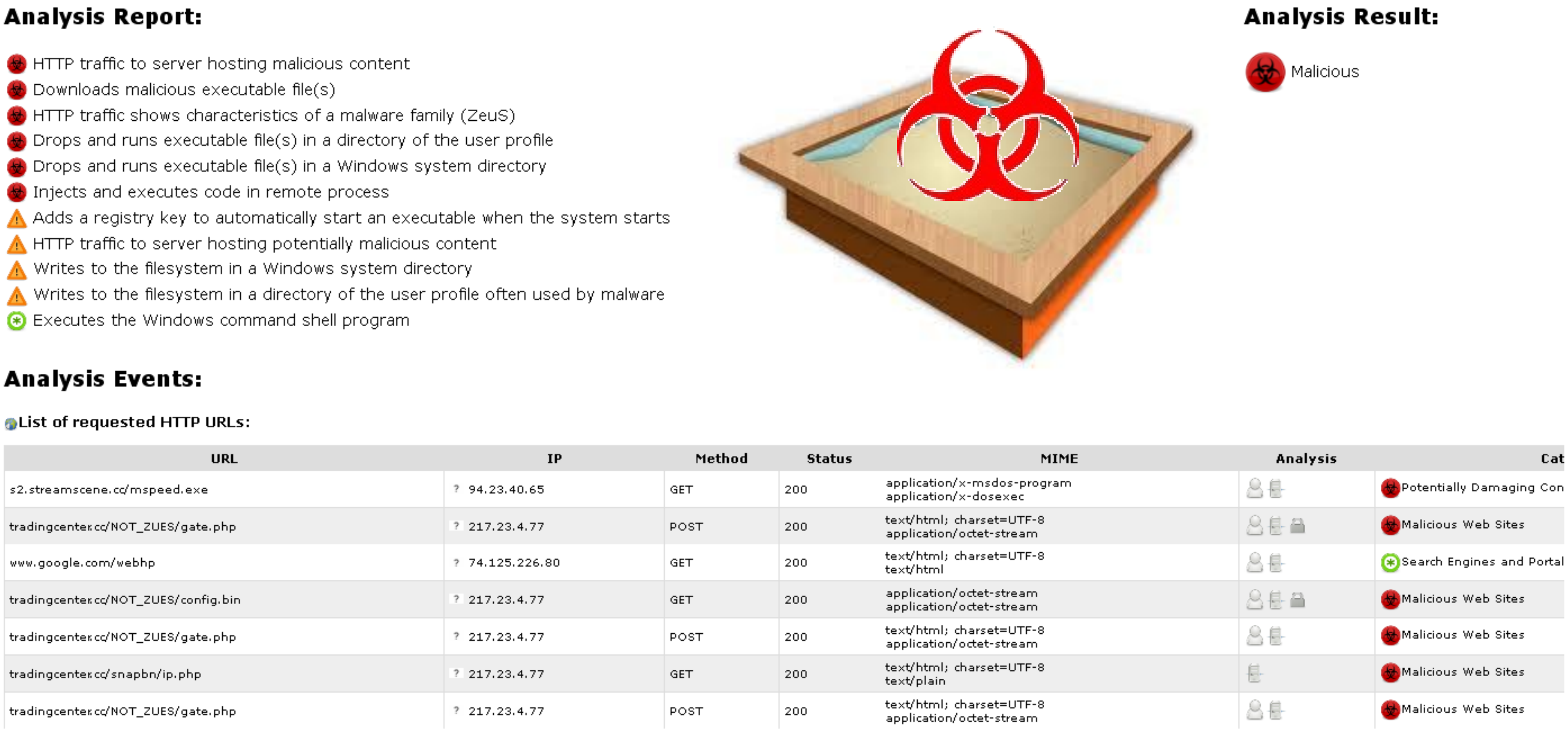
Parameters and Body

Field	Value
EVENTTARGET	upload
_VIEWSTATE	/wEPDwUJODMxNTYNDExZGQpQWr /LYapv1CMcbNp82jHzxWNpQ==

Body:
_EVENTTARGET=upload_VIEWSTATE==/wEPDwUJODMxNTYNDExZGQpQWr
/LYapv1CMcbNp82jHzxWNpQ==

- Know **WHO** was compromised
- Know **HOW** the malware operates (intent)
- Know **WHERE** the data was being sent
- Know **WHAT** was prevented from being stolen

Websense CSI: Malware Sandbox Service



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

Example #3

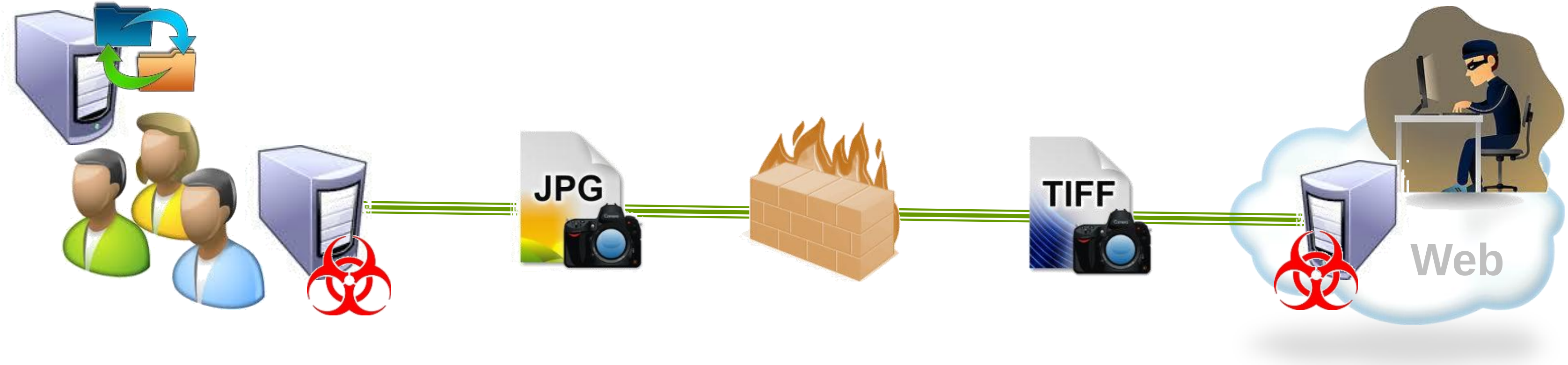
Insider Data Theft

TRITON™

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

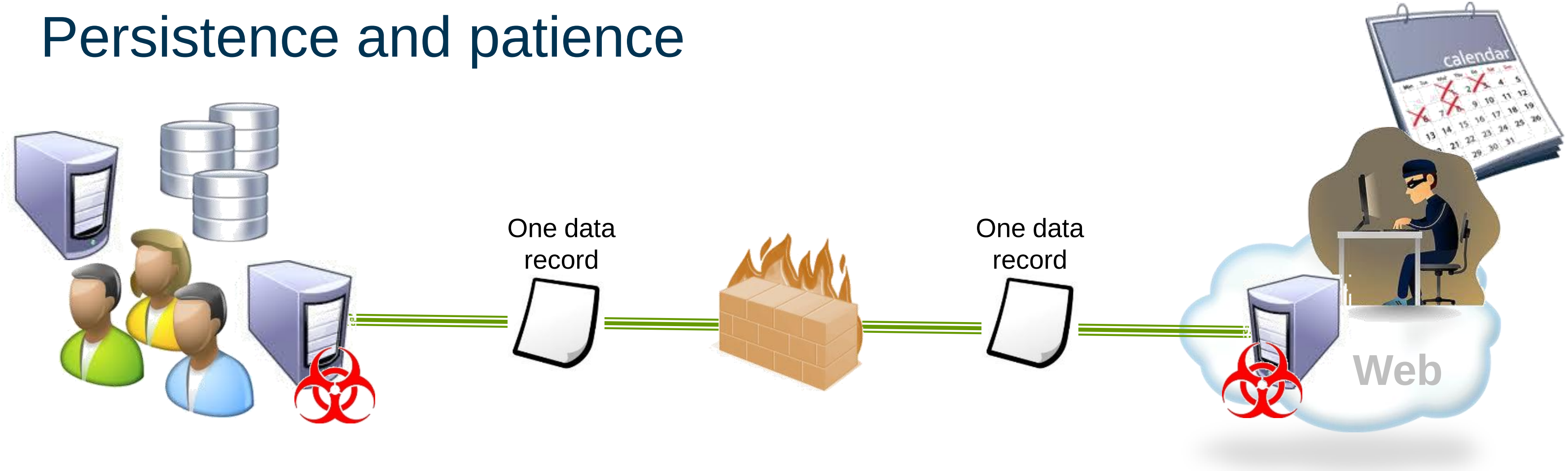
Non-Document Data Theft

- Image files
- Confidential information
- Smart phone pictures
- Blind spot for defenses

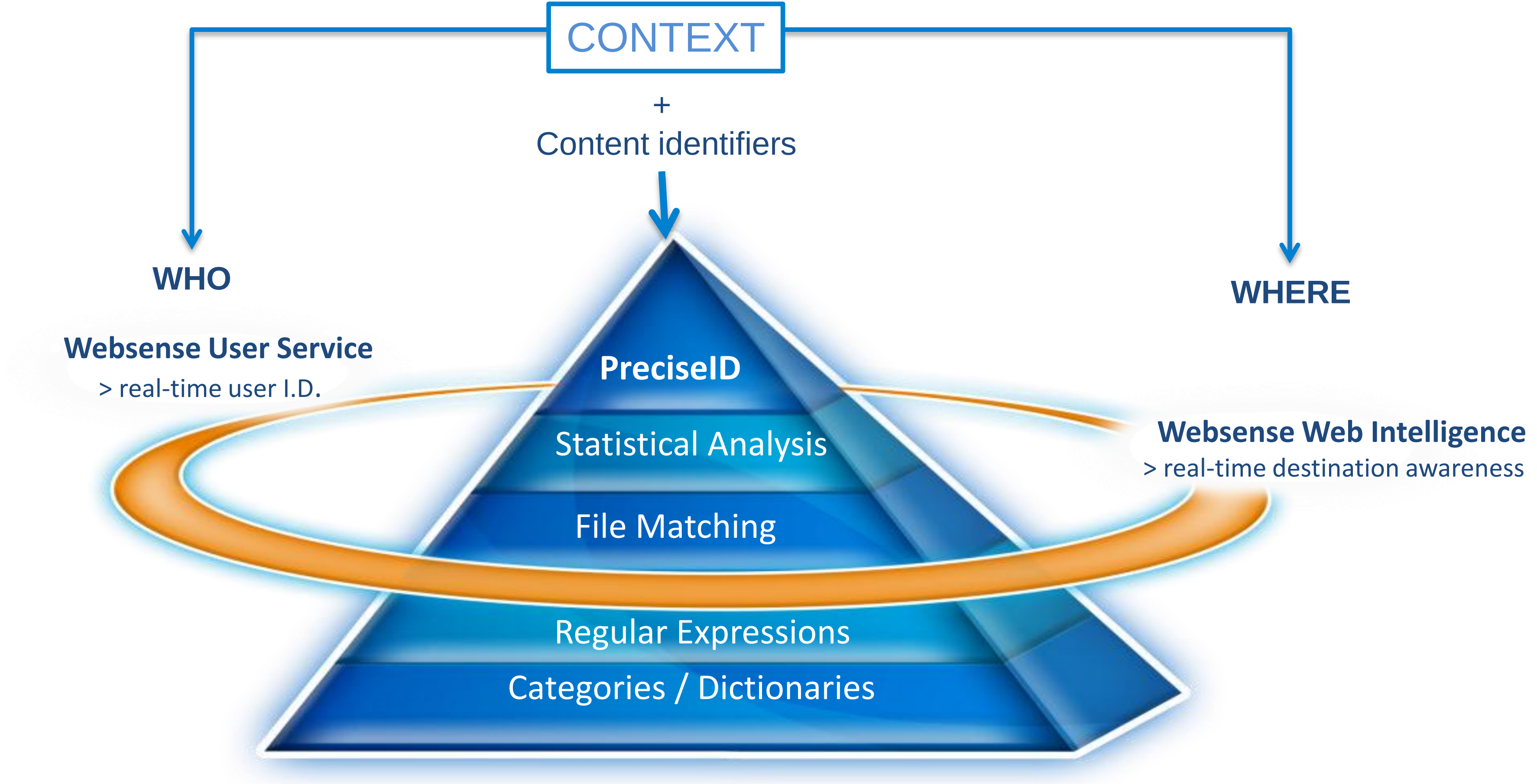


Slow Data Leaks

- Remain below the radar
- Low record count per request/incident
- Steal data in small chunks
- Persistence and patience



Contextual Intelligence



CONTEXT

+

Content identifiers

WHO

Websense User Service

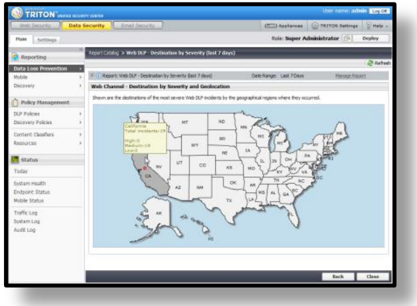
> real-time user I.D.

WHERE

Websense Web Intelligence

> real-time destination awareness

NEW in Data Security v7.7



Report Catalog > Web DLP - Destination by Severity (last 7 days)

Report: Web DLP - Destination by Severity (last 7 days) Date Range: Last 7 Days

Web Channel - Destination by Severity and Geolocation

Shown are the destinations of the most severe Web DLP incidents by the geographical regions where they occurred.

California
Total incidents: 19
High: 0
Medium: 19
Low: 0

Drip DLP

Detect suspicious "low and slow" movement of data

(e.g. 5 SSNs in an hour)

Outbound by Geographic Destination

Create DLP policies by geo for "high profile targets" and high risk geos

OCR

Extract text from images and scanned documents for analysis

No other vendor can do OCR for data in motion!

Machine Learning

Ease discovery projects by automatically finding content that is similar to the content we have learned in the past

Relative Threats – and Websense answer

Accidental

→

EMPLOYEE EDUCATION

Predefined Templates, Notifications/confirm, Self Release

Intentional

(Non-Malicious)

→

VISIBILITY

Unique matches, Actions by Incident Severity, Source and Destination Awareness, Drip DLP

Malicious Insider

→

ADVANCED DETECTION

Drip DLP, App control, OCR Detection

Malicious Outsider

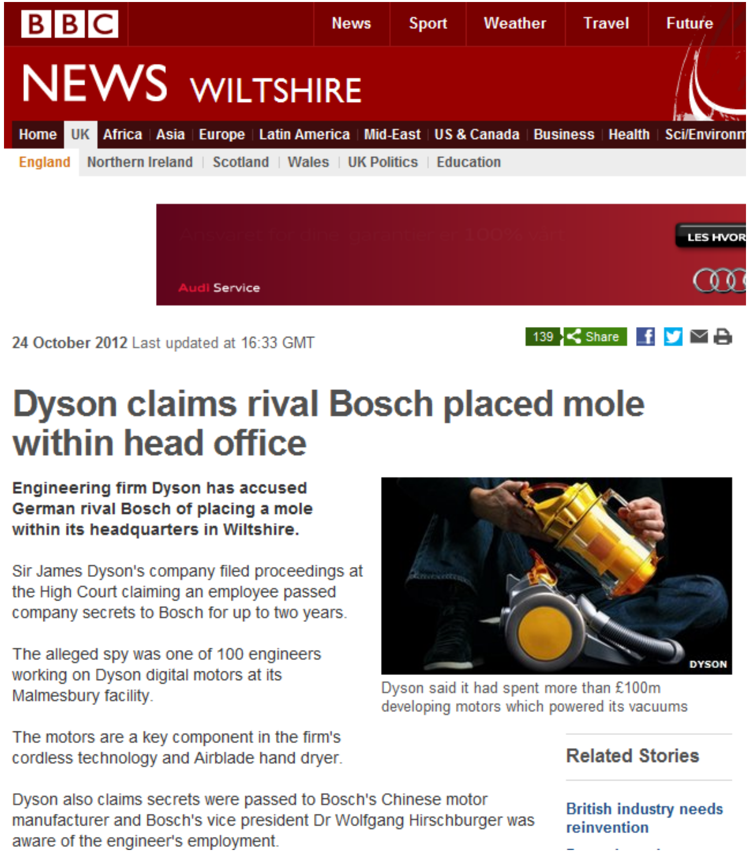
→

WEBSENSE SECURITY LABS (ACE)

SSL Decryption, URL categories, Geo Location, Unauthorized/Proprietary encryption

Recent Example – October 2012

- Industrial Espionage
  - Malicious Insider
  - Targeted engineering blueprints
  - Stolen data sent to major rival over an extended period
  - Filed legal case in the UK High Court



24 October 2012 Last updated at 16:33 GMT

Dyson claims rival Bosch placed mole within head office

Engineering firm Dyson has accused German rival Bosch of placing a mole within its headquarters in Wiltshire.

Sir James Dyson's company filed proceedings at the High Court claiming an employee passed company secrets to Bosch for up to two years.

The alleged spy was one of 100 engineers working on Dyson digital motors at its Malmesbury facility.

The motors are a key component in the firm's cordless technology and Airblade hand dryer.

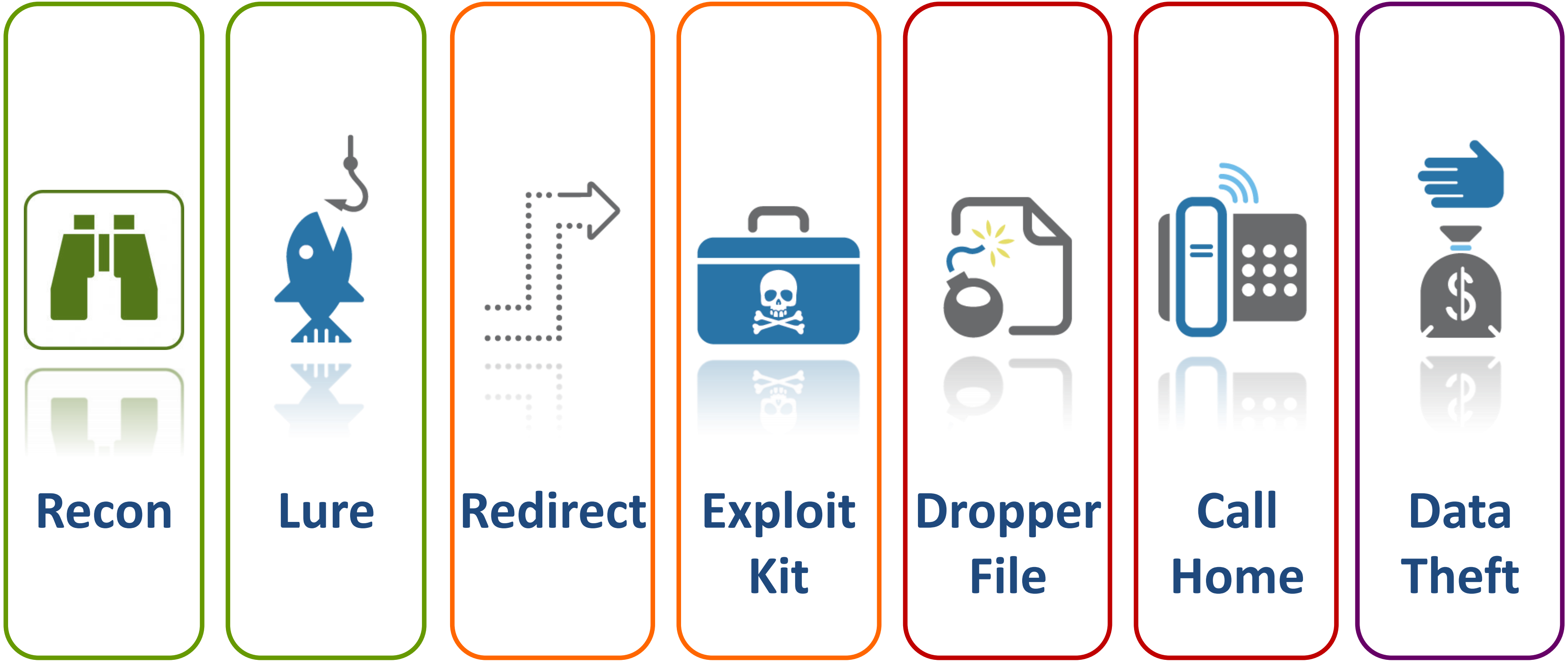
Dyson also claims secrets were passed to Bosch's Chinese motor manufacturer and Bosch's vice president Dr Wolfgang Hirschburger was aware of the engineer's employment.

Dyson said it had spent more than £100m developing motors which powered its vacuums

Related Stories

British industry needs reinvention

Seven Advanced Threat Stages



Recon

Lure

Redirect

Exploit Kit

Dropper File

Call Home

Data Theft

Seven Advanced Threat Stages

Recon

Lure

AWARENESS

- Web & Email
- Facebook, Blogs, Tweets
- Spear-phishing
- Trusted entry
- Targeted
- Dynamic
- Timed

Seven Advanced Threat Stages

Redirect

Exploit Kit

REAL-TIME ANALYSIS

- Browser code & active scripts
- Link analysis
- Exploit analysis
- Composite scoring/ratings
- Predictive

Seven Advanced Threat Stages

INLINE DEFENSES

- App analysis
- Malicious PDFs
- Multiple AVs
- File compress.
- Dynamic DNS
- Botnet & CnC comms

Dropper File

Call Home

Seven Advanced Threat Stages

websense

CONTAINMENT

- Data theft defenses
- Embedded DLP
- Data capture
- Geo-location
- Forensic details & reporting
- Alerts/severity

Data Theft

Conclusion

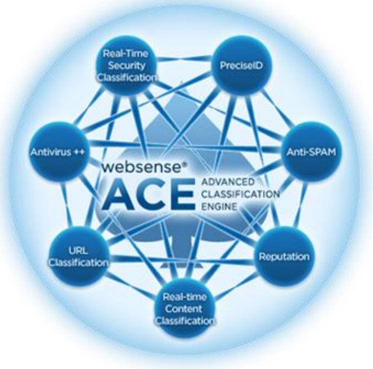
Final Thoughts and Q&A

TRITON™

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

Key Takeaways

TRITON


Real-Time Security Classification
PreciseID
Antivirus ++
Anti-SPAM
websense®
ACE
ADVANCED CLASSIFICATION ENGINE
URL Classification
Reputation
Real-time Content Classification

Advanced Classification Engine (ACE)

ThreatSeeker Network

Analysts Recognize Websense

websense

Gartner

- 2012 **Secure Web Gateway MQ:** Leaders Quadrant
- 2011 Content-Aware **Data Loss Prevention MQ:** Leaders Quadrant
- **Secure Web Gateway Software** 2011 Worldwide Market Share Leader

INFO~TECH research group

- 2012 **WCF** Vendor Landscape: Champion
- 2012 **DLP** Vendor Landscape: Champion & Trend Setter Award

FROST & SULLIVAN

- 2010 Global **Content Filtering** Products Market Share Leadership of the Year Award
- **Web Filtering** Products 2011 Competitive Landscape: Market Leader
- **Web Filtering** Products 2011 Market Share Leader

FORRESTER®

- **Data Leak Prevention Suites** Wave, Q4 2010: Recognized Leader

Gartner

- **2012 Secure Email Gateway MQ:** Visionaries Quadrant

EMA

- **Hosted Message Security Services** Radar Report: Value Leader Best Hybrid Strategy Award

INFONETICS RESEARCH

- **Integrated Content Security Gateways** CY11 Worldwide Market Share Leader

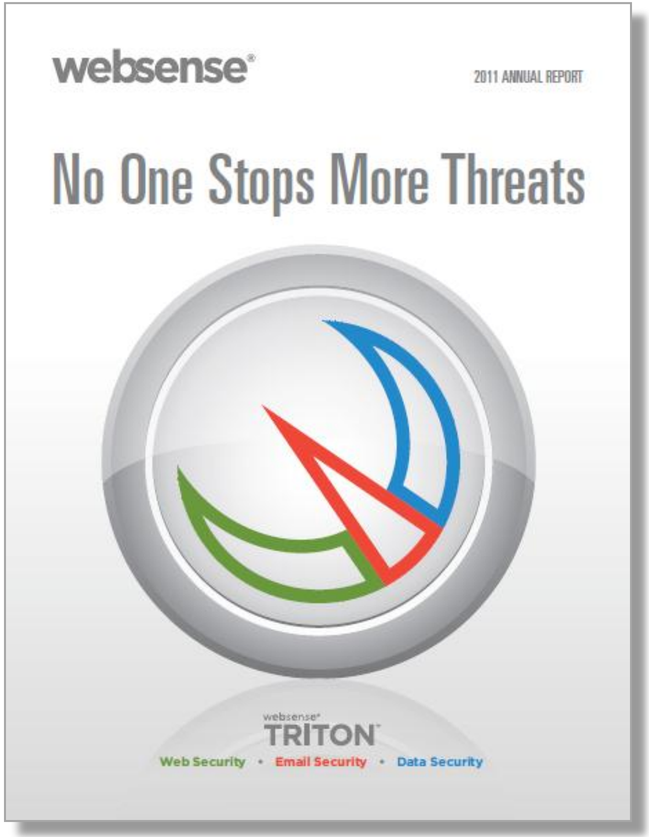
IDC Analyze the Future

- 2012 **IDC MarketScape: WW Web Security Products:** Leaders
- **Web Security:** 2011 Overall Market Share Leader
- **Web Security Appliance** 2011 Market Leader
- **Web Security Software** 2011 Market Leader

THE RADICATI GROUP, INC. A TECHNOLOGY MARKET RESEARCH FIRM

- 2012 Corporate **Web Security** Market Quadrant: Top Player

Let Us Prove It



websense®

2011 ANNUAL REPORT

No One Stops More Threats

websense® TRITON™

Web Security • Email Security • Data Security

Thank You for Listening

Any Questions?