Advanced Threats & Data Theft

New TRITON v7.7 Defenses

Tom Clare, Sr. Director PMM
10 July 2012

TRITON™
- Web security
- Email security
- Data security
- Mobile security

New Defense Game

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

4 Reasons Why Current Defenses Fail

websense

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

Seven Advanced Threat Stages

websense

Seven Advanced Threat Stages

websense

Recon

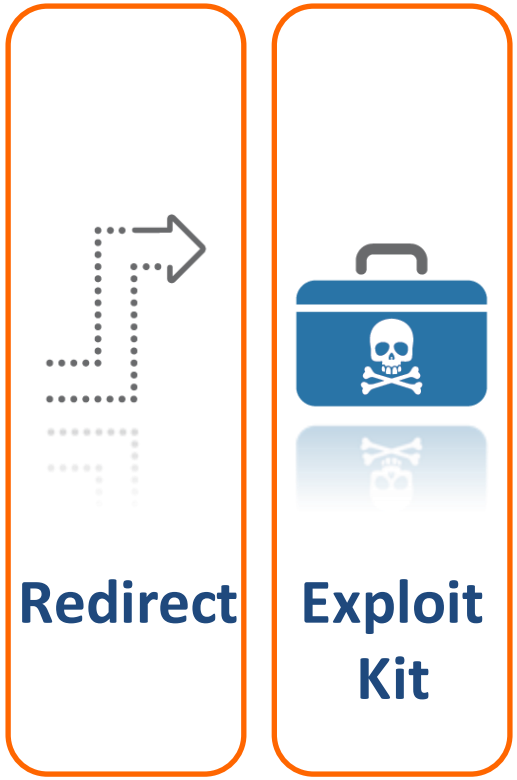
Lure

AWARENESS

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

Seven Advanced Threat Stages

websense



REAL-TIME ANALYSIS

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

Seven Advanced Threat Stages

websense

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

Advanced Threat Techniques

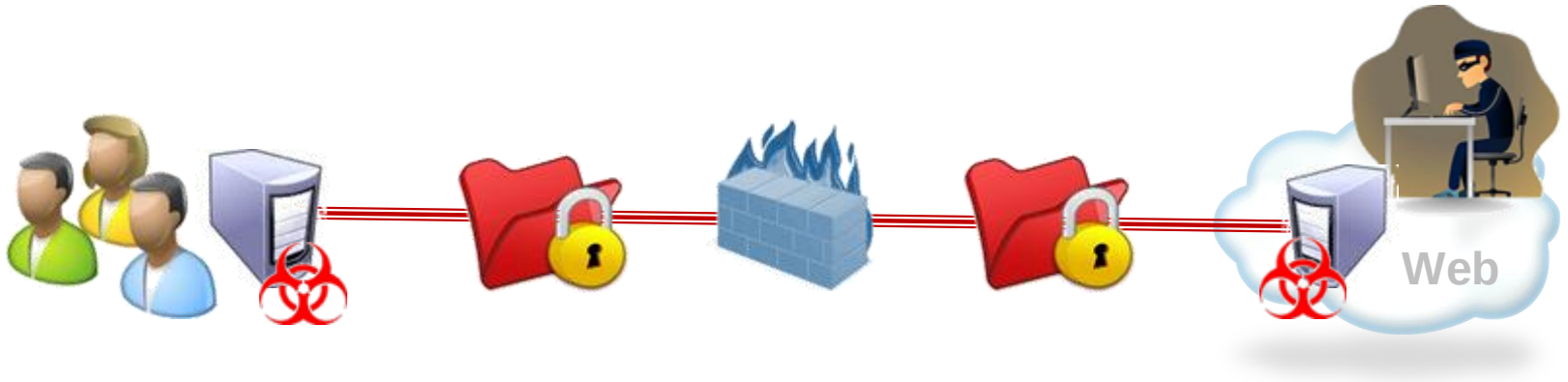
Evading Detection

TRITON™

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

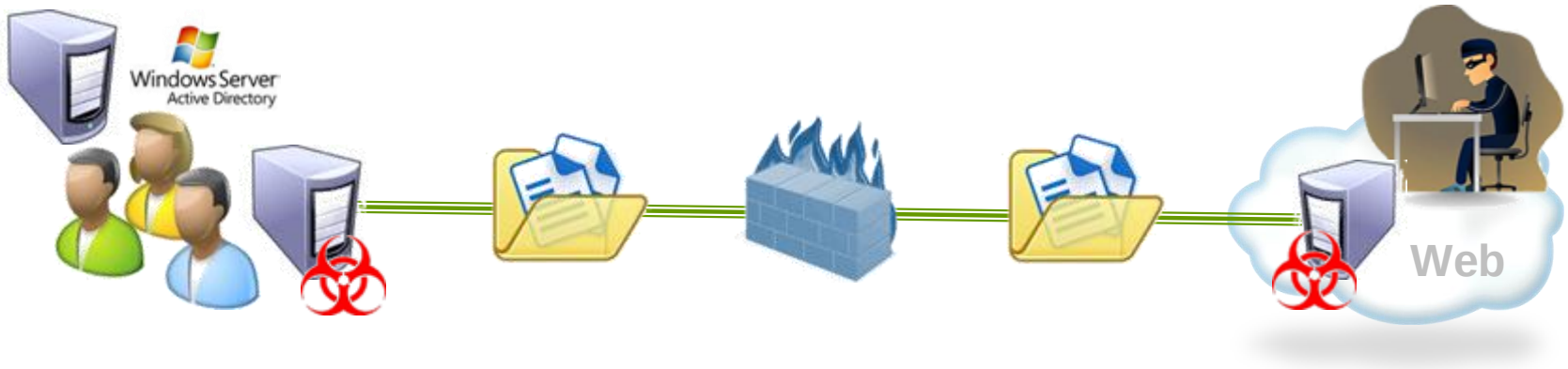
Criminal Encrypted Uploads

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



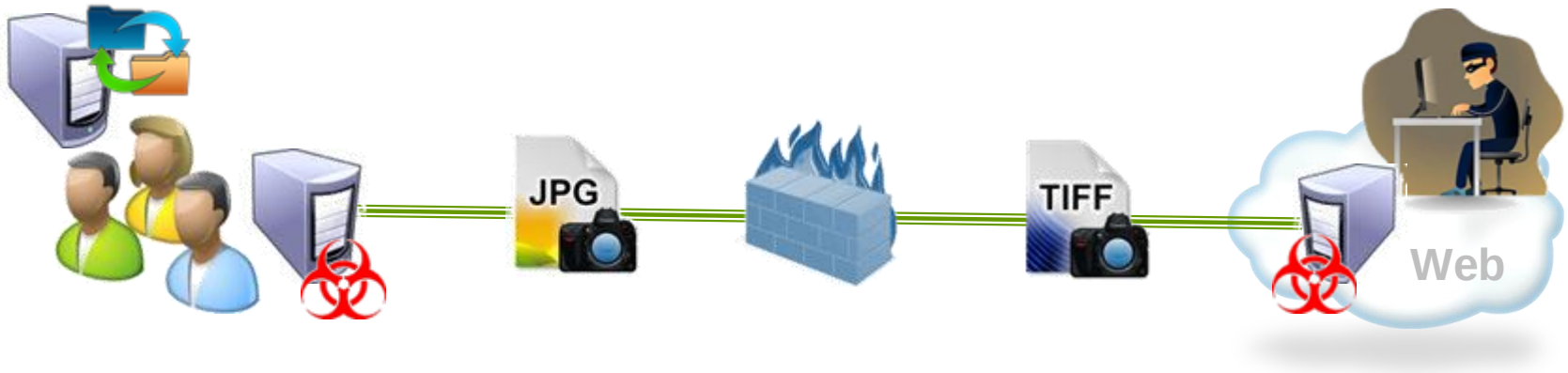
Password File Data Theft

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



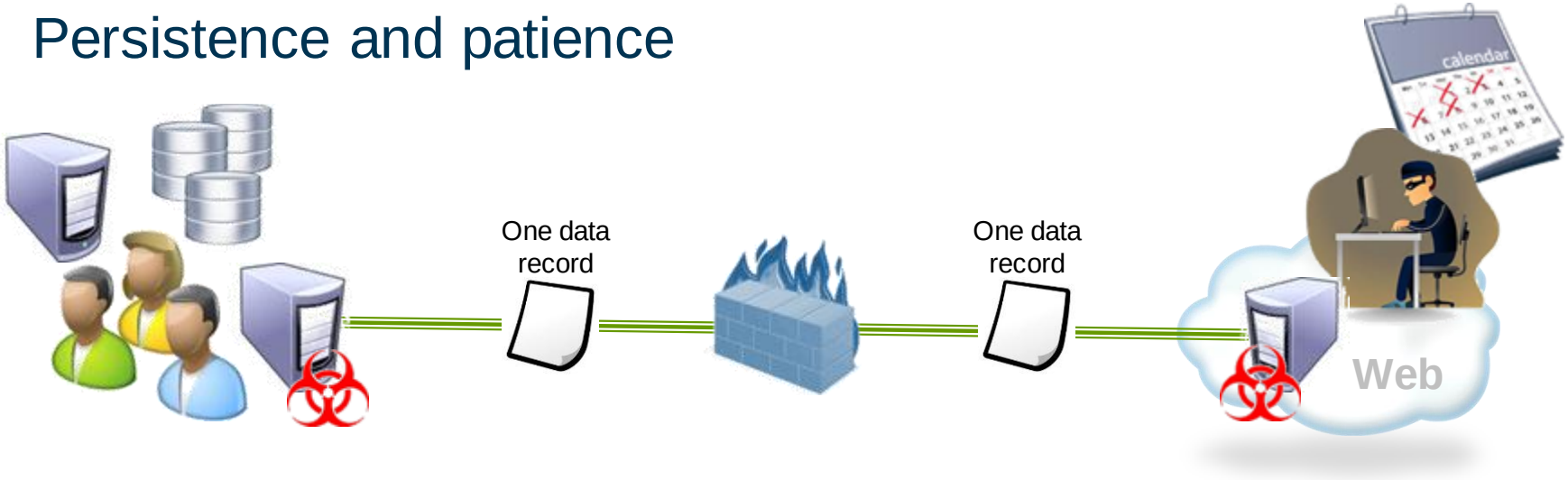
Non-Document Data Theft

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



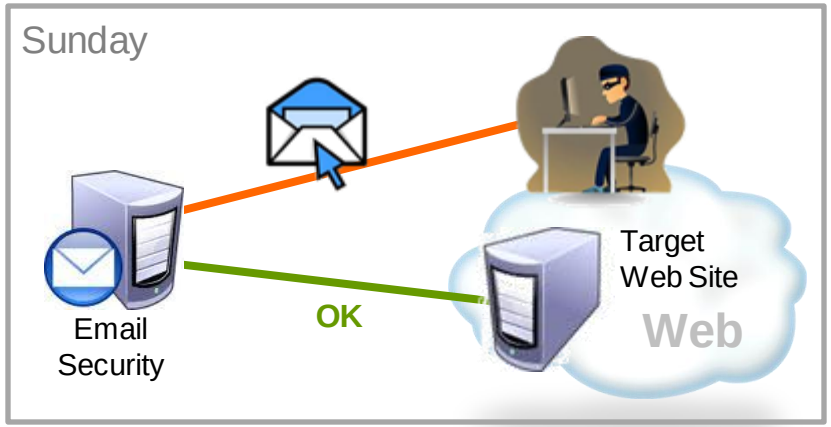
Slow Data Leaks

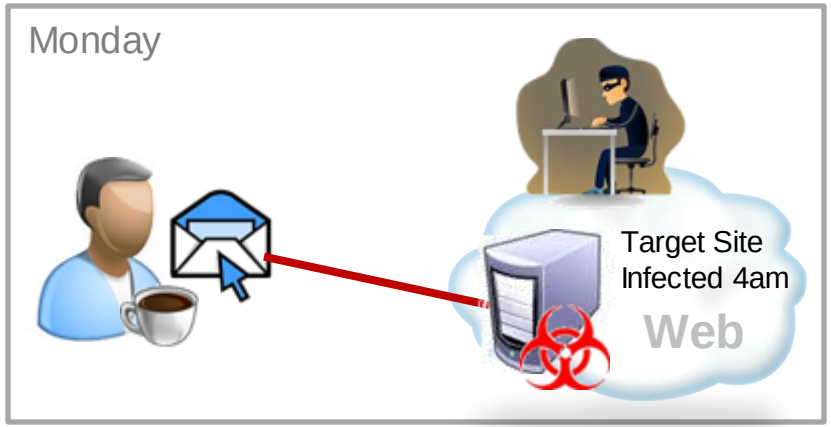
- Remain below the radar
- Low record count per request/incident
- Steal data in small chunks
- Persistence and patience



Email Security Evasion

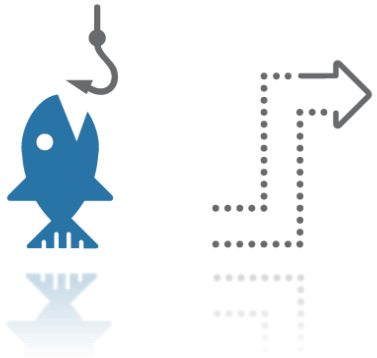
- Spear-phishing technique
- Embedded web link in email lure
- Time malware infection after delivery
- Email security sees a clean link





Recent Example – 6 July 2012

- Financial notification
- Appears as payroll related
- Debit to bank account
- Online transaction report



Subject: FW: ADP Funding Notification - Debit Draft

From: ADP_FSA_Services@ADP.com [mailto:ADP_FSA_Services@ADP.com]
Sent: Friday, July 06, 2012 12:36 PM
Subject: ADP Funding Notification - Debit Draft

Your Transaction Report(s) have been uploaded to the web site:

https://www.flexdirect.adp.com/client/login.aspx

Please note that your bank account will be debited within one banking business day for the amount(s) shown on the report(s).

Please do not respond or reply to this automated e-mail. If you have any questions or comments, please Contact your ADP Benefits Specialist.

Thank You,

ADP Benefit Services

Customer Requirements

Solving Open Issues

TRITON™

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

New Security Requirements

websense

- Protection from advanced threats
- Containment against data theft
- Threat dashboard with severity alerting
- Forensic reporting with SIEM integration
- Malware analysis sandboxing & services
- Performance & availability of defenses

Security Platform

websense®

websense®
TRITON™

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

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

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 Proxy Gateways

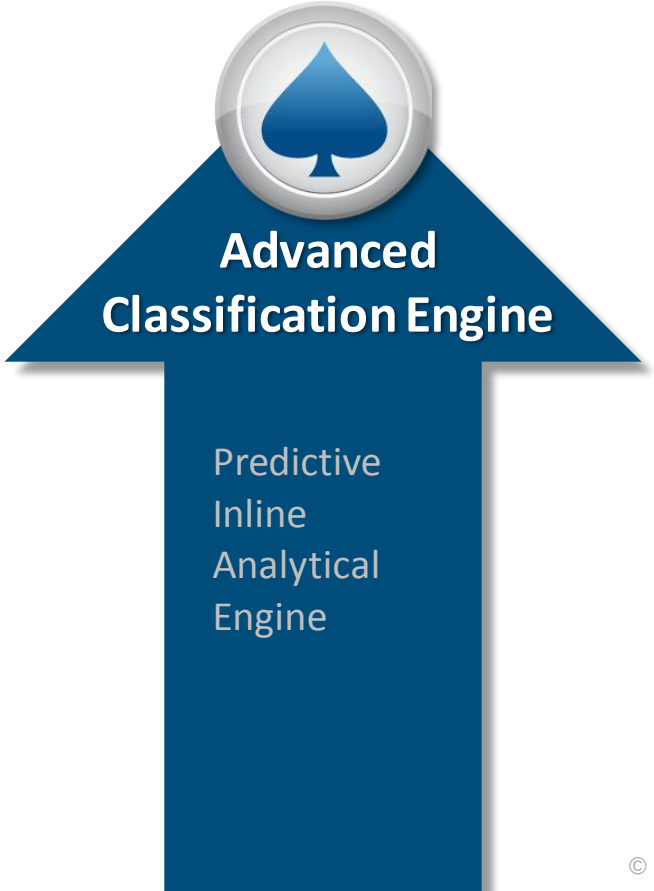
Key New Features

Advancing the TRITON Architecture

TRITON™

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

New ACE Defenses



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

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 →

Protection & Containment

websense

Criminal Encrypted Uploads

Password File Data Theft

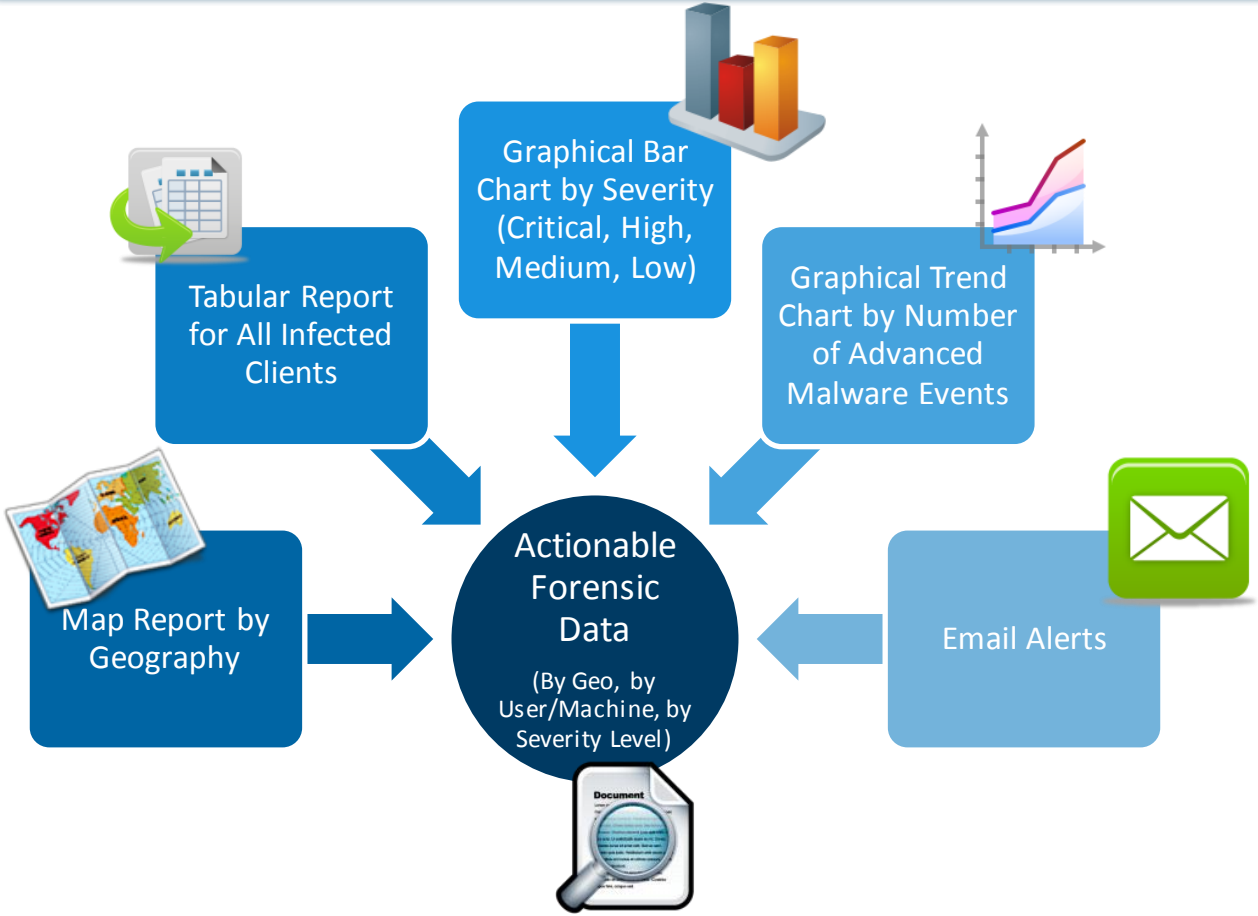
Image OCR/Text Analysis

One data record

Drip (Stateful) DLP

Cloud Sandboxing for Email

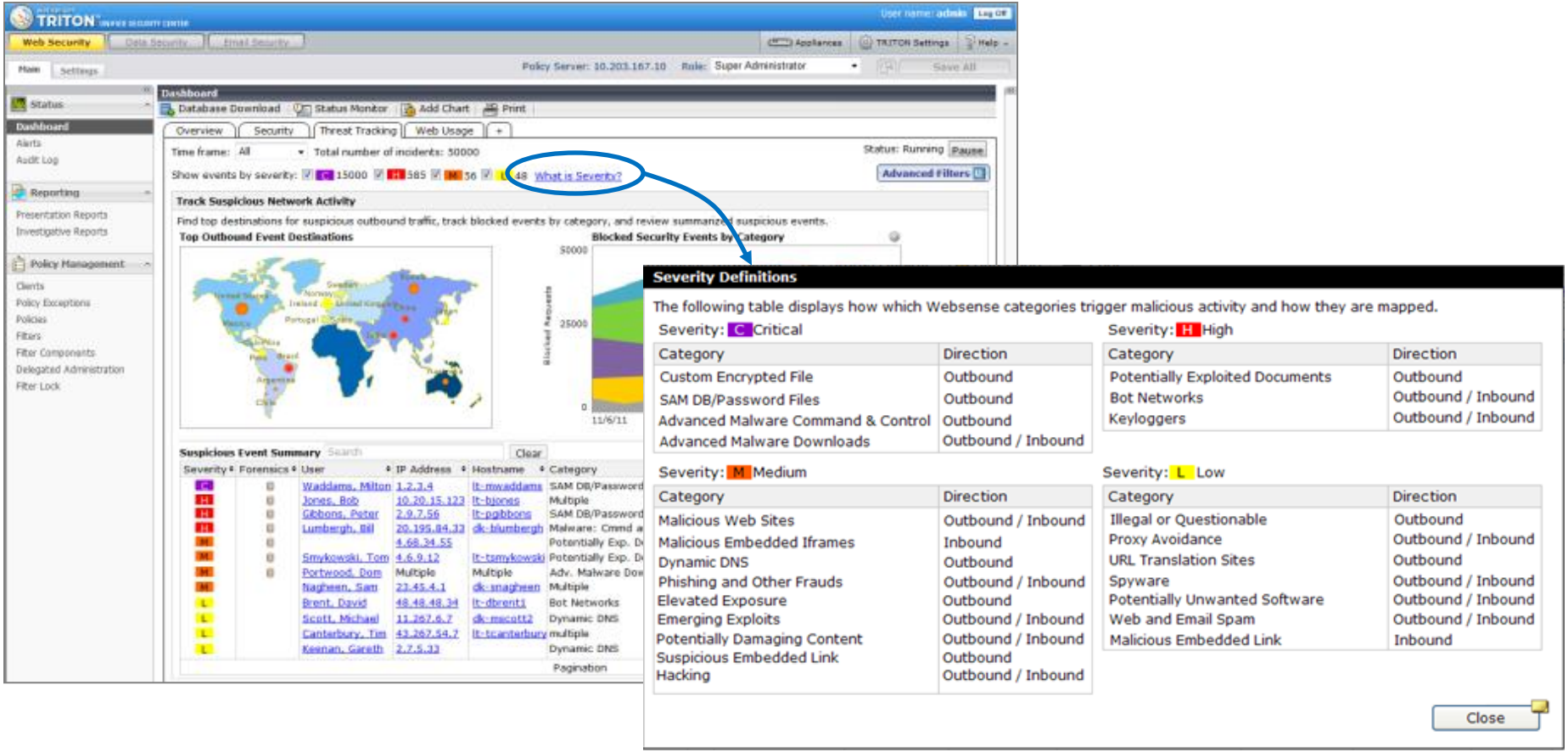
Advanced Malware Reporting Flow



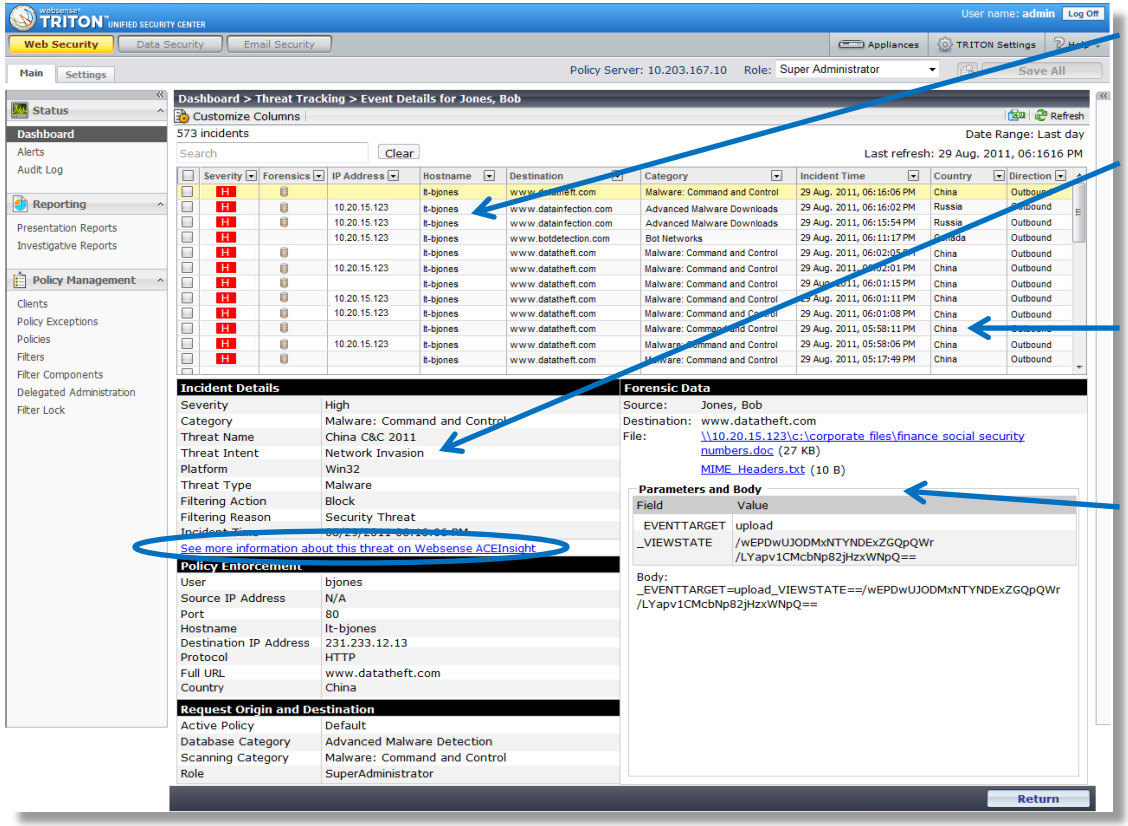
Designed to draw you to actionable data

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

Threat Dashboard



Forensic Reporting



- 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

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:

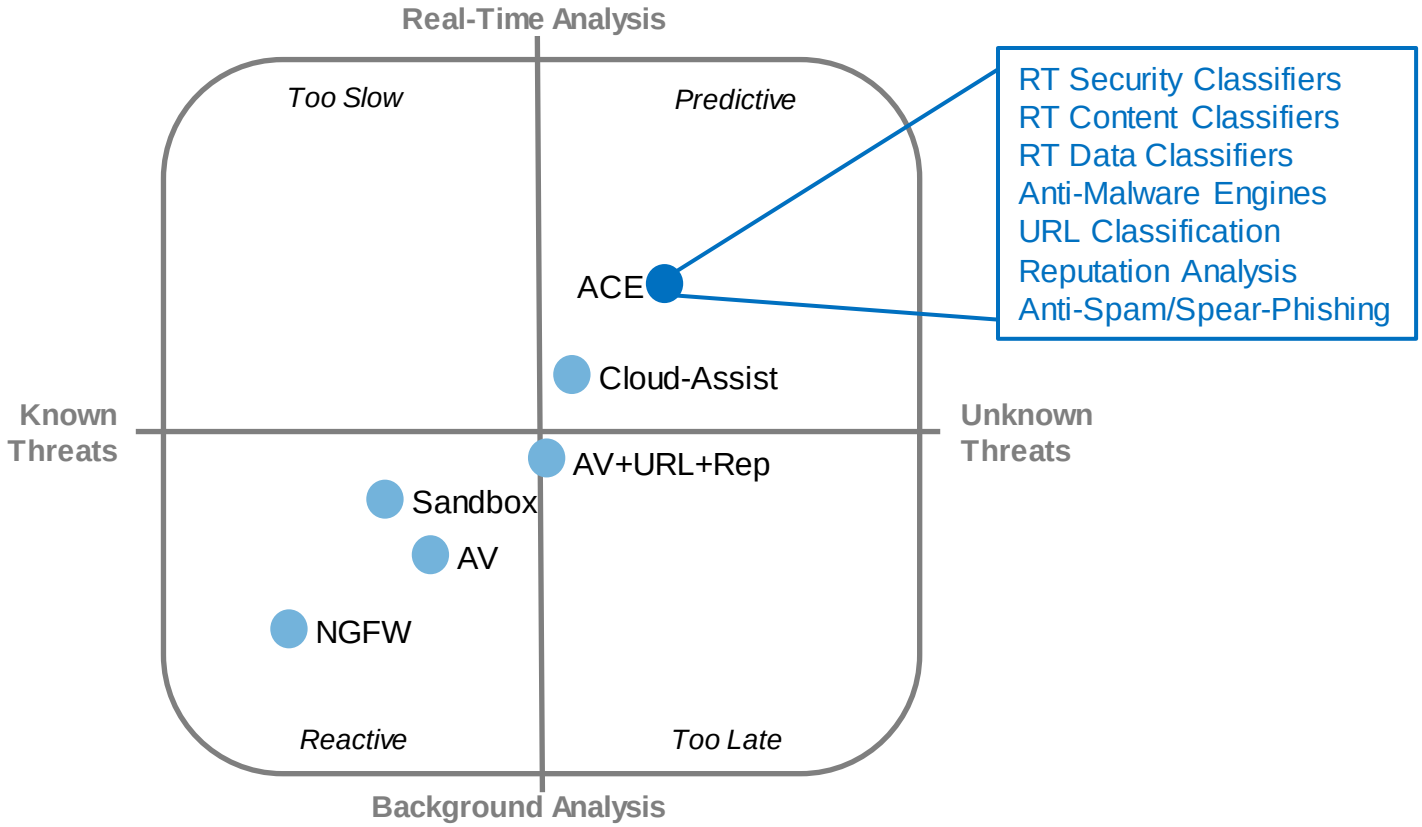
List of requested HTTP URLs:

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

Seven Industry Firsts

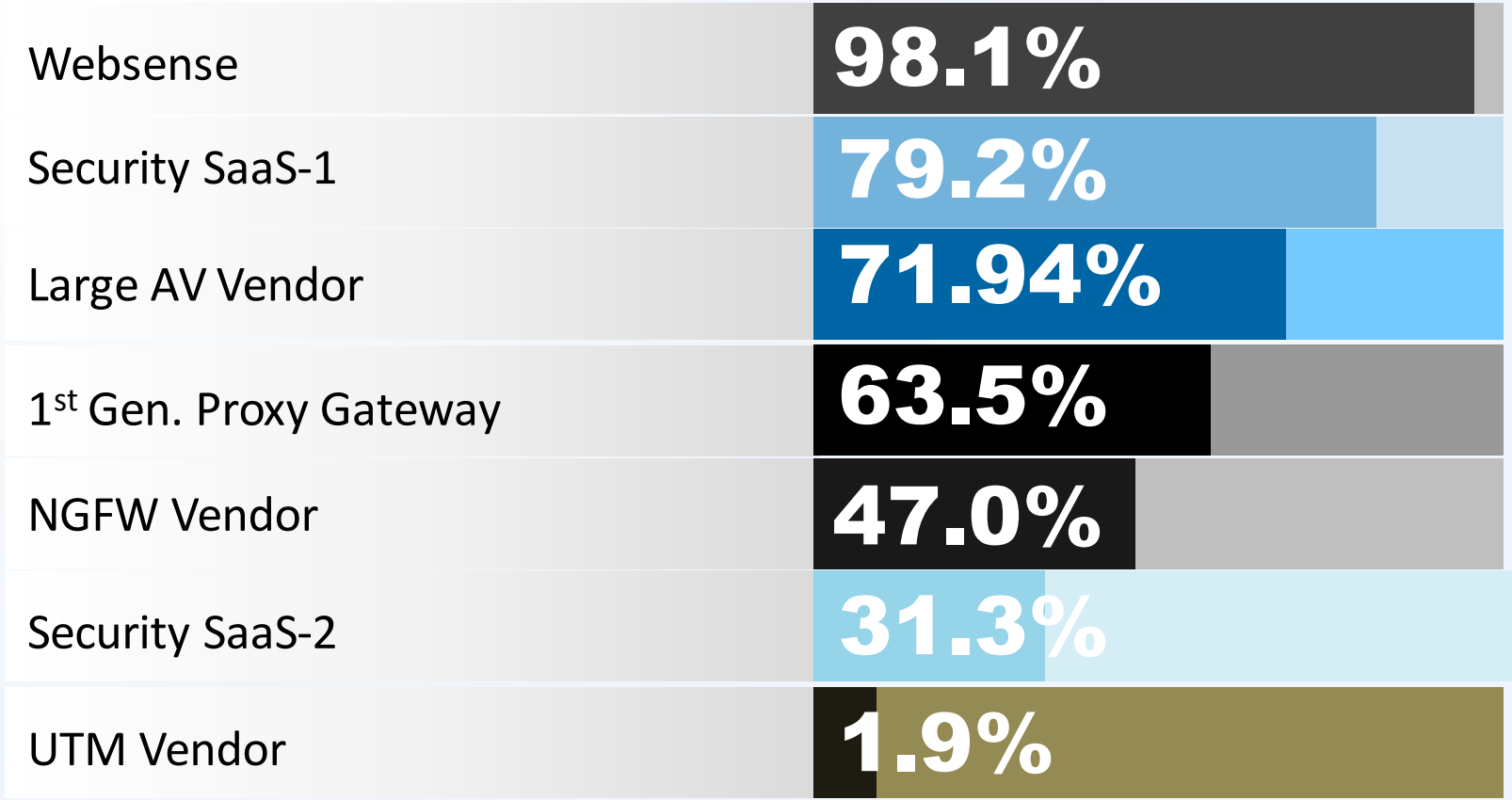
- Online Sandbox Service
- Cloud Sandboxing Email Links
- Criminal Encryption Detection
- Password File Data Theft
- OCR for Data-in-Motion
- Drip (Stateful) DLP
- Forensic Data Capture

Defense Effectiveness



Zero Day Browser Exploits – Q1 2012

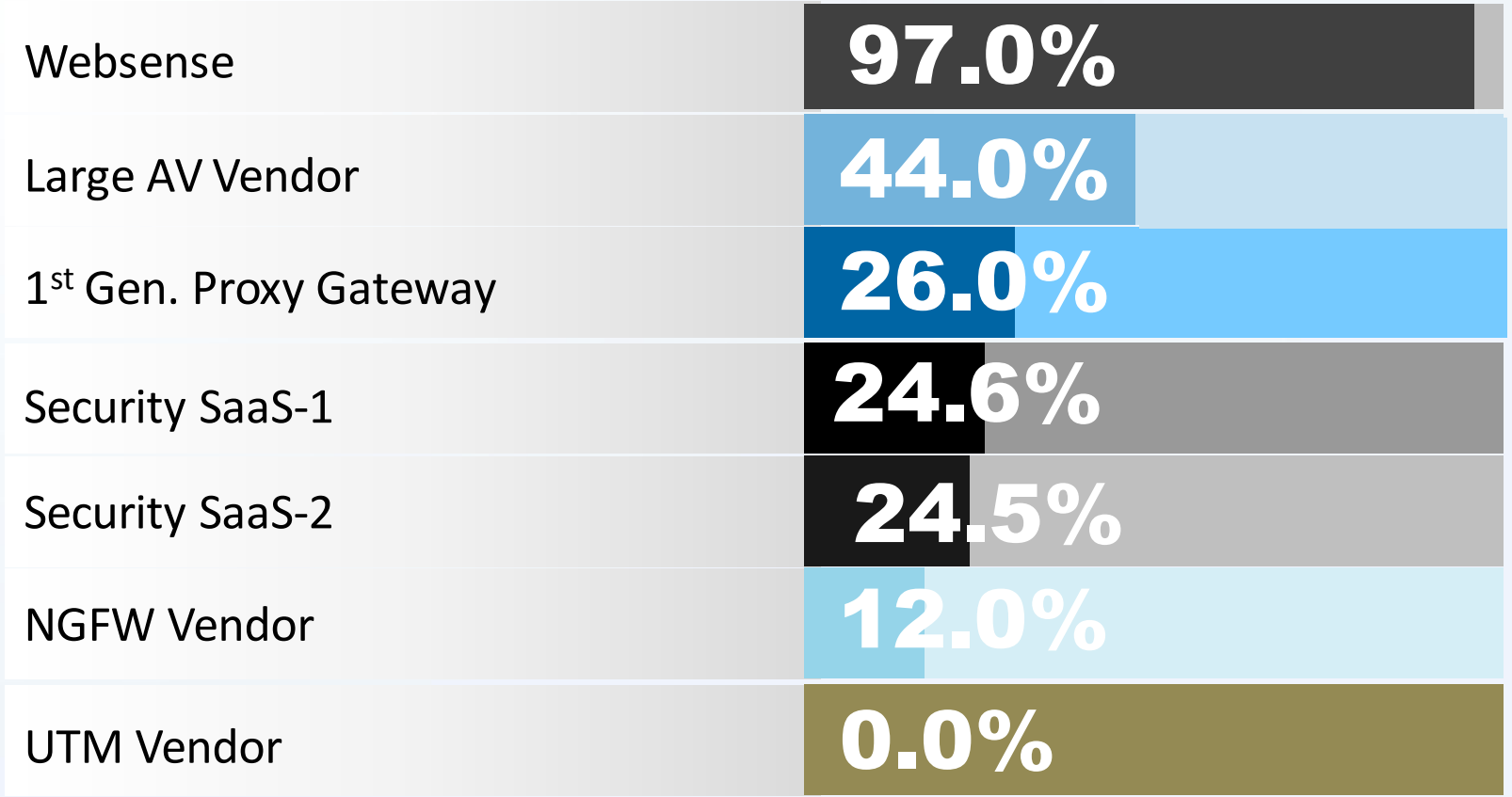
websense®



URLs containing malware, Q1 2012

Botnet Outbound Comms – Q1 2012

websense®



URLs containing malware, Q1 2012

Large Health Organization

websense

PROBLEM:

- Traditional AV & Firewalls not providing protection.
- Increasing volume of incidents, concerns with data theft.
- Workforce increasingly mobile, need end point data protection

SOLUTION:

- 50% reduction in mission critical outages
- Email spam & threats reduced by an extra 5-10% (depending on week)
- 8 weeks to deploy web, email & DLP security, single admin console
- Reduced infrastructure from 16 to 6 appliances

Large Federal Agency

websense

PROBLEM:

- More than **2 million attacks** per month on Federal agencies
- Excessive time invested by IT cleaning up malware infections
- Traditional defenses were not providing protection or enabling new technologies to share research and increase productivity
- Employees access billions of confidential documents & interact with public

SOLUTION:

- 60% reduction in system re-imaging due to malware infections
- Embedded DLP to prevent data loss & theft, plus compliance
- Lower TCO with enterprise license, savings expanded IT operations

Thank You.

TRITON™

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