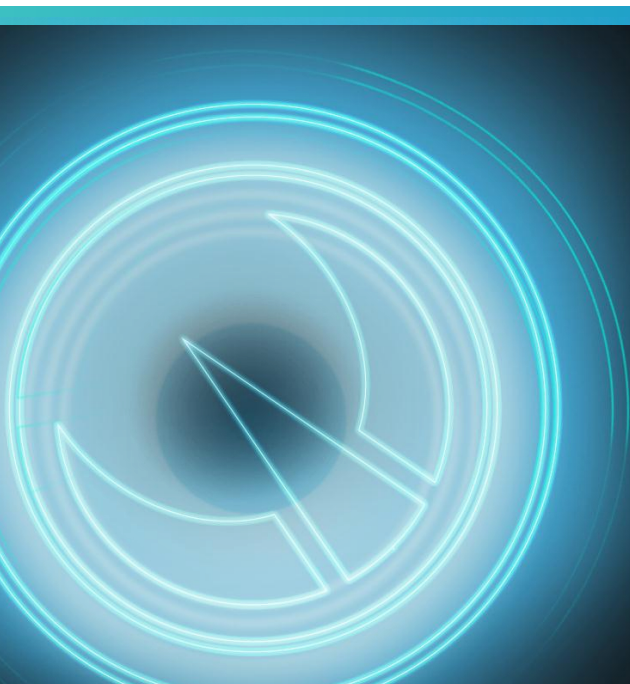


Sami Kovanen, Territory manager, Finland & Baltics



TRITON STOPS MORE THREATS. WE CAN PROVE IT.



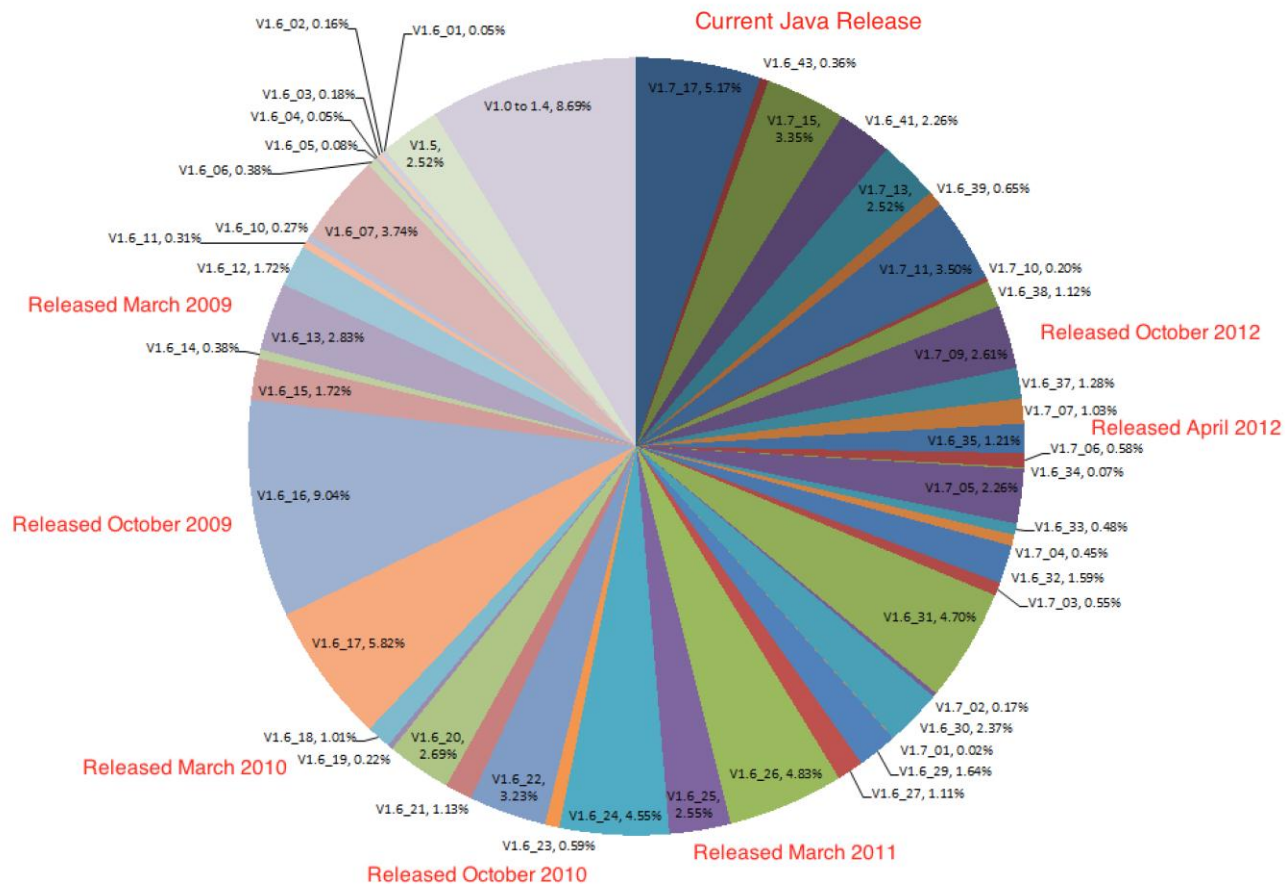
websense®
TRITON™

What has changed in security landscape?

CVE ID Syntax Change - Call for Public Feedback

January 22, 2013

Due to the increasing volume of public vulnerability reports, the Common Vulnerabilities and Exposures (CVE) project will change the syntax of its vulnerability identifiers so that CVE can track more than 10,000 vulnerabilities in a single year. The current syntax, CVE-YYYY-NNNN, only supports a maximum of 9,999 unique identifiers per year.



Self-Encryption and Self-Decryption. Some viruses can encrypt and decrypt their virus code bodies, concealing them from direct examination. Viruses that employ encryption might use multiple layers of encryption or random cryptographic keys, which make each instance of the virus appear to be different, even though the underlying code is the same.

Polymorphism. A polymorphic virus generally makes several changes to the default encryption settings, as well as altering the decryption code. In a polymorphic virus, the content of the underlying virus code body does not change; encryption alters its appearance only.

Stealth. A stealth virus uses various techniques to conceal the characteristics of an infection. For example, many stealth viruses interfere with OS file listings so that the reported file sizes reflect the original values and do not include the size of the virus added to each infected file.

Metamorphism. The idea behind metamorphism is to alter the content of the virus itself, rather than hiding the content with encryption. The virus can be altered in several ways for example, by adding unneeded code sequences to the source code or changing the sequence of pieces of the source code. The altered code is then recompiled to create a virus executable that looks fundamentally different from the original.

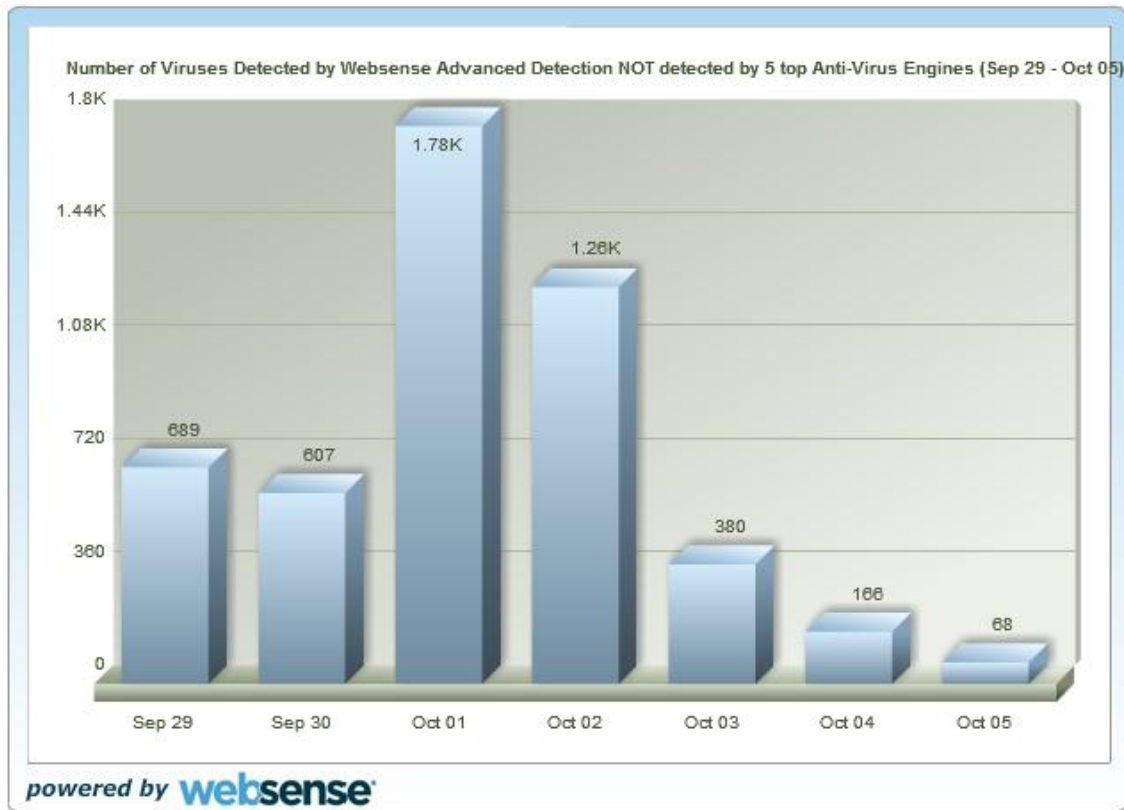
Armoring. The intent of armoring is to write a virus so that it attempts to prevent antivirus software or human experts from analyzing the viruses functions through disassembly, traces, and other means.

Tunneling. A virus that employs tunneling inserts itself into a low level of the OS so that it can intercept low-level OS calls. By placing itself below the antivirus software, the virus attempts to manipulate the OS to prevent detection by antivirus software.

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



websense®
SECURITY LABS



<http://securitylabs.websense.com/>

70 percent of the top 100 Web sites have either hosted or been involved in malicious activity over the last six-month period.

Web Traffic

THE DYNAMIC WEB

- Constantly changing content
- Millions of varied pages per site
- Legitimate sites compromised
- Legacy security systems obsolete
- Requires real-time content analysis

THE KNOWN WEB

- Current events, regional, genre sites
- Less user-generated content
- Reputation, URL databases fairly effective

THE UNKNOWN WEB

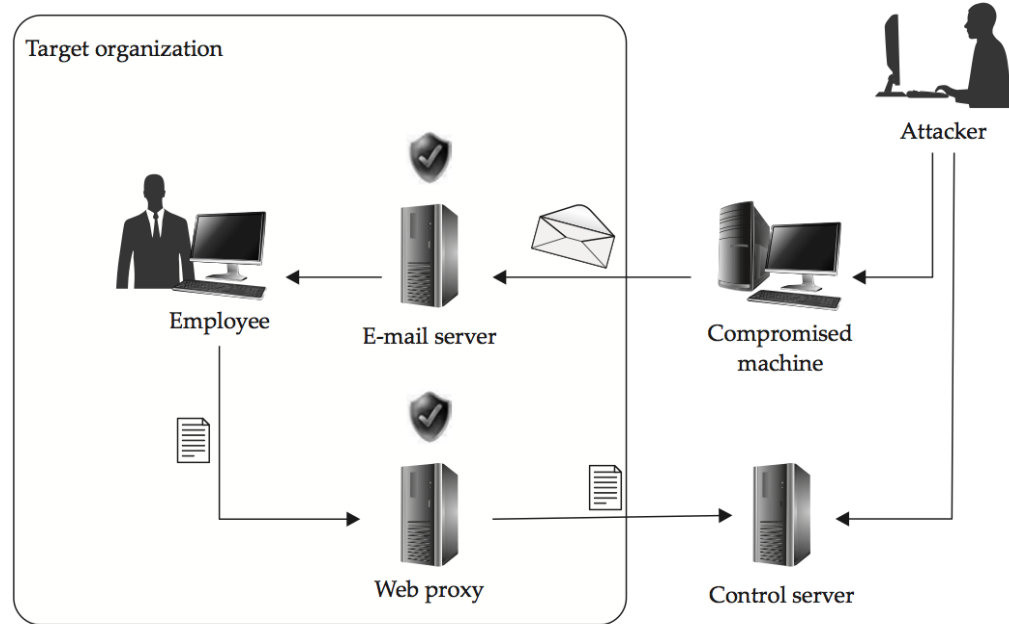
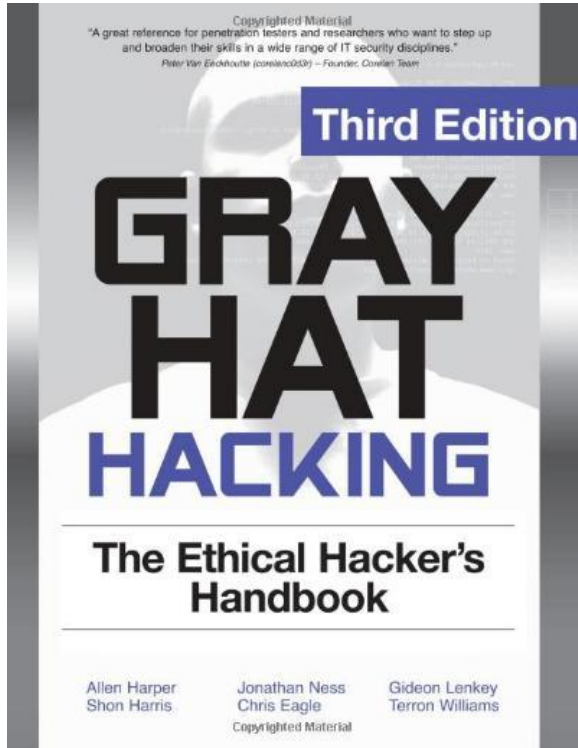
- Junk, personal, scam, adult, etc.
- Million of new sites appear daily
- Reputation and URL databases can't keep up
- Requires real-time categorization and real-time security scanning

Top 100 sites

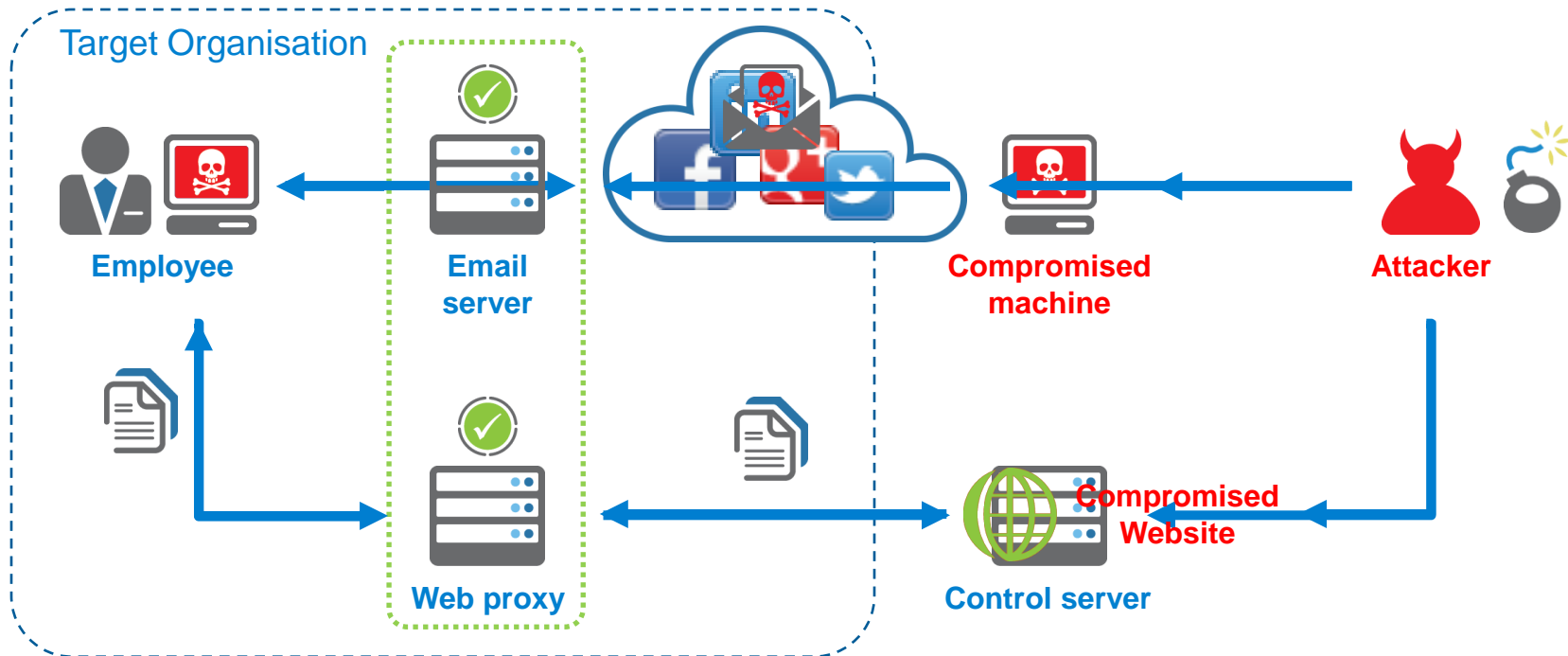
Next 1 million sites

Next 100 million sites

Why many organisations remain highly vulnerable to cyber threats and what you can do to help reduce risk?



7 stages



- Existing Security Deployments based on signature based technology.
- Insight into advanced (signature-less) threats is crucial.
- Threat monitoring **can't** gain insight into previously invisible threats.

**YOU CAN'T PROTECT
AGAINST INVISIBLE THREATS**

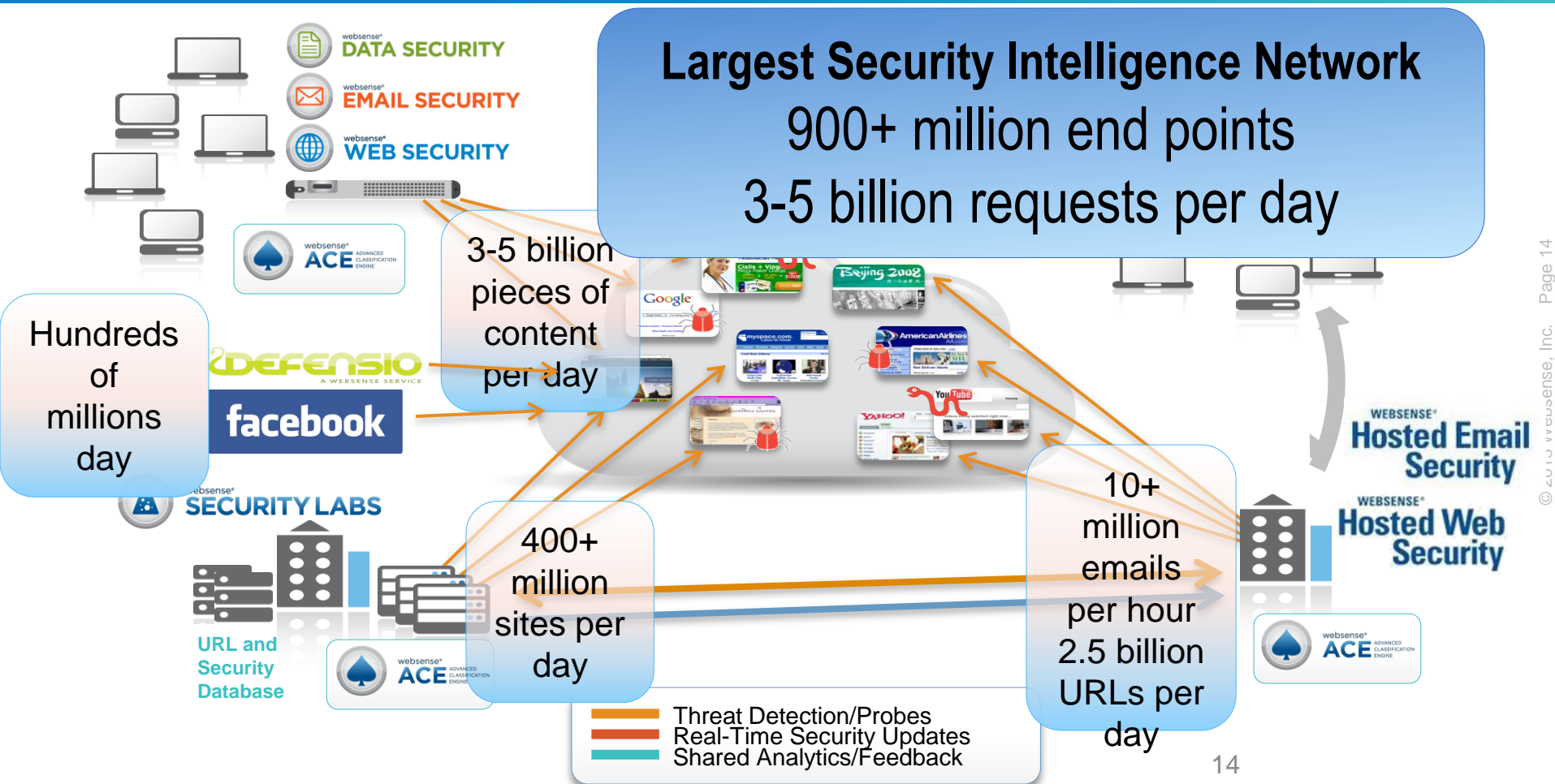




Websense ACE



- **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**
- **Behavioral Analytics**



Correlation view (Detect, Contain, Mitigate)

websense

- **WHO** was target of compromise (Detect)
- **WHAT** was prevented from being stolen (Contain)
- **WHERE** the data was destined (Contain)
- **HOW** the malware operates and technique used for exfiltration (Mitigate)

The screenshot displays the Websense TRITON Unified Security Center interface. The top navigation bar includes 'Web Security', 'Data Security', and 'Email Security'. The main dashboard shows 'Threat Tracking > Event Details for Jones, Bob' with 573 incidents. A table lists events with columns for Severity, Forensics, IP Address, Hostname, Destination, Category, Incident Time, Country, and Direction. Below this, a 'Track Suspicious Network Activity' section features a world map and a 'Blocked Security Events by Category' chart. A 'Suspicious Event Summary' table is also visible, listing various events and their details. The interface includes search filters, a date range selector, and a 'Return' button at the bottom.

Severity	Forensics	IP Address	Hostname	Destination	Category	Incident Time	Country	Direction
High	Malware	10.20.15.123	ft-bjones	www.datasteft.com	Malware: Command and Control	29 Aug. 2011, 06:16:06 PM	China	Outbound
High	Malware	10.20.15.123	ft-bjones	www.datainfection.com	Advanced Malware Downloads	29 Aug. 2011, 06:16:02 PM	Russia	Outbound
High	Malware	10.20.15.123	ft-bjones	www.datainfection.com	Advanced Malware Downloads	29 Aug. 2011, 06:15:54 PM	Russia	Outbound
High	Malware	10.20.15.123	ft-bjones	www.botdetection.com	Bot Networks	29 Aug. 2011, 06:11:17 PM	Canada	Outbound
High	Malware	10.20.15.123	ft-bjones	www.datasteft.com	Malware: Command and Control	29 Aug. 2011, 06:02:05 PM	China	Outbound
Control	Control				Control	29 Aug. 2011, 06:02:01 PM	China	Outbound
Control	Control				Control	29 Aug. 2011, 06:01:15 PM	China	Outbound
Control	Control				Control	29 Aug. 2011, 06:01:11 PM	China	Outbound
Control	Control				Control	29 Aug. 2011, 06:01:08 PM	China	Outbound
Control	Control				Control	29 Aug. 2011, 05:58:11 PM	China	Outbound
Control	Control				Control	29 Aug. 2011, 05:58:06 PM	China	Outbound
Control	Control				Control	29 Aug. 2011, 05:17:49 PM	China	Outbound

bob
datasteft.com
15.1231c:\corporate files\finance social security
s.doc (27 KB)
eaders.txt (10 B)
ady
alue
pload
wEPDwUJODMxNTYNDExZGQpQWw
Yapv1CMcbNp8ZjhzxWNPQ==
load_VIEWSTATE==wEPDwUJODMxNTYNDExZGQpQWw
HxzWNPQ==

Protecting data, everywhere, all the time and all devices.

STRUCTURED DATA

3742-4963-5398-4312

EASY TO PROTECT

UNSTRUCTURED DATA

Intellectual Property

Contracts Customer Mergers Acquisitions Data ideas knowledge processes

blueprints Financial designs Accounts Ideas

property

HARD TO PROTECT



websense®
TRITON™

WEB

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

EMAIL

The **most advanced** email defenses against **blended** and **targeted attacks**.

DATA

- ✓ Content Aware DLP
- ✓ Data Discovery
- ✓ DLP Gateway
- ✓ DLP Endpoint
- ✓ MacOS & Windows
- ✓ Off-Network Prot.
- ✓ Portable Decrypt.
- ✓ 1,700 Policy/Temp.
- ✓ Drip DLP Detect.
- ✓ OCR of Image Text
- ✓ Geo-Location

CLOUD

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

MOBILE

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



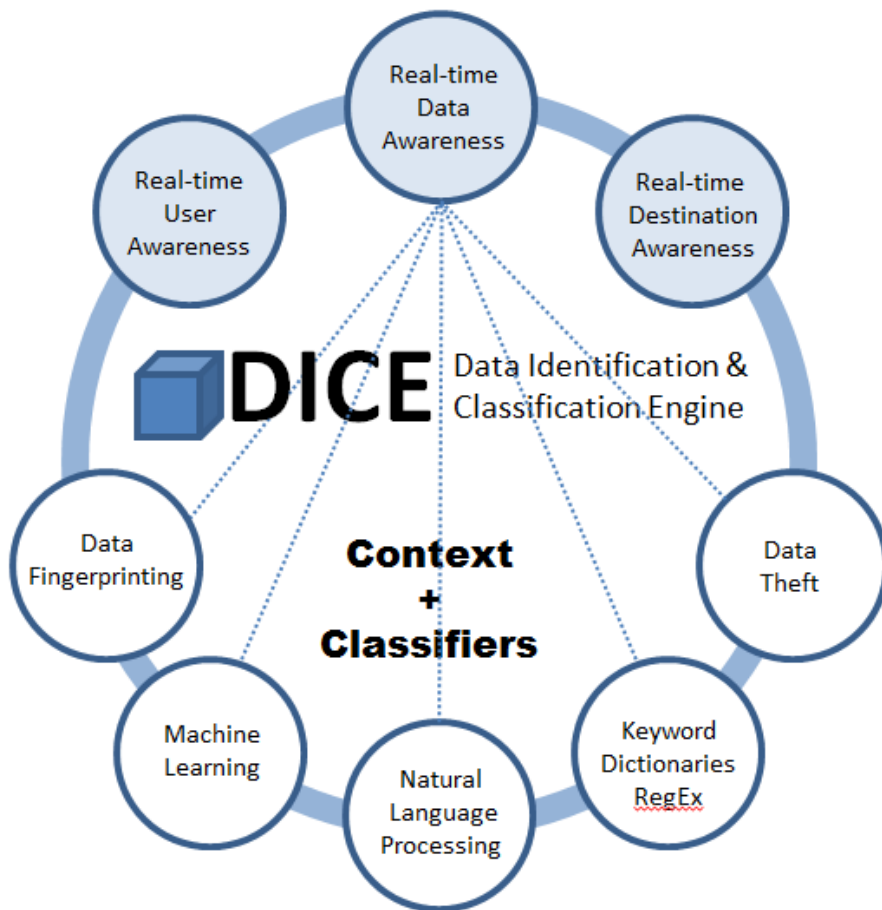
websense®
THREATSEEKER®
NETWORK



websense®
ACE



websense®
SECURITY LABS™



The Websense Data Security Suite uses DICE to classify data in a contextually aware manner.

What to protect



Simple Incident Management

Take Action

List of Relative Incidents

Violation Triggers

The screenshot displays the Websense Triton Unified Security Center interface. The top navigation bar includes links for Web Security, Data Security, Email Security, and Mobile Security. The left sidebar contains a 'Main' menu with 'Reporting' and 'Settings'. The 'Reporting' menu is expanded, showing 'Data Loss Prevention' (highlighted with a blue arrow), 'Mobile Devices', and 'Discovery'. Below this is the 'Policy Management' section, which includes 'DLP Policies', 'Discovery Policies', 'Content Classifiers', and 'Resources'. The 'Status' section shows 'Today', 'System Health', 'Endpoint Status', 'Mobile Status', 'Traffic Log', 'System Log', and 'Audit Log'. The main content area is titled 'Gartner Tagged Incidents' and shows a list of 28 incidents. The table columns are ID, Incident Tag, Incident Time, Source, Policies, Channel, and Destination. The incident with ID 345646 is highlighted. Below the table, the 'Incident: 603004' details are shown, including the severity (Low), action (Quarantined), and channel (Network email). The 'Display: Violation triggers' section lists several rules, including 'Rule: US SSN (default)', 'Rule: SSN: ITIN', 'Rule: Patterns & phrases', and 'Rule: Health Data: ICD9 Code and Description'. The 'Forensics' tab is selected, showing the incident details, including the sender (Jon Stark), recipient (dssdemo@gmail.com), subject (RE: stuff to look at), and attachment (3000.random.customer.records.xlsx(528.92 KB)). A blue arrow points from the 'Incident Details' label to the 'Subject' field.

ID	Incident Tag	Incident Time	Source	Policies	Channel	Destination
603004	Gartner 4.2.01 Quarantined Email that has been release b...	01 Jun. 2012, 03:28:15 PM	Jon Stark	Testing; Email DL...	Network email	dssdemo@gmail.com
344311	Gartner 4.1.01 - simple regex only	31 May. 2012, 09:45:09 AM	Jack London	Testing	HTTPS	mail.google.com
345646	Gartner 4.1.02 Partial Document Match	31 May. 2012, 11:30:48 AM	Sunil Wadwani	Strategic Busines...	Network email	dssdemo@gmail.com
294904	Gartner 4.1.03 Network Registered Data Detection - Salesforce	30 May. 2012, 05:37:31 PM	Jack London	Salesforce Data P...	HTTPS	mail.google.com
346590	Gartner 4.1.04 NOTEXTIP	31 May. 2012, 11:59:06 AM	Sunil Wadwani	NOTEXTIP	Network email	dssdemo@gmail.com
448256	Gartner 4.1.04 OCR and Proximity	31 May. 2012, 11:20:31 PM	10.34.50.129	US PII; Social Se...	HTTPS	mail.google.com
346058	Gartner 4.1.05 Proximity Detection US SSN (Default) near ...	31 May. 2012, 11:43:13 AM	Jack London	US PII; Northwind...	HTTPS	mail.google.com
491754	Gartner 4.1.06 IM with registered data	01 Jun. 2012, 09:02:21 AM	10.34.51.121	US PII; Northwind...	Chat	shaliniwadwani
345681	Gartner 4.1.07 FTP sensitive information	31 May. 2012, 12:20:21 PM	10.34.51.71	Business Document...	FTP	moran.dreamhost.com
295309	Gartner 4.1.08 Webmail Incident	30 May. 2012, 08:54:33 PM	Jack London	Salesforce Data P...	HTTPS	mail.google.com
232466	Gartner 4.1.09 - localized policy	30 May. 2012, 12:46:06 PM	Jack London	Hong Kong PII	HTTPS	dl-web.dropbox.com
345746	Gartner 4.1.10 NOTENGLISH	31 May. 2012, 10:32:52 AM	Sunil Wadwani	Testing; Simplifi...	Network email	dssdemo@gmail.com

Incident: 603004 Severity: Low Action: Quarantined Channel: Network email

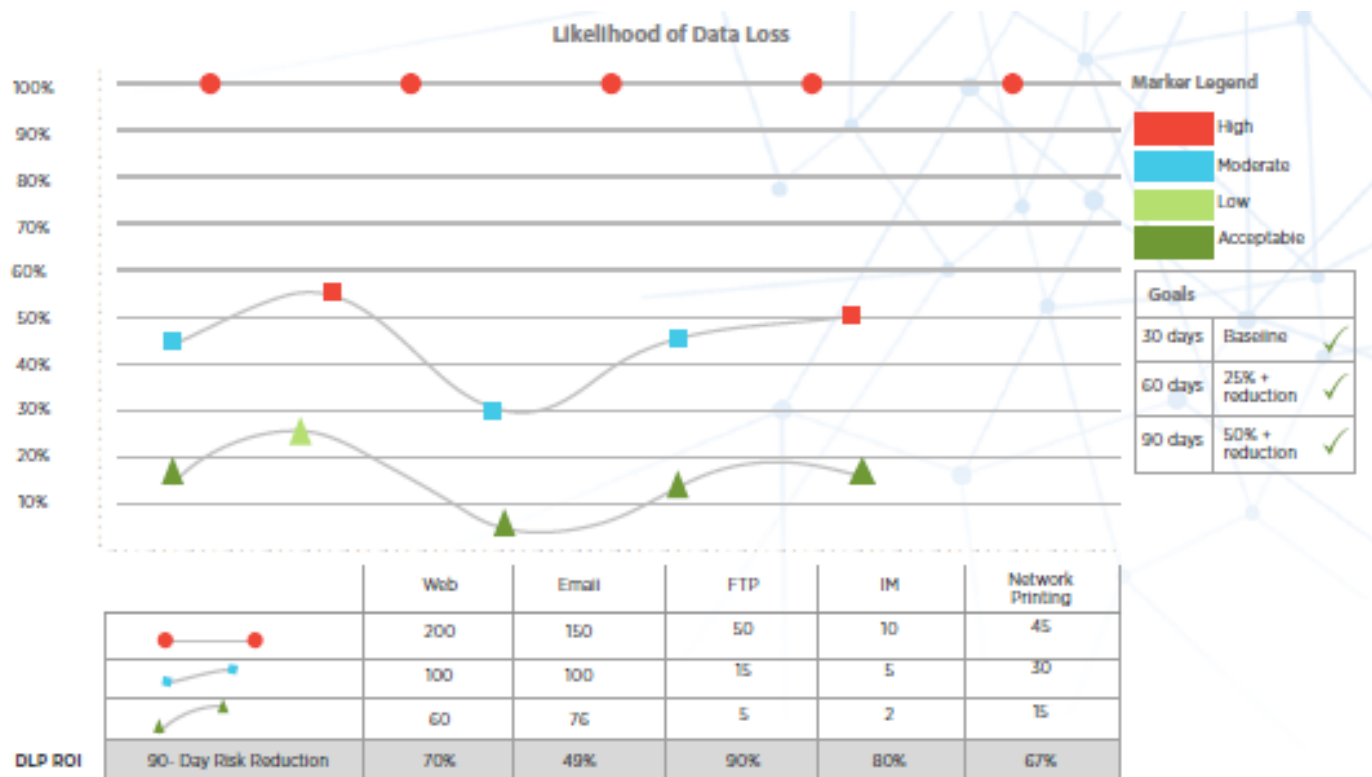
Display: Violation triggers

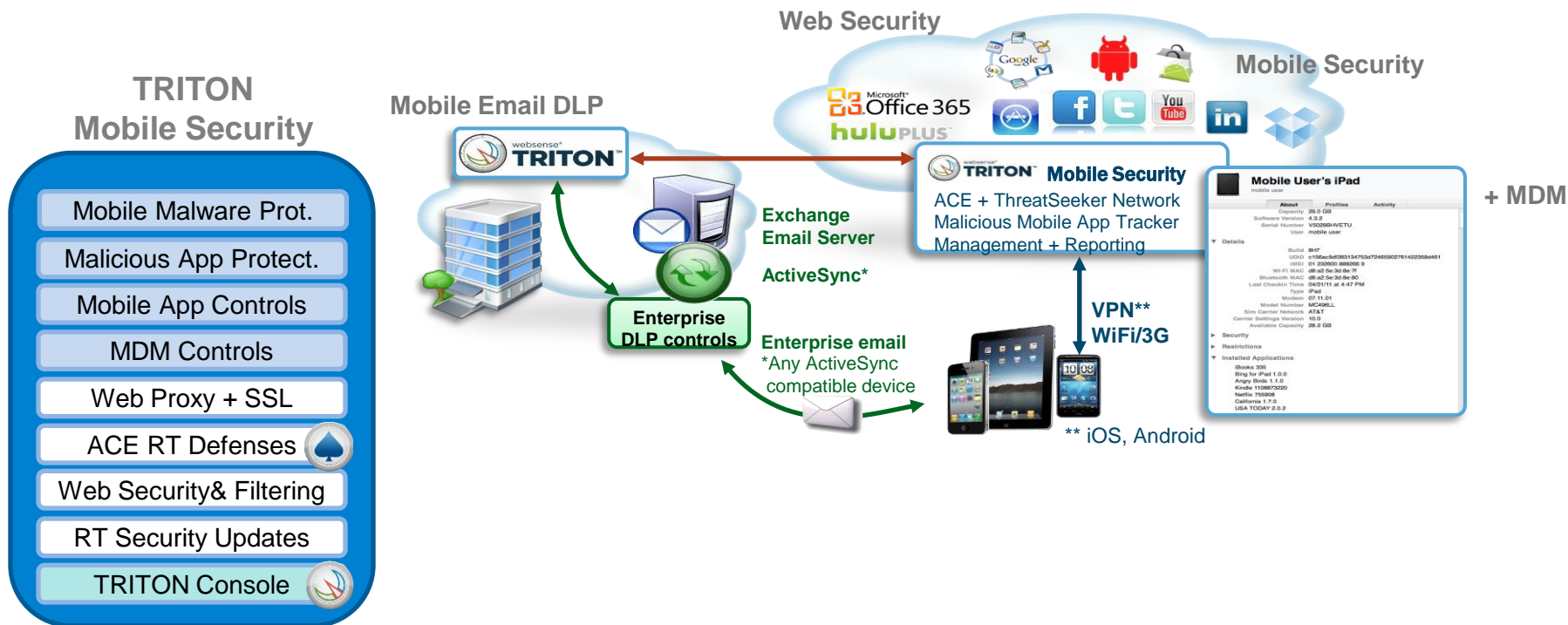
- Rule: US SSN (default)
 - US SSN (Default) (Script)
133-10-7028, 232-76-6826, 143-24-7711, 148-41-5074, 210-47-4463, 121-72-56
- Rule: SSN: ITIN
 - US ITIN (Regular Expression)
973-70-1441, 920-80-7254, 983-80-8555, 991-76-5658, 967-74-9912, 938-82-1
- Rule: Patterns & phrases
 - Patterns & phrases (Email Attribute)
FactoryTestKeyword
- Rule: Health Data: ICD9 Code and Description
 - ICD9 Codes near ICD9 English Descriptions
78, Colon, 750, 990

Forensics Properties History

From: Jon Stark
To: dssdemo@gmail.com
Subject: RE: stuff to look at
Attachments: 3000.random.customer.records.xlsx(528.92 KB)
Message Body

Incident Details





Data security

- Fast implementation
 - Results after 1 month, lower your riskprofile
- EU privacy law requirements included
- What document to where? Right decision making.
- All data, all users all devices
- Automatic learning
- 7 yers leading in Gartner

THREATS STOPPED ACROSS 2,259,348 LIVE SAMPLES



NO ONE
STOPS **MORE** THREATS

