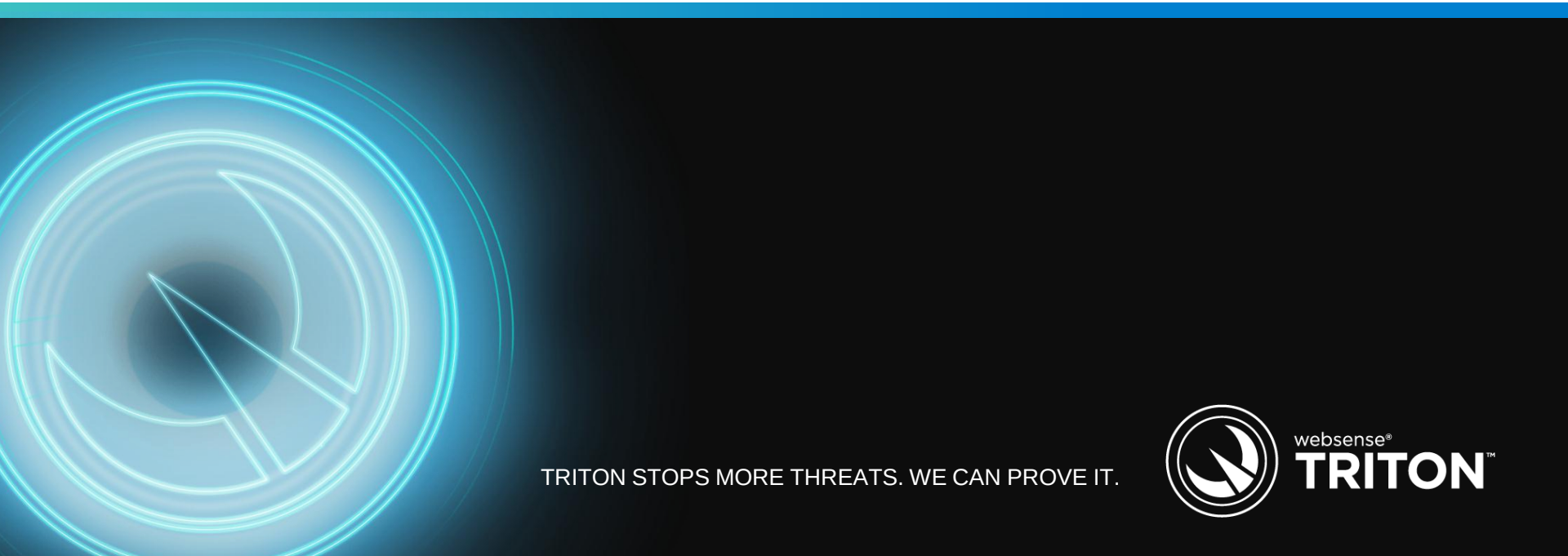
websense

Sami Kovanen, Territory manager, Finland & Baltics



What has changed in security landscape?

Vulnerable

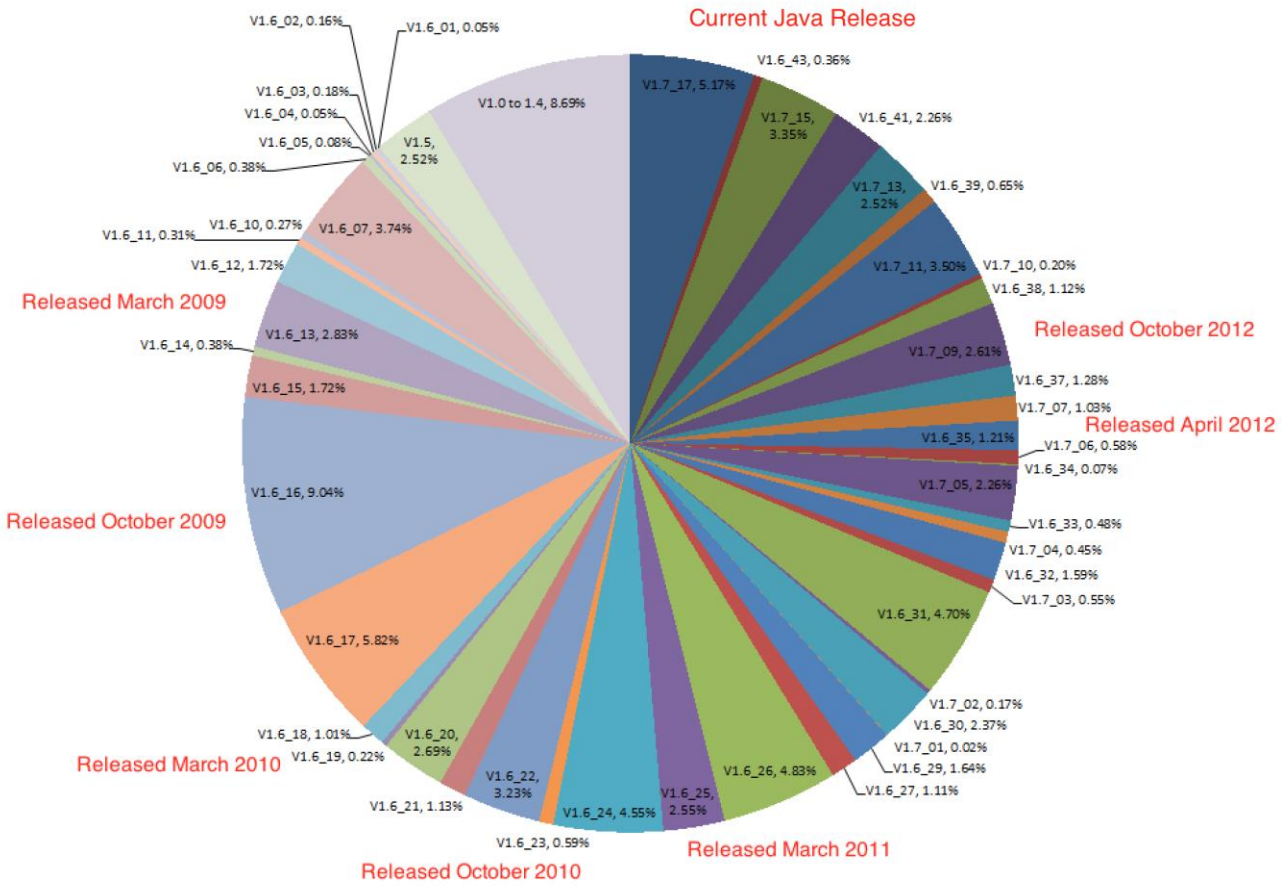
websense

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.

95%



AV evasion

websense

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.

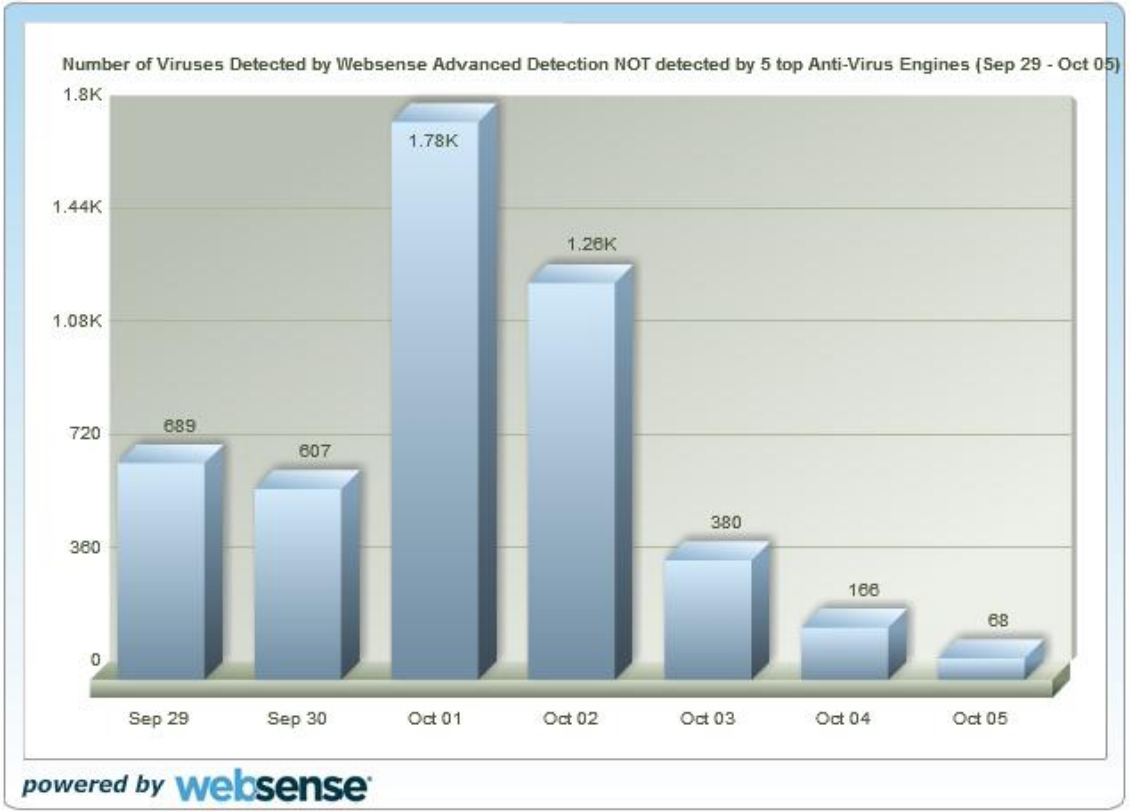
Armoring. The intent of armoring is to write a virus so that it attempts to prevent antivirus software or human experts from analyzing the viruses functions through disassembly, traces, and other means.

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.

ACE - Proven Daily

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

websense® SECURITY LABS

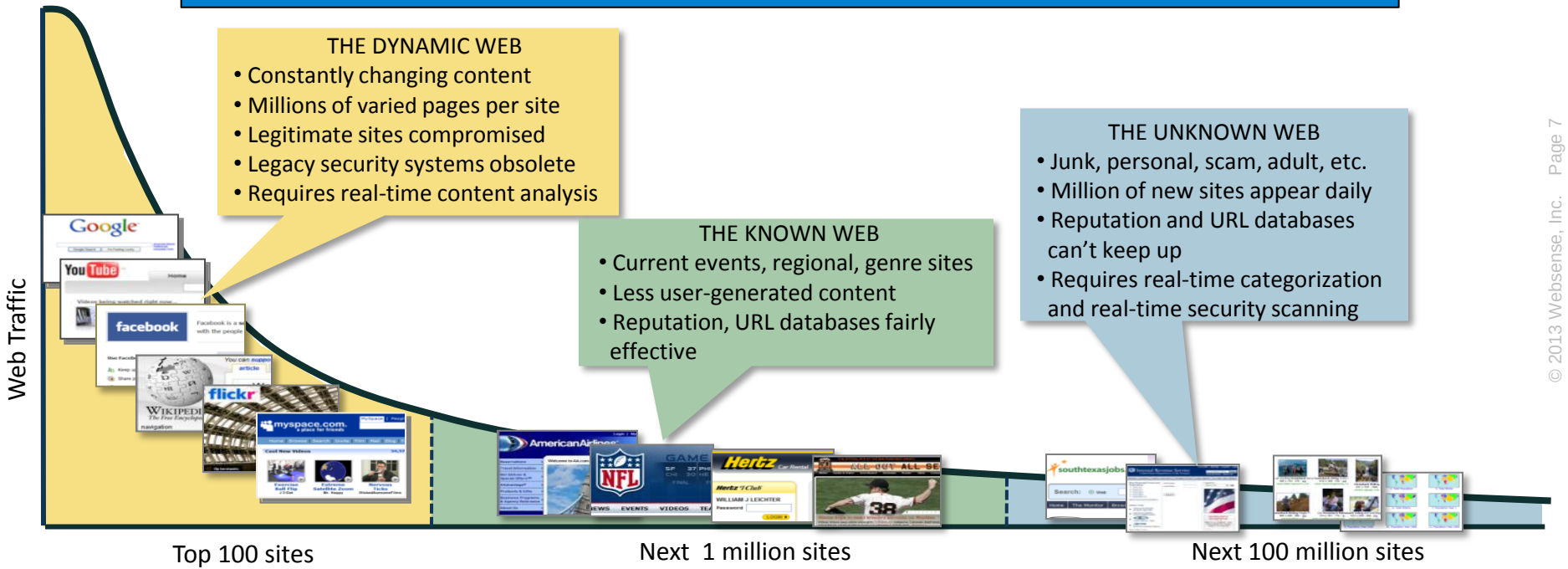


http://securitylabs.websense.com/

Today's Webscape

websense

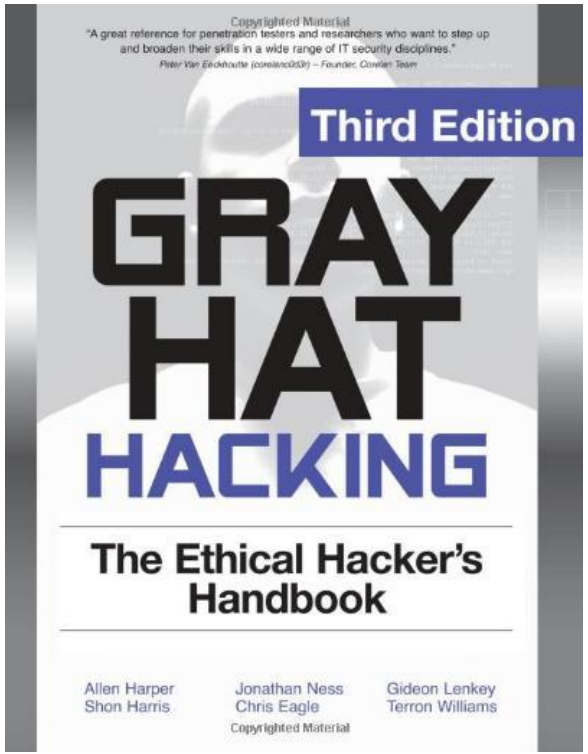
70 percent of the top 100 Web sites have either hosted or been involved in malicious activity over the last six-month period.

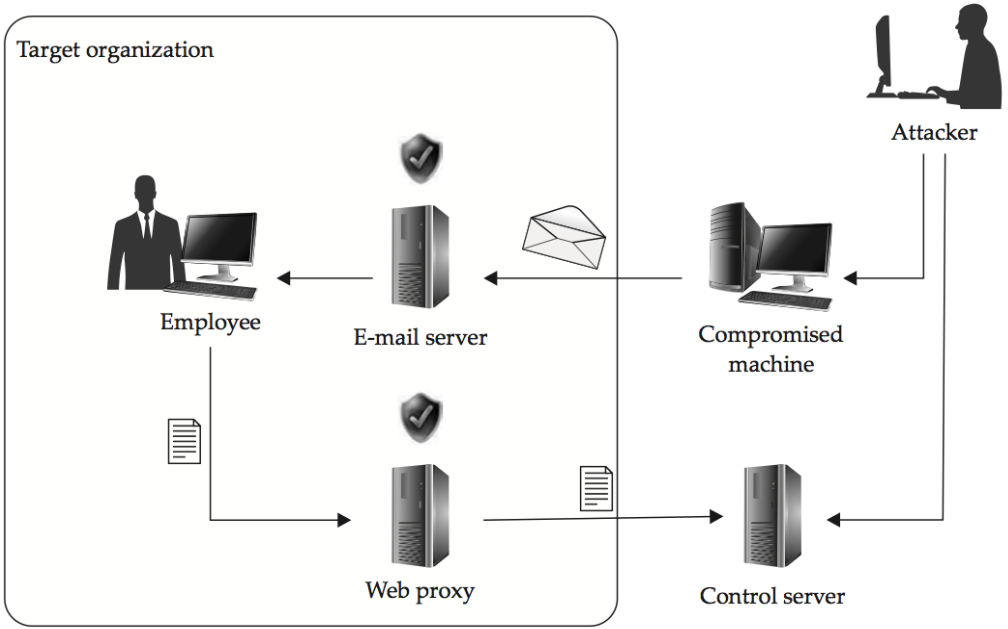


Why many organisations remain highly vulnerable to cyber threats and what you can do to help reduce risk?

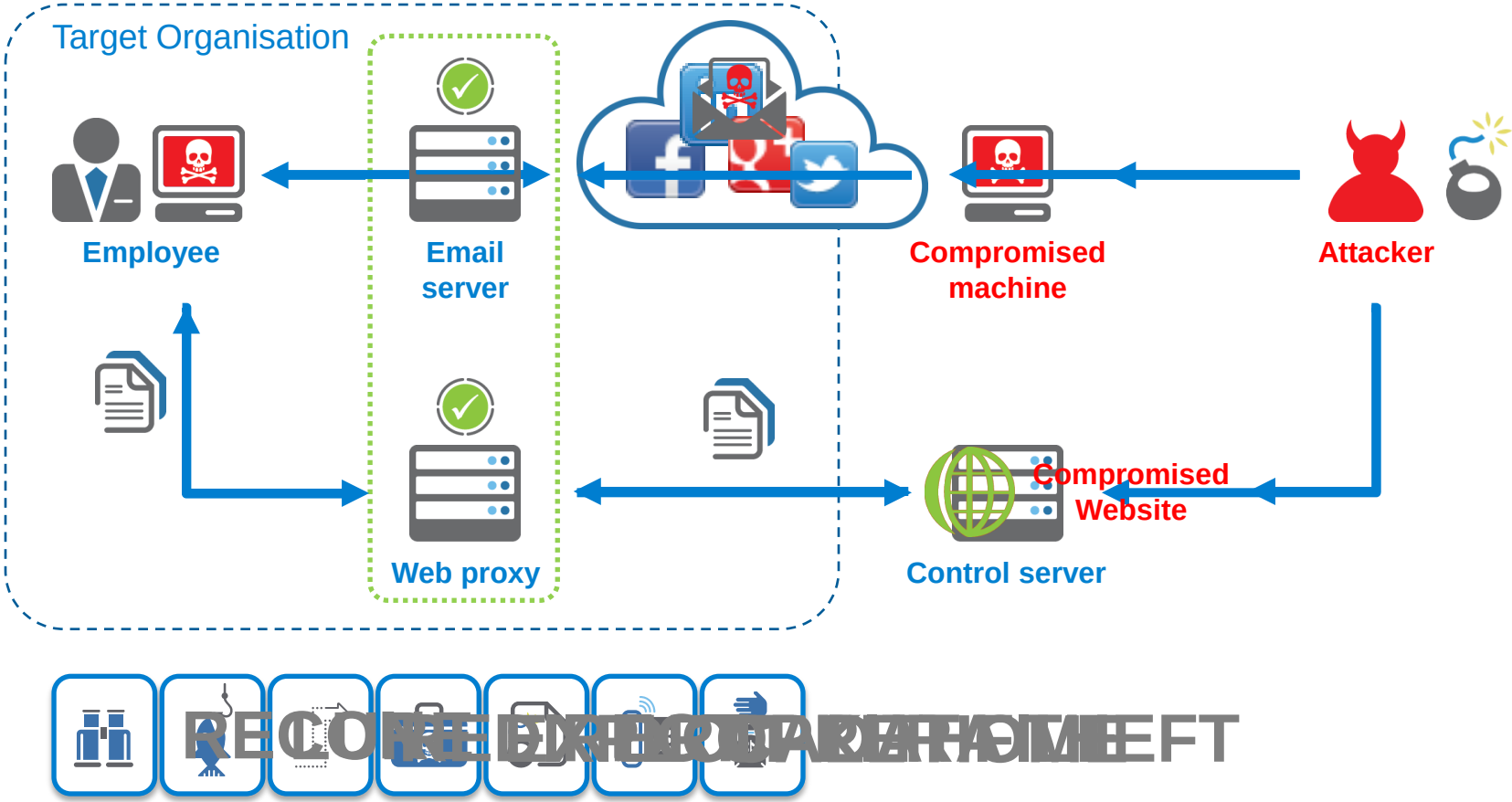
Hackers Handbook – Ch.16 Content security

websense





7 stages



The Need to Know What You Don't Know

websense

- **Existing Security Deployments based on signature based technology.**
- **Insight into advanced (signature-less) threats is crucial.**
- **Threat monitoring provides insight into previously invisible threats.**

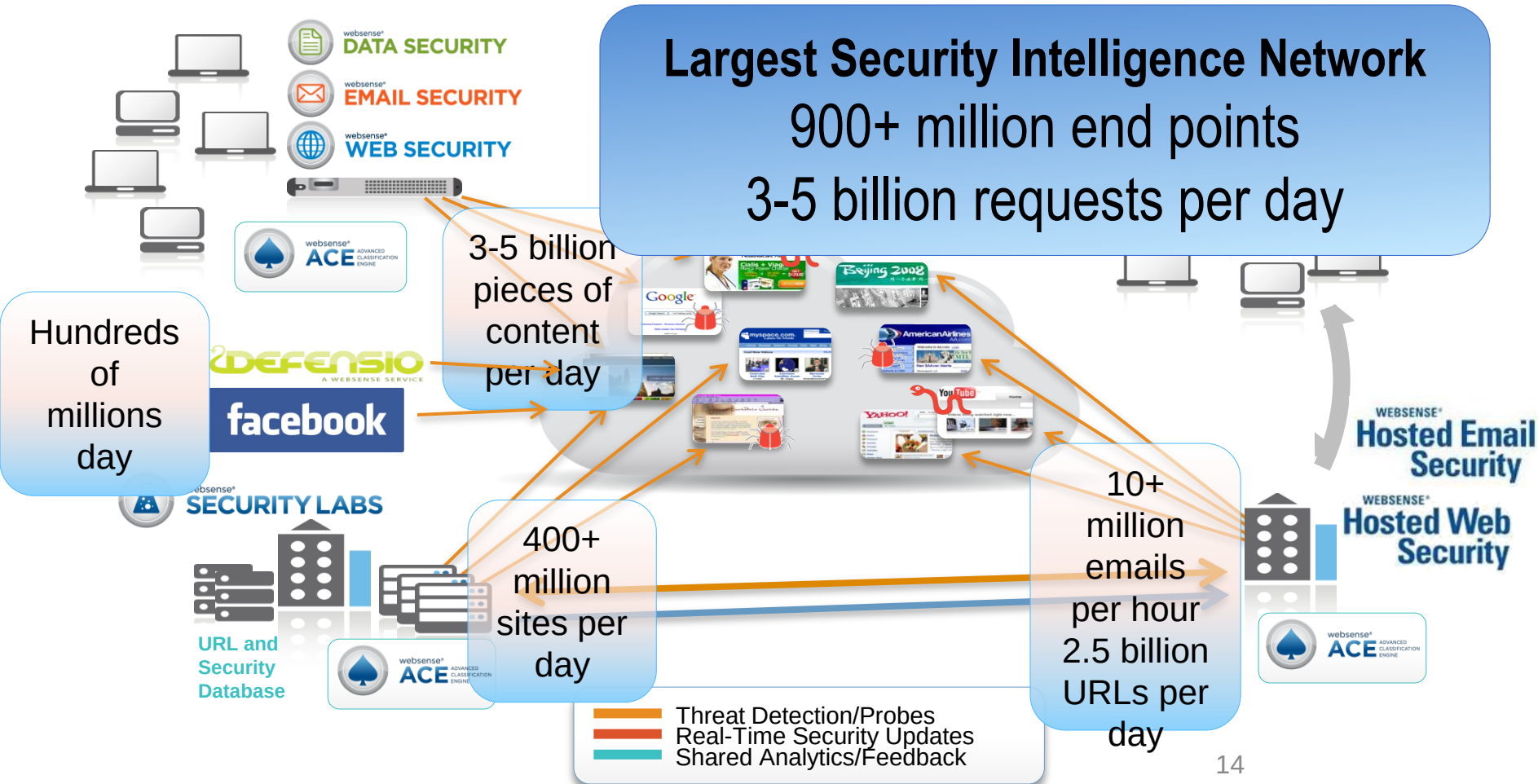
Real-time Threat & Content Analysis

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**

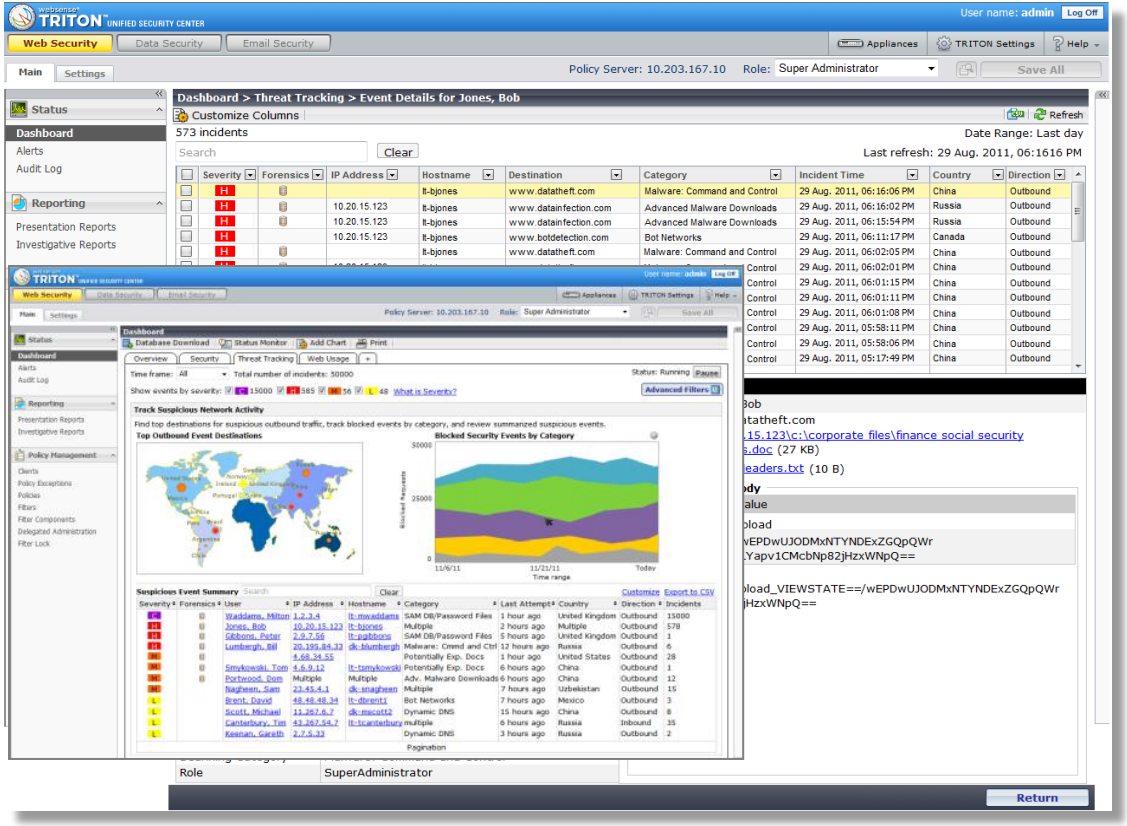
Websense ThreatSeeker™ Network

websense



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)

Protecting data, every ware, all the time and all devices.

The target…past, present and future

websense

STRUCTURED DATA

3742-4963-5398-4312

EASY TO PROTECT

UNSTRUCTURED DATA

HARD TO PROTECT

TRITON Security Platform

websense

websense® TRITON™

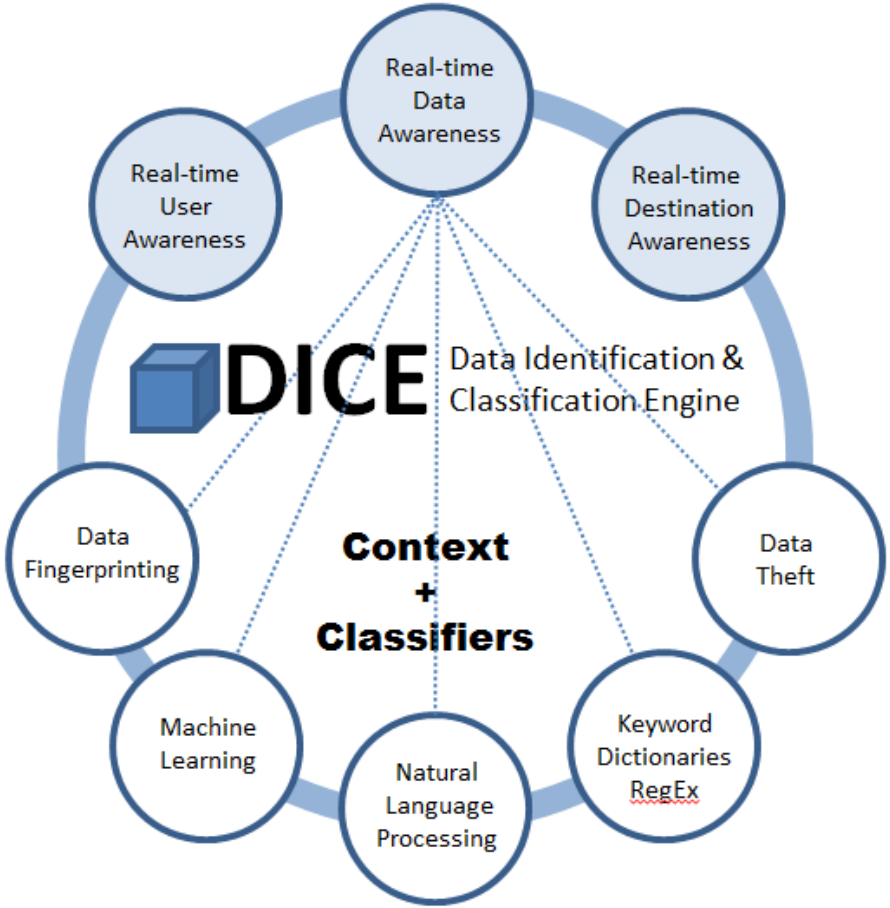
WEB	EMAIL	DATA	CLOUD	MOBILE
The **most effective** anti-malware protection from **advanced threats** and **data theft**.	The **most advanced** email defenses against **blended** and **targeted attacks**.	✓ Content Aware DLP ✓ Data Discovery ✓ DLP Gateway ✓ DLP Endpoint ✓ MacOS & Windows ✓ Off-Network Prot. ✓ Portable Decrypt. ✓ 1,700 Policy/Temp. ✓ Drip DLP Detect. ✓ OCR of Image Text ✓ Geo-Location	The **best protection** for web & email for **any location** at the lowest TCO and easiest deployment.	**Uniquely effective protection** for mobile data from **theft, loss, malicious apps** and **web threats**.

websense® THREATSEEKER® NETWORK

websense® ACE

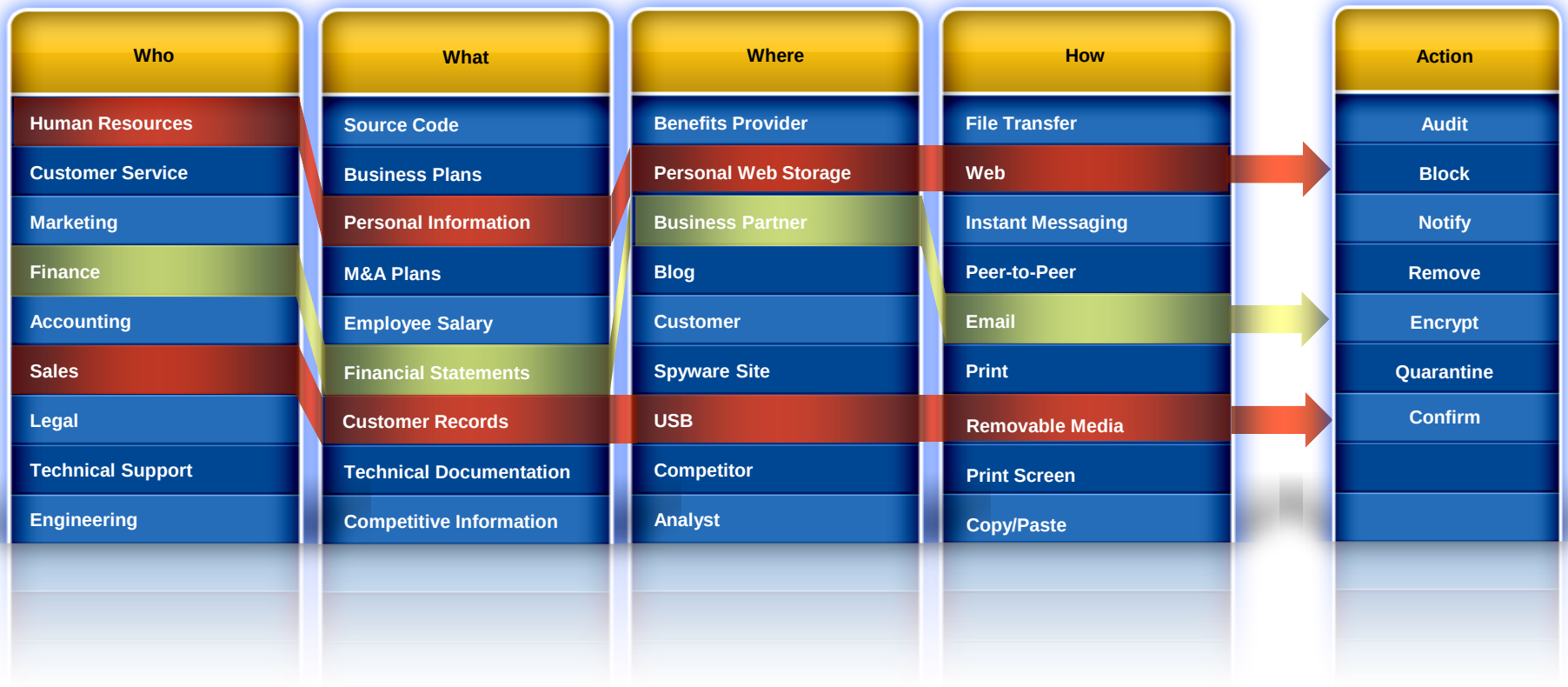
websense® SECURITY LABS™

Data Identification & Classification Engine



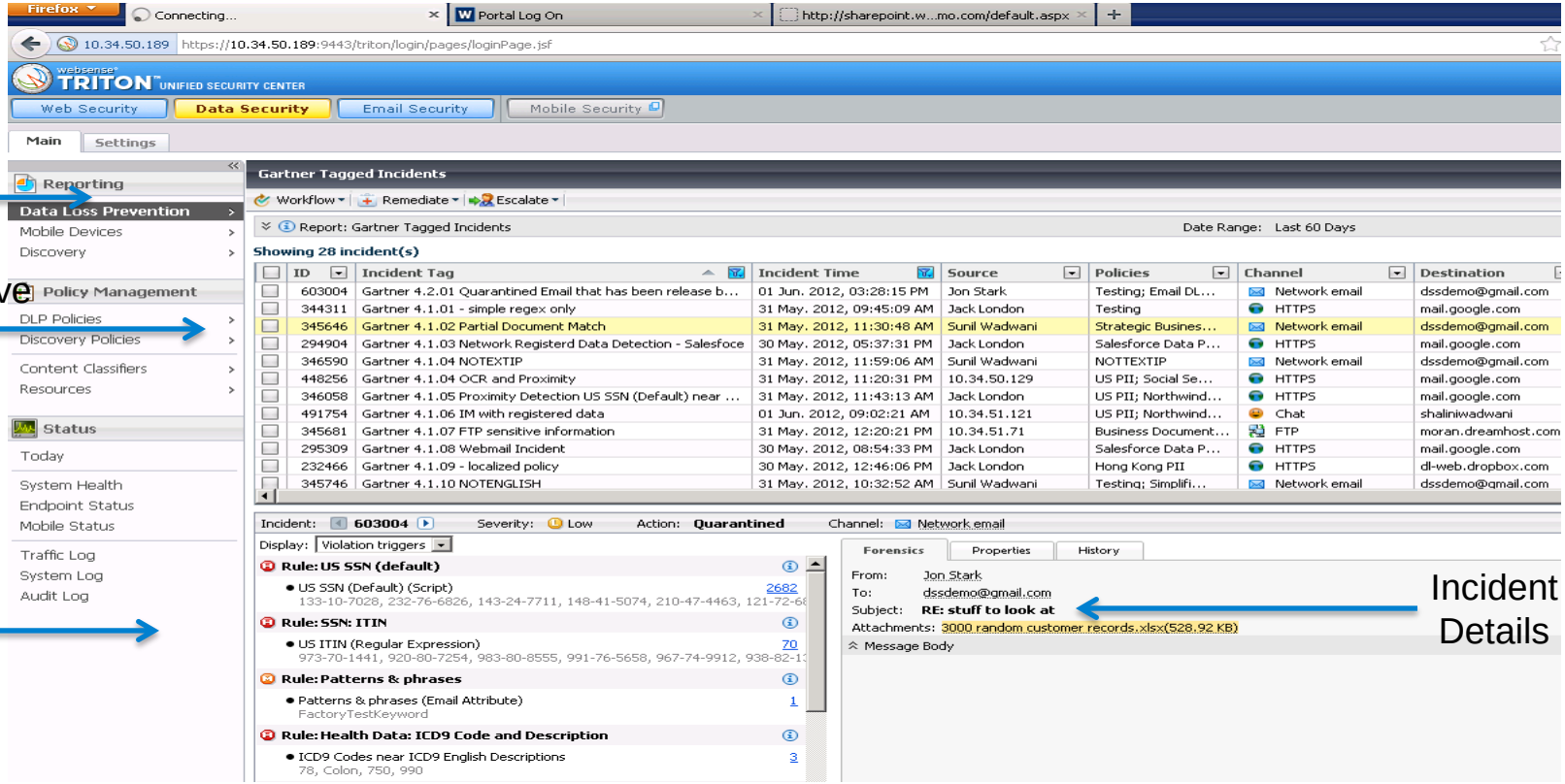
The Websense Data Security Suite uses DICE to classify data in a contextually aware manner.

What to protect



Simple Incident Management

websense



	Web	Email	FTP	IM	Network Printing
	200	150	50	10	45
	100	100	15	5	30
	60	76	5	2	15
DLP ROI 90- Day Risk Reduction	70%	49%	90%	80%	67%

Data security on BYOND

websense

TRITON Mobile Security

- Mobile Malware Prot.
- Malicious App Protect.
- Mobile App Controls
- MDM Controls
- Web Proxy + SSL
- ACE RT Defenses
- Web Security& Filtering
- RT Security Updates
- TRITON Console

Cloud

Benefits

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