

HP Enterprise Security Products – security for the clouds

Jari Salokannel
Security Solutions Architect



cyber crime is increasing...



CRN NEWS, ANALYSIS, AND PERSPECTIVE FOR VARs AND TECHNOLOGY INTEGRATORS

HOME NEWS SLIDE SHOWS VIDEO BLOGS TOOLS REVIEWS HOW-TO RESEARCH LISTS & E...
NETWORKING SECURITY CLOUD STORAGE APPS & OS DATA CENTER CLIENT DEVICES COMPONENTS & PERIF

Washington Post Hack Compromises 1.27 Million Job Seeker Accounts
By **Stefanie Hoffman**, CRN
July 07, 2011 6:05 PM ET

The *Washington Post* on Thursday alerted users that a data breach compromised an estimated 1.27 million accounts on its job seeker site.

Specifically, the *Washington Post* said its "Jobs" site experienced a cyber attack by an "unauthorized" hacker who described as "two brief episodes" June 27 and 28. Hackers made off with user IDs and e-mail addresses that could be used to obtain passwords or other personally identifying information.

The *Post* warned that the stolen e-mail addresses could be used by hackers to launch spam attacks or wage targeted attacks against users.

"We are taking this incident very seriously," the *Post* said. "We quickly identified the vulnerability and shut down the site, pursuing the matter with law enforcement. We apologize for this inconvenience."

The *Post* added that users' Jobs accounts remain unaffected.

Security experts said that the stolen e-mail addresses could be used to execute spearphishing campaigns to

RECENT ARTICLES
10 Biggest Data Breaches Of 2011 [So Far]



The New York Times Business Day Technology

WORLD U.S. N.Y. / REGION BUSINESS TECHNOLOGY SCIENCE HEALTH

Spain Detains 3 in PlayStation Cyberattacks

By **DAVID JOLLY** and **RAPHAEL MINDER**
Published: June 10, 2011

The Spanish police said on Friday that they had apprehended three men suspected of computer hacking in connection with recent attacks on **Sony's** PlayStation Network as well as corporate and government Web sites around the world.



InfoWorld INFOWORLD CHANNELS

SECURITY CENTRAL

Sign in

InfoWorld Home / Security / News / EMC: RSA SecurID info swiped via sophisticated...

MARCH 17, 2011

EMC: RSA SecurID info swiped via sophisticated hack attack

...y exec warns customers that stolen information could be used to more easily penetrate customers' systems

son | InfoWorld Follow @InfoWorld

Add a comment Like 44 people like this. Be the first to like this.



The Cost of a Compromised Web Application/Server

- Sony Play Station Network (PSN) Breach
- LulzSec claimed it only took a single SQL Injection
- What was compromised:
 - Usernames
 - Passwords
 - Credit card details
 - Security answers
 - Purchase history
 - Address information
- Estimated Damages
 - **\$177 Million (USD)**



Hey innocent people whose data we leaked: blame [@Sony](#) | RE: [@joelsack](#)
Fri Jun 03 08:17:51 via web



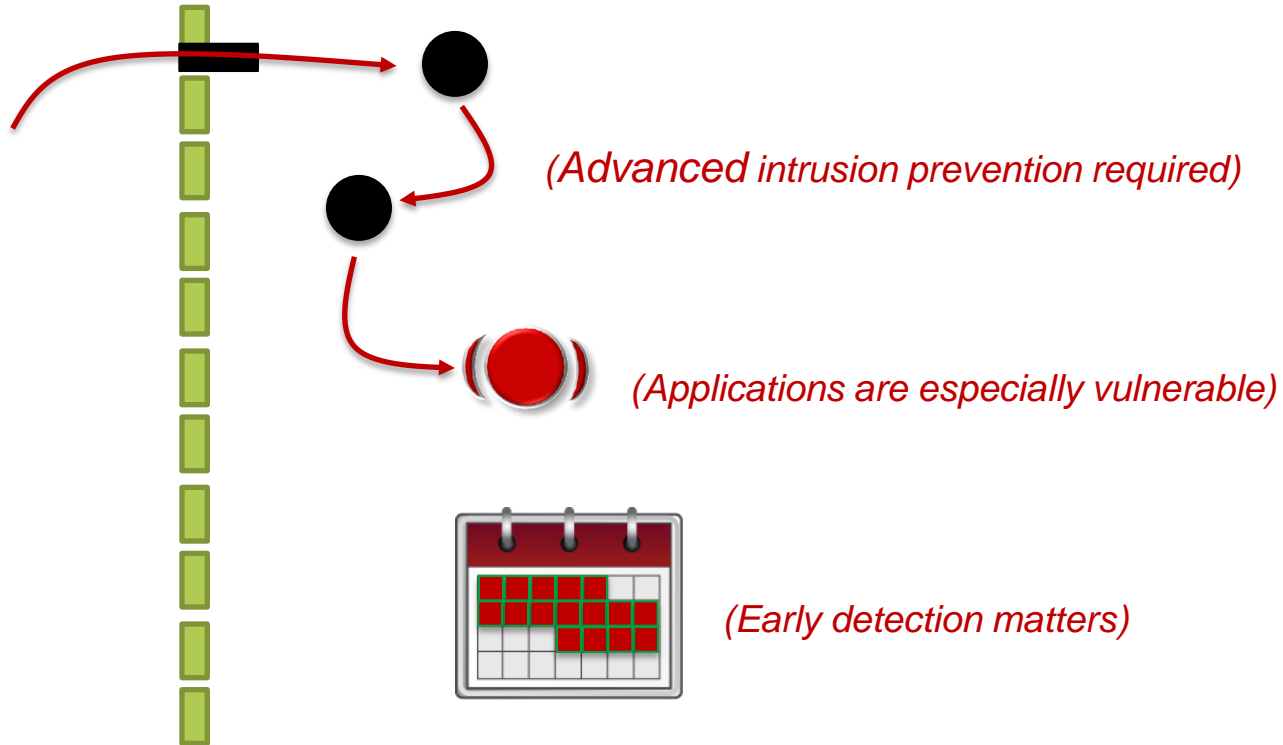
[The Lulz Boat](#)
LulzSec



"Based on information currently available to Sony, our currently known costs associated with the unauthorized network access are estimated to be approximately 14 billion yen in the fiscal year ending March 31, 2012,"



Similar breaches continue...



...While Customers face massive IT shifts

Cloud computing and IT consumerization are remaking IT

Forcing a shift from direct control...



TRANSFORM

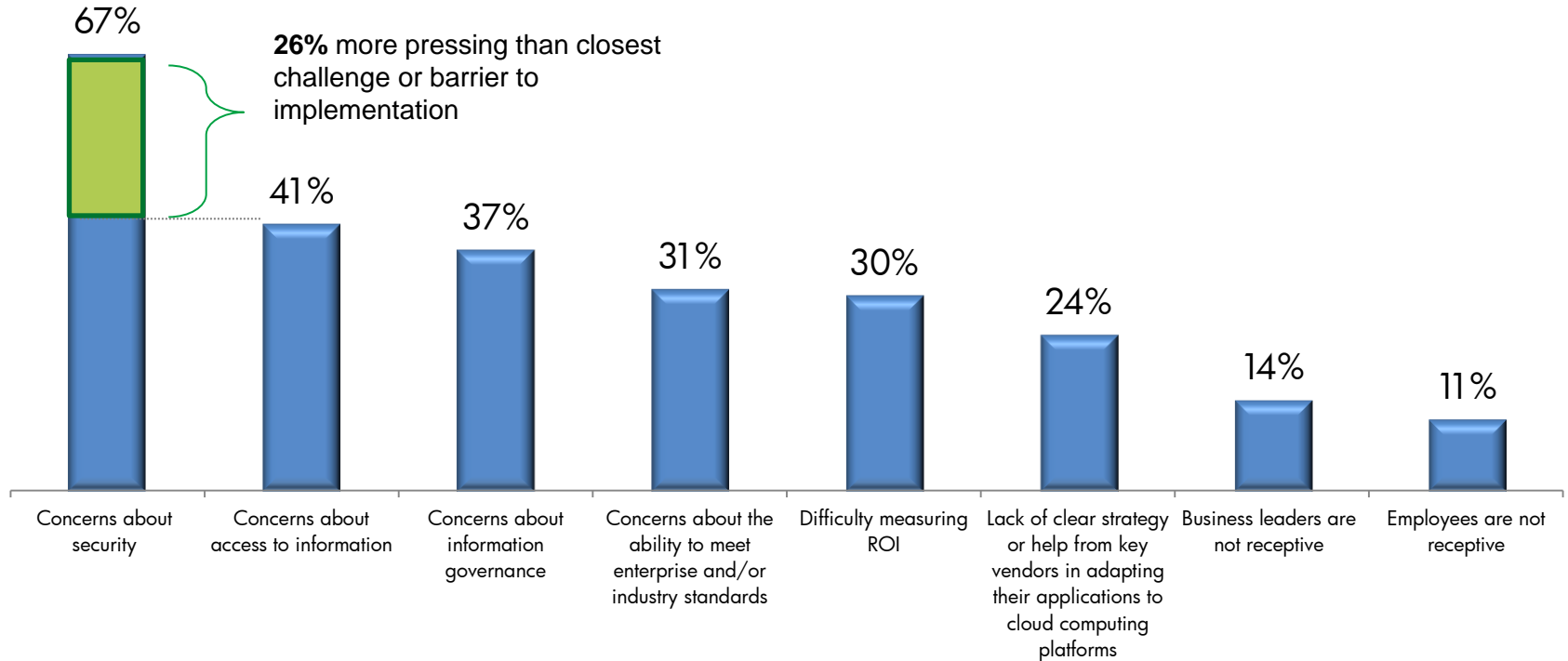
...to a risk/governance model



- Attack surface **grows**
- Visibility/control **falls**

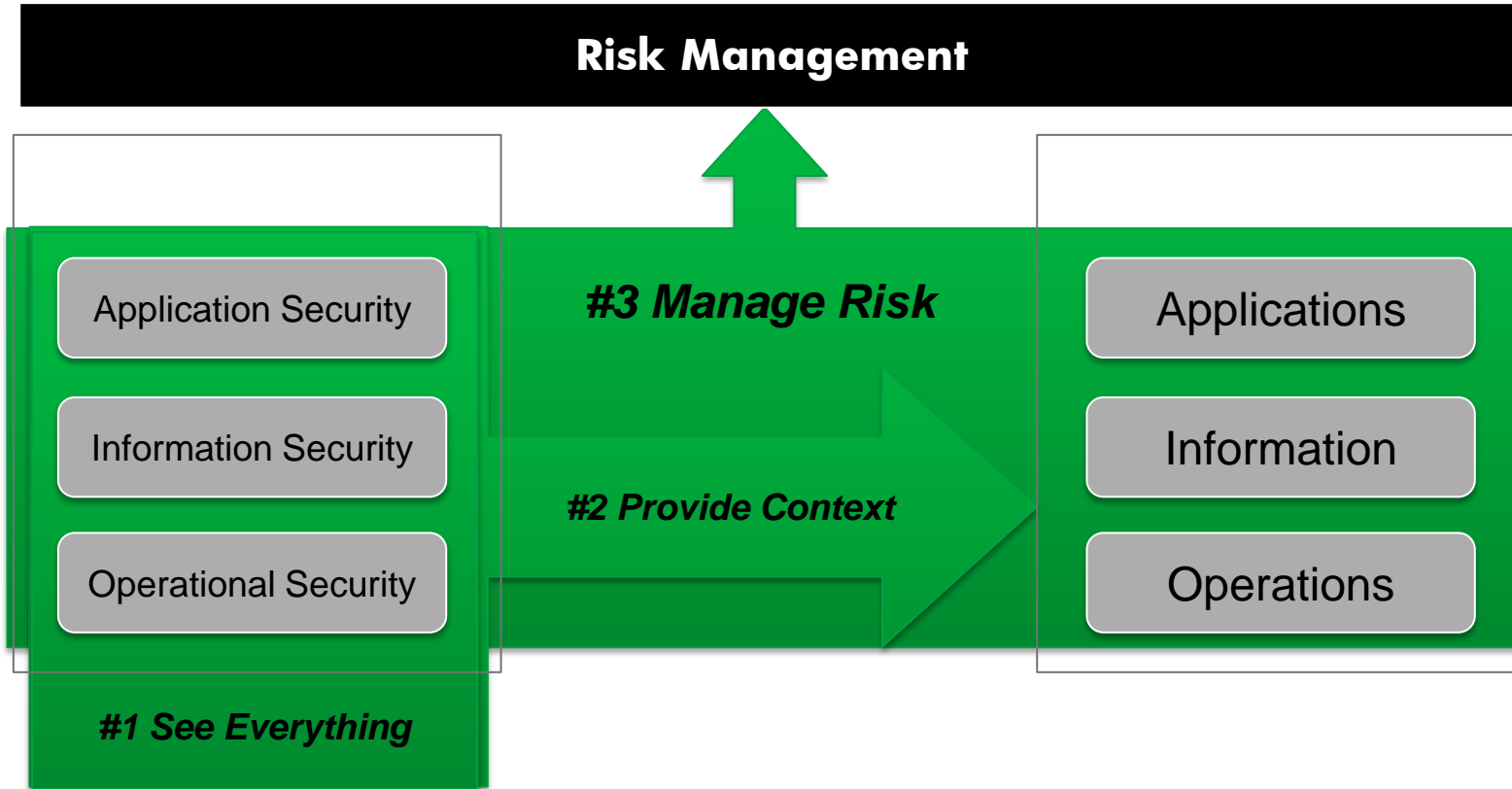


For CIOs, Top Challenge is Security



Q. What are the top three challenges or barriers to implementing a cloud computing strategy at your organization?

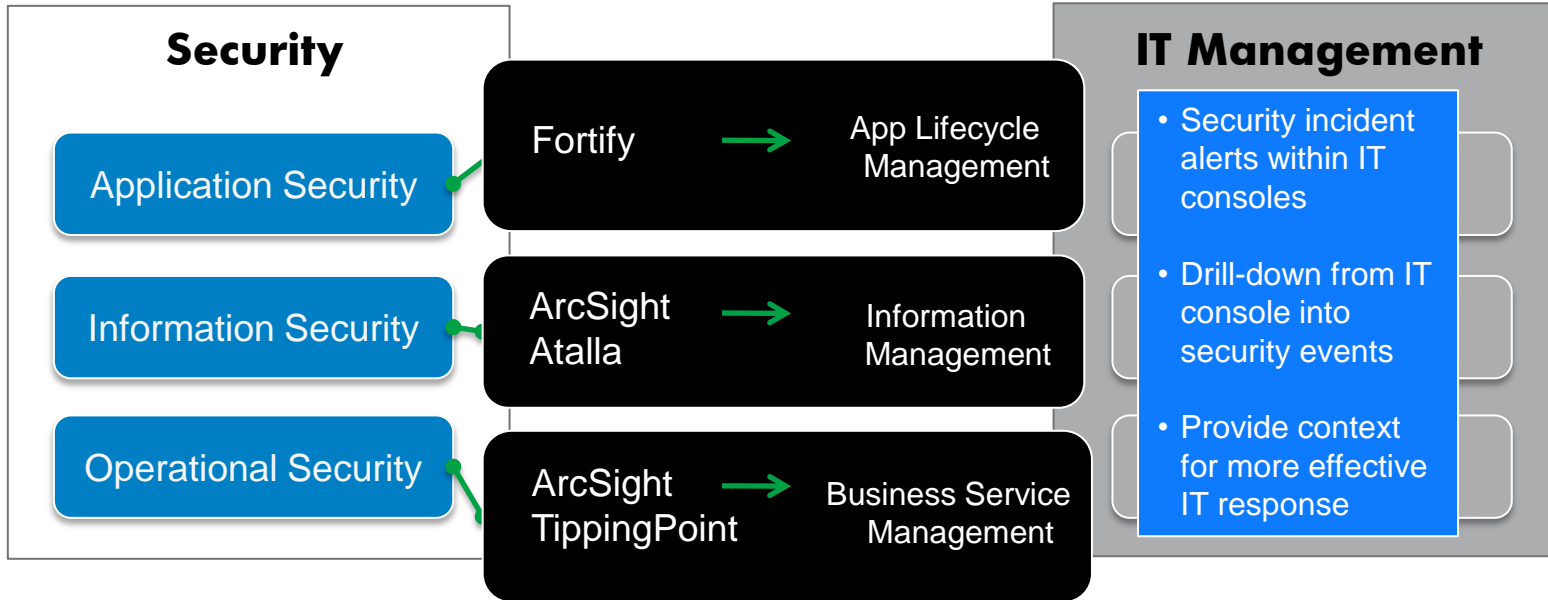
HP ESP: a new security intelligence model



HP ESP: the building blocks

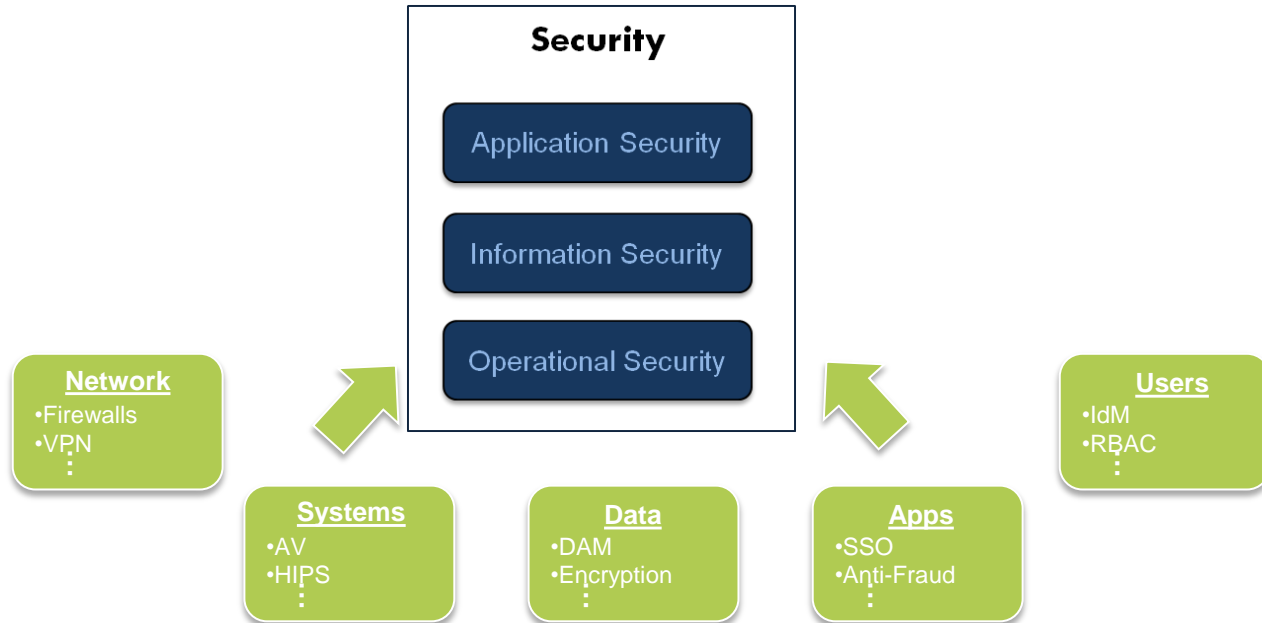
Market-Leading Security Solutions...

...Integrated with Leading IT Management Systems



Enterprise security ecosystem

Integrated with the security landscape for better intelligence and analysis.



Killing the WAF

Web App DV and Scanning

Web App Scan Service

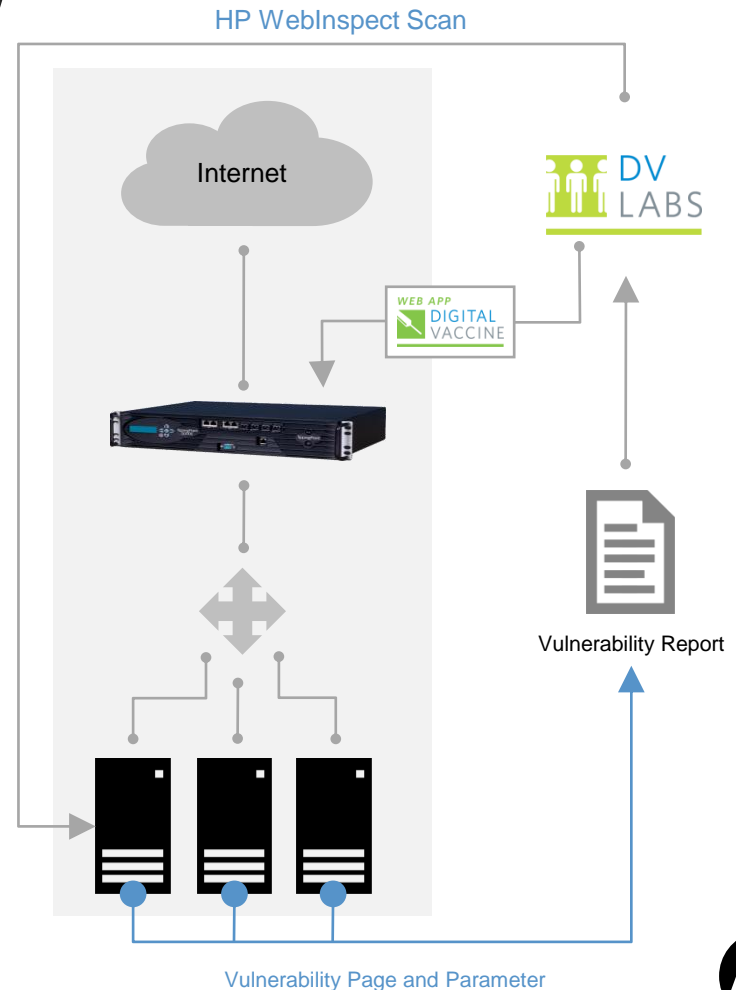
1. Comprehensive Scan
2. Vulnerability report
 - › Input to DV Labs filter creation

Web App DV Filter Service

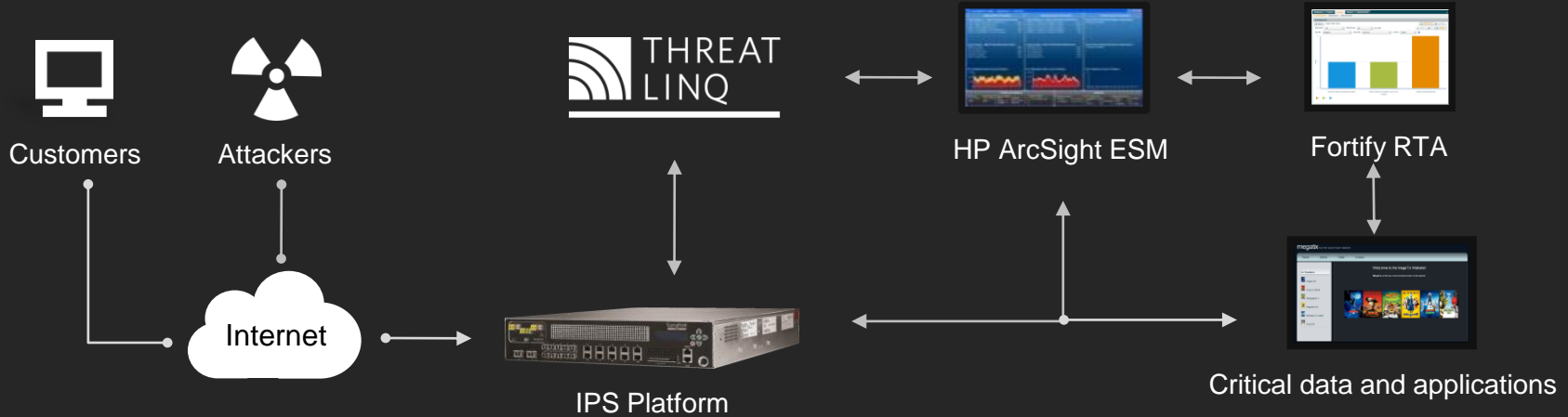
3. DV Labs creates custom Web App filters in 48 hours
4. Web App DV package deployed to IPS – “Virtual Patch”
5. Rescan through IPS to confirm no vulnerabilities

Compliance Reporting

- › PCI-DSS, Internal mandates...



Securing Applications



Bot and Fraud Detection: Cyber Reputation

DVLabs Reputation Database

- › Millions of entries
- › Reputation Score 0-100
- › IPv4 & IPv6 Address
- › DNS Name
- › Meta data



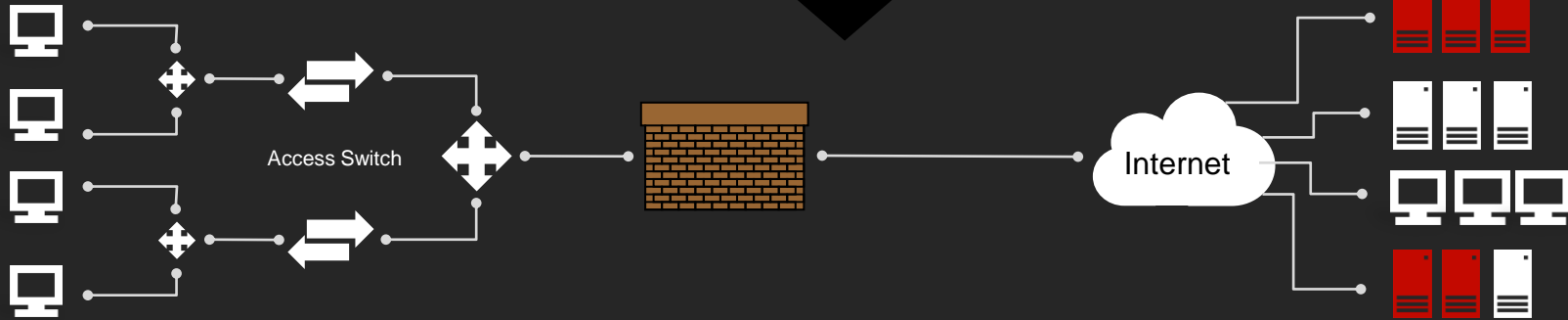
ArcSight ESM



2hr updates

Set Policy Based Upon

- › Reputation Score
- › Country/Geography
- › Device Type - exploit source, malware host, Botnet CnC, spam source



Block Outbound Traffic to Prevent

- Botnet Trojan downloads
- Malware, spyware & worm downloads
- Access to botnet CnC sites
- Access to phishing sites

Block Inbound Traffic to Prevent

- Spam and phishing emails
- DDoS attacks from botnet hosts
- Web App attacks from botnet hosts



HP Enterprise Security <http://www.hpenterprisesecurity.com/>

TippingPoint

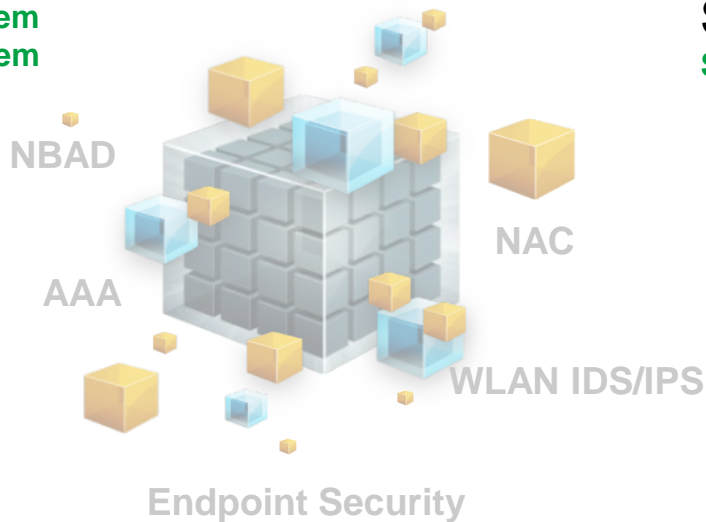
NIPS / NDS

Network based Intrusion Prevention System
Network Defense System



SSA

Software Security Assurance



SIEM

Security, Information and
Event Management



Thank you

