HHS Enterprise Tools

Jack C. Gomes

HHS Security Specialist

December 17, 2008

Table of Contents

- **Introduction & Overview**
- Attack Evolution/Current & Emerging Threats
- Department Drivers & Considerations
- HHS Available Tools Overview

The Department of Health and Human Services (HHS) is faced with increasingly sophisticated threats

"Cyber threats are on the rise"

- *Government Computer News, October 28, 2008*

"Attacks on websites growing in severity"

- *The Boston Globe, November 10, 2008*

Photo Source: King County Department of Transportation

"Chinese hackers pose serious danger to U.S. computer networks"

- *Government Executive, May 29, 2008*

"Latest Browser Threat: Clickjacking"

- *Government Computer News, September 30, 2008*

"Financial crisis leaves bank branches open to social engineering, targeted attacks "

- *Dark Reading, October 8, 2008*

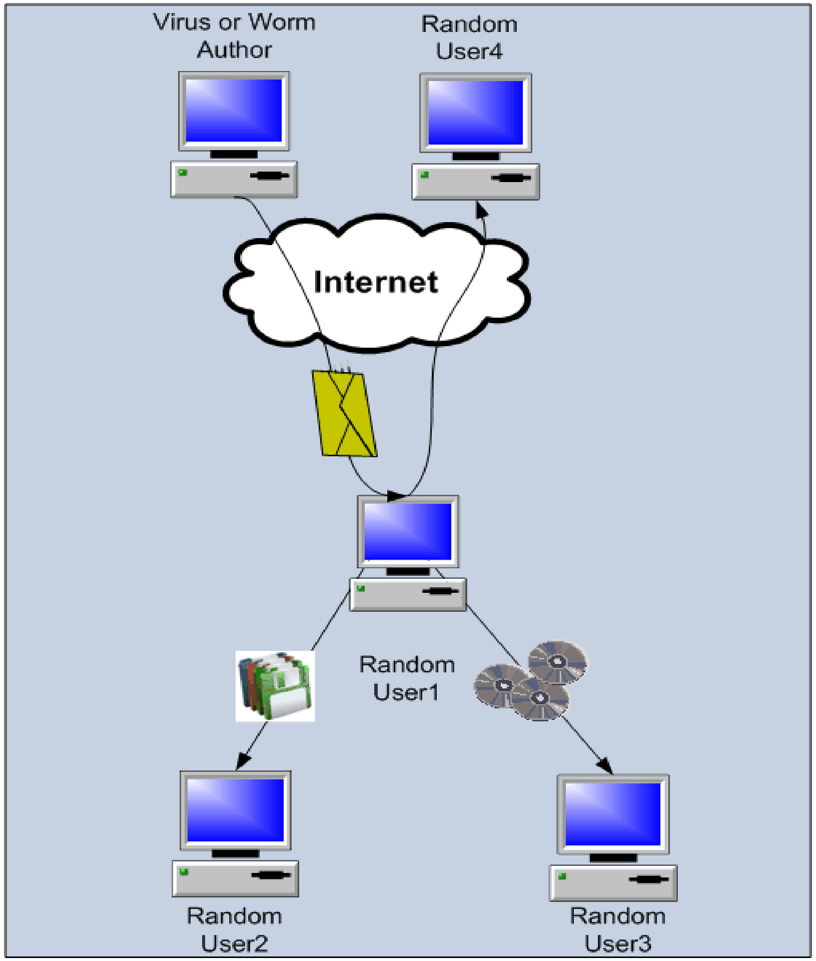
"Targeted Email Attacks: The bulls-eye is on you"

- *The Washington Post, November 14, 2008*

Table of Contents

- Introduction & Overview
- **Attack Evolution/Current & Emerging Threats**
- Department Drivers & Considerations
- HHS Available Tools Overview

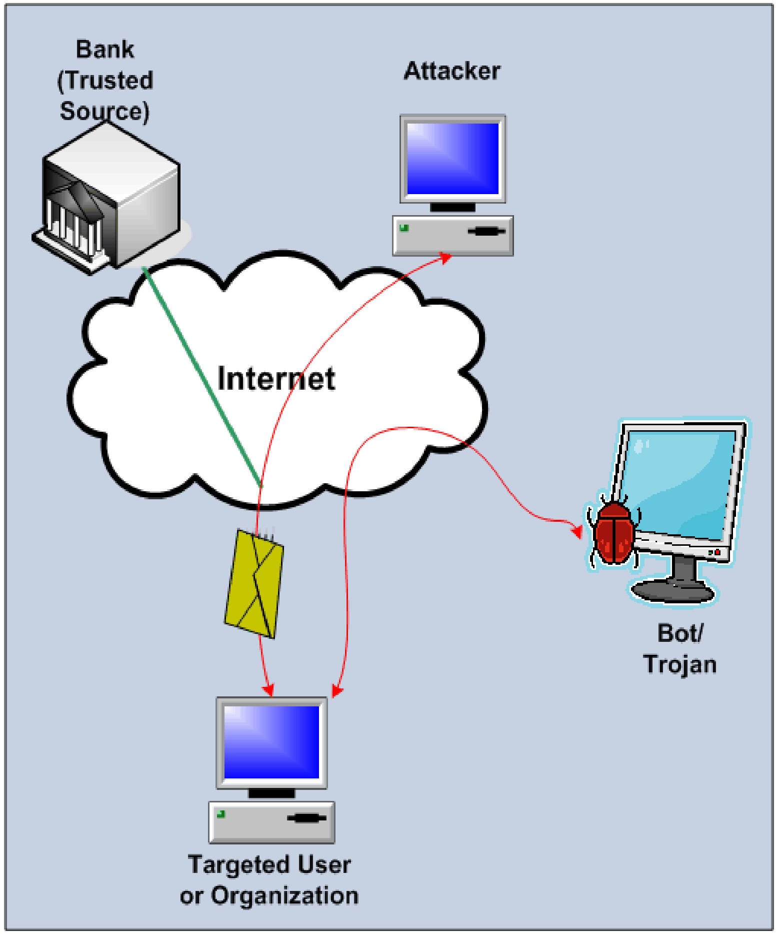
Traditional attacks were identified and mitigated using basic Detect & Disinfect via traditional signature based detection and virus scanning



Traditional attacks were

- Random and wide spread
- Highly visible with fast and effective means of propagation
- Single entities acting independently
- Viruses and worms arriving via disk or email
- Motivated towards obtaining notoriety
- Not primarily aimed toward financial gain
- Simple but effective design tools and exploits to carry out attack

Modern attacks are forcing us to abandon previous methods for mitigation and defense against exploits and adopt more comprehensive and sophisticated detection and remediation techniques



Modern attacks are

- Targeted towards a particular goal and focused on a precise exploitation
- Virtually invisible with extreme sophistication
- Operated in an organized fashion by well funded and coordinated groups of trained individuals
- Delivered via typically trusted sources such as email or compromised websites
- Usually malicious software (malware) such as back door Trojans or Bots
- Primarily motivated toward financial gain
- Launched through sophisticated software demonstrating advanced programming and development lifecycles

Table of Contents

- Introduction & Overview
- Attack Evolution/Current & Emerging Threats
- **Department Drivers & Considerations**
- HHS Available Tools Overview

In 2006, HHS started evaluating the goals, benefits, and challenges that could result from Enterprise oriented tool deployments

Goals

- Cost effective technological solutions
- Uniform tool solutions across HHS
- Holistic, multi-tiered approach to implementing security
- Inter-agency collaboration for implementation and troubleshooting

Challenges

- Restrictive product offerings and limited software diversity choices
- Varying needs of different operating environments
- Central management and reporting
- Difficult and time consuming to replace product solutions

Federal and Departmental requirements as well as economies of scale drove the adoption of the HHS Tools Suite

Tool	Drivers
Gideon Secure Fusion	• Federal Information Security Management Act (FISMA): Required information technology (IT) systems to be maintained in accordance with security configurations • Office of Management and Budget (OMB) Memorandum (M)-07-11, *Implementation of Commonly Accepted Security Configurations for Windows Operating Systems*: Required agencies to adopt configurations for Windows XP and Vista Operating Systems • OMB Memorandum dated July 31, 2007 – *Establishment of Windows XP and Vista Virtual Machine and Procedures for Adopting the Federal Desktop Core Configurations*: Required agencies to use Security Content Automation Protocol (SCAP) compliant tools when monitoring Windows XP and Vista Operating Systems configurations

HHS Tools Suite, cont'd

Tool	Drivers
Check Point (Pointsec)	• OMB M-06-16, *Protection of Sensitive Agency Information*: Required agencies to encrypt all data on mobile computers/devices that carry agency data, unless the data is determined to be non-sensitive
Websense	• Uniform HHS-wide implementation • Significant cost savings per license
Watchfire AppScan	• Recognized need to improve security for millions of web pages employed throughout HHS • HHS procured AppScan for Department-wide use, resulting in decreased cost per license • AppScan is now available for scanning both production websites as well as development

Additionally, HHS wanted to leverage the Department's size to yield economic advantage

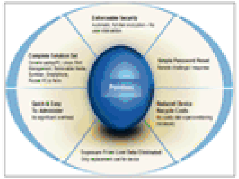
- The HHS-wide procurement of Enterprise software averagely results in a 67% savings per license
- For example, if Operating Divisions (OPDIVs) were to individually purchase Check Point Full Disk and Media Encryption licenses in 10,000 license increments, the cost per license would be approximately $55.00
- The HHS wide procurement of close to 100,000 Check Point licenses resulted in a price decrease to $25.00 per license - Overall, a savings of approximately $3 Million dollars
- Subsequently, HHS began considering other software licenses for HHS-wide procurement

Table of Contents

- Introduction & Overview
- Attack Evolution/Current & Emerging Threats
- Department Drivers & Considerations
- **HHS Available Tools Overview**

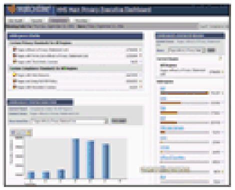
Tools Summary

Check Point (Pointsec)



→ Data Security

Watchfire AppScan



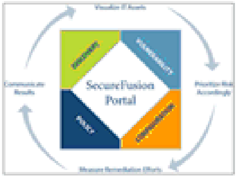
→ Web Application Security

Websense

Websense
Enterprise
Uncategorized URLs
Your company's surfing patterns
Websense database team
Database updated to match your company's surfing patterns
Sites are categorized

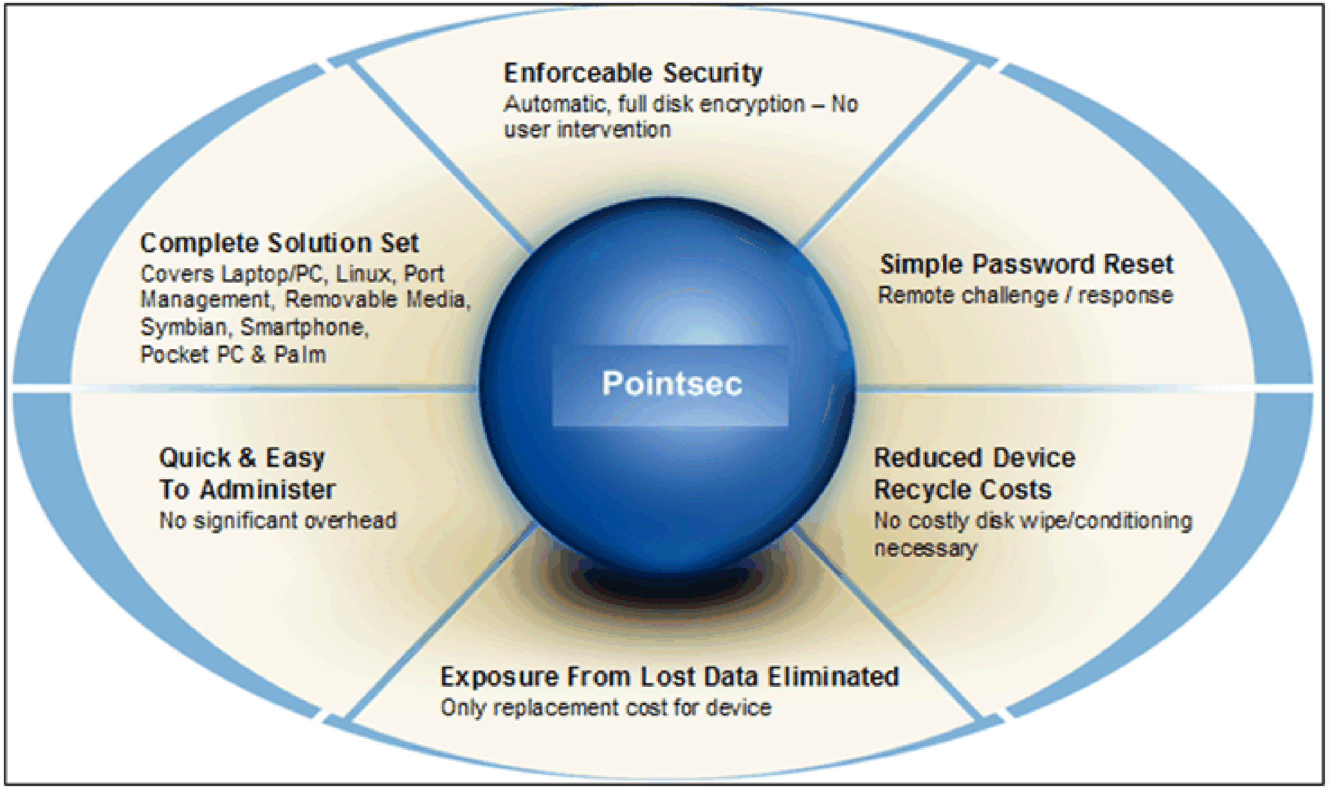
→ Endpoint Security

Gideon SecureFusion



→ Vulnerability & Compliance Scanning

Check Point (formerly Pointsec) Provides data protection



Enforceable Security
Automatic, full disk encryption – No user intervention

Simple Password Reset
Remote challenge / response

Reduced Device Recycle Costs
No costly disk wipe/conditioning necessary

Exposure From Lost Data Eliminated
Only replacement cost for device

Quick & Easy To Administer
No significant overhead

Complete Solution Set
Covers Laptop/PC, Linux, Port Management, Removable Media, Symbian, Smartphone, Pocket PC & Palm

Check Point provides protection for data stored on laptops and removable media

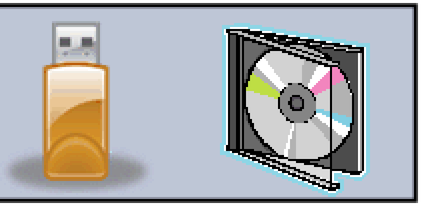
Check Point (formerly Pointsec) Provides data protection, cont'd

- **Challenge**
  - There is a need to safeguard personally identifiable information (PII) contained and used by the Department by protecting information on laptops and portable devices
- **Impact / Requirements**
  - Provide ongoing support and maintenance to OPDIVs for current licenses
  - Enhance encryption and data protection software capabilities to provide extra mobile media and hard disk security for HHS
  - Increase confidentiality of Privacy Information Act

Check Point (Pointsec) Encryption Software provides a variety of encryption products to secure laptops, desktops, portable media, and mobile devices

- **Check Point Full Disk Encryption (FDE)**
  - Provides FIPS 140-2 compliant full disk encryption for Windows and Macintosh platforms

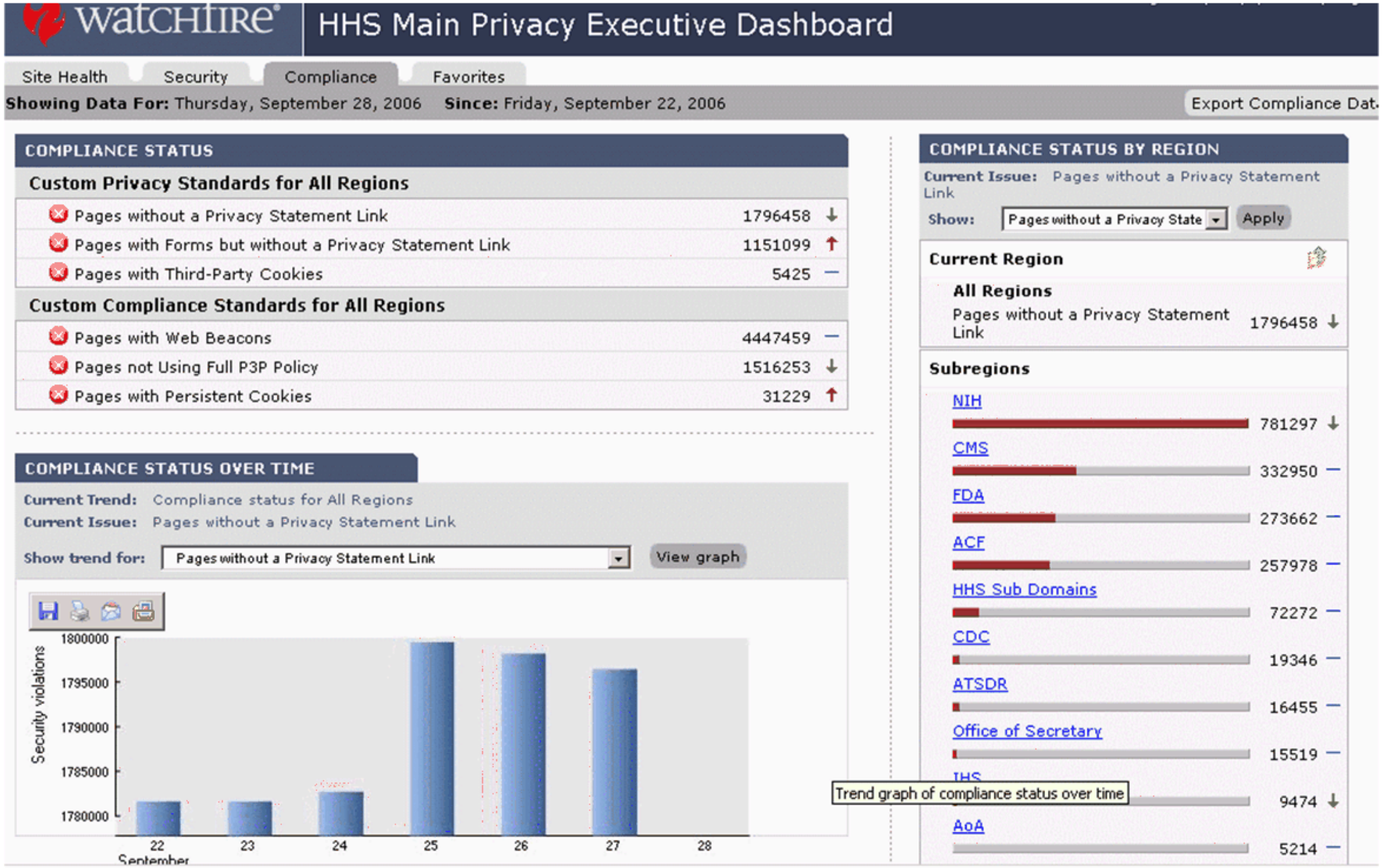
- **Check Point Media Encryption**
  - Check Point's Pointsec Media Encryption (PME)
  - Check Point Protector



- **Check Point Mobile**
  - Encryption for Symbian, PocketPC, Smartphone, and PDA devices

- **Check Point R70 Unified Platform**
  - By the end of calendar year 2009, Check Point will merge each of these individual products into a single unified platform

Watchfire (AppScan): Detects HHS website vulnerabilities



HHS Main Privacy Executive Dashboard

Showing Data For: Thursday, September 28, 2006 **Since:** Friday, September 22, 2006

COMPLIANCE STATUS

Custom Privacy Standards for All Regions		
Pages without a Privacy Statement Link	1796458	↓
Pages with Forms but without a Privacy Statement Link	1151099	↑
Pages with Third-Party Cookies	5425	—
Custom Compliance Standards for All Regions		
Pages with Web Beacons	4447459	—
Pages not Using Full P3P Policy	1516253	↓
Pages with Persistent Cookies	31229	↑

COMPLIANCE STATUS OVER TIME

Current Trend: Compliance status for All Regions

Current Issue: Pages without a Privacy Statement Link

Show trend for: Pages without a Privacy Statement Link

Trend graph of compliance status over time

COMPLIANCE STATUS BY REGION

Current Issue: Pages without a Privacy Statement Link

Show: Pages without a Privacy State

Current Region

All Regions		
Pages without a Privacy Statement Link	1796458	↓

Subregions

NIH	781297	↓
CMS	332950	—
FDA	273662	—
ACF	257978	—
HHS Sub Domains	72272	—
CDC	19346	—
ATSDR	16455	—
Office of Secretary	15519	—
IHS	9474	↓
AoA	5214	—

Watchfire AppScan software identifies vulnerabilities that allow for unauthorized access to web applications

Watchfire (AppScan): Detects HHS website vulnerabilities, cont’d

- **Challenge**
  - Recent incidents within the Department have increased the need to better strengthen vulnerability detection capabilities, which is a means of protecting information contained within HHS systems
- **Impact / Requirements**
  - Increase the baseline IT security posture across the six OPDIVs by enhancing the Department’s AppScan vulnerability detection software
  - Enhance reporting that will enable management staff to tackle incidents and prioritize accordingly
  - Enable a proactive approach to online risk management

Watchfire’s AppScan tool provides scanning and remediation for production and development websites throughout HHS

- There is a significant threat to an agency’s PII if systems are not properly protected and application vulnerabilities are another avenue for gaining access to internal resources
- Several ramifications can come about for an agency that is not properly protecting PII
  - Embarrassment
  - Loss of confidence
  - Legal repercussions
  - Embarrassment for those who have had their information exposed
  - Financial complications

Watchfire’s AppScan tool provides scanning and remediation for production and development websites throughout HHS, cont’d

- Recent incidents across the Federal Government involving the exposure of PII have shown that vulnerabilities on outward facing applications are one area for concern
- It has been determined that there is a need for software that tests for these types of vulnerabilities to prevent future incidents

IBM’s Watchfire AppScan tool was chosen to assist in the scanning, analysis, and reporting of vulnerabilities in web applications to prevent PII incidents

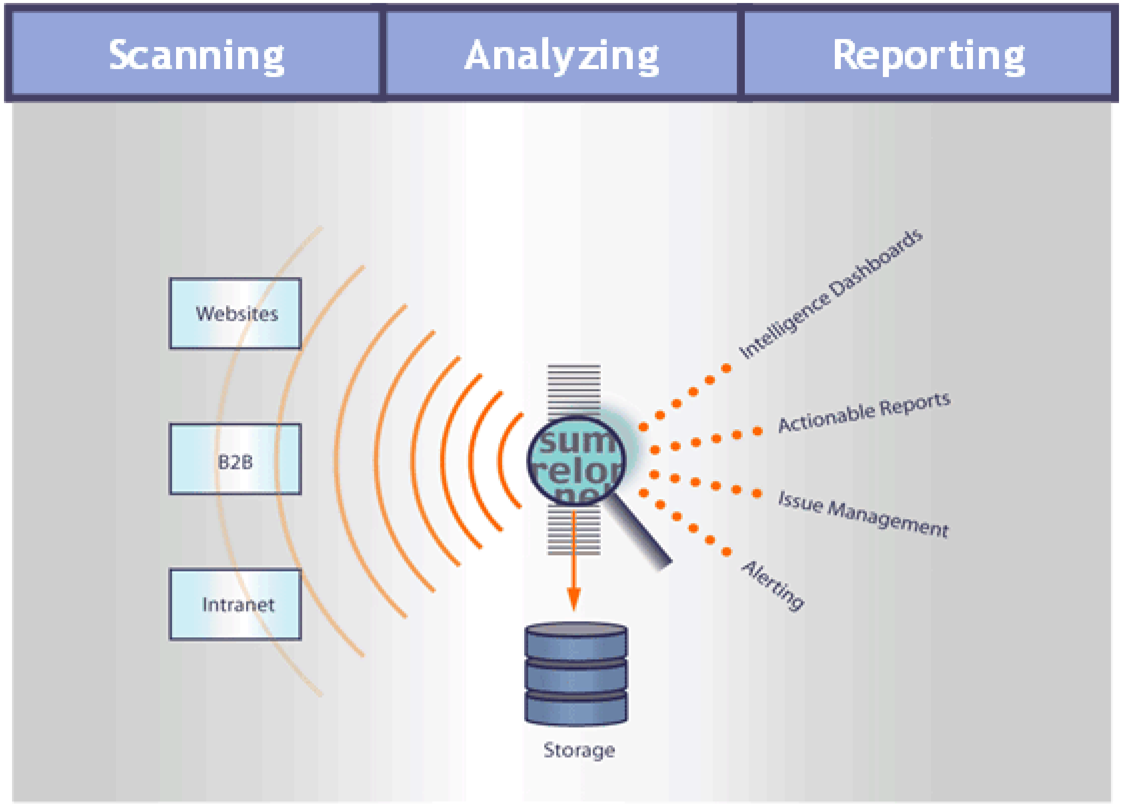


Photo Source: IBM

The tool provides the ability to compile data regarding each scan and to measure an agency's progress in fixing vulnerabilities

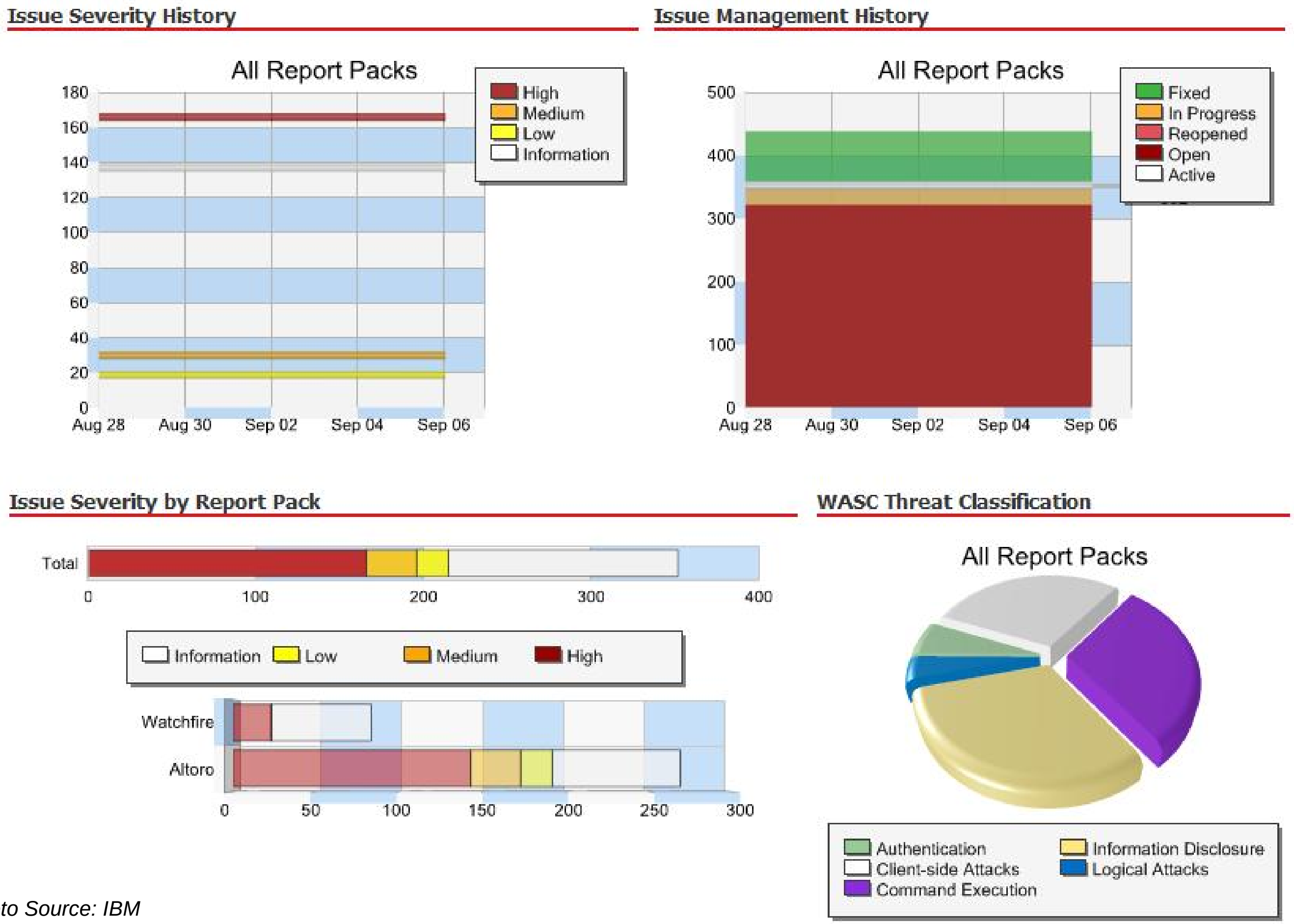
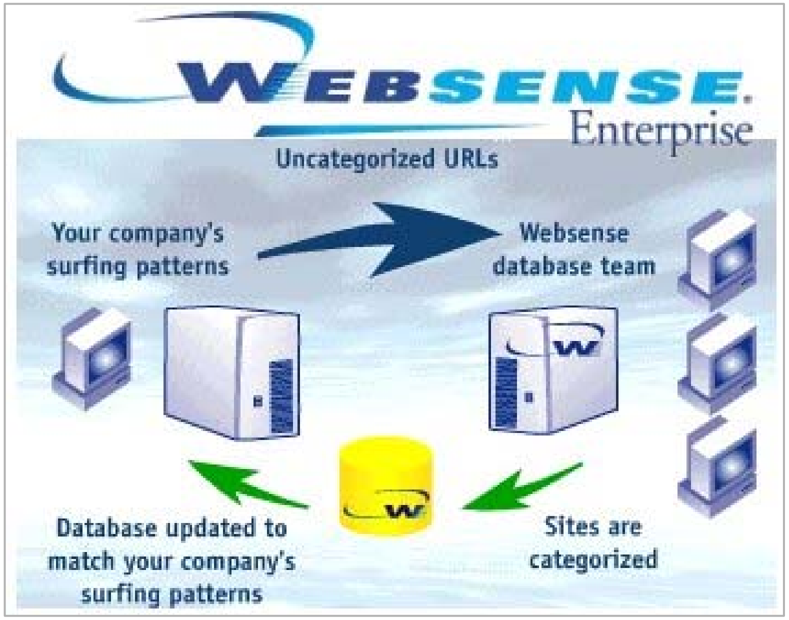


Photo Source: IBM

Indian Health Service (IHS) has used the results from the tool to help improve its security posture

- Implementation at IHS was completed in April 2008
- Training was then conducted for IHS team members in May 2008
- Scans have been run periodically since the deployment was completed
- IHS has shown significant improvement, reducing vulnerabilities by 77% in external facing applications from April 2008 to October 2008
- IHS will continue to work with the IBM team to remediate more issues and to continue to improve security of it applications

Websense: Prevents/detects website security threats in support of endpoint protection

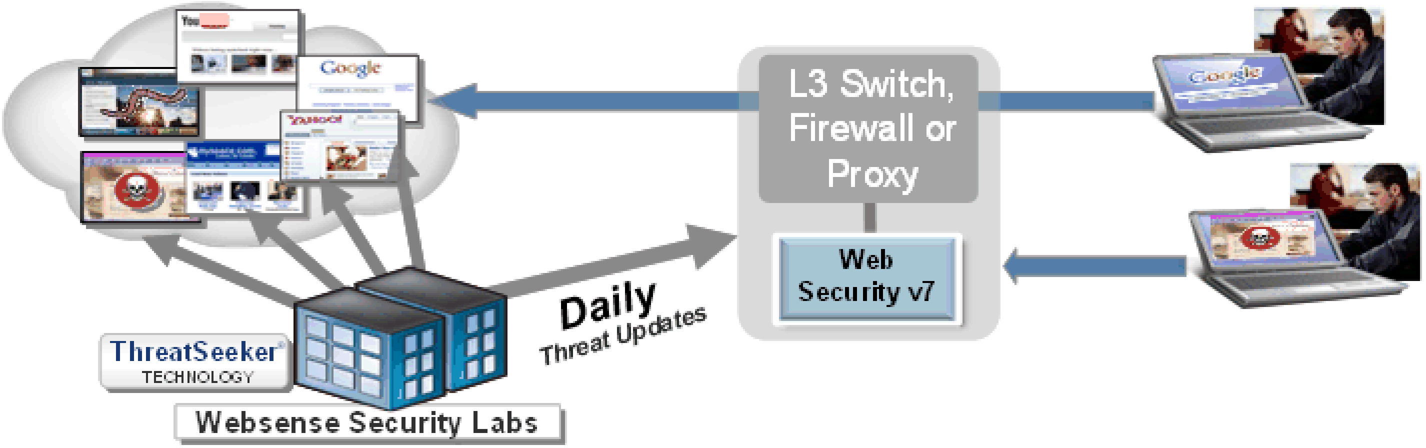

WEBSENSE.
Enterprise
Uncategorized URLs
Your company's surfing patterns
Websense database team
Database updated to match your company's surfing patterns
Sites are categorized

Websense filters inappropriate web traffic in the interest of blocking content that reduces productivity or violates legal regulations

Websense: Prevents/detects website security threats in support of endpoint protection, cont'd

- **Challenge**
  - There is a need for the Department to uncover illegal network activity and monitor all outbound web traffic while protecting HHS users from malicious content
- **Impact/Requirements**
  - Enable an enterprise-wide software license upgrade in order to continue monitoring capabilities of all outbound web traffic
  - Integrate the Department's ability to monitor all outbound web traffic and protect users from malicious content

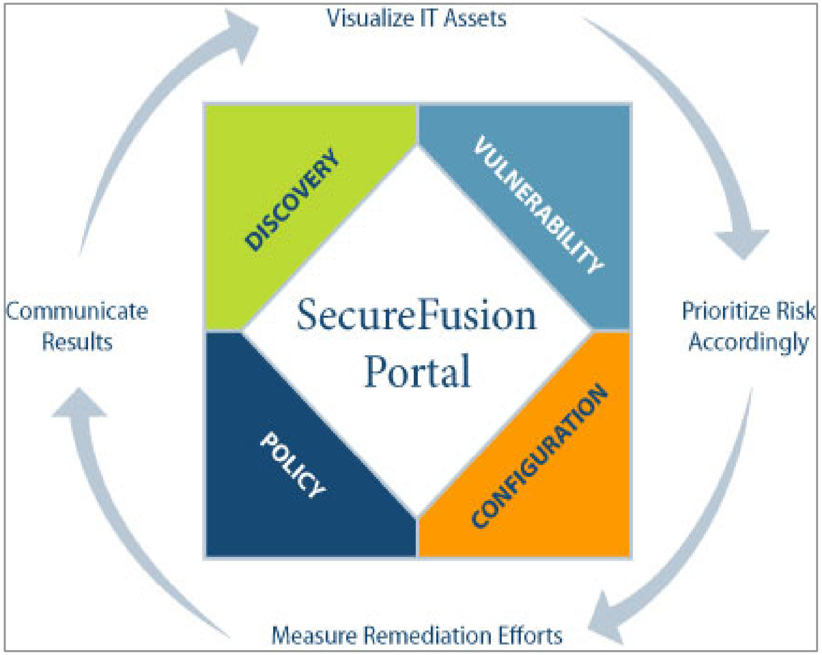
The Websense Enterprise Filtering plus Security Filtering option is currently deployed, which provides a variety of protection for HHS endpoints



The Websense Enterprise Filtering plus Security Filtering option is currently deployed, which provides a variety of protection for HHS endpoints, cont’d

- Functionality
  - Provides URL-Filtering and outbound control over web traffic
  - Enforces web usage policy; blocks malicious and compromised websites utilizing ThreatSeeker intelligence and provides once a day security updates
  - Provides current functionality plus real time security threat updates
  - Trade/service mark scanning and external HHS website scanning are also available
- ***Benefit***: Reduces window of threat exposure, especially on zero-day and rapidly spreading threats

Gideon SecureFusion: Supports endpoint protection, asset management, security vulnerability tracking, and Federal Desktop Core Configuration (FDCC) compliance verification

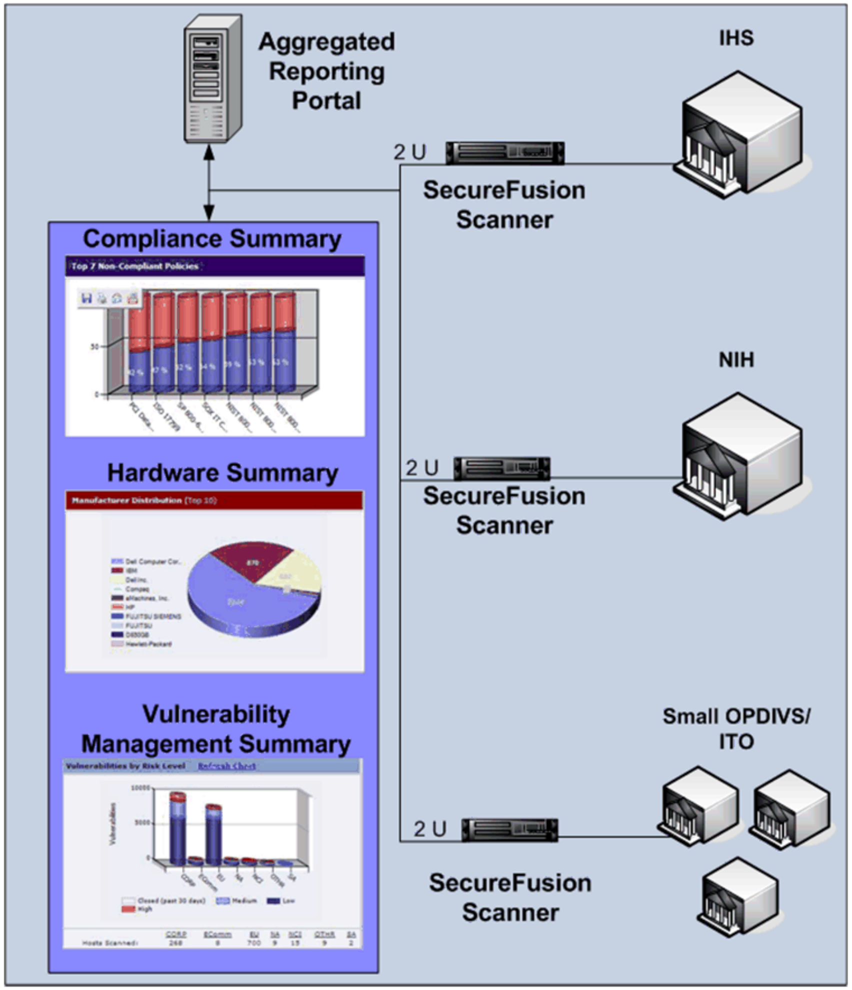


Gideon SecureFusion automates steps of the vulnerability management lifecycle process, while providing enterprise-wide reporting

Gideon SecureFusion: Supports endpoint protection, asset management, security vulnerability tracking, and Federal Desktop Core Configuration (FDCC) compliance verification, cont’d

- **Challenge**
  - There is a need for an automated and integrated tool that identifies and removes vulnerabilities, while fulfilling requirements within FISMA, OMB M-07-11, and FDCC
- **Impact /Requirements**
  - Enable HHS compliance with FISMA, OMB M-07-11, and FDCC
  - Integrate enterprise-wide security configuration reporting capabilities within the Department

Gideon SecureFusion's configuration flexibility coupled with compliant and robust scanning offers a powerful configuration management capability


Aggregated Reporting Portal
IHS
2 U
SecureFusion Scanner
Compliance Summary
Top 7 Non-Compliant Policies
Hardware Summary
Manufacturer Distribution (Top 10)
NIH
2 U
SecureFusion Scanner
Vulnerability Management Summary
Vulnerabilities by Risk Level
Refresh Chart
Small OPDIVS/ ITO
2 U
SecureFusion Scanner

Gideon SecureFusion’s configuration flexibility coupled with compliant and robust scanning offers a powerful configuration management capability, cont’d

- Capabilities
  - Integrated functionality for Vulnerability, Configuration and Policy Management
  - Fast, comprehensive, and continuous asset discovery scanning
  - SCAP Compliant
  - Enterprise scalable and easy to deploy
  - Easily configures scanning templates to accommodate the HHS FDCC Windows XP and Vista Standards

SECURE
ONE HHS

KEEP AMERICA'S
HEALTH AND HUMAN
SERVICES SECURE

Secure One Support
SecureOne.HHS@hhs.gov
(202) 205 - 9581