



## **5<sup>th</sup> Annual IT Security Automation Conference**

BigFix experiences with standards in the Federal government and commercial organizations. How SCAP and other tools can be leveraged to meet regulatory and mandated requirements.

**Jim Hansen, Director, Product Management**  
Security and Compliance

# Session Objectives



- What are the common challenges all organizations face today?
- How can standards such as SCAP be used to reduce the risk?
- How are agencies and organizations using technology and automation to meet their objectives today?
- What other opportunities exist?
- How must the standards and tools evolve to allow them to get there?



# Who is BigFix



BigFix is a leading global provider of **high-performance security and systems management** software for enterprise companies

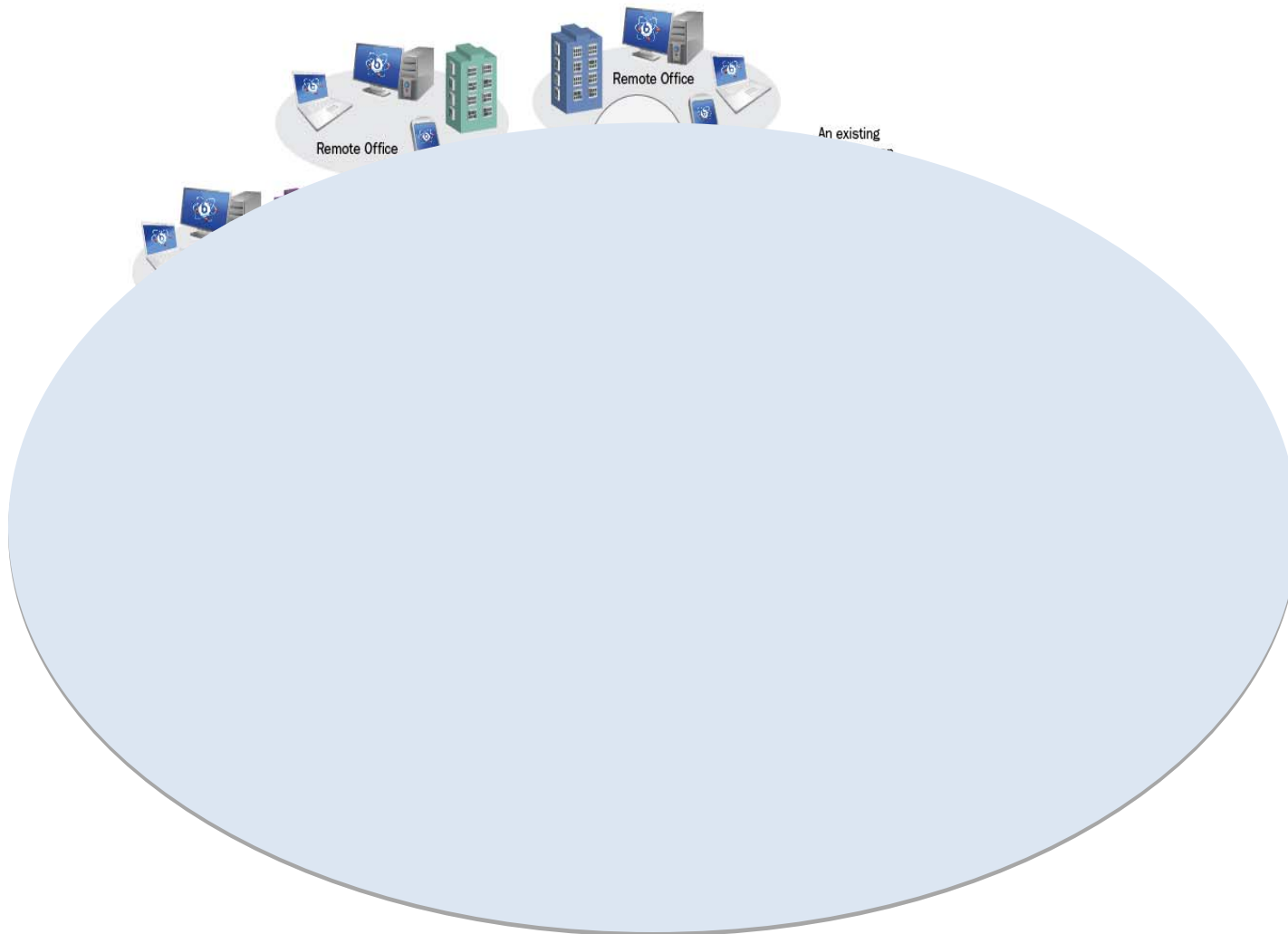
- Global and pervasive deployment across vertical industries
  - Highly complex environments
  - Very large enterprise deployments  
> 100,000 assets
- Innovative BigFix technology platform
  - “Visionary” in EPP and PCLM Gartner Magic Quadrants
  - 19 patents worldwide
  - 32 patents pending worldwide
- Government Certified
  - FIPS 140-2 Level 2
  - Common Criteria EAL3
  - SCAP Certified

## Fast Facts:

- Every day, trillions of \$\$\$ flow through BigFix-managed computers
- Each year, over \$350B in retail transactions is enabled by BigFix technology
- Tens of thousands of hotel reservations are made every day on BigFix-managed computers
- Manage over 5.5M endpoints
- 500, 000 endpoints for FDCC

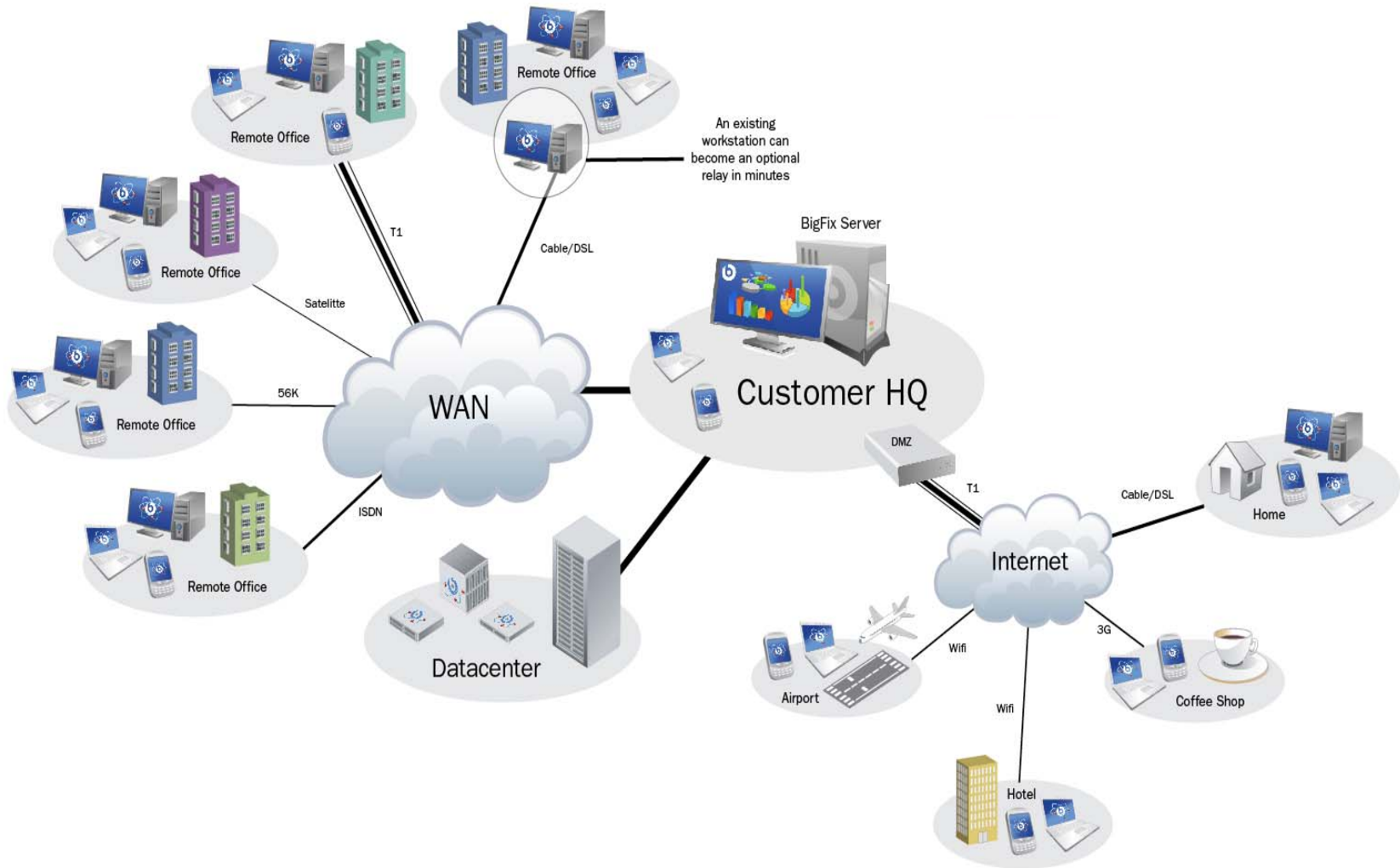


# The World of IT – Circa 2000



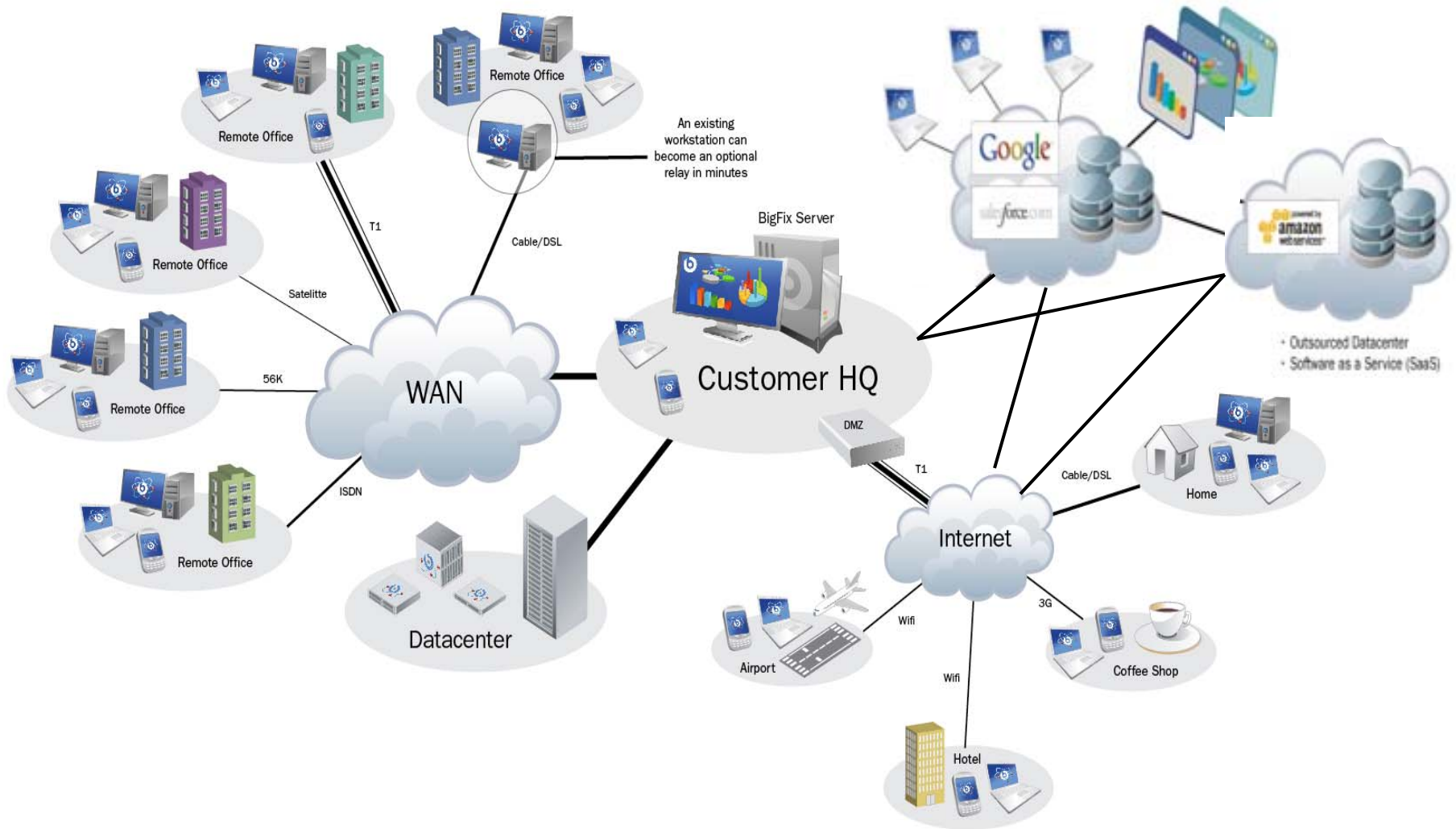


# The World of IT – Circa 2009





# The World of IT – Circa 2012



# The Need for Pervasive, Real-Time Visibility



Where are all my assets and what rogue devices are gaining access to my network?

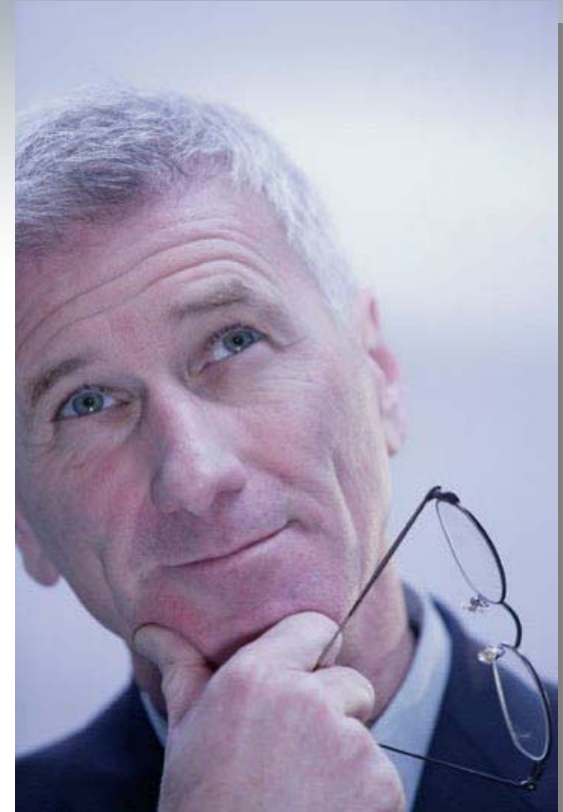
What is the current compliance status for all my desktops and servers?

How can I be sure laptops are in compliance when they are roaming and/or off network?

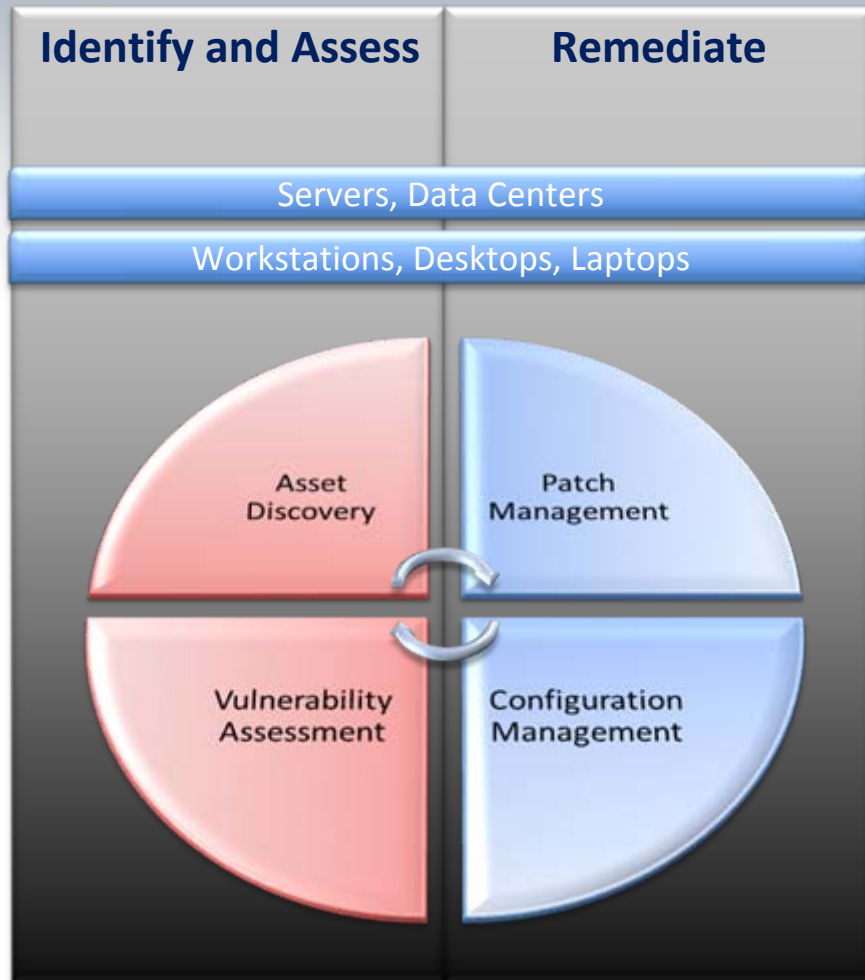
Are they patched, configured properly, vulnerable?

How do I bring laptops, desktops and servers back into compliant status?

How much is this going to cost me and what level of risk can I afford?



# Basic Foundation to Mitigate and Reduce Risk



...no do work at home. (See Remote Workers Still Living Dangerously, Cisco Study Says.)

The new study indicates that users frequently download unauthorized data and applications to their work machines for personal use. About 80 percent of employees use their company-issued PCs for personal email, and about half use their work PCs for personal Web research and online banking.

More than half of end users have changed the security settings on their company-issued laptop to view restricted Websites, even though they knew it was against company policy. About 35 percent say it is "none of the company's business" if they have changed the security settings on their computer, the study says.

insightexpress  
Research for the Right Decision

- Locate and track your assets. You cannot secure what you can't see.
- Identify vulnerabilities and threats and assess for risk
- Patch and Configure systems to mitigate and reduce risk

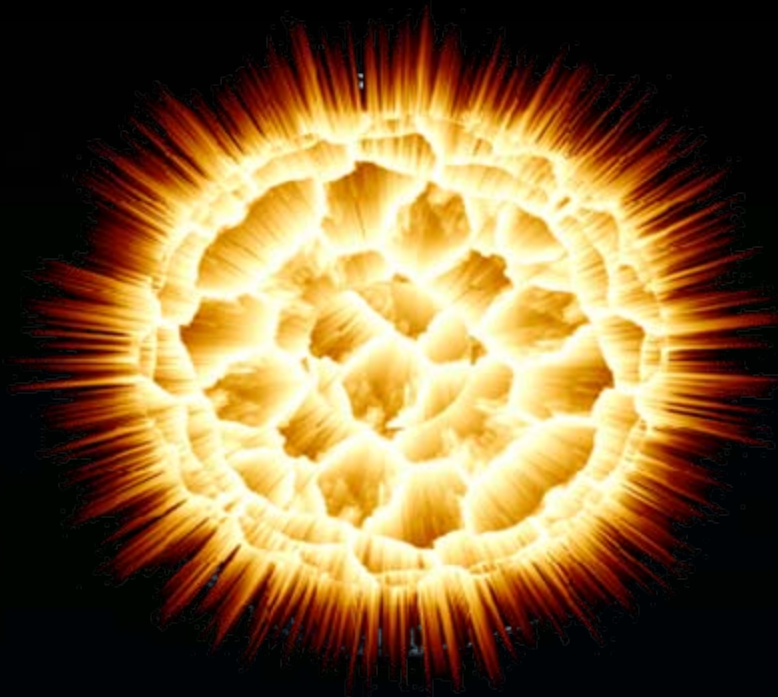
Secunia  
Stay Secure

Fewer than 2 percent of Windows PCs are fully patched with updated and secured software, according to new data gathered by Secunia.

Secunia gathered data during the past week from 20,000 new users (mostly



Ask any organization that has been owned...



*What do you mean we didn't secure the thermal  
exhaust ve...*

# Federal Agency: 65 Hour Countdown



## **Problem:**

- Infrastructure was under attack by a known virus that exploits a known vulnerability caused by a missing patch.
- Existing AV solution failed to stop the virus. Many AV agents either not responding or missing DAT updates
- Existing Patch Management solution failed to report missing patches, thus making the systems susceptible to the exploit.
- Lack of visibility into the current real-time status with no ability to easily get that visibility

## **Challenge:**

- 30,000 distributed endpoints disbursed across 800 physical networks / locations
- Low bandwidth availability with critical business functions requiring availability
- Antiquated hardware and many end of life operating systems (Windows 2000, etc)
- Limited resources to combat the issue and quickly bring it to resolution

# Federal Agency: 65 Hour Countdown



## **Solution:**

- Leverage the BigFix infrastructure to get visibility and control
- Roll-out Bigfix agent to endpoints
- Implement patch policies across all systems and close the patch gap
- Identify AV DAT gaps and roll-out DAT updates for their AV solution
- Rolled out application patches for common applications such as Adobe

## **Results:**

- Installed entire BigFix infrastructure and 16,970 clients within 36 hours
- Reduced the patch gap from 35% to 2% within the first 48 hours
- Deployed 2.5TB+ of SP3 data over the network with no unplanned impact
- Increased AV DAT currency from 64% to 96%
- Eliminated causal patch-related vulnerabilities for all critical systems

## **Next Steps**

- Within 7 days, increased client count to 22,000
- 98% compliance against patches with tighter SLA for deployment
- Implement security configuration for all systems using industry standards
- Focus on SCAP, FDCC, DISA Checklists

# Asset control with full visibility

Basic controls and standards can help increase the infrastructure security and compliance by providing a measurable, consistent baseline of protection.



# Quasi-Federal Agency: Which standard to use?



## **Problem:**

- Failed internal audit of security controls due to misconfigured systems
- Systems continually found to drift from compliance
- No centralized visibility into configuration state
- Organization is distributed into 12 geographical divisions with separate IT organizations.
- Need centralized visibility and distributed management and control

## **Challenge:**

- Central IT responsible for definition and enforcement of policy
- Standards defined internally by Central IT for each platform
- Standards developed internally for all Windows XP, 2K3, 2K8, Solaris, AIX, HP-UX, and Red Hat
- Time consuming, difficult to manage, enforce, assess, and audit

A New Approach is Needed...

# Configuration Standards Organizations

Defense Information  
Systems Agency

<http://iase.disa.mil/stigs/checklist/>

National Institute of  
Standards and Technology

<http://web.nvd.nist.gov/view/ncp/repository>

Center for Internet  
Security

<http://www.cisecurity.org/benchmarks.html>

National Security Agency

[http://www.nsa.gov/ia/guidance/security\\_configuration\\_guides/index.shtml](http://www.nsa.gov/ia/guidance/security_configuration_guides/index.shtml)



Information Assurance Support Environment  
for "Outsourcing" of Information

IA News What's New Contact Notice

### Security Checklists

Security Checklists | SRRs | STIGs | STIG Home Page | Whitepapers

DoD General Purpose STIG, Checklist, and Tool Compilation CD

Documents	Date	Size
Application Security and Development Checklist Version 2 Release 1.5 - Updated!	June 26, 2009	1,291KB
Application Services Checklist Version 1, Release 1.1	Sep 21, 2006	448KB

70+ Security  
Checklists



Automated by the National Cyber Security Division (CS&D)

### National Vulnerability Database

automating vulnerability management, risk assessment, and compliance checking

Vulnerabilities Checklists Product Dictionary NCP Events Impact Matrix Contact Vendor Comments

#### National Checklist Program Repository

The National Checklist Program (NCP), defined by the NIST SP 800-20 Rev. 1, is the U.S. government repository of publicly available security checklists (or benchmarks) that provide detailed low level guidance on setting the security configuration of operating systems and applications. NCP is registering its repository of checklists to conform to the Security Content Automation Protocol (SCAP). SCAP enables standards based security tools to automatically perform configuration checking using NCP checklists. For more information relating to the NCP please visit the [www.nvd.nist.gov](http://www.nvd.nist.gov) or the [www.nist.gov](http://www.nist.gov).

Search for Checklists using the fields below. The keyword search will search across the name, and summary.

Filter: Any  
Target Product: Any  
Product Category: Any  
Authenticity: Any  
Keyword:

128+ Security  
Checklists

CIS Benchmarks/Scoring Tools  
Now Available, Free of Charge!

#### Operating Systems

Benchmark	Version	Updated
AIX	1.01	10/21/2005
Debian Linux	1.0	09/17/2007
FreeBSD	1.0.5	10/21/2005
HP-UX	1.4.2	06/03/2008
Mac OS X 10.4 (Tiger)	2.0	10/16/2006
Mac OS X 10.5 (Leopard)	1.0	05/21/2008
Novell OES/NetWare	1.0	09/14/2006
Red Hat Linux 4 (for RHEL 2.1, 3.0, 4.0 and Fedora Core 1,2,3,4, & 5)	1.0.5	10/01/2006

40+ Security  
Benchmarks

Home > Information Assurance > Guidance > Security Configuration Guides

#### Security Configuration Guides

NSA develops and distributes configuration guidance for a wide variety of software, both open source and proprietary. We strive to provide NSA customers and the software development community the best possible security options for the most widely used products.

NSA does not favor or promote any specific software product or business model. Rather, we promote enhanced security.

Contact us via email at [SNAC@radsum.ncsc.mil](mailto:SNAC@radsum.ncsc.mil).

60+ Security  
Benchmarks  
and Guidance  
Docs

They Consider



and



## Languages



v.1.1.4

eXtensible Configuration  
Checklist Description Format



v.5.3

Open Vulnerability Assessment  
Language

## Enumerations



v.5

Common Configuration  
Enumeration



v.2.2

Common Platform Enumeration



No Version

Common Vulnerability  
Enumeration

## Metrics



v.2

Common Vulnerability Scoring  
System

**More Information:** <http://scap.nist.gov/revision/1.0/index.html>

# Expected Benefits of Using SCAP



- Predefined benchmarks
- Automated assessment
- Consistent measurements
- Increased efficiency
- Reduced cost
- Widespread adoption
- System interoperability





# Limitations Preventing Widespread Adoption



- Increase benchmark availability
- Expand benchmark capabilities
- Simplify the benchmark development
- Add remediation capability to SCAP
- Scoring system for configurations

## **Specific Organizational Goals**

- ✓ Decrease configuration drift
- ✓ Reduce cost of management / measurement
- ✓ Increase overall security for all systems



# Army Unit @ Forte Meade



## Goals:

- Mission and focus to increase security and save lives
- Augment policies set forth by the Directorate of Information Management (DOIM)

## Challenge:

- Lack of visibility into the state of their endpoints
- Need simple, easy to use tool to assess and measure systems against defined configuration settings: Army AGM and other.
- Wanted better, more accurate visibility into security state of systems
- Scan-based solutions do not provide adequate real-time visibility

## Solution:

- Select BigFix to provide real-time visibility into configuration and patch state
- Installed within one hour and remediating systems within 24 hours
- Use BigFix to implement AGM, DISA STIG, and other policies – patch and configuration
- Leverage for third party application support
- Priority focus on securing the environment

# Some Commercial Uses of SCAP / FDCC



- Regulatory compliance – development of policy using SCAP-expressed data streams
  - Examples: PCI, HIPAA, NERC
  - Provides automated control through a common data format
- Enhance interoperability between information systems
  - Correlate external vulnerabilities with actual configuration and patch remediation
  - Information format to enable ITIL initiatives
- System configuration assessment for kiosks and other customer-facing systems that require heavy lockdown
  - Bank/Retail kiosks

# Wrap-up / Summary



- Regulations will increase in demand
- Standards can help simplify policy definition
- SCAP and SCAP validated tools will help automate measurement
- Limitations do exist, but can be overcome
- Standards evolution will continue
- Tool evolution will be necessary
- Increased visibility
- Reduced risk
- Overall reduction in cost



# Questions...



Jim Hansen

Director, Product Management - Security, Compliance  
BigFix, Inc.

[jim\\_hansen@bigfix.com](mailto:jim_hansen@bigfix.com) \* 510.740.0309

[www.bigfix.com](http://www.bigfix.com)