5th 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?

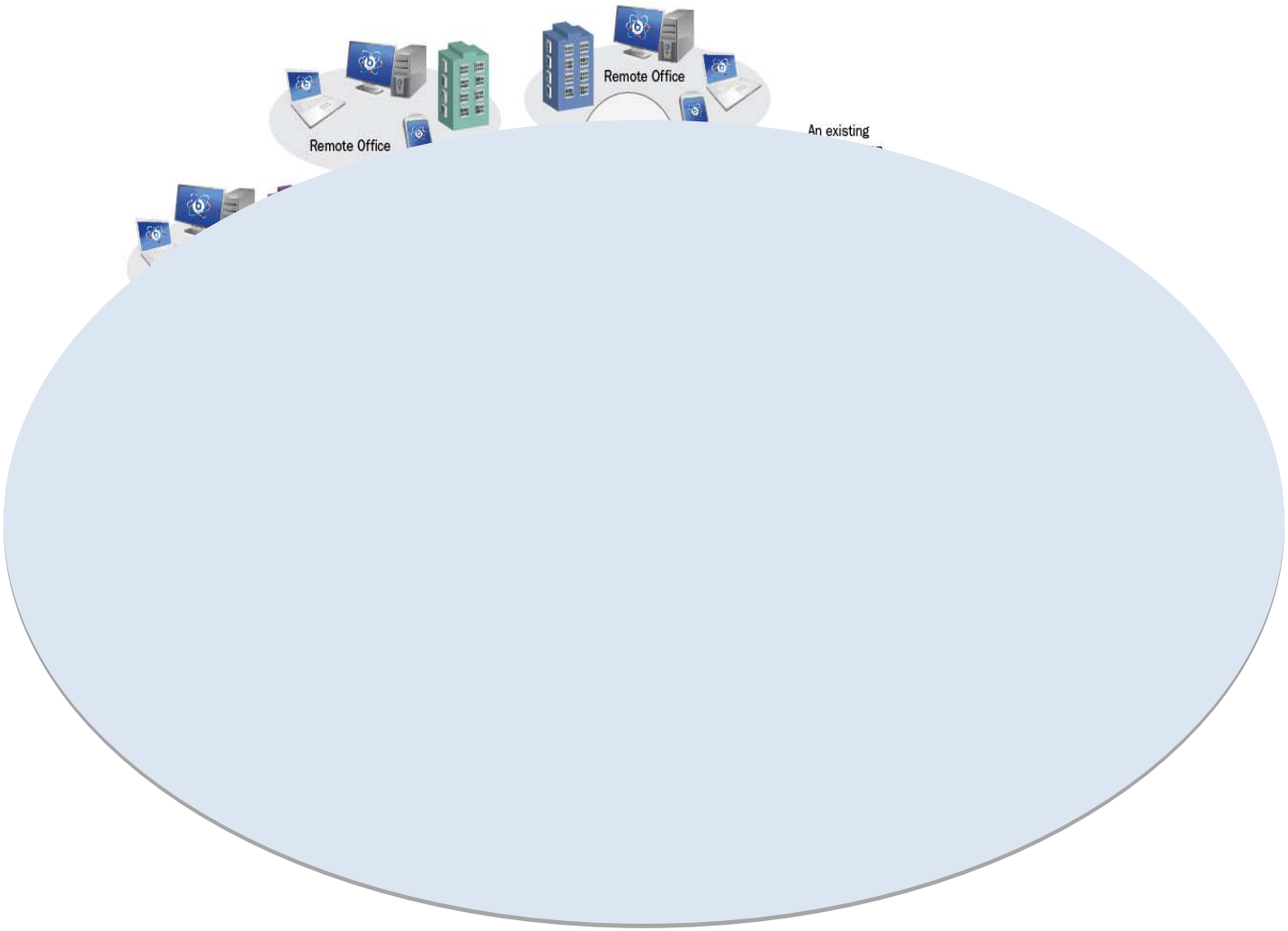
Who is BigFix

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

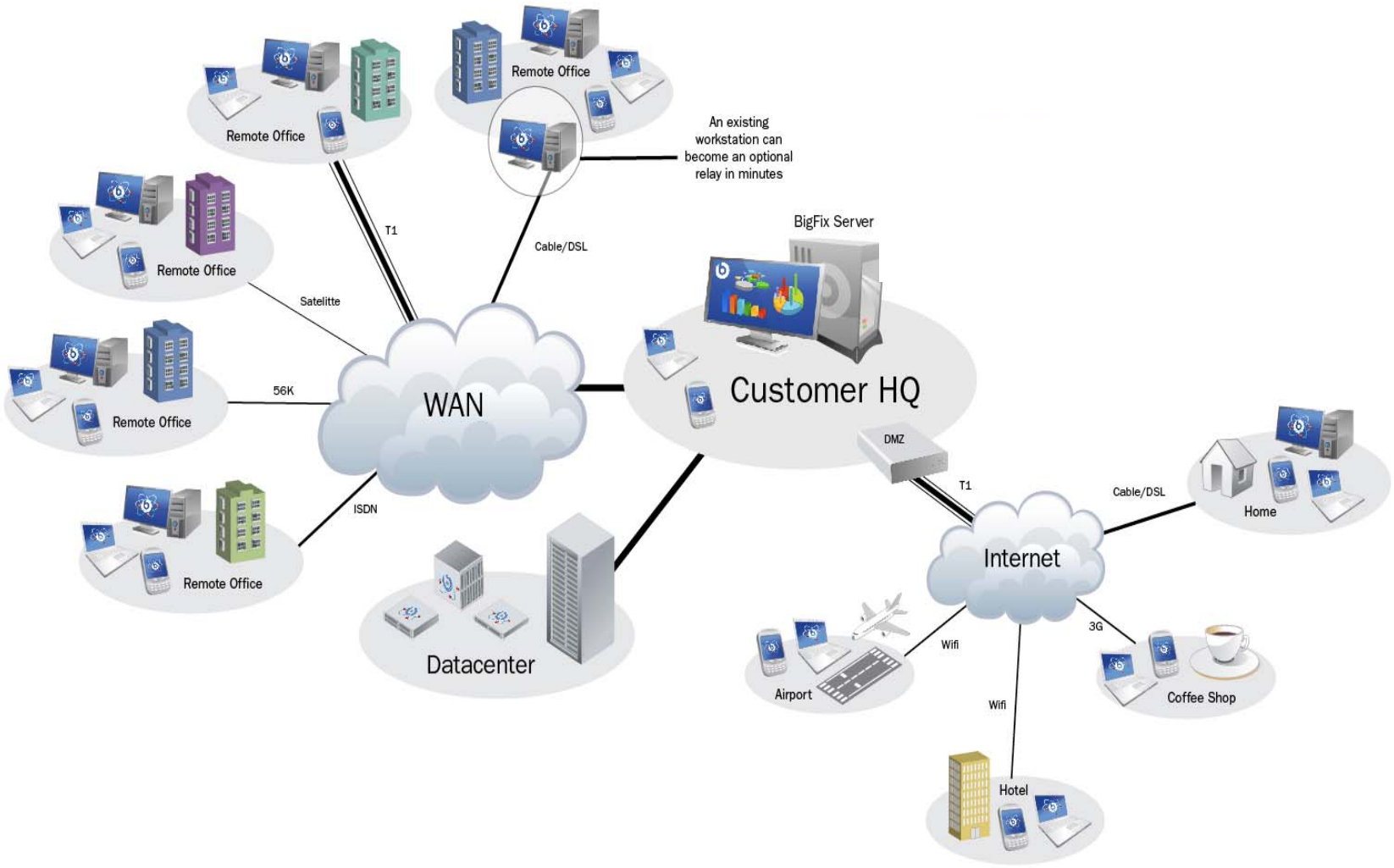
- Global and pervasive deployment across vertical industries
  - Highly complex environments
  - Very large enterprise deployments > 100,000 assets
- Innovative BigFix technology platform
  - "Visionary" in EPP and PCLM Gartner Magic Quadrants
  - 19 patents worldwide
  - 32 patents pending worldwide
- 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

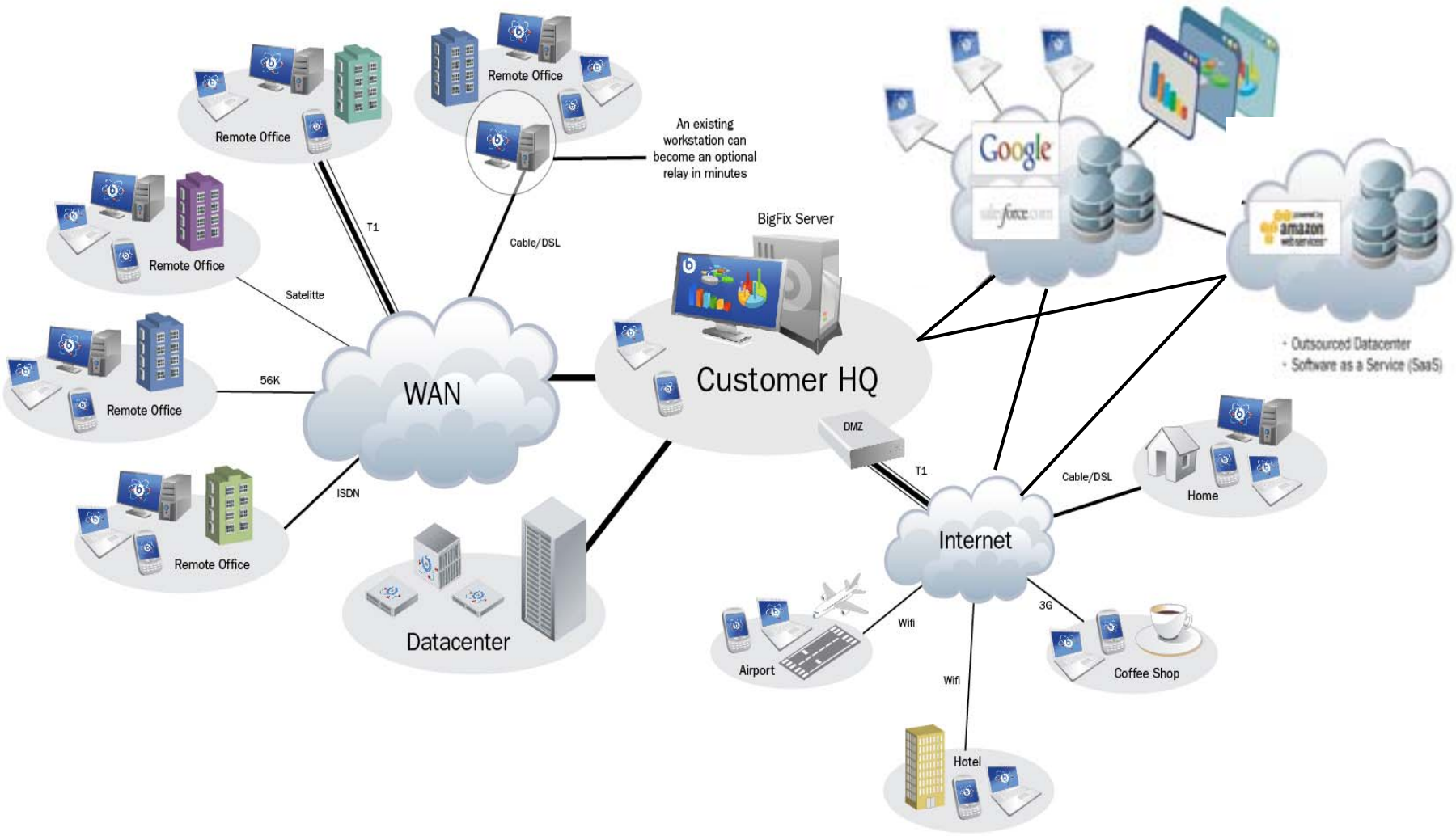
The World of IT – Circa 2000



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?

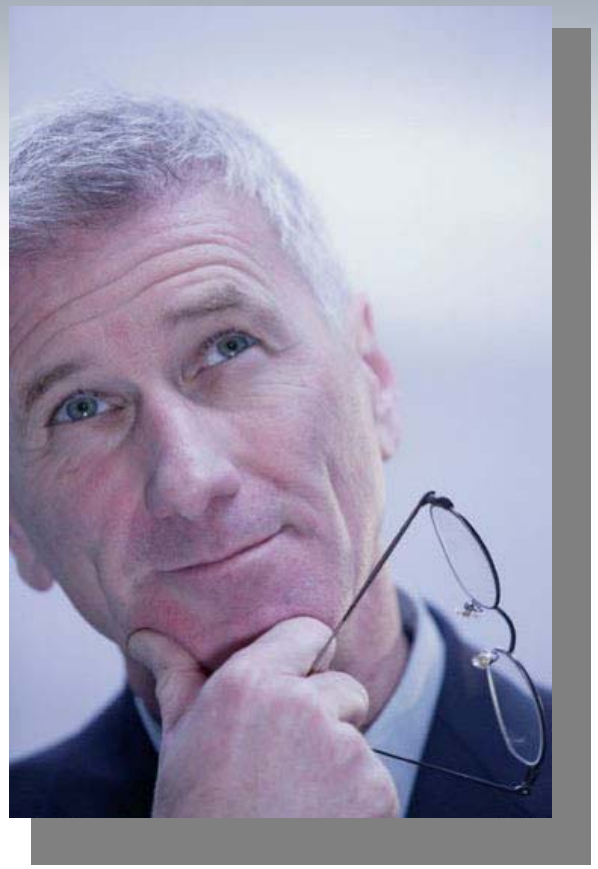
What is the current compliance status for all my desktops and servers?

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

Are they patched, configured properly, vulnerable?

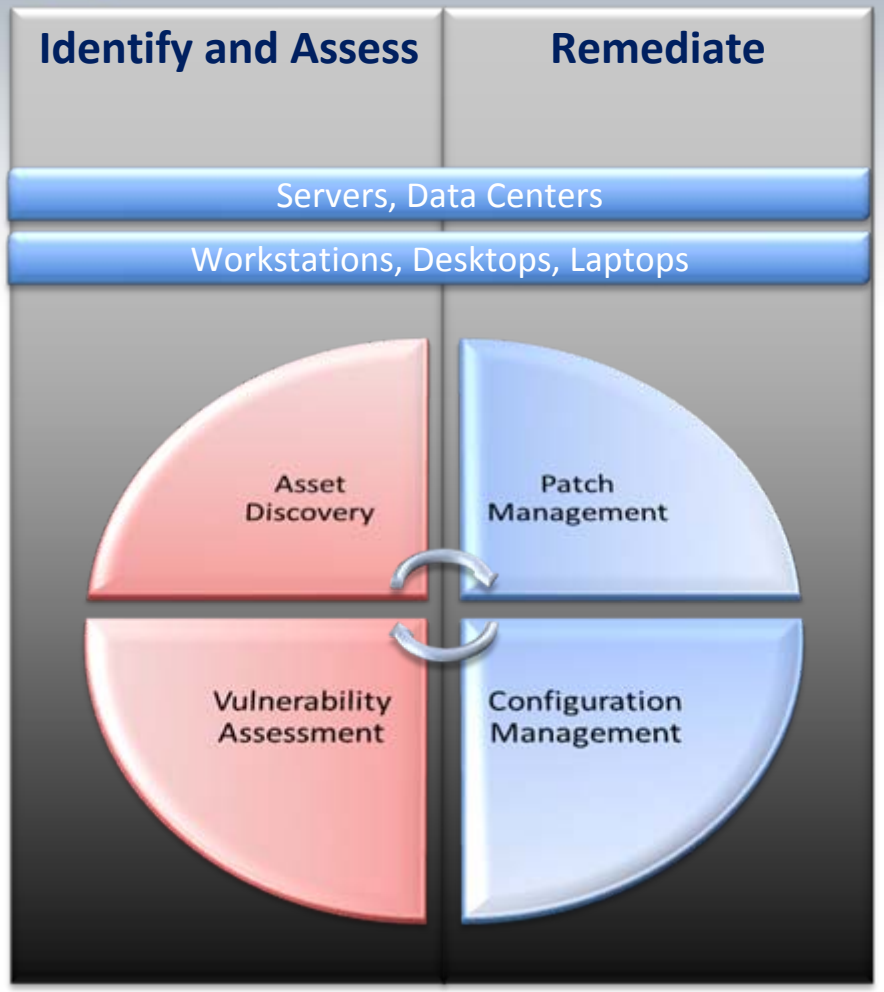
How do I bring laptops, desktops and servers back into compliant status?

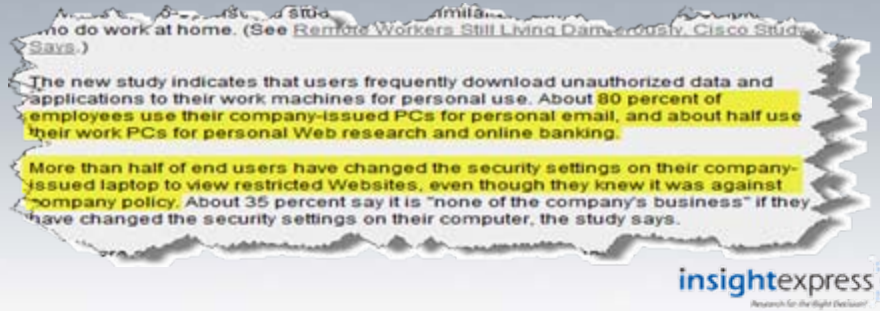
How much is this going to cost me and what level of risk can I afford?



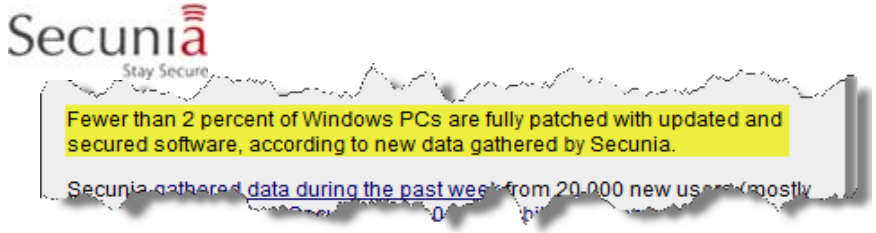
7

Basic Foundation to Mitigate and Reduce Risk

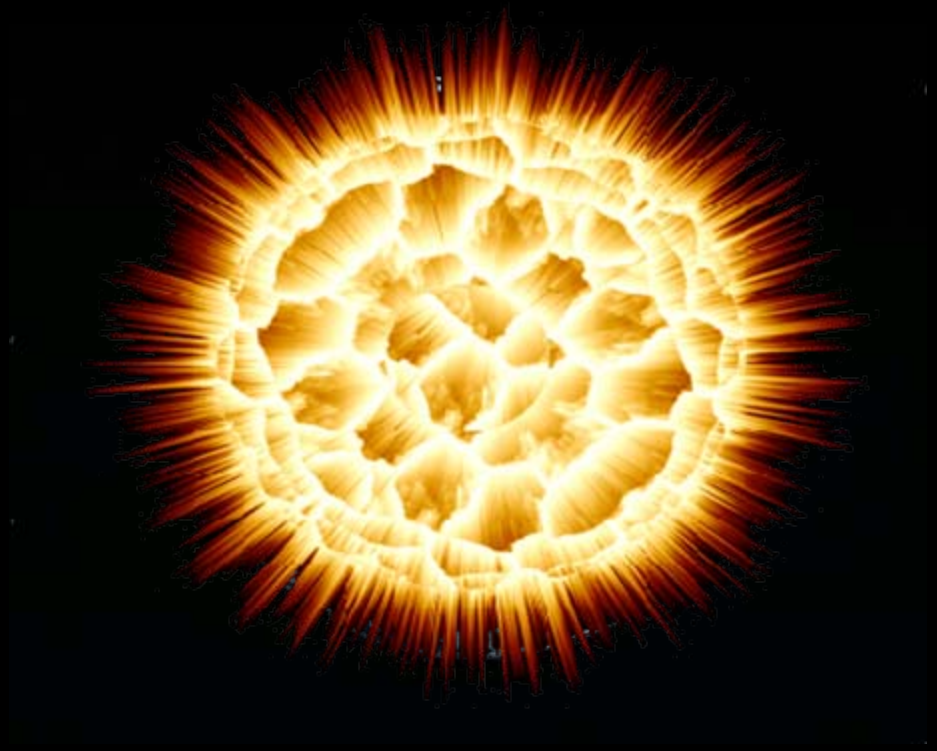




- Locate and track your assets. You cannot secure what you can't see.
- Identify vulnerabilities and threats and assess for risk
- Patch and Configure systems to mitigate and reduce risk



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:

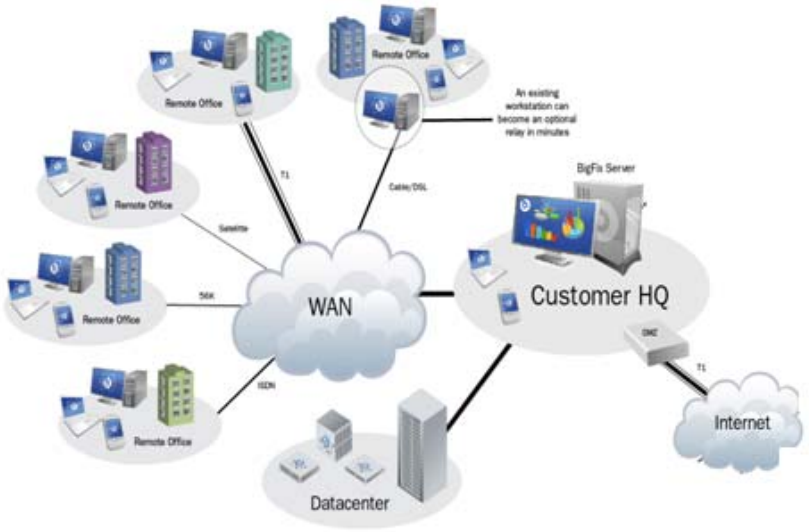
- Installed entire BigFix infrastructure and 16,970 clients within 36 hours
- Reduced the patch gap from 35% to 2% within the first 48 hours
- Deployed 2.5TB+ of SP3 data over the network with no unplanned impact
- Increased AV DAT currency from 64% to 96%
- Eliminated causal patch-related vulnerabilities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

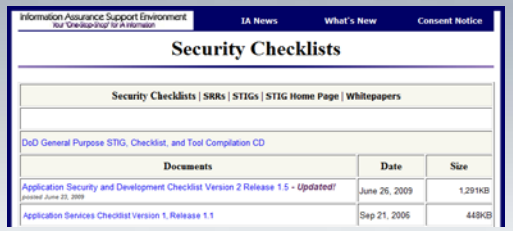
- Central IT responsible for definition and enforcement of policy
- Standards defined internally by Central IT for each platform
- Standards developed internally for all Windows XP, 2K3, 2K8, Solaris, AIX, HP-UX, and Red Hat
- Time consuming, difficult to manage, enforce, assess, and audit

A New Approach is Needed…

Configuration Standards Organizations

Defense Information Systems Agency

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



70+ Security Checklists

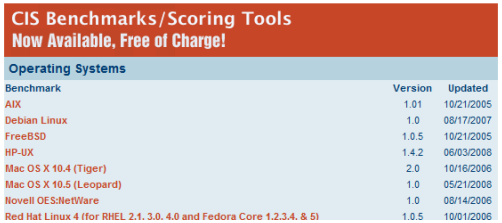
National Institute of Standards and Technology

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

128+ Security Checklists

Center for Internet Security

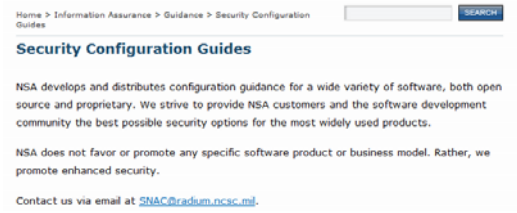
http://www.cisecurity.org/benchmarks.html



40+ Security Benchmarks

National Security Agency

http://www.nsa.gov/ia/guidance/security_configuration_guides/index.shtml



60+Security Benchmarks and Guidance Docs

They Consider SCAP™ and

Languages

XCCDF v.1.1.4

eXtensible Configuration Checklist Description Format

OVAL v.5.3

Open Vulnerability Assessment Language

Enumerations

CCE v.5

Common Configuration Enumeration

CPE v.2.2

Common Platform Enumeration

CVE No Version

Common Vulnerability Enumeration

Metrics

CVSS 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 * 510.740.0309
www.bigfix.com