BIGFIX

Comprehensive, Scalable, Simple Security Configuration and Vulnerability Management

Francis Ong

BigFix, an IBM Company

IBM Tivoli, ASEAN

Value Statement – Who is BigFix

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

The **BigFix Unified Management Platform** provides real-time visibility through a **single infrastructure, single agent and unified console** for systems lifecycle management, endpoint protection, security configuration and vulnerability management.

What is High-Performance

- **Blazing Speed**
  - 100x faster than competing solutions
- **Pervasive Visibility and Control**
  - Heterogeneous support across all computing assets, fixed and mobile, physical and virtual
- **Massive Scalability**
  - 250k endpoints per single BigFix s
- **Extreme Productivity**
  - 1 FTE performing the task of a doze
- **Revolutionary Economics**
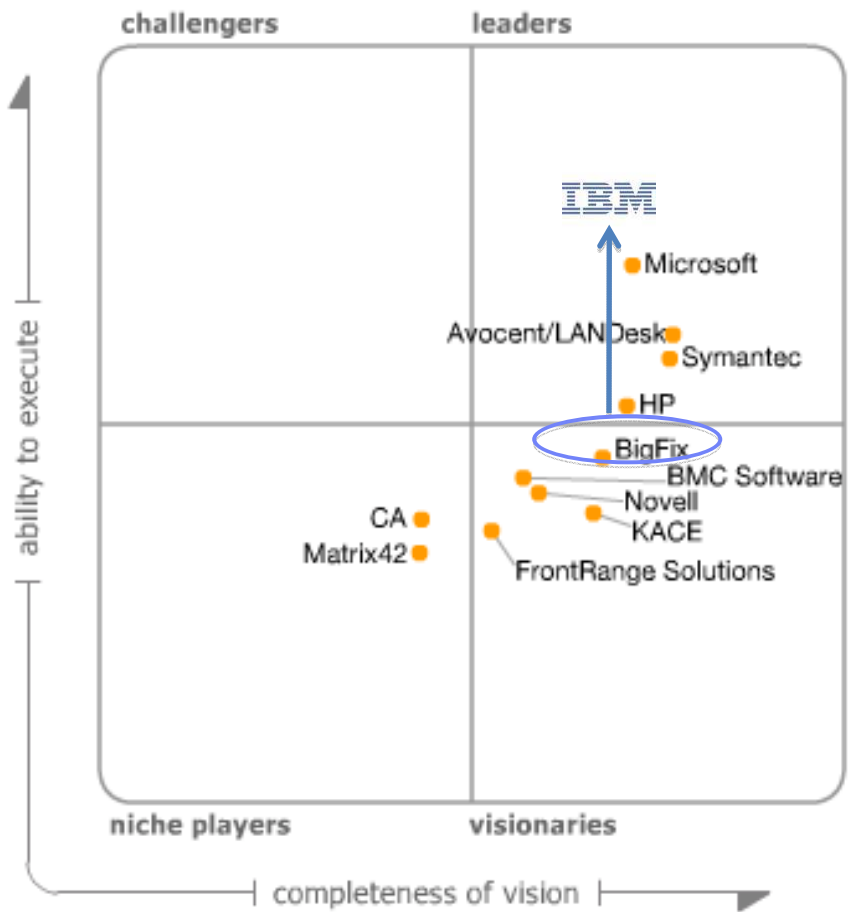 - Proven ROI and the Lowest TCO in the industry
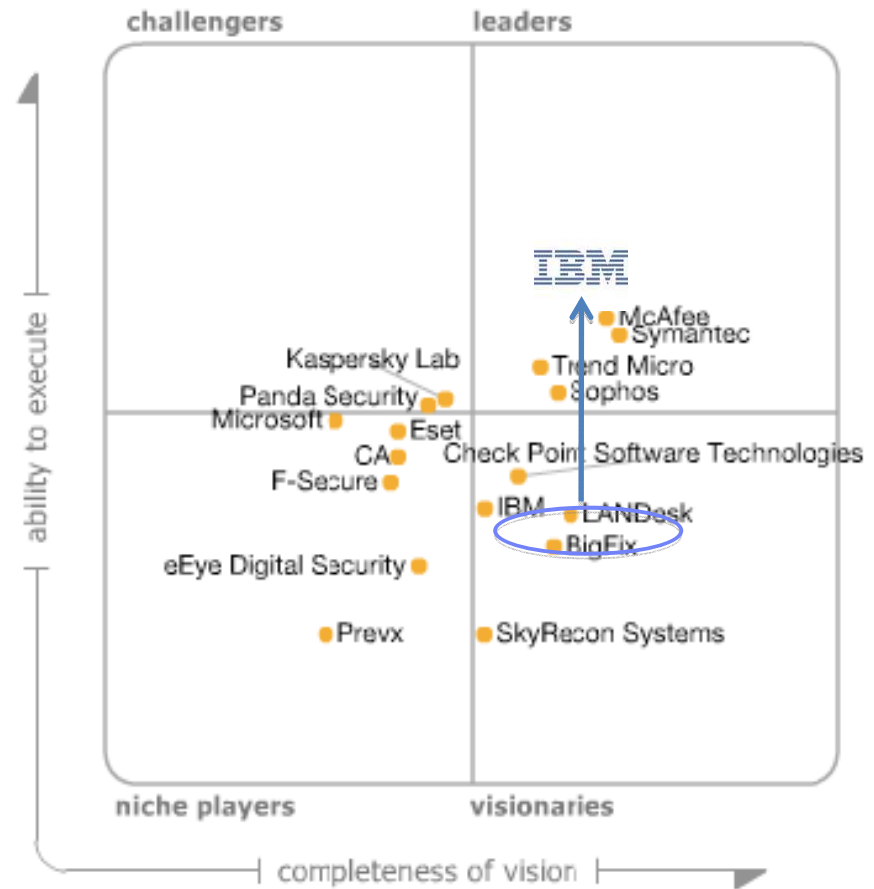
A Winning Team Creates Market Leading Solutions

PC Lifecycle Configuration Mgmt MQ

Endpoint Protection Platform MQ

The Need for Pervasive, Real-Time Visibility

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?

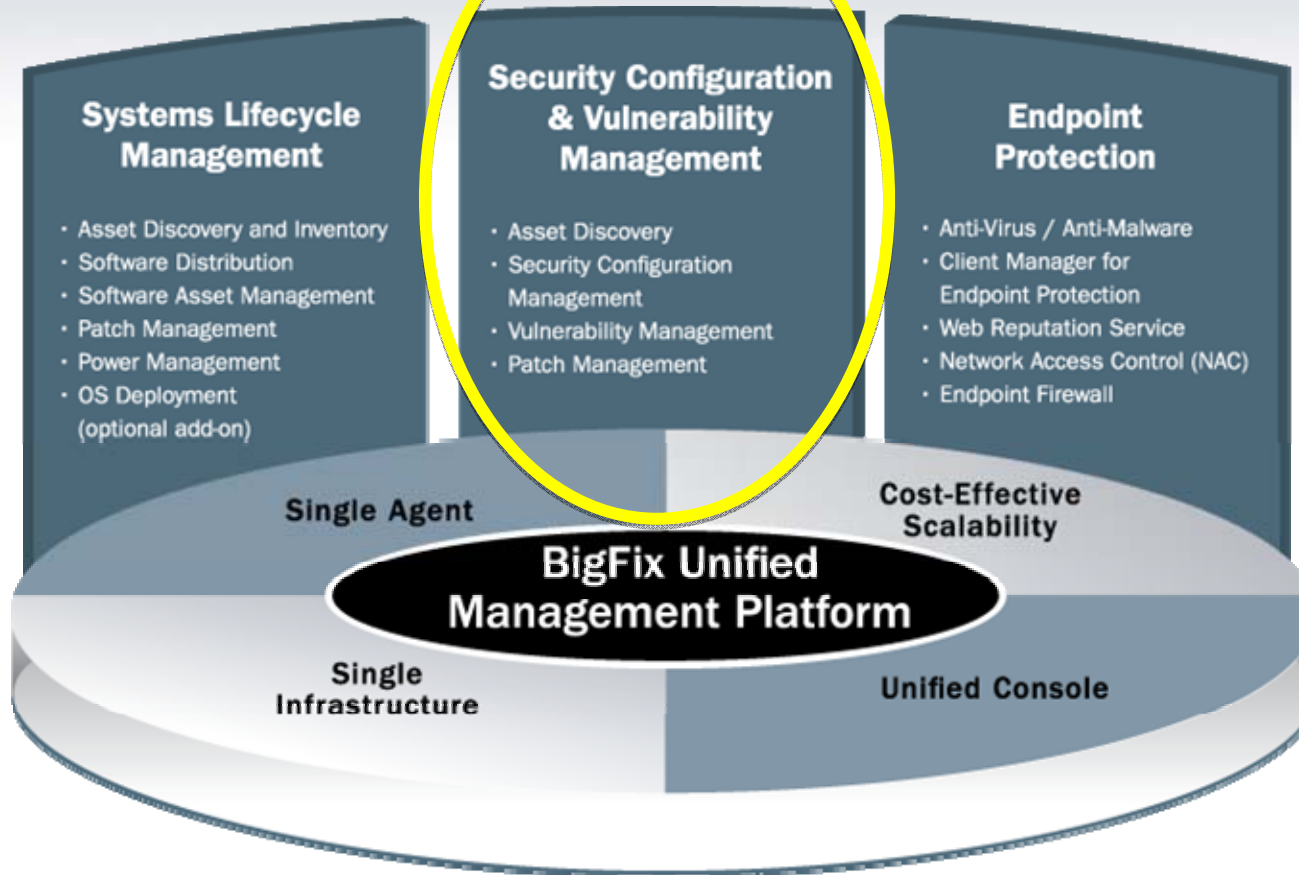**How do I bring laptops, desktops and servers back into compliant status?**

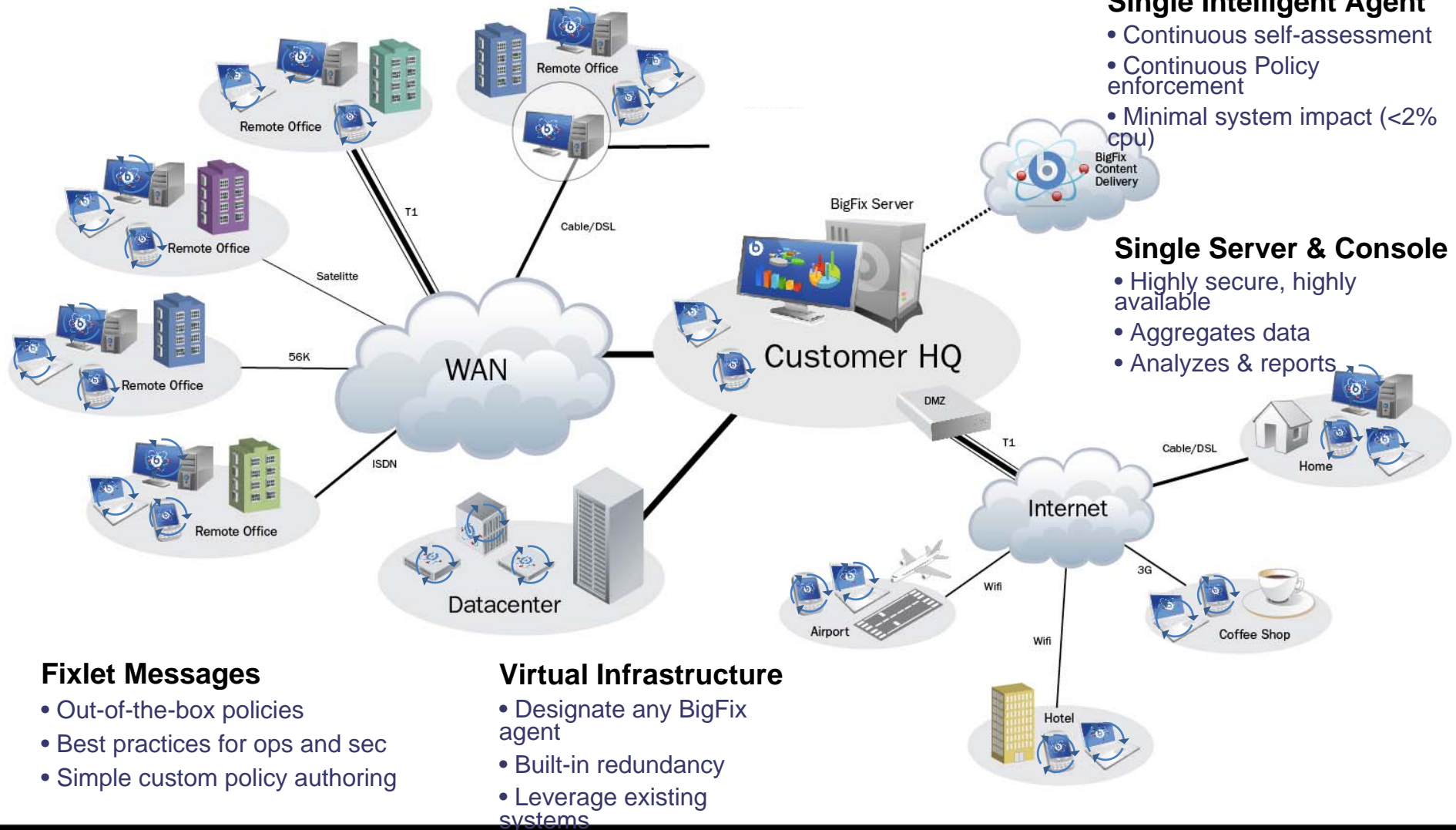**What rogue devices are gaining access to my network?**

BigFix Enterprise Solutions

The BigFix Unified Management Platform provides real-time visibility and control through a single infrastructure, single agent and single console

Systems Lifecycle Management

- Asset Discovery and Inventory
- Software Distribution
- Software Asset Management
- Patch Management
- Power Management
- OS Deployment (optional add-on)

Security Configuration & Vulnerability Management

- Asset Discovery
- Security Configuration Management
- Vulnerability Management
- Patch Management

Endpoint Protection

- Anti-Virus / Anti-Malware
- Client Manager for Endpoint Protection
- Web Reputation Service
- Network Access Control (NAC)
- Endpoint Firewall

Single Agent

Cost-Effective Scalability

BigFix Unified Management Platform

Single Infrastructure

Unified Console

* Product Extensions

BigFix: How it Works

Single Intelligent Agent
- Continuous self-assessment
- Continuous Policy enforcement
- Minimal system impact (<2% cpu)

Single Server & Console
- Highly secure, highly available
- Aggregates data
- Analyzes & reports

Fixlet Messages
- Out-of-the-box policies
- Best practices for ops and sec
- Simple custom policy authoring

Virtual Infrastructure
- Designate any BigFix agent
- Built-in redundancy
- Leverage existing systems

Relevance Language

- Custom made for managing endpoints
- >100 faster than any other environment
- Suitable for IT operations and security groups

Example Relevance
Language vs WMI
showing >100
faster execution

```
Edit 1* - Relevance Debugger                              _ □ X
File  Edit  View  Help

% Edit 1*

// All System Management frameworks will use Windows Management Instrumentation (WMI) API
q: string value of selects "TotalPhysicalMemory from Win32_ComputerSystem" of wmi
A: 2145435648
T: 72.267 ms

// BigFix Relevance Language
q: size of ram
A: 2145435648
T: 0.090 ms

Ln 11        Ch 1        Total evaluation time: 72.357 ms
```
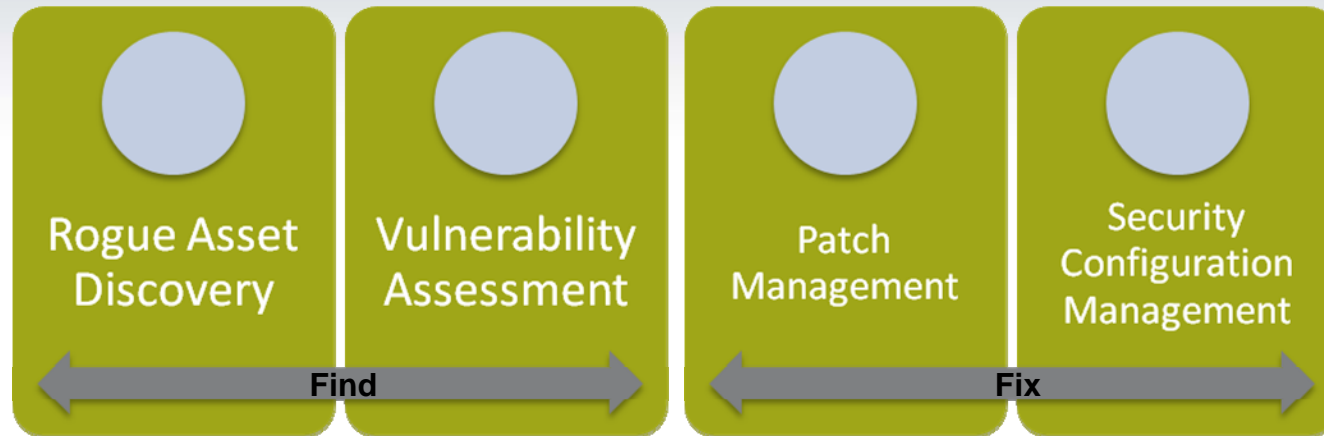
```
Relevance

Relevance 1

name of operating system = "WinVista"

Relevance 2

not ((exists key "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon" of registry AND exists value "AllocateCDRoms"
of key "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon" of registry) AND exists
(value "AllocateCDRoms" of
key "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon" of registry) whose( it as string = "0" ))
```

Discover, Assess, Remediate, Report

Real Infrastructure Consolidation; true systems and security management convergence

Before BigFix	With BigFix

Software Distribution	e.g., HP Openview	
Patch Mgmt	e.g., Microsoft SMS	
Security Configuration Mgt	e.g., NetIQ, CA	
Asset &License Mgt	e.g., Altiris - Asset Manager	
Endpoint Protection	e.g., McAfee EPO	

- 1 wintel server
- 1 fail-over server
- 1 agent on end point
- 1 console
- Implemented in weeks
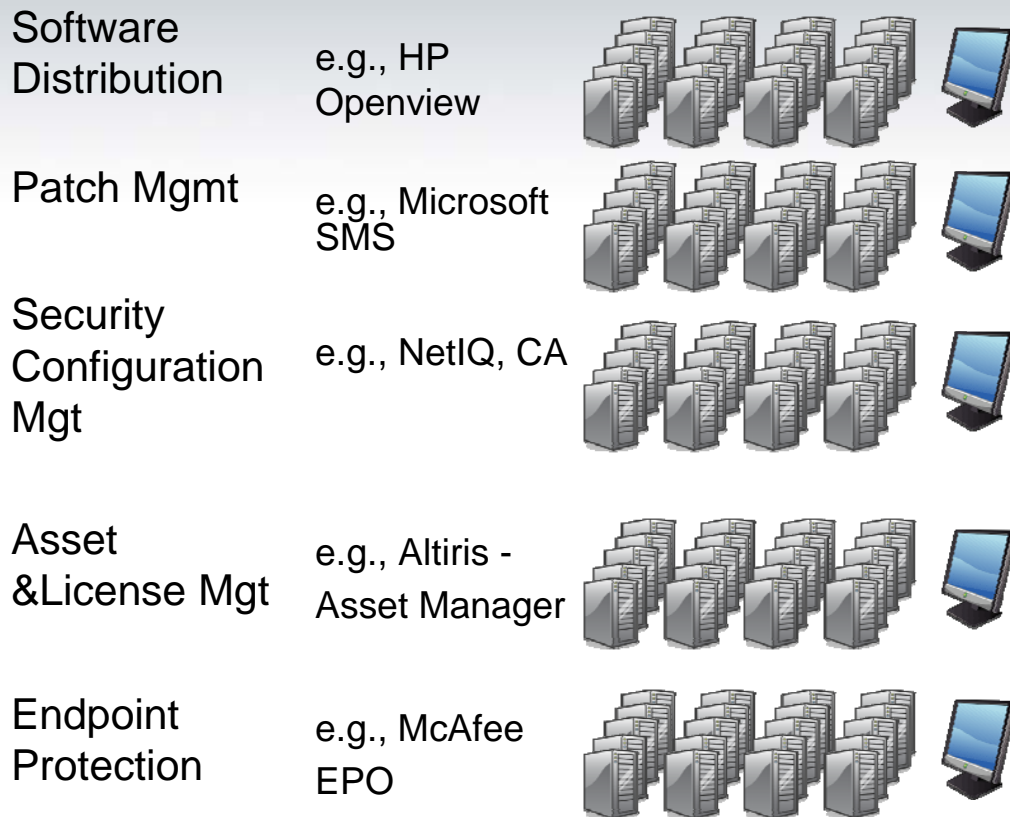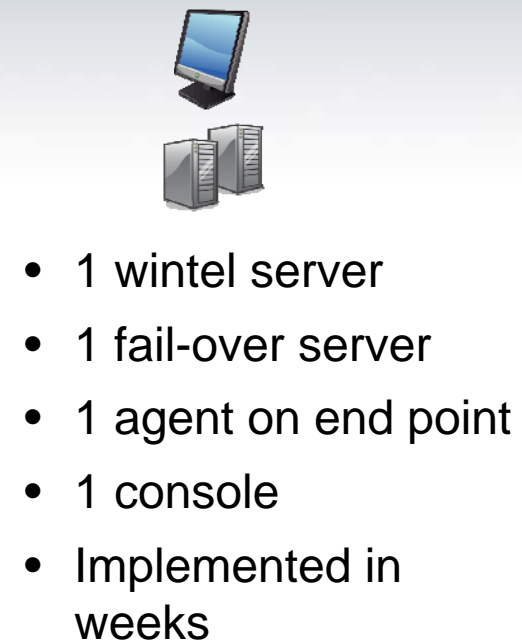
100 - 125 servers/5 different consoles/10 different agents on client, implemented over years

Benefits of the BigFix Approach

✔ Protects endpoints no matter where they are located, how they are connected, or whether they are on or off the network

✔ Minimal network, endpoint impact

✔ Real-time compliance reporting instead of point-in-time assessments

✔ Continuous compliance enforcement

✔ Quick time to implement

✔ Very low implementation, infrastructure, maintenance costs

✔ Unifies endpoint protection, security and vulnerability management to a single agent, single console, single infrastructure

Case Studies

Singapore Press Holdings	PT OCBC NISP Bank	Summit Auto Group (Sumitomo)	PT Astra International Tbk.
5000+ endpoints (workstation / wintel server / unix / linux server)	5000 workstations	4000 workstations	5000 workstations
Bigfix Modules: System Lifecycle Management	Bigfix Modules: Asset Management, Patch Management and Software Distribution.	Bigfix Modules: Asset Management, Security Configuration Management and Patch Management.	Bigfix Modules: Asset Management, Patch Management and Software Distribution.
Challenges: Require a solution to manage heterogeneous platform. In addition to managing mobile devices remotely.	Challenges: No visibility of IT infrastructure. Struggling with Conflickers as IT is unable to patch on a timely basis due to highly distributed network with low bandwidth.	Challenges: Users are using illegal software and P2P at work. IT also wants to prevent users from using USB thumb drives and external storage devices.	Challenges: With over 270 remote sites and some connected by 16kb satellite link, Bigfix is the only solution that is lightweight enough for AI to manage remote sites.
Anecdotes: For the first time, SPH is able to, via the internet, manage mobile devices issued to journalists all over the world that will never dock (physically) their workstation to the HQ network. Also, SPH intensively utilize Bigfix 'Fixlet' to ensure desktops / servers is in compliance.	Anecdotes: We completed FULL scale deployment (3 wks) for 4000 workstations across 460 sites during POC and found 30 Wintel servers that have not been used for an extensive period of time. In addition, OCBC NISP is able to achieved zero-day patching.	Anecdotes: With Bigfix SCM, SAG is able to monitor, enforce IT / Security Policies across their IT environment in an instant. For example, disabling use of certain external storage devices, such as thumb drives and CD-ROM etc, across their highly distributed environment.	Anecdotes: With Bigfix, Astra is able to generate a customize hardware / software inventory report for 5000 workstations in just minutes without any impact to the network.

BigFix Customers Include

Manufacturing

SOLECTRON · Pitney Bowes · TRW Automotive · PILKINGTON · phelps dodge

Energy

Arch Coal, Inc. · FPL · Progress Energy · Entergy THE POWER OF PEOPLE · 中国海洋石油总公司 CHINA NATIONAL OFFSHORE OIL CORP.

Retail / Consumer

Marriott · WAL★MART · STAPLES that was easy · DARDEN RESTAURANTS · Hannaford · Chick-fil-A · AMERICAN EAGLE OUTFITTERS

Technology

intel · LSI LOGIC · KRONOS

Government

Lawrence Livermore National Laboratory · State of California Franchise Tax Board · SEC

Education

Duke UNIVERSITY · Miami-Dade County Public Schools giving our students the world · STANFORD UNIVERSITY

Pharma/Biotech

IVAX · Wyeth · NOVARTIS

Largest deployments

Customer	Seats
One of the US Armed Forces	430,000
Intel	350,000
Walmart	250,000
Sinopec	260,000
Ministry of Rails - China	220,000
Kaiser Permanente	260,000
Deutsche Bank, Merrill Lynch (BOA), Miami Dade Schools (tied)	160,000
Education, Singapore	122,000
Countrywide Financial (now BOA)	90,000
Marriott International	80,000
Suntrust Banks	50,000
Morgan Stanley	50,000