BigFix Endpoint Management

Jan Bojtos
Tivoli Security Channel Leader
Central&Eastern Europe
Simplifying Endpoint Operations and Security

We believe IT and security operations should be simple.

- BigFix allows clients to consolidate IT operations and IT security functions in a single view, delivery model and software offering.
  - Helping to provide...
    - Total visibility
    - Quality of control
    - Speed to remediation
    - High scalability
    - Cost reduction
  - Through....
    - Security configuration and vulnerability management
    - Systems lifecycle management
    - Endpoint protection
    - Power management
  - To help...
    - Improve visibility and central control across desktops, laptops, and servers
    - Consolidate management of multiple endpoint applications
    - Reduce costs associated with endpoint management
    - Simplify endpoint operations and security to drive business value
BigFix Product Portfolio

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

**Security Configuration & Vulnerability Management**
- Asset Discovery
- Security Configuration Management *(FDCC, DISA STIG, etc.)*
- Vulnerability Management
- Patch Management

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

---

**BigFix Unified Management Platform**
- Single Agent
- Cost-Effective Scalability
- Single Infrastructure
- Unified Console

© 2010 IBM Corporation
The Power of Distributed Intelligence

**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
BigFix Unified Management Platform

**Single Management Agent**
- Lightweight, intelligent agent deployed on every desktop, laptop, server, mobile device, server
- Requires only 2-4MB of endpoint system memory
- Real-time, continuous policy processing, remediation, validation, reporting
- Policies remain enforced even when remote devices roam from the enterprise network

**Single Management Console and server**
- 1 server for up to 250,000 devices
- Built in reporting and analysis tools
- Support for automatic multiserver synchronization and nonstop BigFix services even during a disruptive event

**Single policy-based model**
- Special policy language enables to create custom policies and services
BigFix Product Portfolio

Systems Lifecycle Management
- Asset Discovery and Inventory
- Software Distribution
- Patch Management
- Power Management
- Software Asset Management *optional add-on
- OS Deployment *optional add-on

Security Configuration & Vulnerability Management
- Asset Discovery
- Security Configuration Management (FDCC, DISA STIG, etc)
- Vulnerability Management
- Patch Management

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

BigFix Unified Management Platform

Single Agent

Single Infrastructure

Unified Console

Cost-Effective Scalability
BigFix Systems Lifecycle Management

Comprehensive solution for end-to-end systems management which includes:

- Asset Discovery and Inventory Management
- Patch Management / Software Distribution
- Software Asset Management
- Power Management
- OS Deployment
- Remote Control

Features and Benefits

- Dramatically reduced patch cycles and increased first-pass success rates
- Massive scalability and support for remote and intermittently connected devices
- Detection and resolution of corrupted patches
- Closed loop validation in real-time
- Multi-platform support (*nix, Win, Mac)
- Coverage for legacy platforms
BigFix Patch Management

BigFix Patch Management is a comprehensive solution for delivering Microsoft, UNIX, Linux, and Mac patches, as well as third-party application patches, through a single console.

Features and Benefits

- Patch capabilities for multiple platforms: Windows, Linux, UNIX, Mac
- Coverage for a variety of software vendors, such as Adobe, Mozilla, RealNetworks, Apple, and Java
- Real-time reporting that provides information on which patches were deployed, when they were deployed, who deployed them, and to which endpoints
- Scalability—manage more than 250,000 endpoints from a single server
- No loss of functionality over low-bandwidth or globally distributed networks
BigFix Power Management

BigFix Power Management allows IT organizations to enforce conservation policies across the enterprise, while providing granularity that enables application of those policies to a single computer.

Features and Benefits

- Saves up to $50 per year per BigFix-managed device depending on local electricity costs and net energy savings achieve
- Centralized, policy-driven power management of distributed computers scalable from individual machines to entire global enterprises
- Fine-grained controls for hibernation/standby, subsystem-only shutdown, and save-work-before-shutdown options
- Wake-on-LAN support synchronizes systems maintenance processes with power conservation
- Opt-in programs encourage end-user participation as well as Wake-on-Web feature to allow for end-users to remotely connect and turn on their own systems
BigFix Security Configuration & Vulnerability Management

Most External Attacks
- Missing patches
- Miss configuration
- Known and unknown vulnerabilities

Challenges
1. Visibility
   - Assets
   - Policies
2. Control
   - Patches
   - Configuration
3. Enforcement

exposure
BigFix Security Configuration & Vulnerability Management

If I don’t know it I cannot manage it !!!
20% gap between Known and discovered

Discovery

Patch

Config

Policy Assessment

Policy deviation
BigFix Security Configuration & Vulnerability Management

Comprehensive solution for end-to-end security management which includes:
- Asset Discovery
- Patch Management
- Security Configuration Management
- Vulnerability Management

Features and Benefits
- Visibility
- Centralized control
- Dashboard & reporting
- Out of box checklist
- Continuous enforcement of security policies, regardless of network connection status
- Heterogeneous platform support: Windows, UNIX, Linux, and Macintosh
- Reduce costs
- Minimal infrastructure
- Reconciliation
- Rapid response
BigFix Endpoint Protection

If I don’t know it I cannot manage it !!!
20% gap between Known and discovered

Discovery

Report

It is worth to know
What was going on

Assessment

Remediation

Fill the gap
Provide feedbacks

Is there security SW?
Which security SW?
From which vendor?
Is it OK with policy?
BigFix Endpoint Protection

Integrated Endpoint Protection modules include:
- Anti-Virus
- Anti-Malware
- Endpoint Firewall
- Web Protection
- Client Manager for Endpoint Protection
- Network Access Control (NAC)

Features and Benefits
- Prevent infection, identity theft, data loss, network downtime, lost productivity, and compliance violations
- Eliminate security gap with real-time threat intelligence
- Achieve unparalleled visibility into complete enterprise protection
- Combine endpoint protection, security configuration, patch management, and systems lifecycle management tools
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