IBM Security

Intelligence. Integration. Expertise.

IBM

Life on the Endpoint Edge:

Winning the Battle Against Cyber Attacks

IBM BigFix

© 2015 IBM Corporation

Ineffective patch management is a major contributor to breaches.

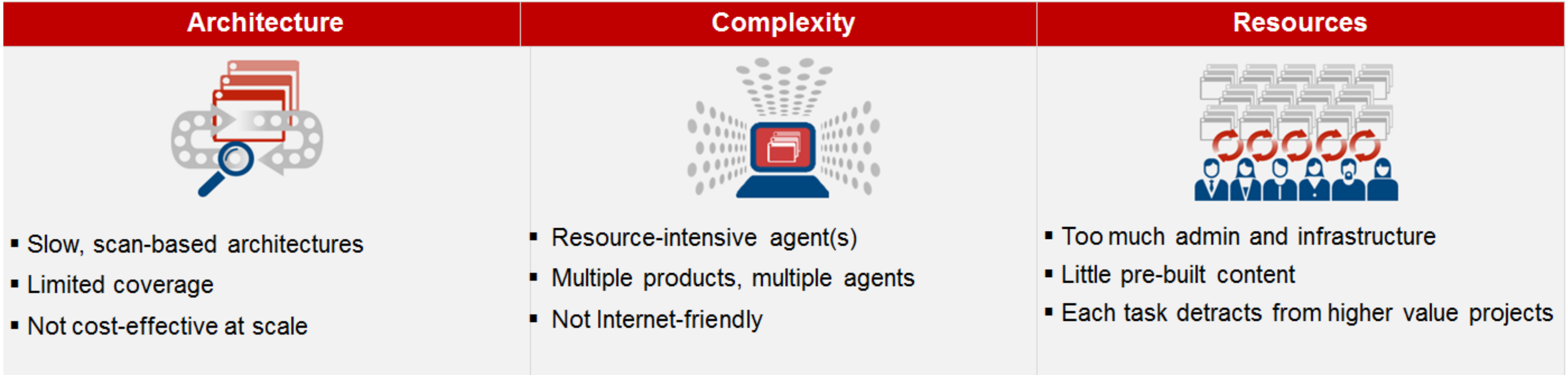
75% Of attacks use publicly known vulnerabilities that could be prevented by patching

99.9% of exploited vulnerabilities were compromised more than a year after the CVE was published

58% of all cyber-attacks originate on an **endpoint**

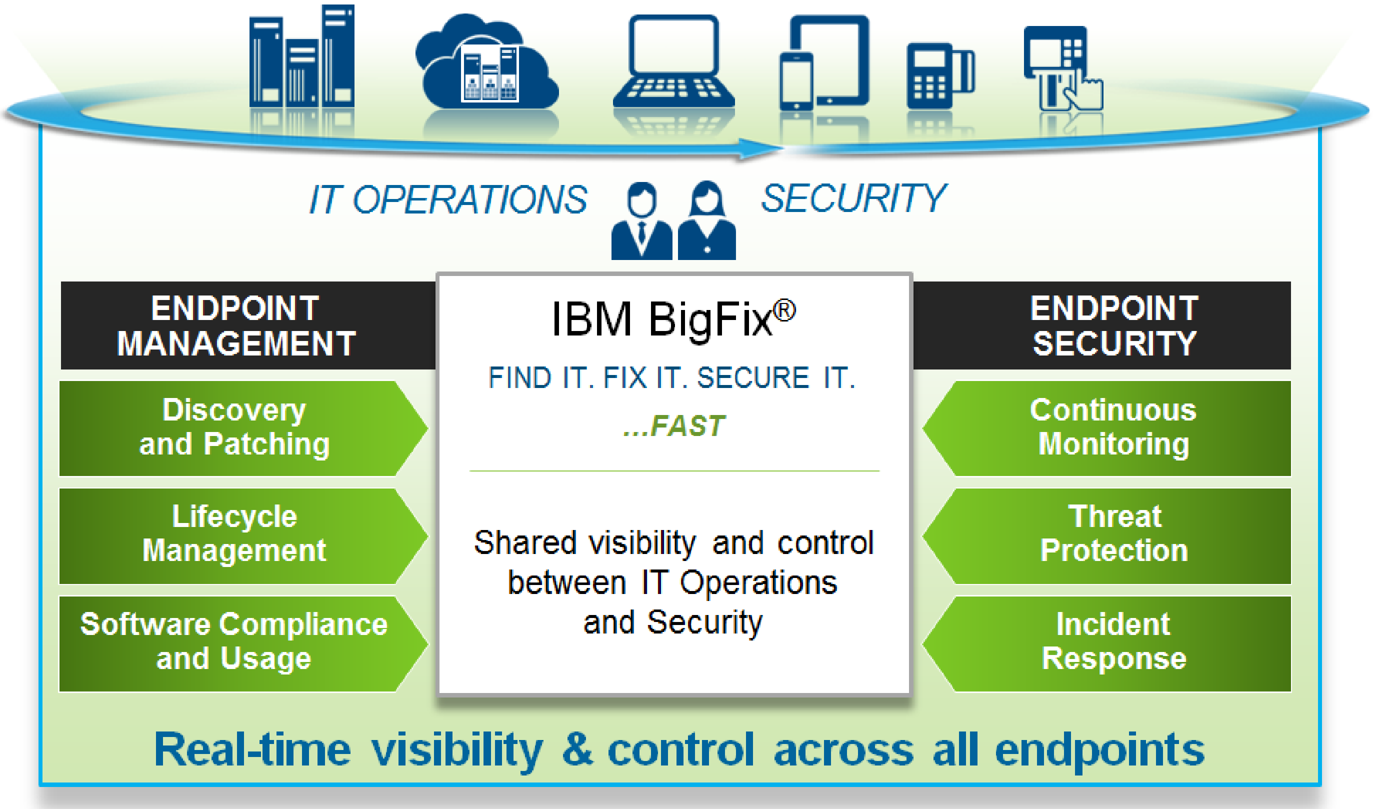
- **Siloed** security and operations teams
- **Disparate** tools and **manual** processes
- Curious users via **phishing** variants
- **Narrow** visibility into highly distributed environments

Why some approaches fail



Architecture	Complexity	Resources
▪ Slow, scan-based architectures ▪ Limited coverage ▪ Not cost-effective at scale	▪ Resource-intensive agent(s) ▪ Multiple products, multiple agents ▪ Not Internet-friendly	▪ Too much admin and infrastructure ▪ Little pre-built content ▪ Each task detracts from higher value projects

IBM BigFix: Unified Endpoint Security & Management



IT OPERATIONS *SECURITY*

ENDPOINT MANAGEMENT

- **Discovery and Patching**
- **Lifecycle Management**
- **Software Compliance and Usage**

IBM BigFix®

FIND IT. FIX IT. SECURE IT.

...FAST

Shared visibility and control between IT Operations and Security

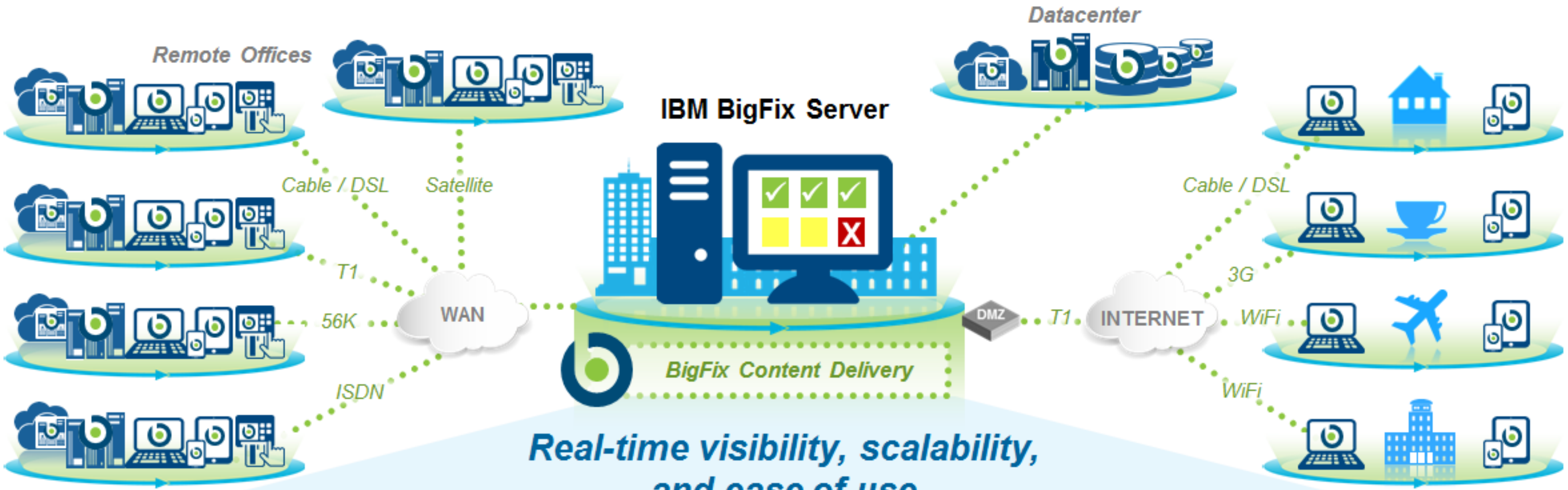
ENDPOINT SECURITY

- **Continuous Monitoring**
- **Threat Protection**
- **Incident Response**

Real-time visibility & control across all endpoints

make it
easy

How it Works



Real-time visibility, scalability, and ease of use

Lightweight, robust infrastructure

- Use existing systems as relays
- Built-in redundancy
- Support / secure roaming endpoints

Cloud-based content delivery

- Highly extensible
- Automatic, on-demand functionality

Single intelligent agent

- Performs multiple functions
- Continuous self-assessment and policy enforcement
- Minimal system impact (< 2% CPU)

Single server and console

- Highly secure and scalable
- Aggregates data, analyzes and reports
- Pushes out pre-defined / custom policies

IBM BigFix – Unified Management and Security

IBM BigFix®

FIND IT. FIX IT. SECURE IT… *FAST*

Lifecycle	Inventory	Patch	Compliance	Protection
▪ Patch Mgmt ▪ Asset Discovery ▪ SW Distribution ▪ Advanced Patching ▪ Remote Control ▪ OS Deployment ▪ Power Mgmt ▪ Sequenced Task Automation	▪ SW/HW Inventory ▪ SW Usage Reporting ▪ Software Catalogue Correlation ▪ SW Tagging	▪ OS Patching ▪ 3rd party App Patching ▪ Offline Patching	▪ Patch Mgmt ▪ Sec Config Mgmt ▪ Vuln Assessment ▪ Comp Analytics ▪ 3rd Party AV Mgmt ▪ Self Quarantine Add-on: ▪ PCI DSS	▪ Anti-Malware ▪ Firewall Add-on: ▪ Data Loss Prevention & Device Control

Available as "Starter Kit" (Patch Mgmt, Asset Discovery, SW Distribution)

BigFix Web UI

Flexibility

- Web client improves accessibility and eliminates the dependency on Windows only endpoint

Visibility

- Visibility into subscribed sites and status of endpoints

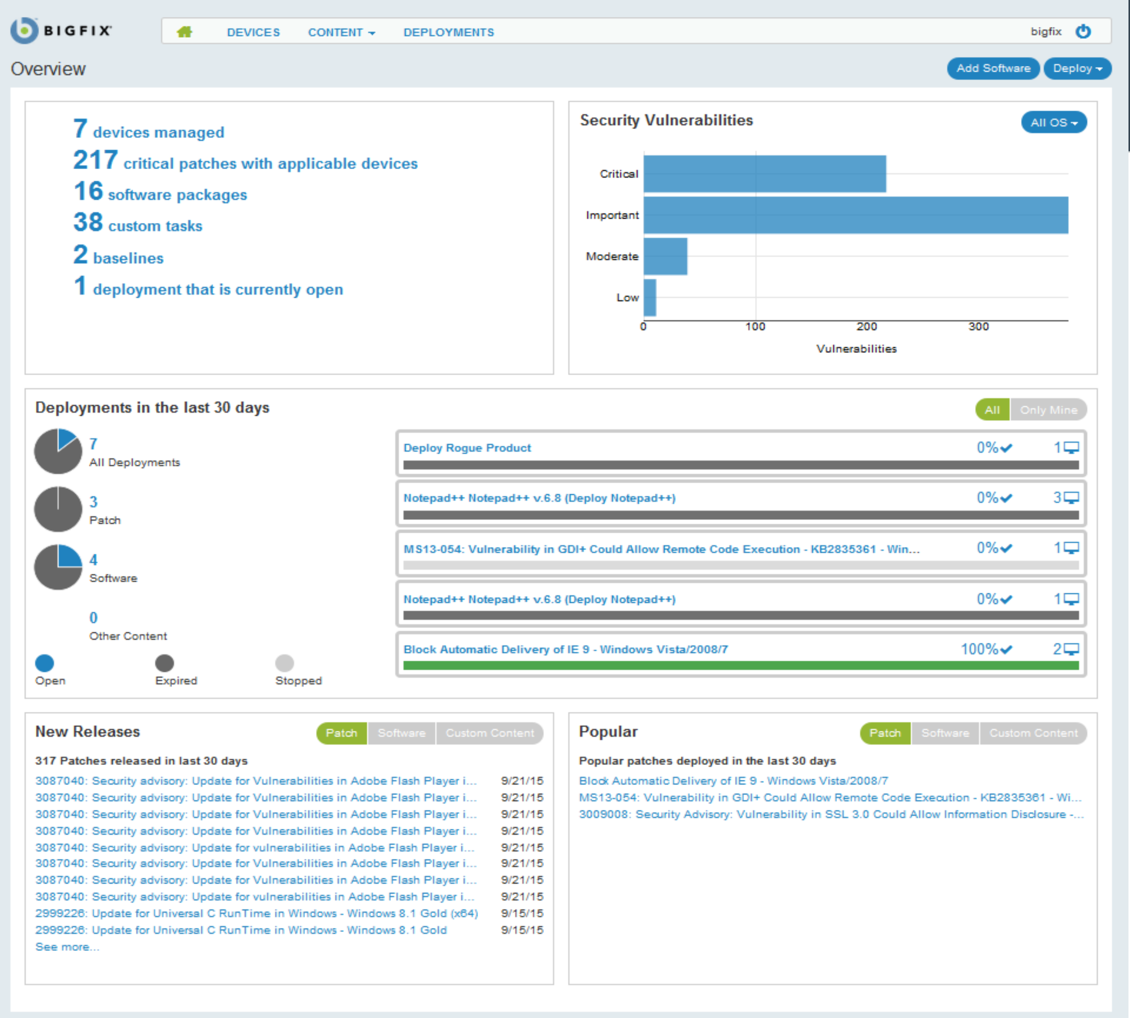
Usability

- Simplified workflow making it easier to navigate

Performance

- Faster data refresh and access

https://alpha.bigfix.com/



Overview

7 devices managed
217 critical patches with applicable devices
16 software packages
38 custom tasks
2 baselines
1 deployment that is currently open

Security Vulnerabilities

Deployments in the last 30 days

7 All Deployments
3 Patch
4 Software
0 Other Content

Deployment	Completion	Devices
Deploy Rogue Product	0% ✓	1
Notepad++ Notepad++ v.6.8 (Deploy Notepad++)	0% ✓	3
MS13-054: Vulnerability in GDI+ Could Allow Remote Code Execution - KB2835361 - Win...	0% ✓	1
Notepad++ Notepad++ v.6.8 (Deploy Notepad++)	0% ✓	1
Block Automatic Delivery of IE 9 - Windows Vista/2008/7	100% ✓	2

New Releases

317 Patches released in last 30 days

Patch	Date
3087040: Security advisory: Update for Vulnerabilities in Adobe Flash Player i...	9/21/15
3087040: Security advisory: Update for Vulnerabilities in Adobe Flash Player i...	9/21/15
3087040: Security advisory: Update for Vulnerabilities in Adobe Flash Player i...	9/21/15
3087040: Security advisory: Update for Vulnerabilities in Adobe Flash Player i...	9/21/15
3087040: Security advisory: Update for vulnerabilities in Adobe Flash Player i...	9/21/15
3087040: Security advisory: Update for Vulnerabilities in Adobe Flash Player i...	9/21/15
3087040: Security advisory: Update for Vulnerabilities in Adobe Flash Player i...	9/21/15
3087040: Security advisory: Update for vulnerabilities in Adobe Flash Player i...	9/21/15
2999226: Update for Universal C RunTime in Windows - Windows 8.1 Gold (x64)	9/15/15
2999226: Update for Universal C RunTime in Windows - Windows 8.1 Gold	9/15/15

See more...

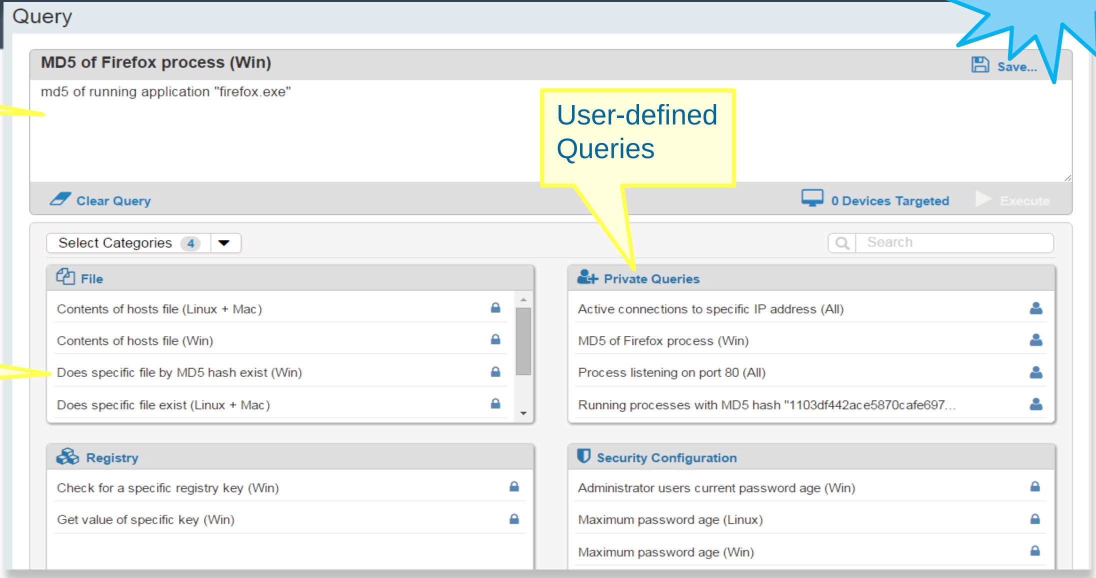
Popular

Popular patches deployed in the last 30 days

Block Automatic Delivery of IE 9 - Windows Vista/2008/7
MS13-054: Vulnerability in GDI+ Could Allow Remote Code Execution - KB2835361 - Wi...
3009008: Security Advisory: Vulnerability in SSL 3.0 Could Allow Information Disclosure -...

BigFix Query (via the BigFix Fast Query Channel)

Beta



Query

MD5 of Firefox process (Win)

md5 of running application "firefox.exe"

File

- Contents of hosts file (Linux + Mac)
- Contents of hosts file (Win)
- Does specific file by MD5 hash exist (Win)
- Does specific file exist (Linux + Mac)

Private Queries

- Active connections to specific IP address (All)
- MD5 of Firefox process (Win)
- Process listening on port 80 (All)
- Running processes with MD5 hash "1103df442ace5870cafe697...

Registry

- Check for a specific registry key (Win)
- Get value of specific key (Win)

Security Configuration

- Administrator users current password age (Win)
- Maximum password age (Linux)
- Maximum password age (Win)

Query Editor

User-defined Queries

Pre-defined Queries

Get The Right Answer, Not Just Any Answer

Rapidly interrogate endpoints with BigFix Query

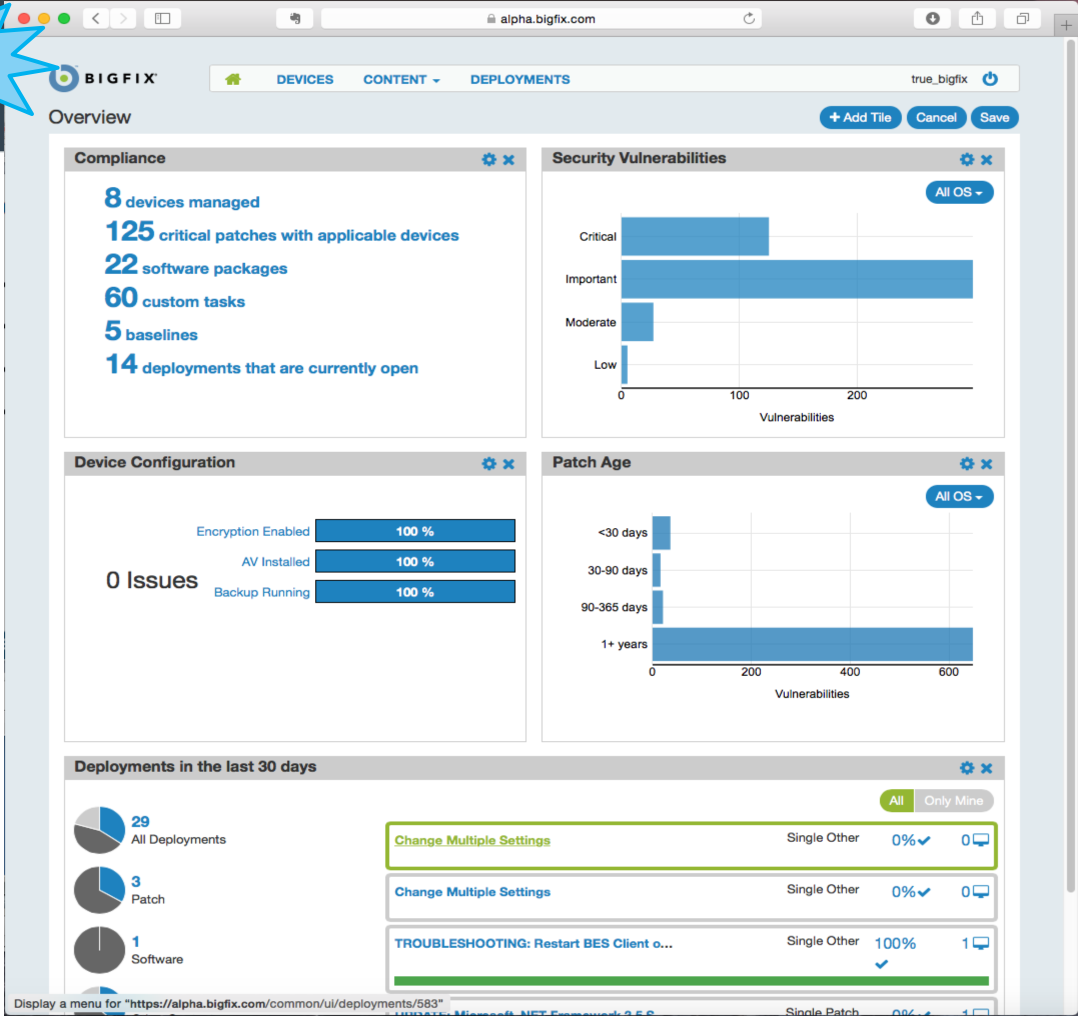
- ✓ Pre-defined queries enable rapid time-to-value
- ✓ Create and share user-defined queries
- ✓ Queries can target individual endpoints, groups or broadcast to your enterprise
- ✓ View query results in tabular format, export to CSV
- ✓ Integrations to/from BigFix Query within the BigFix WebUI
- ✓ Query execution leverages the BigFix Fast Query Channel
- ✓ Built on the power of proven BigFix relevance.

The Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision. The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract. The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.* ***Subject to IBM NDA*

CSO Dashboard

Beta

- ➢ Leverage OOTB compliance dashboards and tiles
- ➢ Customize your views leveraging structured BigFix objects
- ➢ Reporting widgets enable a range of views
- ➢ Drill-down into details of devices and security objects



8 devices managed

125 critical patches with applicable devices

22 software packages

60 custom tasks

5 baselines

14 deployments that are currently open

0 Issues

Encryption Enabled	100 %
AV Installed	100 %
Backup Running	100 %

29 All Deployments

3 Patch

1 Software

Change Multiple Settings	Single Other	0% ✓	0
Change Multiple Settings	Single Other	0% ✓	0
TROUBLESHOOTING: Restart BES Client o...	Single Other	100% ✓	1
UPDATE: Microsoft .NET Framework 3.5 S...	Single Patch	0% ✓	1

Display a menu for "https://alpha.bigfix.com/common/ui/deployments/583"

- ▪ Quickly understand the security posture of your organization

Advanced Patching – Who needs it?

Anyone with clustered servers! No more weekend Pizza Parties

Business Challenge:

- **Patching the Operating System or Application version for Clustered Windows Servers** is complicated, and can costs 100's of hours per month. (Typically involves weekend work)
- If a mistake is made in patching "mission critical applications" it can cost $Thousands to $Millions per hour.

Gov't Agency	***Before BigFix***: Manual effort for 28 3-Node clusters ***16 person days.*** ***Now***: **Less than 3 days (~80% savings) doing the same work Smarter!**
Semiconductor Company	***Pre-Prod***: Manual effort for patching Multi-Node clusters ***11.5 hours.*** ***Early POC results***: **30 Minutes (99% savings)** "…So far Bigfix is looking like a real winner !"

http://www.youtube.com/watch?v=x1LRAaFJZaI&feature=youtu.be

How a retail giant responded to the Shellshock / Bash bug

Resolving a critical issue on ~600 servers in under four hours with IBM BigFix

Managing 27,000 servers across 3,000+ locations with two IT staff

Major US Retailer

PREPARE (less than 3 hours)

- Issue discovered and teams mobilized
- Teams created necessary patch scripts within a fixlet and tested manually
- Fixlets were pushed to the BigFix server for distribution

Total Time
~ 4 Hours

SCAN (less than 30 minutes)

- Scanned and deployed to ~600 servers in less than 30 minutes
- New systems reporting online were automatically addressed within minutes based upon their group membership

DEPLOY (less than 30 minutes)

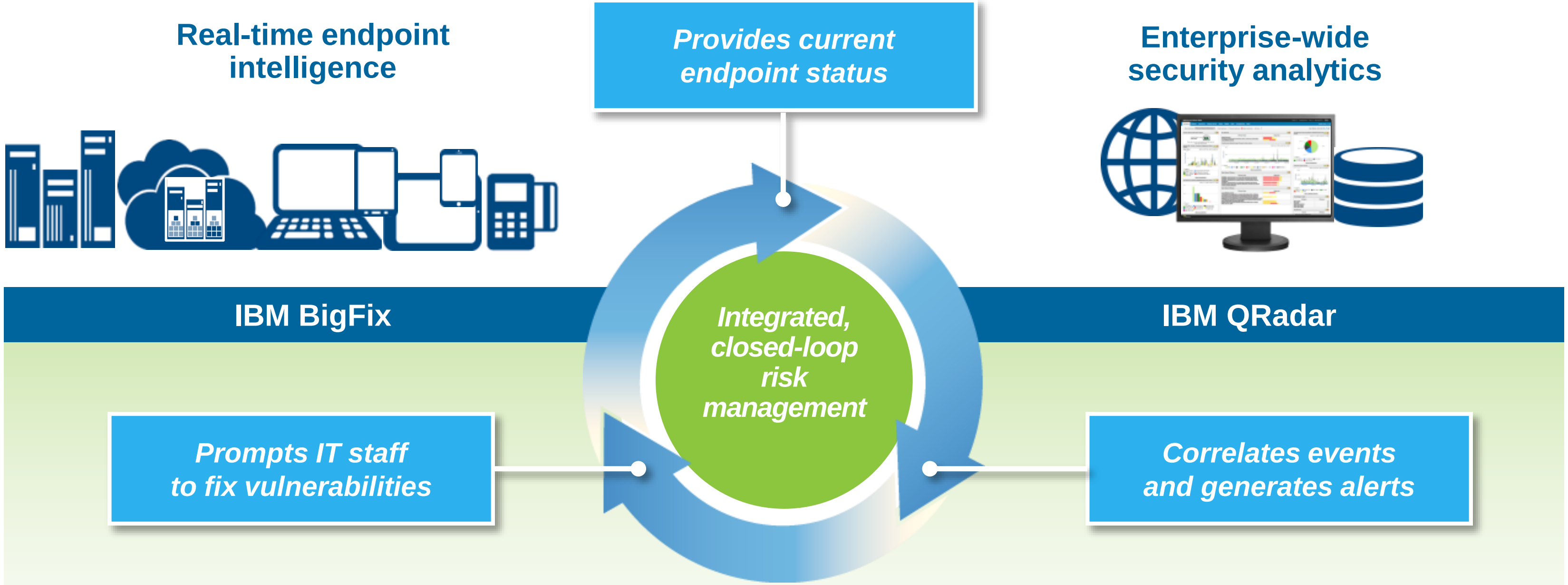
- Endpoint management team executed analysis of systems to determine which systems were vulnerable
- Corrective actions were implemented using IBM BigFix

A Race to the finish!

The BigFix team remediated 600 servers in same the time it took the datacenter team to address just 35 servers. (would have taken them 8hrs)

Major US Retailer

Prioritize risks and expedite remediation of vulnerabilities



Real-time endpoint intelligence

Provides current endpoint status

Enterprise-wide security analytics

IBM BigFix

Integrated, closed-loop risk management

IBM QRadar

Prompts IT staff to fix vulnerabilities

Correlates events and generates alerts

- Improves asset database accuracy
- Strengthens risk assessments
- Enhances compliance reporting

- Accelerates risk prioritization of threats and vulnerabilities
- Increases reach of vulnerability assessment to off-network endpoints

IBM BigFix

Find It.

Discover unmanaged endpoints and get real-time visibility into all endpoints to identify vulnerabilities and non-compliant endpoints

Fix It.

Fix vulnerabilities and apply patches across all endpoints on and off the network in minutes regardless of endpoint type or network connectivity

Secure It.

Continuously monitor and enforce compliance with security, regulatory and operational policies while proactively responding to threats

Low hanging fruit

75% of attacks use publicly **known vulnerabilities** that could be **prevented** by patching

- Think **patch management 101**
  - Endpoint & vulnerability discovery across devices, OS, location
  - Automated patching and remediation
  - Quarantine non-compliant endpoints
  - Enforce continuous compliance
- Ensure proper **password procedures**
- Implement **two-factor authentication**
- Invest in end-user **education**

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

THANK YOU

www.ibm.com/security

IBM Security

Intelligence. Integration. Expertise.