BIGFIX

CONSOLIDATE KEY SECURITY CONFIGURATION MANAGEMENT SERVICES

FROM REACTIVE FIRE-FIGHTING TO PROACTIVE, PREEMPTIVE RISK MANAGEMENT

BIGFIX IN THE REAL WORLD:
SCVM Customer stories

1. **The Problem:** A global financial services firm instituted a policy that requires users to keep sensitive documents in a specific, secure, backed-up location. Many users didn't follow the policy and kept this critical information scattered on local drives—leading to highly visible compliance issues at the highest levels of the company.

   The BigFix Solution: BigFix administrators immediately locate local files/documents for all users and automatically move them to the proper location, while keeping track of where the violation occurred and who's responsible.

2. **The Problem:** The IT staff of a federal agency manages a highly secure network of 15,000 PCs distributed globally. Federal mandates required that they gain visibility into the use of thumb drives across their network.

   The BigFix Solution: Within a few weeks of deploying BigFix, which was implemented on a single morning, IT staff was able to log the serial numbers of any thumb drive used on their network. This enables them to monitor use of the drives, minimize data leaks, and trace violations to specific personnel.

3. **The Problem:** In order to increase staff accountability, a large bank's policy states that certain computers need specific static IP addresses and that changing these addresses would result in serious compliance and security issues.

   The BigFix Solution: BigFix administrators quickly created a custom task that automatically reset a machine's IP address to the specified one anytime someone tried to change it. The result is that critical policies are continuously enforced, maintaining required configurations and managing risk.

INCREASE EFFECTIVENESS

While Reducing Cost and Complexity

When it comes to security and vulnerability management, there is a big difference between knowing what the problems are and successfully resolving or—better yet—preventing them. All enterprises want to protect their environments from threats. IT organizations struggle to balance the need to secure the infrastructure and prove compliance to industry regulations.

To answer these dual concerns—"How do I protect my environment?" and "How do I report on compliance to get approval from regulators?"—a solution is needed that provides real-time visibility and enforcement into security configurations and settings enterprise-wide. BigFix Security Configuration and Vulnerability Management consolidates services including vulnerability management, automated security configuration management, and security patch management to cut costs, reduce complexity, and lower security risks.

Product Benefits

- Increase speed and accuracy with real-time, host-based configuration management
- Use a single tool to both discover vulnerabilities and remediate them
- Take advantage of a single unified management infrastructure to coordinate more efficiently among IT, security, desktop and server operations, and other teams
- Consolidate and automate key information security services enterprise-wide
- Enjoy real-time visibility into security-critical endpoint client (desktop, mobile/laptop, server) configuration specifications
- Shorten remediation cycles—patch deployment, software updates, vulnerability fixes—from weeks to days and hours
- Extend security management to mobile clients on or off the network
- Set alarms to instantly notify administrators of anomalous conditions or suspected rogue activities

SYSTEM AND SERVER REQUIREMENTS

Supported Operating Systems for BigFix Server

- Windows 2000 Server SP 2+/2003/2008

Database Requirements for BigFix Server

- SQL Server 2000 SP4/2005

Supported Operating Systems for BigFix Console

Any of the following:

- Windows XP/2000/2003 Vista/2008

SUPPORTED OPERATING SYSTEMS

For BigFix Agent

All of the following:

- Windows
- Mac OS X
- Solaris
- IBM AIX
- IBM zLinux
- HP-UX
- VMware ESX Server
- Red Hat Enterprise Linux
- SUSE Linux Enterprise
- Red Hat Linux
- Fedora Linux

Note: Functionality may vary by supported platform. For an updated listing of supported OS versions, please see http://support.bigfix.com.

PRODUCT CERTIFICATIONS

Common Criteria Certified EAL3

cve.mitre.org

oval.mitre.org

FIPS VALIDATED 140-2
FIPS 140-2 Inside

Product Features

- Continuous enforcement of security policies for both desktop and mobile computers, regardless of network connection status
- Quickly identify rogue assets that enter the network and take steps to eliminate or otherwise locate them for remediation or removal
- Host-based vulnerability assessment with severity scoring and a 99.9% accuracy rate
- Security patch management and security updates for major operating systems and common commercially available applications
- Ability to define and assess client compliance to security configuration baselines
- Heterogeneous platform support: Windows, UNIX, Linux, and Macintosh
- SCAP certified for FDCC

SCVM Solution Components

- **BigFix Security Configuration Management** provides a comprehensive set of technical controls that help IT organizations achieve compliance and best practices goals through detecting and enforcing organizational policies on their systems.
- **BigFix Vulnerability Management** lets IT organizations discover, assess, and remediate vulnerabilities before they can exploit weaknesses.
- **BigFix Patch Management** collapses patch and update time scales, reduces staff workloads, cuts cost, and increases the effectiveness of operating system and application patch processes.
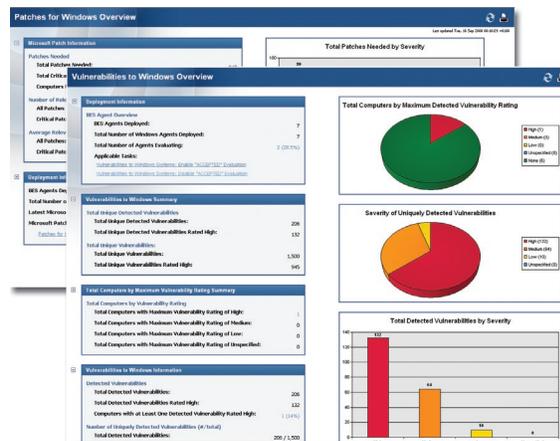
Monitor compliance in real time via customized dashboards

About BigFix

BigFix®, Inc. is a leading provider of high-performance enterprise systems and security management solutions that revolutionizes the way IT organizations manage and secure their computing infrastructures.