BIGFIX

THE RIGHT PRESCRIPTION AT CONCORD HOSPITAL

CASE STUDY

AT A GLANCE

Concord Hospital, the second busiest acute care hospital in New Hampshire, has gained multiple benefits from its BigFix installation, ranging from much improved patch compliance to hardware and software inventory.

KEY CHALLENGES

- Maintain high quality IT service levels with limited staff and budget
- Balance security needs against needs of multiple constituencies that include hospital staff, affiliated doctors and consultants and general public visiting the facility
- Gain maximum practicable visibility into all assets on the network whether manageable by Concord Hospital IT or not
- Manage to specialized healthcare legal and regulatory requirements.

CONCORD HOSPITAL
Always here for you.

IMPLEMENTATION HIGHLIGHTS

- BigFix installed on 3,300 endpoint computers at Concord Hospital and Capital Region Healthcare organization
- Patch management
- Asset inventory
- Software license tracking
- Antivirus client management
- BigFix AntiPest™ anti-spyware solution

RESULTS

- Improving from 60 to 93 percent patch compliance
- Reduced time required for patch actions from weeks to hours
- No malware outbreaks since installing BigFix in 2004
- Asset inventory supports capital budgeting and planning
- Up to 25 percent savings in software licensing costs by identifying and removing under-utilized software
- Documented assurance that PCs interacting with clinical systems meet HIPAA compliance requirements

Using BigFix to cut back on shelfware has saved the Hospital up to 25 percent on software licenses, depending on the software package.

Mark Starry,
Manager of Enterprise Security, Concord Hospital

Concord Hospital is a regional medical center that provides comprehensive acute-care services and healthcare programs to people throughout New Hampshire. Concord Hospital serves as a cornerstone for its parent company, Capital Region Health Care (CRHC), a charitable health delivery system committed to the concept of community-based healthcare.

The hospital has worked hard to cultivate a reputation for clinical and patient service excellence. As an example of its progressive approach to automating health service delivery, Hospitals and Health Networks magazine has named Concord one of the USA's "Most Wired Hospitals" every year since 2001.

Mark Starry, Manager of IT Infrastructure and Security at Concord Hospital says, "Automating healthcare delivery holds the keys to lowering costs and improving the quality of care. You can simply do everything better, from supply chain to prescription processing and evaluation, when you replace paper with bits and bytes. On the other hand, everything has to be executed from a background of absolute trust in the integrity of the systems, data and processes that deliver patient services."

The collaborative nature of Concord Hospital's relationships with various stakeholder groups—Hospital staff, affiliated professionals and general public—has led to a three level approach to managing information security at the Hospital. Infrastructure that supports Hospital-owned assets and employees can be directly managed by the Concord Hospital IT organization.

Professional affiliates can be granted conditional access to the Concord network if they meet a security dress code. The hospital provides wired and Wi-Fi Internet access to visitors and general public, but keeps this service segregated from the Hospital's enterprise network.

In 2004, the Hospital decided that it was time to opt for a dedicated patch and endpoint security configuration management solution. In its evaluation, it rejected the patch management tool bundled with the operating system on desktop PCs as it delivered very "gappy" distribution of patches and updates. In the evaluation process, BigFix differentiated itself from two other third party competitors by offering centralized administration, complete automation of patching processes on both local and remote systems, real-time visibility into patch and configuration status and potential for usages that went beyond software patching and updating.

BigFix was recommended to Concord Hospital by Xantiv, a regionally-based value-added reseller who could locally support the BigFix-based solution. "Xantiv played a catalytic role in making BigFix known to us and briefing us on how it might meet our requirements," says Starry. "While our experience with BigFix's own support and services has always been positive, it's good to work with people like Xantiv who have a long standing relationship with us."

Security Strategic Review

The widely publicized virus and worm outbreaks in 2003 triggered a major review of security at Concord Hospital. After responding to a number of malware attacks, in particular the "Slammer" worm, the Hospital recognized that it would need to upgrade its approach to endpoint security, especially its software patching processes. According to Starry, "Worms and viruses caused us nervous moments in 2003 as they slowed down our systems. It was clear we would have to step up our information security programs."

At the time, Hospital IT staff identified weaknesses in three areas: process efficiency, coverage and visibility. At the time, patches were mostly sneaker-netted around the hospital and to affiliates--time consuming, labor-intensive and error-prone process. Furthermore, audits revealed anywhere between 40-to-60 percent patch compliance on vulnerable systems, when the Hospital's internal standards called for 97 percent compliance. Finally, the Hospital lacked visibility into patch status and other critical endpoint security configuration information.

BIGFIX EVALUATION, SELECTION AND DEPLOYMENT

By all accounts, the BigFix installation at Concord Hospital has been a significant success. Concord IT staff report patch and update actions that used to require weeks to execute now transact in as little as 15 minutes, with complete visibility into progress and status. Overall patch compliance figures have gone from 40-to-60 percent to about 93 percent. Starry comments, "While 93 percent falls slightly short of our 97 percent goal, this is still a significant improvement. Furthermore, with help from BigFix, we know where the hang-ups are and are optimistic about resolving this."

In addition to using BigFix to drive an active patch and update program, the Hospital has deployed the BigFix antivirus client manager to enable it to see and control its third party antivirus software from the same BigFix console it uses for patch and update processes, asset inventory and discovery, and security configuration status reporting. Through these measures, neither Concord Hospital's operations nor its security integrity have been disturbed by any malware attacks or incidents since installing BigFix in 2004.

BEYOND SOFTWARE PATCHES AND UPDATES

Additional uses of BigFix have also paid dividends at Concord Hospital. They are starting to use BigFix to license usage and have expanded automated patch management to cover widely used applications such as Adobe document management products, Apple QuickTime, and Microsoft Office suite software. The IT staff have used the BigFix Enterprise Suite's Fixlet scripting language to perform customized tasks such as managing third party anti-virus client definition files and making adjustments to DNS server settings.

Finally, the asset inventory and reporting capabilities of the BigFix Enterprise Suite are helping the Hospital with meeting data security and privacy standards set by the Health Insurance Portability and Accountability Act (HIPAA) and other legislation. BigFix asset configuration reporting information helps assure that computers interacting with clinical systems meet HIPAA requirements for security integrity, and reliability.

SUMMING UP

Mark Starry says, “We have been very impressed with the BigFix solution and highly recommend it to colleagues in the healthcare industry. We’ve been impressed with how it has helped meet our goals and we’re finding new uses for it all the time. This may be a subtle but significant point, but one thing that really helps is that we can add to our repertoire of security configuration management services while using the now familiar BigFix console and management infrastructure. One tool set, one infrastructure, keeps learning curves flat when adding new services.”

BigFix: Breakthrough Technology, Revolutionary Economics

BigFix, Inc. offers the IT industry’s only intelligent enforcement engine that enables real-time visibility and control of globally distributed desktop, mobile and server computer infrastructures. Built on a revolutionary technology platform, BigFix continually assesses and manages the health and security of enterprise computing devices at the velocity of change.

Without requiring massive investment in dedicated management resources, BigFix automates enterprise-scale malware defense, asset management, software inventory and distribution, vulnerability assessment, policy enforcement, power conservation, and patch management, without compromising network performance, end-user productivity, or security.

BigFix delivers outstanding return-on-investment through slashing IT infrastructure costs of ownership and management complexity while enabling IT organizations to elevate security configuration management from chronic pain point to positive business value resource.