An integrated energy company reduces endpoint patch times by 86 percent

IBM BigFix solution manages thousands of endpoints across 24 time zones

Overview

The need
This integrated energy company needed to speed and strengthen its ability to monitor and patch 10,000 desktop and server endpoints across 24 time zones.

The solution
The company implemented the IBM® BigFix® solution to monitor and report endpoint status and push patches to PCs, laptops and servers across its network.

The benefit
The company reduced patch cycle time by 86 percent and consolidated its server infrastructure by 88 percent, making the environment easier and less expensive to maintain.

This integrated oil company and Fortune 100 Corporation explores, produces, transports and refines crude oil and natural gas. It operates in 23 countries and has over 10,000 employees.

Highly distributed endpoint environment

The discovery of shale oil and natural gas throughout the world has dictated where energy companies must do business and how quickly they must adapt to new business conditions.

This energy company has servers and desktops in 23 countries across 24 time zones. Such a decentralized endpoint environment, along with issues such as the 256K of bandwidth in some remote locations makes it difficult to provide a consistent and adequate level of service. "Managing our endpoints across so many locations is a real challenge," says a senior manager of global infrastructure operations for the company. "We have to reach out to many thousands of desktops and laptops, wherever they are, making sure they're patched, secure and available."

The manager explains that the company's existing Microsoft System Center Configuration Manager (SCCM) endpoint management environment became unwieldy and expensive to maintain as the company's operations expanded, requiring more than 50 SCCM servers, including six SQL servers. Moreover, it was difficult to use, unduly lengthening patch deployment times to the company's distributed environment. "To deploy a patch, it used to take anywhere from three to seven days," he says. "We needed to respond much quicker to issues with endpoints."

" … we're able to deploy a patch in as little as 24 hours, as opposed to up to seven days previously," says a senior manager of global infrastructure operations for the company.

Simplifying endpoint management

The company implemented the IBM BigFix solution to patch its laptop and desktop endpoints and more than 2,000 servers worldwide. IBM worked with the company to design the system, build the servers, install the software, train the company's server administration team and patch its servers. IBM then provided the same set of services for the desktop and laptop endpoint environment.

"We switched to IBM BigFix because its architecture is much easier to manage, much less difficult to install and run, and because it makes patching our desktops and servers so much easier," the manager says. To illustrate that newfound architectural simplicity, he points out that the company replaced its sprawling SCCM server environment with just six dedicated servers for the BigFix solution.

As for how it affected the company's patch deployment processes, the manager says his company uses the BigFix solution to produce various endpoint status reports daily, weekly and monthly. "We have one daily report that shows the status of PCs and laptops on the network," he says. "By the next day, we're able to see how many desktops were patched and how many need some form of remediation, and we're able to deploy a patch in as little as 24 hours, as opposed to up to seven days previously. If an endpoint is missing BigFix, we install it in 30 minutes. BigFix is simply easier to use and maintain than SCCM, and it works."

Managing endpoints, consolidating infrastructure

- Reduces patch cycle time by 86 percent
- Consolidates server infrastructure by 88 percent
- Centralizes control over thousands of endpoints worldwide

Solution components

Software
- IBM® BigFix®

Take the next step

To learn more about the IBM BigFix solution, please contact your IBM representative or IBM Business Partner, or visit the following website: **ibm.com**/security/bigfix

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.

WGC12427-USEN-00