Brit Insurance enhances vulnerability management

With IBM Tivoli Endpoint Manager for Patch Management

Overview

Business challenge

Brit Insurance faced a large volume of security patches without which the infrastructure would have myriad 'critical' vulnerabilities. The company had used Microsoft Windows Server Update Services (WSUS) to apply the patches missing from its workstations, but needed an automated tool capable of a controlled rollout of patches to its large server landscape.

Solution

As part of a broader vulnerability management exercise, Brit Insurance selected IBM® Tivoli® Endpoint Manager for Patch Management, built on BigFix® technology, to automate the rollout of operating system patches to its estate of 750 Microsoft Windows servers. When this first stage is complete, the company will also use the solution to automatically deploy non-Microsoft patches (currently done manually).

Brit Insurance is an international general insurance and reinsurance group specialising in commercial insurance and today employs around 750 people. The company has offices in a number of countries around the world, including the USA, Australia and Japan, and hosts the bulk of its business-critical applications and data in its UK data centre.

The IT infrastructure – and, in particular, the server infrastructure – at Brit Insurance had grown rapidly, but security management practices struggled to keep pace with the increasing burden of applying security software patches across the server and workstation estate. Initially the Administrators used the Microsoft WSUS tool to apply operating system patches to the workstations, but this solution did not automate the patching of non-Microsoft software nor provide vital management information. More importantly, it addressed only end user devices; it was less suited to servers.

"We are bound by FSA and Information Commissioner's Office regulations to be secure – and having demonstrable controls is a requirement for compliance , relying on other protective layers such as firewalls and anti-virus is arguably insufficient" says Brit Insurance's Group Security Manager. "Caught between the volume and frequency of security patches on one side, and staffing pressures on the other, it was clear that we required significant automation to constrain costs and increase accuracy, and enable us to better manage the risk of rolling out patches across the production server environments."

Automated solution

After running an internal exercise to determine the functional and non-functional requirements, Brit Insurance worked with Gartner Group to review possible solutions. Weighted scores were created for each option, and products scoring lower than 70 percent against requirements were rejected. The five vendors on the eventual shortlist were invited to present their solutions to the Brit Insurance team. Key requirements included: the ability to uninstall unsuccessful patches, the ability to automate third-party patching in addition to operating system patching, and ease of use.

Business Benefits

Having the correct patches in place reduces security risks and strengthens compliance with external security guidelines. Using the IBM Tivoli solution, Brit Insurance has been able to tackle its security issues without significant administrative effort and in a controlled, relatively low-risk, non-disruptive manner.

"Conceptually, software patching is an element in vulnerability management," says the Group Security Manager. "There are two pillars in that – detection and response – and we selected IBM Tivoli Endpoint Manager for Patch Management as our second pillar."

Brit Insurance's specialised requirements for patching meant that it was not simply an out-of-the-box solution. Rather, Brit Insurance worked with Tivoli consultants to customise the solution. "Tivoli Endpoint Manager is an automated solution as standard, but we needed fine-grained control over which servers receive patches and when," comments an Infrastructure Manager at Brit Insurance. "We agreed some consultancy time with Tivoli to get the automation side of things in place. Rolling out the software for our workstations was much more straightforward, as we were simply replacing an existing tool – WSUS – rather than introducing a whole new approach, as we were with the server landscape."

Staged rollouts

While Tivoli Endpoint Manager would be capable of automatically deploying relevant patches to the entire Brit Insurance server estate overnight, the company needed to mitigate the risk of business disruption caused by patch conflicts.

"The most important lesson we learnt from the initial workstation patching exercise was not to patch all in one go," says the Group Security Manager. "Our appetite for risk in the server environment is low, so we're taking a measured approach that deploys patches to selected groups of servers in a series of staged rollouts."

Brit Insurance has created several groups of servers in Tivoli Endpoint Manager, called test, bulk 1, bulk 2, bulk 3 and control. Patches are automatically rolled out to the test group first, and any negative effects are noted and resolved. The patches are then deployed to each of the remaining groups in turn. "By staging the patching using Tivoli Endpoint Manager, we pragmatically reduce the risk of disruption to production systems because it is impractical to regression-test each application per patch" says the Group Security Manager. "By being seen to take a pragmatic approach to reduce risks, we also safeguard confidence in our broader programme of security initiatives."

The infrastructure team is now adding servers to the 'monthly conveyor belt', choosing the appropriate group based on an assessment of each individual server's specific risk profile. "Where we have an application that is deployed across test, development and production servers, we might put test and development in an earlier group, and production in a later group," says the Infrastructure Manager. "For a resilient clustered server environment, we could choose to put one of the production servers in an early group, and the other in a later group. In both cases, if a patch breaks something, we have a chance to rectify the situation before any real damage occurs."

Solution Components

Software

- IBM® Tivoli® Endpoint Manager for Patch Management

"Crucially, having the Tivoli solution in place means that we can patch business-critical production servers in a controlled, automated way, with relatively little effort. It reduces the patching risks, and enables me to enforce security standards more rigorously across the application teams."

— Group Security Manager, Brit Insurance

Brit Insurance is using Tivoli Endpoint Manager to provide management information on the number of servers in each deployment group and the overall status of the rollout. Equally, the solution provides compelling visualisations of status for non-technical managers. "We can also easily see who is logged into any workstation – a capability we didn't have before," adds the Infrastructure Manager. "And we can quickly see which servers are running short of disk capacity; we have other system monitoring tools that can do this, but it's quicker and easier with Tivoli Endpoint Manager."

Secure operations

The deployment of IBM Tivoli Endpoint Manager for Patch Management has transformed software patching at Brit Insurance. In the past, each server would be fully patched when initially deployed, but would then lose currency. Servers would receive occasional ad-hoc patches – but with 125 servers to each administrator, Brit Insurance struggled to manage the problem. With the Tivoli solution, servers receive new Windows patches within a month of publication by Microsoft, or immediately when facing an imminent threat.

Brit Insurance's focus will now switch to patching non-Microsoft software such as Java and Adobe Acrobat. These non-Microsoft patches will also be managed using the Tivoli solution.

"Security drove this project, but the most visible benefits are in other areas such as reliability and consistency," says the Group Security Manager. "Crucially, having the Tivoli solution in place means that we can patch business-critical production servers in a controlled, automated way, with relatively little effort. It reduces the patching risks, and enables me to enforce security standards more rigorously across the application teams."

The Infrastructure Manager concludes: "Now that more and more of our servers are fully patched, we have fewer unexplained reliability issues, and far greater confidence in the overall security and reliability of our servers and workstations."

For more information

To learn more about IBM Tivoli Endpoint Manager for Patch Management, contact your IBM sales representative or visit: **ibm.com**/software/tivoli/solutions/endpoint

IBM United Kingdom Limited
PO Box 41
North Harbour
Portsmouth
Hampshire
PO6 3AU

Produced in the United Kingdom
September 2011

Please Recycle

Tivoli® software

TIC14198-GBEN-01