Softcat Takes the Sting out of Perpetual Patching with Ivanti Patch for Windows

Profile:
A leading provider of technology solutions and services

Location:
Marlow, England

Industry:
IT

Website:
https://www.softcat.com/

Solutions:

- Ivanti® Patch for Windows

Benefits:

- Ends the 90-day WSUS patching cycle and reduces time to patch critical servers by 72 days
- Provides scanning, deployment, and reporting that helps ensure patches were applied
- Cuts patching overhead dramatically, allowing admins to focus on larger security issues

If you wish to remain a leading Managed Services Provider of technology solutions and services, you must defend against software vulnerabilities in your infrastructure. However, with the company growing at unprecedented rates, the Managed Services Team at Softcat faced managing a sprawling estate of 200 Windows servers that lacked a consistent, automated patching solution.

In response, Softcat created an Information Security team to compile best practices that would help it maintain control over this critical process—practices it planned to share with equally overwhelmed customers.

"Our situation was typical of a fast-growing Windows organization," Softcat's security analyst Tim Lovegrove says. "We deployed WSUS to assist with Windows patching, but it was hard to administer and track, even on updates to the Windows OS, and harder still across our critical third-party applications. We wanted to know that every machine on the network would receive essential updates automatically."

A key issue, only 25 percent of Softcat's servers had been assigned owners with responsibility for patching the server. Like most WSUS deployments, Softcat had used Group Policy settings to assign machines but not to determine ownership.

Moving from an All-Consuming Patching Cycle

The WSUS patching cycle also took 90 days to complete, which was too long in today's fast-moving world and opened the door to risk. Each quarter it took Softcat's Microsoft system admins a month to identify and schedule the appropriate WSUS patches to ROLL OUT, and then another two months to complete the deployments. At the end of each 90-day window, the patching cycle began again.

The 2017 ransomware outbreaks were the final catalyst for change. Although Softcat had patched the vulnerabilities months before, the events escalated the 'What If' debate to senior management.

As Lovegrove recalls, "Our Managed Services teams were heavily involved in helping customers recover from ransomware attacks last year, often working 24x7 shifts. Although Softcat itself was unaffected, we witnessed firsthand the effects of neglecting updates. That led us to examine our own internal procedures for patching, escalating the issue to the forefront of our network and security efforts."

The solution needed to achieve three goals: 1) significantly reduce patching overhead, 2) decrease the patching cycle from 90 to no more than 30 days, and 3) automate as much of the process as possible and provide proof patching had occurred.

With Any Automation, Success Lies in the Detailed Preparation

Softcat ships thousands of Ivanti Patch for Windows licenses to its customer base and receives positive customer feedback. Given the solution's high regard, Softcat chose to deploy it internally within 30 days of testing it in the lab. Upon deployment, Patch for Windows scanned the Softcat estate. This provided a complete software inventory and immediately determined that 25 servers were redundant and no longer in use.

For the remaining 175 servers, the next stage was to assign server ownership within the 10 teams that run those servers. Armed with the asset inventory, Lovegrove offered owners six options for scheduling patches. They picked the option most appropriate to the role the server and its apps played in the organization, and that determined the machine groups for Ivanti's automated patching treatment. Reporting levels were also established, offering a central view and reports on deployed patches, missing patches, and vulnerable machines.

Ivanti Patch Offers Flexible Options to Fit the Server's Purpose

Softcat estimates it has reduced patching overhead by 70 percent while increasing patching coverage. This includes third-party apps such as Java and Adobe Flash and Reader, and browsers such as Firefox, which are so often missed in a server estate. For the company's most critical servers, Patch for Windows reduced the patching window from 90 to under 18 days.

Lovegrove notes: "It's definitely a timesaver. Knowing this is in my back pocket, I can focus on wider or more esoteric security issues, instead of spending time fiddling around with what should be a simple process." And adherence to the three KPIs has earned Lovegrove's team the confidence of Softcat senior management.

Lovegrove summarizes his experience for others facing patching overhead: "Ivanti Patch for Windows isn't just a more comprehensive patching solution. It's an intelligent, granular solution that offers the flexibility to specify patch groups and categories and provides the visibility needed to help ensure patches get deployed."

Note: Softcat's results are specific to its total customer environment / experience, of which Ivanti is a part. Individual results may vary based on each customer's unique environment.

Learn More


www.ivanti.co.uk


+44 (0) 1344 442100


sales@ivanti.com