Ivanti helps the Bott Group prevent most cyber attacks

Profile:
A leading manufacturer of workshop equipment, in-vehicle equipment, and workplace storage solutions

Location:
Bude, Cornwall, UK

Industry:
Manufacturing

Website:
www.bottltd.co.uk

Website of Partner:
http://satisnet.co.uk

Solution:
Ivanti® Patch for Windows

Benefits:

- Automated patch management for the Windows OS and third-party applications
- Tools that deliver on the UK's Cyber Essentials framework for better cybersecurity
- Time to concentrate on core business goals

A world leader in the manufacture, installation, and fit of professional workplace storage solutions, the Bott Group provides services to 10,000 customers worldwide. That means it must protect an equally impressive collection of workstations and servers to keep corporate and personal data private. Bott wanted to comply with the UK government's Cyber Essentials controls to safeguard government contracts as well as attract new private sector business. Like other respected cybersecurity frameworks, the UK government endorses back-to-basics controls like patching, privilege management, and secure configuration that could prevent around 80 percent of cyber attacks.

Better patch management

Moving from Microsoft Windows Server Update Services (WSUS) to a patch management solution with increased visibility and a more robust feature set would help pave the way for Cyber Essentials certification. Certification requires Bott to demonstrate ongoing patch management across the organization to help keep software up to date and eliminate vulnerabilities before they're exploited.

After an onsite demonstration by cyber threat management provider Satisnet Ltd, Bott adopted Ivanti® Patch for Windows due to its ease of use and rich security tools. Its underlying scanning engine performs security patch and hotfix assessment with detailed granularity. It captures missing patches and more, including logging the appropriate security bulletin name, detailing the files in each hotfix, and applying only the latest patches, not those that came before.

Shaun Parnell, Bott's Information Technology Technician in Bude, recalls: "There simply wasn't another product with the capabilities and ease of use of Ivanti Patch for Windows. We rely on it for centralized patch distribution every two weeks to meet our Cyber Essentials obligations.".

From a central console the solution scans for all available patches and flags which OS patches and application updates are available since the last refresh. It prioritizes critical patches and the distribution policy is set for after work hours. Patch for Windows can scan all endpoints at all sites, deploy patches, and initiate a blanket shutdown following successful deployment. When users return to work, they're unaware an update was applied. The solution also minimizes bandwidth consumption because Patch for Windows downloads the patches just once.

"Patch for Windows automates and schedules patching, so we stay focused on other projects and users get their work done without disruption. It's also easy to prove compliance," said Parnell.

Reporting back on the success of each update is the final Cyber Essentials requirement, and Patch for Windows lets Bott know exactly which apps and versions are running across its Microsoft estate. The solution also helps identify if someone downloaded an unauthorized application. Using Patch for Windows' reporting functions, Bott can pinpoint who, what, and when—and remediate appropriately.

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

 **www.ivanti.com**

 **+1-888-253-6201**

 **sales@ivanti.com**