The Co-operative Food enhances PCI DSS compliance

Boosting endpoint security with more effective patch management

The co-operative

Overview

The need

The Co-operative Food wanted to develop a more unified approach to patch management, in an effort to improve compliance with PCI DSS standards and enhance security across its retail network.

The solution

The IBM® BigFix® solution helps the company to centralise and streamline the patching process, delivering more effective patch management for an endpoint environment comprising some 19,000 devices.

The benefit

Near-real-time, automated patch discovery and management helps ensure that endpoints maintain appropriate patch levels. Integrated reporting helps demonstrate compliance with PCI DSS requirements.

The Co-operative Group Ltd. is a British consumer cooperative, wholly run and owned by its members. It is the largest organisation of its kind in the Europe, with over six million members. The group comprises a diverse range of businesses, the largest of which is The Co-operative Food: a chain of food and convenience stores employing some 70,000 people.

The Co-operative Food's retail estate is vast, and encompasses approximately 2,800 stores across the UK. The company manages an extensive network of endpoint devices, including tills, servers and back-office workstations, which are essential to the smooth running of daily business.

Achieving PCI compliance

As a company in the retail sector, it is vital for The Co-operative Food to maintain compliance with the Payment Card Industry Data Security Standard (PCI DSS), which was created to increase controls around cardholder data to reduce credit card fraud. PCI DSS requires all retailers accepting payment cards to comply with a number of standards, one of which is ensuring that all endpoint devices have the latest security patches installed. All critical security patches must be installed within one month of release.

To help The Co-operative Food to take full advantage of the range of capabilities offered by the BigFix solution, IBM ran a four day training course for members of the IT department's support function. "The training provided by IBM was excellent," states Neil Wakefield, System and Process Change Manager, The Co-operative Food. "I have never seen a more enthused group of people return from a course."

Solution components

Software
- IBM® BigFix®

Neil Wakefield, System and Process Change Manager at The Co-operative Food, explains: "In the past, we did not have a joined-up way of patching our tills and other endpoint devices. We only applied patches when we needed to bring a particular till image up to date. As part of our efforts towards PCI DSS best practices, we realised that we needed to radically overhaul our approach to patch management if we were to improve compliance and avoid penalties."

The Co-operative Food recognised that improved patch management would also help to drive greater efficiency in its IT environment. With a comprehensive patching strategy, the company would be able to obtain near-real-time information on software and hardware versions, and reduce the amount of effort involved in keeping its vast endpoint estate patched and compliant.

Selecting a comprehensive patch management solution

The Co-operative Food commissioned Gyrocom Limited to perform an evaluation of patch management solutions on the market. After reviewing offerings from five vendors, Gyrocom presented The Co-operative Food with two final options, one of which was the IBM BigFix solution.

"IBM was the clear front-runner and made our decision an easy one," notes Wakefield. "The IBM team offered us a proof-of-concept demonstration free of charge: we installed BigFix on our own server and used it to manage a small number of endpoints. We immediately recognised the capability and value of the solution and moved forward with a pilot phase."

The Co-operative Food negotiated a deal with IBM, which stipulated that the company would not have to commit to a full licence for the IBM software until the pilot phase was completed. This helped to mitigate the business risk of investing in the new solution. The Co-operative Food signed a full contract with IBM in early 2012 and began a full roll-out of the BigFix solution soon afterwards.

"With IBM BigFix we will be able to guarantee that all of our endpoints are patched appropriately, and we will be able to provide solid proof that we have a regular, fully documented patch process in place. This will be a huge step in helping us to move closer to full PCI DSS compliance."

—Neil Wakefield, System and Process Change Manager, The Co-operative Food

The company is nearing the final stages of the implementation, with the BigFix solution now providing comprehensive coverage for more than 18,500 endpoint devices. The solution places a single intelligent agent on each endpoint, which sends regular messages to a central management server and pulls patches and configurations to the endpoint when necessary to comply with a relevant policy.

As a result of the agent's intelligence and speed, the central management server always knows the compliance and change status of endpoints, enabling rapid and up-to-date compliance reporting.

Solid training from IBM

To help The Co-operative Food to take full advantage of the range of capabilities offered by the BigFix solution, IBM ran a four day training course for members of the IT department's support function. "The training provided by IBM was excellent," states Wakefield. "I have never seen a more enthused group of people return from a course."

The Co-operative Food plans to create a small group of super users who will then be able to train more users internally to use the new software. Wakefield adds: "We anticipate that it will be an easy sell to bring new users on board with BigFix, given the incredibly positive response that we have seen so far."

Improved endpoint visibility and control

The IBM BigFix solution provides The Co-operative Food with a comprehensive solution for patch management that allows the company to see, change, enforce, and report on patch compliance status in near-real time, through a single console.

The solution will significantly change the way that The Co-operative Food approaches patch management, offering a unified strategy for handling the discovery and deployment of patches, helping to ensure greater patch compliance and saving valuable time and resources.

Wakefield explains: “In the past, our patch discovery process involved creating a bespoke dial to discover what software and operating system versions our tills were running. We had to manually repeat this audit whenever we needed to upgrade a certain till, and the process would typically have to be run overnight. While this was not a particularly difficult task, manually auditing thousands of tills could become very tedious.

“In comparison, BigFix offers us real-time information on the patch status of every device from a single point of control. Now we can instantly obtain the compliance and change status of all our endpoints, which will dramatically improve security and management across our network.”

The solution eases the management burden for IT staff by continuously enforcing patch policy compliance. Instant access to the patch status of each device reduces the time and effort that the company’s deployment team spends on monitoring and managing endpoints.

In the future, The Co-operative Food plans to extend the solution to manage software updates for its tills. This will build on the value of the BigFix system, helping ensure that all point-of-sale devices are regularly maintained with the latest software versions.

Enhanced reporting and regulatory compliance

Integrated BigFix reporting capabilities allow The Co-operative Food to access up-to-the-minute dashboards and reports that provide a global view of its endpoint environment, indicating which patches were deployed, when they were deployed and to which devices. This enhanced reporting ability helps The Co-operative Food to provide solid documentation that its retail network is compliant with current PCI DSS patching requirements.

The BigFix solution can help ensure compliance with PCI and other standards automatically, with a comprehensive library of more than 5,000 "out of the box" compliance rules. By reducing the need for manual detection and remediation to bring devices back into a compliant state, the BigFix solution can significantly reduce the risk and cost of maintaining constant compliance.

"In the past, we simply did not have a consistent approach to patching, full stop," remarks Wakefield. "With IBM BigFix, we will be able to guarantee that all of our endpoints are patched appropriately, and we will be able to provide solid proof that we have a regular, fully documented patch process in place. This will be a huge step in helping us to move closer to full PCI DSS compliance."

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

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

Produced in the United Kingdom
July 2015

References in this publication to IBM products, programs or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program or service is not intended to imply that only IBM's product, program or service may be used. Any functionally equivalent product, program or service may be used instead.

All customer examples cited represent how some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication is for general guidance only.

This document is current as of the initial date of publication and may be changed by IBM at any time.

It is the user's responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Please Recycle

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.

WGC12440-GBEN-00