DCM Infotech

Case Study

Professional Services

Managed Patching Services across 20000 end points and ensured Zero Malware related work disruptions

Our client is a North America based IT automation giant. They operate from more than a 50 locations in North America. In additions to their offices they also have a field force which is spread across the United States and Canada.

We were already providing them with managed services on the complete stack from the operating system (IBM AIX, MS Windows), networks, storage(IBM/EMC), mail (Lotus Domino) databases (Oracle) hypervisor (VMWare), service desk (ServiceNow).

Company Overview

Launched in Japan, Ricoh has been in business since 1936

Ranks 335 in the list of Fortune 500 world's largest corporations

Industry leader with 90,141 employees and annual

IT Environment

Complete stack from the operating system (IBM AIX, MS Windows),

Linux server

Databases (Oracle) hypervisor

CHALLENGES

Incumbent tool put a large load on the network and had low first time patch

Availability of skilled resources on the IBM Bigfix tool and increasing operational cost

Time consuming vulnerability assessment

SOLUTIONS

Customer achieved Zero GAP on compliances of the patches.

Well-defined Change Management process

Constant monitoring release of new patches.

IMPACT

Suggested HCL Bigfix

They reduced annual software spend by assessing application usages.

The Operational costs have been kept in control there is better compliance as well.

MANAGED PATCHING SERVICES ACROSS 20000 END POINTS AND ENSURED ZERO MALWARE RELATED WORK DISRUPTIONS

Being a multi-billion-dollar public limited entity they have a lot of compliances to be adhered to from a licensing standpoint. In addition, they also wanted to ensure that non-compliance does not cause operational challenges. So they wanted to be sure that all their software was updated with the necessary patches and known vulnerabilities taken care off.

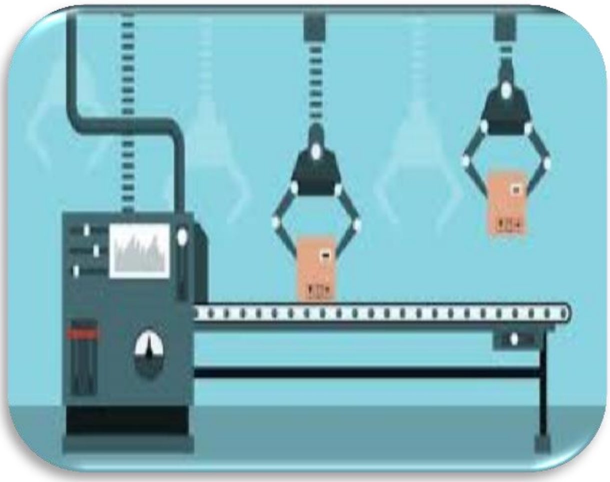
Customer was using different tool to manage inventory of their IT assets and to do patch management of their end points. This tool had been used by the customer for more than 4 years and they were looking to do a Tech-Refresh since the workloads had changed. They were now using more Apple desktops and Laptops and Linux servers.

The architecture of the incumbent tool put a large load on the network and had low first time patch through rates.

CHOOSING THE RIGHT SOLUTION

Based on the ask of the customer and after evaluating various options, the customer decided to go in for solution based on IBM BigFix. While evaluating a tool and buying it is a long drawn process, the objective of the tool is to get an outcome. In this case the customer wanted to ensure that vulnerabilities are continuously identified and systems patched to ensure that there is no disruption of work due to any malicious attack.

We initially had an architect onsite to handle any teething issues but as the things moved we handled everything from our offshore center in India. Patches can make systems unstable sometimes.



Given the plethora of software and the quantity of end points we set up a test-bed at the customer facility where a combination of standard sample hardware and typical software, that they use, was set-up. This ensured that in case there were any issues on the test bed then the roll-backs can be done quicker. Once something runs successfully then the patches are sent out into all the specified set of machines. Since different software vendors come out with patches at different frequencies and not all patches are available from the IBM site directly, our team monitors for new patch release and then builds the fixlets using Rest APIs.

By having people constantly monitoring the release of new patches by the software vendors, our team ensures that there is no gap in the knowledge of known vulnerabilities at the customer site.

Our managed IT services team has a well-defined Change Management process which has been built in coordination with the customer. Based on the availability of patches from the software vendor, the team coordinates with the application owners, users etc. Once they receive an approval the team builds the fixlets and deploys on a test bed. Once the test bed is stable then the roll-out takes place across the complete environment.

THE BENEFITS

With the migration to IBM Bigfix, customer was able to achieve Zero GAP on compliances of the patches. They reduced annual software spend by assessing application usages. With the dedicated team in place they have had zero loss of productivity due to malware attacks. The Operational costs have been kept in control there is better compliance as well.