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

Highlights

- *Identified and provide accurate, real-time information about your endpoints — regardless of operating system, location or connectivity.*
- *Reduced annual software spend by assessing application usages*
- *Zero loss of productivity due to malware attacks.*
- *DCM's large team of certified BigFix engineers helped the customer get a faster RoI*

The Client:

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) hyperviser (VMWare), service desk (ServiceNow).

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.

Challenges:

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

The cost of skill and time involved to perform vulnerability assessment for the plethora of applications across all the end points was enormous.

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

Suggested 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

Contact Us

India:
316, Udyog Vihar,
Phase-II,
Gurgaon- 126016

USA:
39159 Paseo Padre Pkwy
Suite 303, Fremont,
CA 94538

Email us:
sales@dcminfotech.com

Visit us:
www.dcminfotech.com

Version - 2019/C07/1.0

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:

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