

Patch Management Implementation

Implementing BigFix for Efficient Patch Management in an International Travel Service Provider

Our customer is an international travel service provider specializing in airline ticketing, hotel booking, and taxi bookings for B2B clients. They cater to multinational corporations (MNCs), managing bookings for their employees who provide personal and travel details. This sensitive information necessitates robust security measures to protect against potential breaches.

Company Overview

Specializing in airline ticketing, hotel booking, and taxi bookings for B2B clients

Operates in over 100 countries across the Americas, Asia Pacific, Africa, Europe, and the Middle East.

Recognized as a leading global travel management company in various industry awards.

IT Environment

200 Virtual Machines (VMs)

1500 PCs (Windows OS)

Windows and a few Linux servers



CHALLENGES



Prolonged patch cycles increase vulnerability risks.



Multiple locations made coordination and timely updates challenging.



Continuous Patch Releases: Monthly Microsoft updates kept the team behind schedule.

SOLUTIONS



BigFix automates seamless patching across environments.



Comprehensive Deployment: BigFix agents installed, servers configured, patches automated.



Training and Ongoing Support: IT team received training, ensuring continuous assistance.

IMPACT



Achieved compliance within 30 days, ahead of the next patch release.



Kept systems up-to-date, reducing vulnerabilities and ensuring compliance.



IT team members received thorough training & ongoing support on BigFix usage,

Case Study | Patch Management

USING BIGFIX FOR PATCH MANAGEMENT IN GLOBAL TRAVEL

TECHNICAL CHALLENGES IMPACTING THE BUSINESS

The primary challenge was ensuring all end-user devices and servers were patched for known vulnerabilities. The manual patch management process was time-consuming and inefficient, focusing first on Zero Day vulnerabilities and then other patches. Key issues included:

- **Extended Patch Cycles:** It took over 80 days to achieve compliance, leaving systems vulnerable. This was a major concern for the customer, since it could impact their business directly. (As per an annual report from CISA, detailing the top exploited vulnerabilities. In 2023, many of these were zero-day vulnerabilities, emphasizing the importance of timely patching.)
- **Geographically Dispersed Operations:** Multiple locations added complexity to the patching process.
- **Continuous Patch Releases:** Monthly patches from Microsoft meant the team was perpetually behind schedule.

II a. Importance of Patching

Patching is crucial for maintaining the security and functionality of IT systems. Here's why:

- **Security:** Patches fix vulnerabilities that could be exploited by hackers to gain unauthorized access, deploy malware, or steal data.
- **Compliance:** Regular patching helps organizations comply with industry regulations and standards, avoiding potential fines and legal issues.
- **Performance:** Updates often include performance improvements and bug fixes, ensuring systems run smoothly.

II b. How Hackers Exploit Known Vulnerabilities

Hackers actively seek out and exploit known vulnerabilities to compromise systems. Here's how they do it:

- **Zero-Day Exploits:** These are vulnerabilities that are exploited before the vendor has released a patch. Hackers use these to gain initial access to systems.
- **Publicly Known Vulnerabilities:** Even after patches are released, many systems remain unpatched. Hackers exploit these known vulnerabilities to infiltrate networks.
- **Exploit Chains:** Hackers often use multiple vulnerabilities in sequence to escalate privileges and move laterally within a network.



CHOOSING THE RIGHT SOLUTION AND MEETING THE DEADLINES

To address these challenges, the customer evaluated various patch management solutions. BigFix was chosen for its ability to automate the entire patch management process across both test and production environments and across different operating systems without a challenge.

Implementation of BigFix

The implementation of BigFix involved several critical steps:

- Assessment and Planning
- Deployment
- Automation and Testing

THE BENEFITS

The implementation of BigFix yielded significant improvements:

- **Reduced Patch Cycle Time:** Achieved compliance within the 30-day cycle, well before the next sets of patches were released.
- **Enhanced Security:** Ensured all systems were up-to-date with the latest security patches, reducing vulnerability exposure. This had a direct impact on business since they are now compliant with their customer data handling guidelines.
- **Operational Efficiency:** Freed up IT resources to focus on other critical tasks, improving overall productivity.
- **Scalability:** BigFix's scalability allowed seamless management of the growing IT infrastructure.