SUCCESS STORY

BANK OF KHYBER AUTOMATES PATCH MANAGEMENT AND CUTS COSTS BY 20% WITH JBS-IVANTI SOLUTION

Overview

The Bank of Khyber partnered with Jaffer Business Systems (JBS) to strengthen cybersecurity and streamline IT operations. They took the initiative to deploy Ivanti Patch Management across the enterprise, reducing operational costs by 20% and significantly enhancing threat detection capabilities through machine learning and real-time intelligence.

This initiative reflects the Bank's proactive approach to cybersecurity, leaving no stone unturned in eliminating vulnerabilities and preventing potential exploitation. As a provincial bank with strategic importance, maintaining a robust security posture is a vital step for regulatory requirements and the preservation of public trust. The Bank's commitment to finding solutions like automated patch management is a pivotal stance in an era of escalating cyber threats against financial institutions, highlighting its dedication to operational resilience, data integrity, and customer confidence.

Solution Overview

- **Solution Partner:** JBS (www.jbs.live)
- **Solution Implemented:** Ivanti Patch Management

Challenges

Vulnerability Exposure	Significant risk of ransomware, malware, and other cyberattacks which could lead to serious consequences including the encryption of core banking systems and service disruptions.
Operational Inefficiencies	Increased risk and consumption of valuable IT resources due to the manual patch deployment created weak spots that could put the network at risk.
Escalating Costs	Diversion of skilled IT professional from strategic tasks to mundane managing of updates spiked the probability of human error and inflated IT maintenance costs.

The Solution Provided by JBS

JBS implemented Ivanti Patch Management to automate and **standardize BOK's vulnerability remediation processes.** This enabled faster, more reliable patch deployments across all systems and **improved security posture organization wide.**

How It Solved the Challenges

AI-Driven Threat Intelligence

Ivanti leverages machine learning and real-time threat feeds to prioritize and resolve high-risk vulnerabilities first. This proactive approach ensures critical threats are patched swiftly, reducing potential attack surfaces.

- Smart Threat Detection Powered by Machine Learning: It helps reduce the risk of security vulnerabilities by automatically detecting and fixing outdated or exposed software **using advanced machine learning and real-time threat intelligence**. It regularly scans devices to find known weaknesses and applies the necessary patches to close those security gaps. By analyzing factors like exploitability and threat trends, the solution prioritizes the most critical vulnerabilities, which are most likely to be targeted by hackers, so they get addressed first. This proactive, data-driven approach ensures systems stay secure and up to date, significantly **lowering the chances of cyberattacks, data breaches, or service disruptions.**

IT Workload Reduction

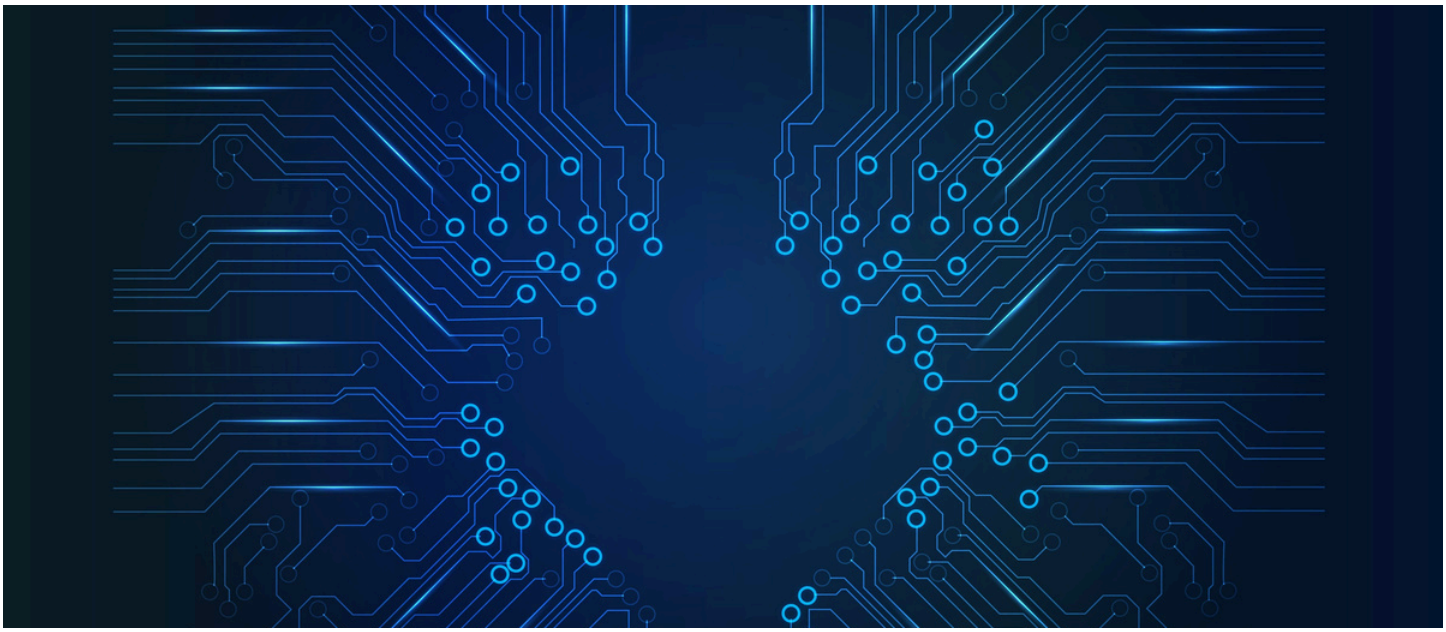
Automated vulnerability scanning and patch deployment across systems, the organization **cut down manual IT workload by 25%**. This not only reduced operational bottlenecks but also freed up skilled team members to focus on strategic priorities like infrastructure optimization, system upgrades, and business-aligned innovation.

Prototype-Based Automation

To ensure consistency and accelerate deployment across varied systems, the solution introduced a prototype-based automation framework utilizing standardized patch deployment templates. This approach minimized configuration errors by eliminating manual adjustments and enforcing uniform settings across environments. As a result, **rollout timelines improved significantly**, even in complex, multi-platform infrastructures, while **reducing the risk of deployment failures and post-patch issues.**

Cost Optimization

The Bank of Khyber achieved measurable cost savings by transitioning to an automated, centralized patch management framework. Replacing fragmented tools with the Ivanti platform allowed the Bank t**o eliminate redundant software, reduce maintenance complexity, and cut training overhead.** With risk-based prioritization ensuring critical vulnerabilities were addressed first, the Bank avoided unnecessary updates, maximizing efficiency while minimizing spend. These combined improvements led to a **20% reduction** in operational costs.



Why JBS

- A **proven track record** of successful project deliveries with measurable outcomes
- **Expert-level certifications** in cybersecurity, guaranteeing deep technical expertise and best-in-class implementation

Key Benefits of the Solution

- 20% reduction in operational costs
- 25% reduction in IT team workload
- Real-time visibility and reporting
- Automation-driven error reduction
- Enhanced cybersecurity posture
- AI & machine learning-powered threat detection
- Improved compliance and audit readiness
- Consolidation of patching tools and workflows

Conclusion

With JBS's expertise and Ivanti's intelligent automation, the Bank of Khyber transformed its patch management operations achieving lower operational costs, improved threat response, reduced IT workload, and a significantly stronger security posture.

Contact Us

For more information on how JBS can revolutionize your IT operations please visit www.jbs.live or contact us at marketing@jbs.live