

Scaling Managed Services Without Scaling Risk

How JKC built a proactive, secure MSP with N-able

Overview

JKC is a Slovak IT services provider delivering infrastructure management, cybersecurity, virtualization, and managed services across public and private sectors. As security expectations accelerated, JKC reached a critical inflection point: continuing to rely on fragmented tools and manual processes would limit their ability to scale and increase operational risk.

By adopting N-able N-sight, Cove Data Protection, EDR, and MDR, JKC established a more proactive, resilient MSP model. The result was improved service stability, stronger security outcomes, and the ability to meet higher customer and regulatory expectations without adding operational complexity.

Company snapshot

- **Company:**
JKC s.r.o.
- **Founded:**
2008
- **Headquarters:**
Trenčín, Slovakia
- **Employees:**
2-10
- **Core focus:**
IT infrastructure management, cybersecurity, virtualization, RMM, data protection, VR based cyber training
- **Primary customer segments:**
Public administration, municipal IT, state institutions, private sector



The challenge

JKC supports organizations operating in an increasingly hostile security landscape. Public sector customers face stricter regulatory requirements, rising attack frequency, and heightened scrutiny around availability, response times, and documentation.

Before adopting a centralized platform, JKC relied on multiple disconnected tools and manual workflows. There was no single, real-time view of customer environments. Issues were often discovered only after users reported them. Patching and updates required manual coordination. Reporting and documentation demanded additional effort.

While these processes were effective at smaller scale, they created friction as more systems came under management. Proving proactive security, meeting service level commitments, and preparing for regulations such as NIS2 required better visibility, automation, and consistency. Continuing without change would have constrained growth and increased risk.

JKC reached a tipping point where fragmented tools and manual processes could no longer support growing customer and **regulatory demands**.

Solutions and results

N-sight: Establishing operational control

Initially adopted in 2016 for remote support, JKC adopted N-sight as the foundation of its managed services operations. With centralized monitoring and management, the team gained continuous visibility into device health, system status, and security posture across all customer environments.

Key processes were automated, including operating system patching, third-party software updates, device health monitoring, alert prioritization, and deployment of endpoint protection. Standardized templates and policy based configuration enabled new customer environments to be onboarded quickly

and consistently, with monitoring, patching, and security controls applied from day one.

This shift reduced manual maintenance work, improved response times, and allowed the team to manage more systems without increasing workload. Many issues are now detected and addressed before users are impacted, improving overall service stability.



EDR: Proactive endpoint defense

As attacks grew more sophisticated, JKC implemented N-able EDR to strengthen endpoint protection across customer environments. Behavioral detection and real time analysis provided a level of visibility that traditional tools could not.

EDR has detected and helped prevent ransomware attempts, suspicious PowerShell activity, unauthorized access attempts, malware infections, and lateral movement within networks. In one case, early stage ransomware behavior was identified and the affected device isolated immediately, preventing the threat from spreading and avoiding potential downtime.

With real-time behavioral insights, detailed incident timelines, and centralized investigation, JKC can now respond earlier and with greater confidence when threats emerge.



Cove Data Protection: Making continuity predictable

To deliver backup and recovery as a reliable managed service, JKC deployed Cove Data Protection. Cove's cloud first design, automated monitoring, and verification aligned well with JKC's proactive service model and the needs of Slovak municipal environments.

Backup monitoring became more structured and dependable. Automated alerts reduced the risk of unnoticed failures, while recovery processes

became faster and more predictable. Operational time spent managing backups decreased, freeing capacity for higher value work. Customers gained greater confidence in data protection and clearer reporting to support compliance and transparency.



Adlumin MDR: 24/7 security without building a SOC

For customers with higher security and compliance expectations, JKC added N-able Adlumin MDR. MDR provides continuous monitoring and expert threat analysis without requiring JKC to build or staff an internal security operations center.

Suspicious activity is investigated by security specialists, with clear escalation when action is required. This significantly reduced the internal burden of alert investigation and allowed the team to focus on customer relationships and service development. Offering managed 24/7 security also strengthened JKC's credibility and enabled engagement with customers that require always on protection.

JKC moved from reactive, manual operations to a standardized, automated, and continuously monitored service model that detects and resolves issues before users are impacted.



Business outcomes

By building its MSP model on N-able, JKC achieved a fundamental shift from reactive support to proactive service delivery.

Key outcomes include:

- Reduced downtime through earlier detection and automated remediation
- Faster response times and fewer escalations
- Stronger cybersecurity posture across customer environments
- Improved compliance readiness, including NIS2 alignment
- More reliable backup and recovery
- Greater transparency and reporting for customers

Outlook

JKC plans to continue expanding its managed services portfolio on the N-able platform. As security expectations rise across public sector and SME markets, the team sees opportunities to scale efficiently, introduce additional automation, and deliver higher value services. With N-able as the operational backbone, JKC is positioned to reach new customers, enter new business areas, and continue evolving its MSP practice without increasing operational risk.

Customer perspective



"If I could share one thing about N-able with other MSPs, it would be that it's not just the platform itself. It's the people behind it. **The tools help MSPs scale and automate efficiently, but what really makes the difference is the support.** We always feel like we have real partners to rely on."

Branislav Jandušík, Director, JKC s.r.o.



To see how you can create business resilience, visit **N-able.com**



This document is provided for informational purposes only and should not be relied upon as legal advice. N-able makes no warranty, express or implied, or assumes any legal liability or responsibility for the information contained herein, including for the accuracy, completeness, or usefulness of any information contained herein. The N-able trademarks, service marks, and logos are the exclusive property of N-able Solutions ULC and N-able Technologies Ltd. All other trademarks are the property of their respective owners.

© 2026 N-able Solutions ULC and N-able Technologies Ltd. All rights reserved.