

Automated Server Patching: Eyes On. Hands Off.

LSZ CIO Kongress Loipersdorf
Oktober 2025

Erik Rusek, PwC | Partner
Sven Gakstatter, Tanium | Director Strategic Accounts



The Challenge

Server patching has become an impossible equation that gets harder every month - here's what's actually happening in most organisations.



Operational realities



Internal Politics



The timing problem



Low success rates



Weekend work

60%

of breaches exploit known vulnerabilities
with available patches

\$4.5m

average EU data breach cost

It's Not Maintenance, It's Cybersecurity

Most organisations treat patching as a technical maintenance task - but high-performing companies treat it as business continuity insurance.

Patching is
maintenance we
have to do

VS.

Patching is risk
management that
we control

Does patching require choosing between speed and safety?

Strategic shift – patching as an event, to patching as a background process –
livestock not pets

Towards an Automated Solution – Eyes on. Hands off.

Proven technology + specialist expertise = complete automation that makes patching a background task that happens without fail.

Eyes on.

- ✓ Oversight of IT estate to deliver patches regularly and reliably
- ✓ Complete data on live status of servers, endpoints, operating systems and applications
- ✓ Elimination of visibility gaps of unknown and unmanaged assets

Hands off.

- ✓ Automate regular critical server patch tasks
- ✓ Deliver low-touch solution that reduces FTE and manual intervention
- ✓ Support and oversight from proven experts to ensure server patch compliance and availability

Eyes On. Hands Off.

What:

- Unified patching
- Business rules integration
- Full process automation
- Real-time visibility
- Best practices from large scale companies

How (distinctions):

- Simplified process
- No infrastructure overhead
- Peer-to-peer technology
- Policy-driven controls
- Managed service model

Proof Points and Business Case

Automated patching pays for itself through risk reduction, infrastructure cost elimination, people cost optimization, and service improvement.

Risk removal

Close exploit windows, pass audits and safeguard reputation by enforcing consistent, automated patching.

Infrastructure cost elimination

Remove costly cache servers, tool sprawl, licensing overhead, and heavy network demands.

People cost optimization

End resource-heavy, weekend-reliant patching, freeing teams to focus on other initiatives.

Service improvement

Cut patch cycles from months to days and dramatically improve first-pass success rates.

98% improved patch compliance

85% reduction in patching infrastructure

72% reduction in labor costs

75% reduction in patch cycles

Customer reference cases will be presented at the CIO Kongress

Thank you!

Wir sind der Taktgeber für Ihren digitalen Wandel

Professionell, selbst wenn es schwierig ist.

Wir wirken Unmittelbar.

Gemeinsam Langfristig.

Aber Sicher!

pwc.com

