

Intelligent Patch Automation

Powered by Gluware™ Platform

Challenges of Modern Patch Management

Patch management remains one of the most critical yet challenging aspects of cyber risk management. The rapid pace of vulnerability disclosures, complex production environments, and limited tolerance for downtime make timely remediation difficult. The rise of AI-enabled attacks has further increased the urgency, allowing threat actors to identify, automate, and rapidly iterate exploits at greater speed and scale. As a result, manual patching processes are increasingly difficult to sustain, leaving known vulnerabilities unaddressed and exposing organizations to unnecessary risk.

Intelligent Patch Automation Service

Vandis' Intelligent Patch Automation Service, powered by Gluware™, transforms patch management from a manual, reactive process into an automated, scalable security function. By accelerating vulnerability remediation, reducing operational burden, and improving compliance, it helps organizations strengthen security while minimizing business disruption.

Vandis Service Highlights

- Recurring device and firmware patches in hours, **not days or weeks**
- CVE monitoring with weekly reports
- Emergency CVE patching of Critical CVSS
- Packages designed to meet the needs of **SMB to Enterprise**

Intelligent Patch Automation Delivers Up To:

95%

Reduction in
Network Outages

100%

Network Compliance
in Hours vs Days

300x

Faster OS Upgrades
with 0% Defects

40+

Simultaneous Device
Updates at Once

99%

Global Network Changes
Made <24 Hours

90%

Reduction in
Troubleshooting Time

Source: Gluware

Service Inclusions

Recurring Monthly Firmware and Patch Management: For Gluware-covered network infrastructure devices, including release-level reviews and change control coordination.

Automated Post-Patch Validation: Ensure device stability and performance.

Detailed Reporting: Provides visibility into completed work, planned activities, risks, and key outcomes.

CVE Monitoring: Leveraging feature-aware vulnerability detection, the service, cross-references active device configurations and live network states against CVE advisories.

Emergency CVE Patching: Proactively defend your environment against emerging threats with Emergency CVE Patching for critical vulnerabilities (CVSS 9.0+), delivering rapid remediation to reduce risk and maintain security, with up to three emergency patching events included as part of the service.

Packages for Businesses of all Sizes: Vandis Intelligent Patch Automation can fit your budget. **Contact Us Today!**



Network Topology Supports Documentation and Compliance

Why Vandis?

A comprehensive network and security strategy that spans your hybrid and premise environments is mission critical for your organization. Vandis' high-level engineering capabilities and close relationships with market leading and niche manufacturers allow us to make timely recommendations. With over 40 years of experience, Vandis has the proven ability to navigate today's everchanging technology and business landscape and the resources and expertise to successfully manage projects on a regional, national, and global scale.

To learn more about Vandis' Managed Services, contact us at info@vandis.com.

Key Benefits

- **Improved consistency across the network estate:** Standardized patch management ensures updates are deployed and validated consistently across supported devices.
- **Reduced operational burden for internal IT teams:** Free internal teams from routine maintenance, allowing them to focus on strategic priorities and critical business needs.
- **Lower risk of missed updates or delayed remediation:** Regular firmware and software updates help reduce risk and keep critical maintenance on track.
- **Improved security and vulnerability response:** Regular patching reduces exposure to known vulnerabilities, while MSP support enables rapid response to critical security threats.
- **Greater stability and reduced downtime:** Proactive patching addresses defects, stability issues, and vendor-recommended fixes, reducing risk of unplanned outages.
- **Stronger auditability and compliance support:** Documented patching provides clear visibility into completed work, exceptions, and risks, supporting compliance and audit readiness.
- **Access to specialized expertise and disciplined execution:** Expert oversight and proven processes drive consistent, reliable patching.