



Patch Management

Addressing vulnerability gaps

Today's evolving technology and the prevalence of malware leave companies and organizations at a higher risk for security exploits. To help combat these risks, vendors supply a seemingly endless stream of patches that challenge even highly skilled teams to maintain patched endpoints.

Schneider Electric's Patch Management solution simplifies patching OEM and third-party assets across your fleet of servers, workstations, PLCs, and other IT/OT devices. Additionally, it automatically updates non-critical assets and schedules updates for critical assets during specific maintenance windows to help reduce effort and costs. Now your team has more time to focus on critical process tasks.

What are patches?

Patches are application, firmware, and operating system updates that address security vulnerabilities in vendor products. Vendors send users notifications when updates are available to download. Distributing and applying these updates helps reduce attack vectors, protect network assets, and create a more secure environment. This results in continued uptime and improved system performance and features. **Failure to apply security patches is one of the most common reasons for security breaches.**

Key benefits

- **Provides visibility** into asset vulnerabilities and available patches
- **Saves time and reduces operating costs** by patching systems more effectively through a central console
- **Decreases security risks** and helps improve system performance
- **Saves time and resources** with Schneider Electric's tested and validated patches

Did you know?

Most major system providers, such as Microsoft, regularly release patches on the second Tuesday of every month called 'Patch Tuesday.'

Some attackers reverse-engineer patches to identify the underlying vulnerability to create methods to exploit that vulnerability. These attacks often start within one day after 'Patch Tuesday,' giving rise to the term 'Exploit Wednesday.'


se.com/cybersecurity-services


Life Is On


Schneider
Electric


Key capabilities

Schneider Electric's Patch Management solution provides the necessary tools to manage the security and updates of the operating system and third-party applications from a single console:

 **Close vulnerability gaps with proactive protection.** Patches are released daily to fix newly-discovered vulnerabilities in popular software tools. But until these fixes are installed – on all of your systems – your processes remain vulnerable to cutting-edge cyberthreats. Schneider Electric's integrated vulnerability assessments help you to identify systems and applications that require updates and to easily roll out patches on-demand or according to a schedule.

 **Policy-based compliance.** Create and leverage pre-built dashboards and reports for patch compliance based on predefined policies, continually monitor endpoint systems, automatically remediate systems that don't meet minimum standards, and clearly document compliance improvements.

 **Keep systems operational with fail-safe patching.** It's rare, but even well-tested patches can introduce problematic bugs or incompatibilities with your other software. That's why Schneider Electric's solutions automatically create full-system backups before applying any new patches – protecting business-critical data and making it seamless to roll back your computers to a known working state if needed.*

 **Regulatory implications.** Many organizations must maintain a certain level of compliance with internationally recognized regulatory bodies. Doing so helps address patch management and safeguards the company and network assets. A diligent patch management program can protect systems and prove that security is crucial in your operational practice.

Why Schneider Electric?

Schneider Electric offers an in-depth approach to securing customer networks. Security patches are tested and validated on behalf of your organization. This includes building a lab, hiring expert resources to perform the testing/validation of patches, and then documenting the results. Our team ensures updates do not impact or conflict with running applications or operations. Schneider Electric can also help customers deploy centralized and approved patches for various applications.

As a world-leading OT cybersecurity company, Schneider Electric follows industry standards and best practices to help customers minimize cybersecurity risks. Patch management is part of our Cybersecurity Application Platform service, offering customers access to vendor-agnostic validated updates through a single platform. To help save time and resources, we can apply patches at custom frequencies, such as during planned outages or system maintenance periods.

Experienced, capable, and globally available

Our global team of cybersecurity experts understands the distinct needs and challenges of OT systems and technologies. Our focus is on finding solutions that fit your unique requirements, regardless of the systems you use to help implement and customize the right level of security to meet your specific needs.

*This feature is available for customers who have Schneider Electric's Backup & Restore solution.

Within **30**
days

recommended
time to apply newly
released patches.

Our services allow
you to focus on what
you do best while
ensuring your entire
network's safety.

Contact us

Learn more
about our **Patch
Management
Services** and
full range of
solutions that
support needs
for cybersecurity
protection
across all
business types
and industries.

se.com/cybersecurity-services

Life Is On

Schneider
Electric

Schneider Electric Industries SAS
35, rue Joseph Monier - CS 30323
F92506 Rueil-Malmaison Cedex