Circet France Transforms Patch Management Across 6,000 Endpoints, Ensuring Secure Nationwide Connectivity with Action1

A leading French telecom provider embraces a proactive, ISO 27001-aligned approach to vulnerability management, enabling safe, uninterrupted service delivery

Company Profile:

Circet France is a leading provider of telecom infrastructure installation, specializing in the deployment, modernization, and maintenance of fixed and mobile networks. As a partner to major telecom operators, Circet supports the development of fiber optics, 5G, and future technologies, serving connectivity needs across the country.

Headquarters: Solliès-Pont (83), France

Industry: Telecommunications

Website: www.circet.fr

Endpoints Managed: 6,000

Battling Lack of Structure and Visibility Gaps Amid a Growing Threat Landscape

As a leading telecom company in France, Circet plays a critical role in deploying and maintaining the infrastructure that powers the nation's connectivity, from fiber optics to 5G. With such responsibility, ensuring uninterrupted operations and strong cybersecurity is crucial to maintaining Circet's high service standards and safeguarding critical national infrastructure.

One of the strategic goals of the IT team at Circet was to achieve a unified, comprehensive patch management strategy to proactively mitigate security risks across the diverse IT environment. Despite multiple layers of protection being implemented, the team lacked a reliable solution to automate the deployment of security updates—a key aspect of a robust and timely vulnerability remediation process. **"Our approach to patch management lacked structure and automation to effectively address vulnerabilities,"**

explained Franck Andreux, Chief Information Security Officer & Cybersecurity Manager at Circet France. This fragmented setup left the team without sufficient visibility into vulnerabilities and installed patches, increasing the risk of delayed updates, compliance gaps, and exposure to potential cyberattacks.

In addition, due to limited visibility into endpoints and the lack of automation and reporting capabilities, the IT team had to rely on manual effort for patching and compliance—an inefficient process that consumed valuable time and resources. **"We wanted to proactively strengthen our cybersecurity by adopting more powerful and centralized tools,"** said Franck Andreux. **"For us, as an ISO 27001-certified organization since 2022, a consistent security framework is a cornerstone of our IT strategy."**

Franck and his team decided to search for a robust, all-in-one solution that would help streamline vulnerability and patch management for both OS and third-party applications.

Finding the Platform That Covers It All

After a thorough evaluation of solutions, the IT team at Circet France chose Action1 for its powerful autonomous endpoint management features, including unified, automated OS and third-party patching, and comprehensive vulnerability scanning and assessment in real-time. In addition, the team appreciated Action1's scripting capabilities and the ability to deploy and manage custom packages, delivering even more value for their IT operations.

Driving Security, Efficiency, and Compliance Through Automated Vulnerability Management

One of the immediate benefits of deploying Action1 was elevated visibility and control over the IT environment from a single console. Real-time visibility, powered by Action1, laid the foundation for building a structured and efficient vulnerability remediation process. **"We regained full control over our machines,"** said Franck Andreux. **"Action1's vulnerability scanning and endpoint assessment give us a clear view of our environment and associated risks."**

With these insights in hand, the IT team implemented an advanced patch management strategy. Leveraging Action1's automation capabilities and its flexibility to customize patching policies in several ways—including the use of pre-production phases to test patches before global deployment across thousands of endpoints—the team refined the patching process to eliminate potential disruptions. As a result, Circet's team was able to remediate over 10,000 vulnerabilities, substantially reducing their threat surface and improving security.

Another significant gain for Circet was improved IT efficiency achieved by automating routine tasks, such as deployment of updates, running scripts, and removal of unauthorized software. For example, the team easily managed the upgrade of endpoints from Windows 10 to Windows 11 through an automation policy, instead of installing the updated OS version on each device manually, saving countless hours of work.

Now, Circet's entire IT infrastructure is managed by a single full-time technician using Action1, allowing the rest of the team to focus on other initiatives.

With Action1, we regained full control over our machines. Now we benefit from a more secure environment, faster response to critical vulnerabilities, and increased operational efficiency.

Franck Andreux, Chief Information Security Officer & Cybersecurity Manager at Circet France

Franck Andreux noted that Action1 became essential for maintaining ISO 27001 compliance within their organization. Its powerful automations, advanced deployment capabilities, and built-in audit trail help the team stay aligned with ISO 27001 security standards. **"Today, we benefit from improved traceability, a significant reduction in manual interventions, and a more secure environment with shorter response times in case of critical vulnerabilities,"** explained Franck.

With Action1, the IT team at Circet has evolved into a structured, proactive force in vulnerability management. The company has not only raised its security posture but also unlocked new levels of operational efficiency—empowering the team to stay ahead of emerging threats with confidence.

SIGN UP
action1.com/signup

WATCH DEMO
action1.com/watch

SWITCH TO ACTION1
action1.com/switch

Corporate Headquarters: 2929 Allen Parkway, Suite 200 Houston, TX 77019

www.action1.com

Phone: +1-346-444-8530