TECNALIA Secures Innovation, Supports Employee Mobility, and Ensures Regulatory Compliance with Action1

Autonomous, cross-OS patching and real-time visibility ensure consistent security policies while maintaining seamless operations

tecnalia
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

Company Profile:

TECNALIA is a leading applied research and technological organization in Europe. The organization drives innovation across key strategic domains including the circular economy, smart manufacturing, digital transformation, energy transition, health and food, urban ecosystem and sustainable mobility.

Headquarters: Derio (Bizkaia), Spain

Industry: Research & Development (R&D)

Website: https://www.tecnalia.com/

Endpoints Managed: 2,000

Managing Security Challenges in a Distributed Research Environment

As one of the largest applied research and technology centers in Europe, TECNALIA bridges the gap between academia, industry, and government, enabling the development of working prototypes across multiple strategic sectors. The organization brings together more than 1,500 professionals and operates across a distributed network of approximately 2,000 endpoints. With a highly mobile workforce collaborating across Europe and a hybrid work model, the IT department faces significant challenges in maintaining secure, reliable, and consistent IT operations across a complex, multi-platform environment.

Prior to implementing a modern patch management solution, TECNALIA relied on Windows Server Update Services (WSUS), which only addressed operating system updates and left third-party applications unmanaged. The organization also explored Microsoft Intune for deployment through the Microsoft Store, but encountered limitations in visibility and control over deployment outcomes, including installation failures and inconsistent update status tracking.

The lack of centralized visibility emerged as a critical operational challenge. “With nearly 2,000 endpoints spread across different

Key Results

- Automated cross-OS patching, including third-party applications, with critical updates deployed within a week.
- Compliance with GDPR, NIS2, and the Cyber Resilience Act.
- Centralized, real-time visibility into vulnerabilities, patch status, logs, and software inventory.
- Reduction of IT operational overhead through automation of manual processes.

locations and networks, having visibility into patch status is essential — without it, managing security becomes unmanageable," says Aitzol Zubizarreta, CIO at TECNALIA. The absence of a unified view of endpoint health and security posture made proactive vulnerability management nearly impossible, increasing the risk of security incidents and operational disruptions.

Additionally, as a research institution engaged in sensitive projects with corporate and public sector partners, TECNALIA must adhere to stringent regulatory frameworks, including the General Data Protection Regulation (GDPR), the NIS2 Directive, and the upcoming Cyber Resilience Act. These requirements place significant pressure on the IT team to maintain a robust and auditable security posture.

Given the organization's reliance on vast amounts of data and intellectual property, any security lapse could compromise research integrity and operational continuity. "Our mission is driven by the data and information we generate," explains Aitzol.

"If our systems are compromised by ransomware or unpatched vulnerabilities, our operations halt. That's why it's critical that every endpoint is patched, monitored, and compliant with our security policies." To address these challenges, TECNALIA sought a scalable, unified patch management solution capable of managing a diverse, distributed environment across multiple operating systems and geographies.

Seeking a Solution Built for Scale and Flexibility

TECNALIA's IT team conducted a comprehensive evaluation of several patch management platforms. While some solutions offered limited capabilities in software deployment, others lacked European infrastructure, raising concerns about data residency and compliance.

Action1 stood out due to its ease of deployment, robust automation for both operating system and third-party application updates, and its ability to manage large-scale software installations. The organization frequently deploys heavy industrial applications such as MATLAB, SolidWorks, and ANSYS, which require significant bandwidth and reliable delivery across global networks. "There are few platforms that can deploy a five-gigabyte software package globally with consistent reliability — Action1 is one of the few that can do this effectively," says Aitzol. This capability proved essential for maintaining operational continuity across TECNALIA's distributed research sites.

From Fragmented Updates to Centralized Control

With Action1, TECNALIA established a unified, cross-OS patch management framework that ensures consistent security policies across all endpoints. "Our operations are highly mobile, so we rely on Action1 to ensure patching is applied consistently, regardless of location," explains Aitzol. The organization has implemented a policy requiring critical security patches to be deployed within seven days of release.

Action1 also enables automated patching of third-party applications, including common tools like Zoom, Microsoft Visual C++, and FileZilla, as well as mission-critical research software such as MATLAB, SolidWorks, and ANSYS. This ensures that all systems — from standard office applications to specialized engineering tools — remain secure and up to date.

To minimize risk during deployment, the IT team adopted a phased rollout strategy using update rings. The environment is segmented into three groups: IT staff first, followed by the digital business unit (approximately 150 employees), and finally the remainder of the organization. This approach allows for controlled deployment, validation, and rapid issue resolution, ensuring a smooth transition across the entire fleet.

Centralized visibility has been transformative. From a single, intuitive console, the IT team now has real-time insight into vulnerabilities, missing patches, deployment status, logs, and a complete software inventory. "It's a comprehensive solution — the level of visibility and control we now have is a game-changer," says Aitzol. This shift has enabled TECNALIA to move from reactive patching to a proactive, policy-driven security model.

Flexibility Beyond Patching

Beyond core patch management, Action1's scripting capabilities have enabled TECNALIA to automate a range of IT processes. A notable example is the transition from Trend Micro XDR to Microsoft Defender. The team developed a custom script that verifies Defender's activation status and, if not enabled, deploys it while removing the legacy agent. This streamlined migration process eliminated manual intervention and reduced the risk of configuration errors.

Built-in reporting tools also supported the organization's migration from Windows 10 to Windows 11, allowing the team to quickly identify compatible devices and verify prerequisites such as storage availability and system requirements.

Protecting What Powers Innovation

With Action1's automated patching, real-time visibility, and flexible scripting capabilities, TECNALIA has established a proactive and resilient approach to vulnerability management. This foundation strengthens the organization's security posture, supports regulatory compliance, and ensures operational continuity — all critical to protecting intellectual property and enabling the transformation of research into tangible technological advancements.

> **These days, cybersecurity threats are pervasive. Even a single unpatched endpoint can serve as an entry point for attackers. Since our operations depend entirely on data, losing control would be catastrophic. Action1 provides the visibility, automation, and flexibility we need to stay ahead of threats and protect our mission-critical systems.**
>
> **Aitzol Zubizarreta, CIO at TECNALIA**

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

Phone: +1-346-444-8530

www.action1.com