Advanced Learning Partnership Eliminates Hidden Vulnerabilities Across 23 Schools

ADVANCE LEARNING PARTNERSHIP

The Organization

Advanced Learning Partnership (ALP) is a Multi Academy Trust based in County Durham, supporting 23 schools – 9 secondary and 14 primary – serving approximately 9,000 students. With nearly 5,000 endpoints across multiple sites, ALP's IT team delivers secure, reliable technology services that support teaching, learning, and trust-wide operations, with a strong focus on cybersecurity and compliance.

Website: https://alplearning.org.uk/

Headquarters: County Durham, UK

Managed Endpoints: ~5,000

Industry: Education (Multi Academy Trust)

Securing a Multi-Academy Trust at Scale

With schools increasingly targeted by ransomware and phishing attacks, ALP's IT team recognized the need to strengthen and standardize its patch management strategy. They were looking for visibility, consistency, and trust-wide control.

Before implementing Action1, patch management across ALP's schools was inconsistent and decentralized. While Microsoft updates were handled through Windows Update for Business, third-party patching was largely manual and varied from site to site. There was no trust-wide policy defining remediation timelines and no centralized way to measure compliance or enforce consistent standards across all 23 schools. As a result, each site operated somewhat independently, creating gaps in visibility and governance.

The absence of centralized oversight meant the IT team had limited insight into their true vulnerability exposure. They could not easily determine which devices were missing critical patches, how many vulnerabilities existed across the organization, or whether remediation efforts were consistent. While Microsoft patching felt manageable, the lack of visibility into third-party software posed a significant concern.

Key Results

- Centralized visibility across nearly 5,000 devices, uncovering hidden security risks and enabling immediate action to fix them.
- Established a trust-wide patch policy with 7-day SLAs for critical vulnerabilities, resolving issues 3–7 days faster, and staying ahead of threats.
- Consolidated tools into one platform, reducing complexity and costs while delivering clear, board-ready visibility into risk and compliance.

At the same time, external pressures were intensifying. Insurance requirements demanded demonstrable patch management practices, updated Department for Education (DfE) standards emphasized ongoing maintenance and security controls, and ransomware attacks against educational institutions were becoming increasingly common. A structured, centralized approach to patch management was no longer optional – it was essential.

Rapid Implementation and Immediate Visibility

After evaluating multiple vendors, including NinjaOne, Panda, Kaseya, Datto, and PDQ, ALP selected Action1 for its balance of capability and ease of use. The IT team needed a platform robust enough to manage nearly 5,000 endpoints while remaining intuitive for technicians and senior network managers alike. Action1 quickly distinguished itself during the evaluation process, offering both the functionality required and a user experience that made adoption straightforward. “It’s rare that you get capability and ease of use in the same package,” says Ian Simpson, Senior Network Manager.

The deployment was just as seamless as the evaluation. Agents were rolled out within minutes, and configurations from a test environment were replicated across schools in approximately ten minutes. Within hours, ALP gained centralized visibility across nearly 5,000 endpoints. For the first time, the IT team could clearly see both operating system and third-party vulnerabilities across the entire trust.

The initial vulnerability reports were eye-opening. One discovery underscored the urgency: legacy Photoshop installations bundled with Flash and Shockwave revealed more than 300 vulnerabilities per device across 60 to 80 machines. Armed with this visibility, the team was able to remove unsupported software, prioritize remediation efforts, and significantly reduce overall risk exposure across the organization.

Standardized Patching, Faster Remediation, and Operational Efficiency

With full visibility in place, ALP established a standardized, trust-wide patch management framework across all 23 schools. The IT team defined clear remediation timelines, addressing critical and high vulnerabilities within seven days, and resolving medium and low vulnerabilities within thirty days. Each school operates

within its own organization in Action1 but follows a centralized template, ensuring consistent governance while allowing local flexibility. For the first time, patching was measurable, enforceable, and consistent across the entire trust.

Automation and centralized dashboards significantly improved remediation speed and operational efficiency. Devices are now patched reliably, while technicians can proactively identify and resolve vulnerabilities before scheduled patch cycles. Instead of reacting to issues, the team now stays ahead of patching timelines.

“We’re three or four days ahead of where we would normally have been, sometimes more than a week,” Ian mentions. In addition, scripting capabilities allow the team to remotely manage system configurations, control upgrades, and deploy fixes without physically visiting devices, saving valuable time across campuses. Beyond faster remediation, Action1 helped ALP simplify its environment and strengthen governance. By consolidating third-party deployment tools into a single platform, the team was able to reduce complexity and licensing costs. Centralized reporting now gives leadership a clear, while real-time visibility has strengthened ownership and accountability across the IT team.

Building a More Resilient Digital Environment for Education

For Advanced Learning Partnership, Action1 transformed patch management from a fragmented, reactive process into a centralized, proactive security strategy across 23 schools. By delivering visibility, standardized governance, and automation, Action1 strengthened ALP’s cybersecurity posture while improving operational efficiency and team confidence.

In an education environment where resilience matters more than ever, Action1 now plays a central role in protecting thousands of devices — and the students and staff who rely on them every day.

Corporate Headquarters: 708 Main St, 10th FL Houston, TX 77002
Phone: +1-346-444-8530
www.action1.com