Ark Schools Ensure Equal Opportunities for Safe Learning for Every Child with Action1

By unifying patch management and automating compliance, Ark Schools safeguard 30k+ students and 3,500+ staff across 39 schools.

Company Profile:

Ark is an education charity that strives to ensure that all children, regardless of their background, have access to a great education and real choices in life. Ark operates a range of education ventures including Ark Schools, a network of 39 schools serving 30k+ students and employing over 3,500 staff. Being in the education space, Ark must make sure it meets strict cybersecurity and compliance regulations without exhausting its own IT resources.

Headquarters: London, England

Industry: Education

Website: www.arkonline.org

Endpoints Managed: 10,000+

Fragmented Tools and Time-Consuming Compliance

Protecting sensitive student and employee data, ensuring safe access to learning resources, and maintaining an uninterrupted learning experience are strategically important for the Ark Schools' IT department. However, with campuses spread across multiple cities, their highly distributed network adds layers of complexity to managing cybersecurity.

To maintain a modern security posture, Ark follows national standards like Cyber Essentials, which require patching critical vulnerabilities within 14 days – a demanding mandate for a network spanning over 10,000 geographically distributed endpoints. Maintaining compliance meant jumping between multiple dashboards to gather essential data on vulnerabilities, missing patches, and installed updates.

The organization used Microsoft Intune and SCCM to push out patches, yet these tools lacked the ability to verify whether those updates had been applied without purchasing costly log analytics. Instead, the IT team relied on manual checks, with no clear way to detect if patches had failed or been deferred by users.

Key Results

- Nearly 90% faster patching cycles, reduced from two months to one week.
- Simplified compliance with Cyber Essentials and the Department for Education (DfE) guidance.
- Consistent patching and vulnerability management across 10,000+ distributed endpoints from a single platform.

Compounding these issues was the presence of third-party applications, including specialized educational software such as exam programs and 3D modelling tools that did not support auto-updates. Staff had to manually track and apply updates to these applications, adding to the workload.

Tyler Owen-Thomas, Cybersecurity Lead at Ark Schools, recalls how challenging this was: It was a time-consuming approach that left Ark's IT infrastructure exposed to additional security risks. Without a single source of truth for endpoint status, the patching process could take as long as two months and required the involvement of nearly the entire IT team. To streamline patching, Ark sought a solution that offered powerful automation capabilities and real-time visibility into vulnerabilities and updates.

Simplifying Security Across 39 Schools

After evaluating several vendors, Ark selected Action1 as their patch management and endpoint security platform. "**Out of all the solutions we tested, Action1 was by far the easiest to implement and learn**," highlights Tyler Owen-Thomas, Cybersecurity Lead. Not only did Action1 give them visibility that improved internal security, but it also allowed unified patching for both operating systems (OS) and third-party applications, and automation and customization capabilities.

Unified patching for both OS and third-party applications eliminated the need to manage separate tools or rely on manual updates for niche applications. Thanks to Action1's cloud-native architecture and P2P patch distribution, Ark's IT team can now deploy updates to Windows, browsers, and third-party programs from a single platform, ensuring timely vulnerability remediation and consistency across its 39 schools.

With the ability to upload custom software packages into Action1, Ark can keep industry-specific applications – such as exam software and 3D modelling programs – up to date without manually updating each device.

Finally, Ark's IT team has made extensive use of role-based access control (RBAC). With dozens of schools and multiple IT role levels, RBAC allows Ark to assign permissions in line with their organizational structure and security policies. Some team members can view data without making changes, while cybersecurity leads and managers retain full administrative control. This not only improves security but also helps junior staff to learn by observing real-time data safely.

Full Visibility Leads to Improved Accountability and Compliance

One of the major benefits to Ark was simplifying compliance with Cyber Essentials and guidance from the Department for Education (DfE). Now, with Action1's single console, the IT team has real-time visibility into vulnerabilities as well as installed and pending patches across all endpoints, instead of having to jump between eight different dashboards. Combined with automated patching and greater control over their machines, this makes it far easier to consistently meet the recommended 14-day patching requirements. "**While we tried to follow Cyber Essentials standards as much as possible, there was no consistent process in place. Action1 helped us solidify those SLAs,**" said Tyler.

Another significant gain for Ark was reducing their patching cycle from two months to just one week, which can now be managed by just one person. "**In the past, the whole team had to be engaged to gather compliance data. Now I can just run an automation or view a report**," Tyler stated.

Operationally, disruption was reduced through carefully timed patch deployments. Desktops can now be patched overnight, while servers follow a two-step schedule with testing before full rollout, ensuring the critical updates are applied without impacting teaching or learning activities. The team also benefited from the Update Rings feature, deploying updates to devices and servers in two phases: test deployments on the first Thursday of each month, followed by a full rollout to the rest of the IT environment on the second Thursday.

Ark transformed its cybersecurity approach to Action1's autonomous, unified patch management and real-time visibility. The shift from mostly manual work to centralized automation helped free up IT resources, strengthened compliance, and improved operational reliability. With Action1, Ark can meet modern cybersecurity standards while continuing to focus on its mission: delivering high-quality education for children, regardless of their background.

> **Action1's visibility, single-dashboard approach, and ease of use have been gamechangers. It's freed up resources, improved compliance, and made life much easier for the team.**
>
> **Tyler Owen-Thomas, Cybersecurity Lead**

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