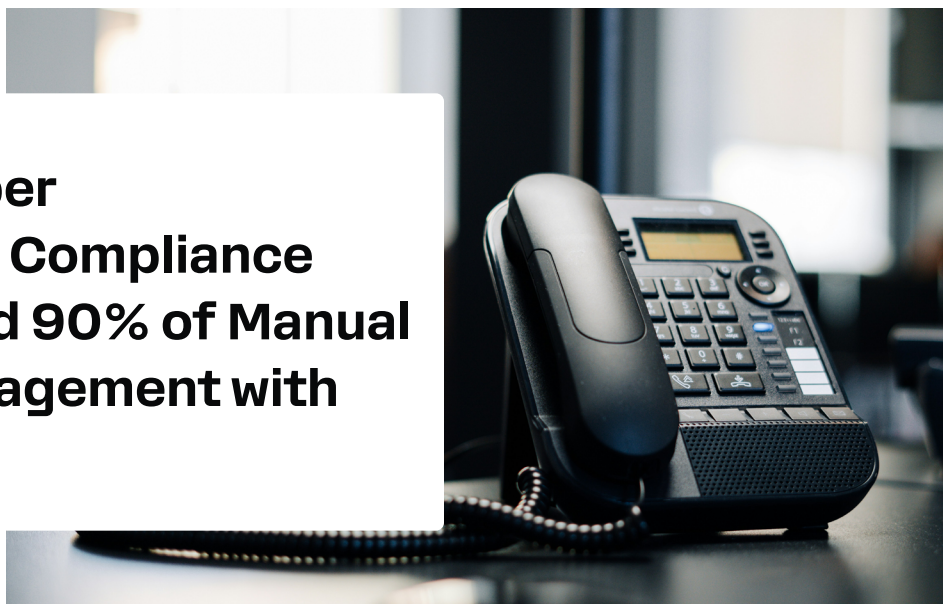


How WeAreFiber Strengthened Compliance and Eliminated 90% of Manual Endpoint Management with Action1



Global BPO transforms patch management, improves compliance readiness, and gives its IT team complete endpoint visibility.



The Organization

WeAreFiber (Fiber Group) is a global Business Process Outsourcer (BPO) delivering inbound customer support, data management, and smart sourcing services to organizations around the world. Headquartered in Tirana, Albania, the company operates across five locations in Albania, Italy, and Kosovo, supporting more than 1,200 employees.

Website: www.wearefiber.com

Headquarters: Tirana, Albania

Managed Endpoints: 1000

Industry: Business Services

From Limited Visibility to Complete Confidence

As a business that serves customers across multiple regulated industries, WeAreFiber must continuously maintain compliance with GDPR, ISO 27001, SOC 2 Type II, and PCI DSS requirements. Ensuring every endpoint remains secure and compliant is critical – not only for protecting customer data but also for maintaining client trust and contractual obligations.

As WeAreFiber continued to grow, its existing endpoint management approach could no longer keep pace. Multiple tools, custom-built solutions, and legacy Windows technologies created fragmented visibility across the environment, making it difficult to determine the true health and compliance status of endpoint devices.

Even more concerning, compliance checks revealed that systems appearing healthy on paper were actually missing critical Group Policy configurations due to operating system corruption. Although no security incidents had occurred, the discovery exposed a significant visibility gap that traditional tools failed to detect.

Key Results

- Eliminated approximately 90% of manual endpoint management tasks through automation.
- Reduced compliance risk by enforcing aggressive internal SLAs of 1 day for critical vulnerabilities and 3 days for high-severity issues.
- Transformed audits into routine operations with continuous compliance reporting and real-time endpoint visibility.

Manual remediation also placed a growing burden on the IT team. Helpdesk staff spent countless hours validating patch status, confirming policy enforcement, and troubleshooting endpoint issues instead of focusing on higher-value security initiatives.

“We discovered that what our previous systems reported wasn’t always reality. That lack of confidence made compliance and risk management much more difficult than it needed to be,” mentioned Rinor Hoxha, CTO.

Finding a Modern Replacement for Legacy Tools

WeAreFiber evaluated a range of commercial and open-source solutions, including NinjaOne and FleetDM, while

searching for a modern replacement for aging Windows technologies such as WSUS and custom scripting.

After deploying Action1’s free edition, the team quickly recognized that the platform delivered exactly what they were looking for: centralized visibility, comprehensive patch management, intuitive reporting, and a user experience that simplified daily operations without unnecessary complexity.

Beyond the technology itself, the team appreciated Action1’s customer-first approach. Rinor said, “It felt like Action1 wasn’t adding features simply for the sake of having more features. They were listening to customer needs and solving real problems.”

Deployment was completed in approximately one month across nearly 900 managed endpoints. The implementation itself was smooth, with most delays attributed to internal scheduling rather than the platform.

Continuous Compliance with Faster Remediation

Today, Action1 serves as WeAreFiber’s centralized platform for endpoint management, software deployment, configuration management, vulnerability remediation, and compliance reporting. To strengthen its security posture, the organization has established aggressive internal service-level agreements, aiming to remediate critical vulnerabilities within one day, high-severity vulnerabilities within three days, medium-severity vulnerabilities within ten days, and low-severity vulnerabilities within thirty days whenever patches are available.

Through Action1's automation capabilities – including patching, scripting, reporting, alerts, and endpoint grouping – the IT team can consistently meet these targets while maintaining tight control over its highly restricted environment. Comprehensive reporting and custom alerts continuously verify that Microsoft Active Directory Group Policies are not only configured correctly but are actively enforced on every endpoint, allowing the team to quickly detect and remediate configuration drift before it becomes a compliance concern.

This shift has fundamentally changed WeAreFiber's approach to compliance. Rather than treating audits as high-pressure events that require weeks of preparation, continuous visibility and automated reporting have made compliance an everyday practice. As a result, audits have become significantly less disruptive and far more predictable.

Giving the IT Team Time to Focus on Security

By automating patching, software deployment, reporting, and routine endpoint management, Action1 has eliminated approximately **90% of the manual work** previously required to maintain endpoint security. The remaining manual effort is primarily related to underlying hardware or operating system issues rather than day-to-day administration.

With routine maintenance now automated, the Helpdesk team no longer spends valuable time manually verifying patches or checking compliance across hundreds of devices. Instead, team members have been able to develop new skills and shift their focus toward Security Operations Center (SOC) activities, strengthening the organization's overall security capabilities without increasing headcount.

Today, Action1 supports nearly every stage of the endpoint lifecycle, from provisioning new devices and deploying software to enforcing configurations, automating patch management, and continuously monitoring compliance. Role-based access controls allow different teams to access only the functions they need, while Endpoint Groups enable staged deployments that minimize operational disruption and ensure updates are rolled out safely across the environment.

A Stronger Security Posture for Future Growth

As WeAreFiber continues to expand across multiple countries and support new customers, Action1 provides the confidence that every endpoint can be monitored, secured, and kept compliant at scale.

The platform has strengthened visibility, accelerated vulnerability remediation, reduced operational overhead, and made compliance an ongoing process rather than a periodic exercise.

For an organization where failing compliance can jeopardize customer contracts, that confidence has become invaluable.



Today we're much more confident in our security posture. We can respond faster, prove compliance more easily, and our team spends far less time on manual work while contributing more to overall security.

Rinor Hoxha, CTO



SIGN UP

action1.com/signup



WATCH DEMO

action1.com/watch



SWITCH TO ACTION1

action1.com/switch