Ecobank Enhances Security through Automated Third-Party Patching Across 16,000 Endpoints with Action1

The Organization

Ecobank Group is the leading private pan-African financial services group with unrivaled African expertise. Present in 35 sub-Saharan African countries, as well as France, the UK, UAE, and China, its pan-African platform provides a single gateway for payments, cash management, trade, and investments.

Website: https://ecobank.com/

Headquarters: Lomé, Togo

Managed Endpoints: 16,000

Industry: Finance

The Challenge

Ecobank, being a pan-African banking group with numerous offices and branches across Africa, needed to remain at the forefront of technological innovation in the continent's banking industry. Having such a robust IT infrastructure with third-party applications demanded that the bank constantly reduce its exposure to potential cyber threats, particularly the ones stemming from unpatched vulnerabilities in these applications using a time and cost saving solution that provided support for third-party patching.

"The presence of unpatched apps posed a risk to our IT environment, adversely affecting our risk scoring," remarked Enoch Sappor, Systems Security Engineer Group Technology Cyber Security.

In addition, Ecobank wanted to effectively monitor, identify, and uninstall unwanted software on its endpoints, which could pose security risks. To enhance their security position and maintain the desirable low-risk scores, Ecobank decided to find a solution that could implement third-party patching while providing them with greater control over their geographically dispersed endpoints.

Key Results

- Streamlined third-party patching for a distributed network of 16,000 endpoints.
- Enhanced security and risk score.
- Improved visibility and control over the IT environment.

With Action1's third-party patching capability, we can easily patch our systems on a large scale and address security vulnerabilities. This will help us continue to serve our customers and stakeholders, timely and securely across the continent without the fear of malware.

Enoch Sappor, Systems Security Engineer Group Technology Cyber Security

The Action1 Solution

Following a thorough evaluation of various patch management solutions, Ecobank opted for Action1. They chose Action1 for its third-party patching capabilities, time and cost savings, ease of use, and scalable cloud-native architecture.

The Benefits

Efficient third-party patch management. By implementing Action1, Ecobank streamlined third-party patching and ensured continuous remediation of vulnerabilities in third-party applications such as Chrome and Adobe across their distributed network, improving their security position and mitigating the risk of ransomware.

Reduced vulnerabilities and enhanced risk score. Ecobank opted for Action1's comprehensive feature set, which includes intuitive third-party patching, the ability to detect and bulk-remove unwanted software on endpoints, and an aggregated dashboard that provides instant visibility into vulnerabilities. Together, these capabilities proved valuable to Ecobank, leading to a reduction in security vulnerabilities across their geographically dispersed endpoints, improving the bank's overall risk score, and reinforcing their technology-driven approach to banking.

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

www.action1.com

Phone: +1-346-444-8530