How GNT Took Control of Patching and Slashed Critical Vulnerabilities by 80%

Company Profile:

GNT is a global producer of natural food colorants. With operations spanning the United States, Germany, and the Netherlands, GNT plays a key role in the global food supply chain by providing natural alternatives to artificial dyes for majority brands and producers. They support roughly 600-700 employees with over 1,000 endpoints.

Headquarters: Mierlo, Netherlands

Industry: Food and Beverage

Website: https://exberry.com/en/

Endpoints Managed: 1,050

From Mounting Vulnerabilities to an Urgent Need for Visibility

GNT is a global producer of natural food colorants used in everyday food and beverage products around the world. Because their ingredients directly support manufacturers, farmers, and retailers across the supply chain, cybersecurity is not just a technical necessity for them – it's essential to maintain operational continuity. Any disruption caused by a cyber incident could have downstream effects on food and production availability.

Initially, GNT relied on ManageEngine for patch management, but in practice the solution struggled to consistently update all applications – especially older and legacy packages. As a result, vulnerabilities accumulated over time, and the IT team had to spend hours each week manually investigating patch failures and validating remediation. At one point, GNT was tracking around 800 total vulnerabilities, many of them requiring manual intervention. Among these, 200 were critical, leaving the organization at risk.

While Microsoft updates were handled, visibility into third-party patching and application coverage was limited and did not align with the GNT team's needs. This lack of reliable insights meant the

Key Results

- Critical vulnerabilities dropped by 80% within a few months of deployment, significantly reducing the attack surface.
- Manual troubleshooting efforts were nearly eliminated, saving hours of work weekly.
- Automated patch cycles replaced ad-hoc patching, creating a reliable, streamlined process.

IT team had to approach third-party patching manually, increasing operational burden.

GNT found itself facing hundreds of unresolved vulnerabilities alongside an increasingly complex IT landscape. Walid Derey, Security & Network Administration at GNT, together with his colleagues, began searching for a solution focused on patching and vulnerability management, seeking to regain control over their IT fleet, reduce manual effort, and protect operations against security threats.

A Strategic Shift Toward Efficient, Automated Patch Management

GNT evaluated several platforms before ultimately choosing Action1. They initially deployed and tested Action1 on around 15 devices before deciding to deploy it across their entire device network. In just a few months after deploying Action1, critical vulnerabilities dropped from 200 to just 40, an 80% reduction. Walid attributes this directly to Action1's reliability and robust patching automation, noting that his team now addresses critical vulnerabilities within two days in most cases.

Today, the IT department has adopted a unified, automated, and structured approach to managing security updates. By leveraging update rings and group-based automations, and separate patching cycles for distinct endpoint groups, the team can deploy updates in a staggered and controlled manner aligned with their internal security policy, eliminating the chaos of ad-hoc patching and saving hours of work daily.

"Action1 saves us a lot of time – patch management is now mostly about reviewing and approving updates," Walid says. "Before, releasing a fix often meant two to three hours of troubleshooting. Now, the process is fast and smooth."
Walid and his team also highlight Action1's prebuilt scripting feature as a significant benefit. The ability to run scripts in real time, view output, and take immediate action further reduces manual overhead and gives GNT finer control over their environment.

Solving the Challenges of Legacy and Hard-to-Patch Software

Action1 also immediately provided transparency into their third-party applications, enabling the team to see their status and determine whether they needed to be reinstalled, updated, or replaced. While other tools offered a similar interface, Walid notes that they were "far less effective when it came to patching third-party software."

The IT team appreciates that Action1 helps them manage patching even in situations where updates were typically postponed or problematic. Walid explains, “It was a nice thing to have a product that would update things that usually didn’t want to be updated. The issue with the business was that a lot of old packages were being used, even applications that were allowed to be updated later.”

A Reliable Platform Built for Real-World Security Challenges

With Action1, GNT has regained control of its patch management process, reduced critical vulnerabilities, established automation cycles, and saved hours of manual troubleshooting each week. By focusing on patching, visibility, and vulnerability reduction, Action1 delivered exactly what GNT needed: a reliable, adaptable platform that strengthens cybersecurity without adding complexity.