SkyBox Labs Outperforms Its Security Policy KPIs, Patching Critical Vulnerabilities Faster with Action1

SKYBOX LABS

The Organization

SkyBox Labs is a full-service game development studio that has participated in developing numerous AAA game titles and projects, both independently and in collaboration with major game publishers.

Website: skyboxlabs.com

Headquarters: Vancouver, Canada

Industry: Technology

Providing Flexible Workplace Brings Security Challenges

Being a successful game development studio requires attracting top talent to drive innovation. As a company recognized among the top employers in Canada, SkyBox Labs offers a hybrid work format, ensuring the flexibility that people value. However, this flexibility brings security challenges, especially given the increasing number of cyber-attacks in the gaming industry. "With all the machines that are remote right now, we need to eliminate any vulnerabilities that could be exploited to ensure the security of our intellectual property (IP) and that of our partners," says Marc Speed, the Head of Cybersecurity at SkyBox Labs.

As a certified CISSP professional, Marc has developed and implemented a comprehensive IT security policy, which includes a 14-day timeframe for deploying critical updates. However, the solution the company was using to manage updates, Automox, was not sufficient because it required too much scripting, didn't provide the IT team with built-in reports that were essential for ensuring critical security controls, and did not adequately streamline patching.

Key Results

- Outperformed 14-day critical patching KPI, reduced to 11-12 days.
- Streamlined third-party patching for distributed endpoints.
- Improved security and control through built-in reporting.
- Annual cost savings of $20,000.

To reduce workload and ensure security, Marc started looking for an all-in-one solution that would enable SkyBox Labs to discover and prioritize vulnerabilities, streamline patching for both Windows and third-party apps, and provide real-time visibility and control over endpoints across the organization, no matter where they are located.

Finding All-in-One Platform

Marc and his colleagues evaluated several solutions, including NinjaOne and Tanium, but chose Action1 because it is a cloud-native platform offering the feature set that meets their needs, such as powerful patching, vulnerability discovery, and comprehensive built-in reporting. Additionally, Action1 is a cost-effective solution that saves them $20,000 annually.

Elevated Security for Hybrid Workplace

When Marc ran the vulnerability discovery for the first time, Action1 discovered multiple critical vulnerabilities in third-party apps such as Chrome, Firefox, and Adobe, which he was previously unaware of. Each of these vulnerabilities increased security risks for his organization, so he appreciates that Action1 allowed him to address them easily through a single view.

Since then, he has been using the Action1 vulnerability discovery feature at least once a week to detect vulnerabilities on remote and in-office endpoints. Additionally, he has established a set of patching policies to deploy critical updates organization-wide. He finds the Action1 Software Repository particularly helpful in this regard, as it streamlines the deployment of critical updates for commonly used third-party apps such as web browsers. He can even add custom packages for security tools used by his organization, such as AV, and keep them updated as well. Overall, thanks to Action1's customizable and reliable patching, Marc has managed not only to meet their 14-day timeframe to patch critical vulnerabilities but also to outperform it by reducing it down to 11-12 days.

> **I found that Action1 patching works really well. In a few steps, I can find missing updates, set up a patching policy, and schedule a reboot – and then it just goes and does it.**
>
> **Marc Speed, the Head of Cybersecurity at SkyBox Labs**

Moreover, thanks to Action1's customizable automations and granular endpoint group settings, Marc has tailored patching schedules to different teams' needs. "Some teams might have slightly varying levels of urgency when it comes to patching. Action1 enables me to set different patching policies depending on each team's needs,"

Finally, the Action1 reports have proved to be invaluable in providing Marc with visibility into whether critical security controls are met. For example, he no longer needs to write PowerShell scripts to understand how many devices are missing enabled BitLocker, as it is a built-in report in Action1, simplifying the identification of machines lacking encryption.

To sum up, Action1 has become a mission-critical solution for SkyBox Labs, which helps them maintain a flexible workplace while ensuring adherence to strict security policies, mitigating the risk of compromise due to unpatched vulnerabilities.

SIGN UP
action1.com/signup

WATCH DEMO
action1.com/watch

SWITCH TO ACTION1
action1.com/switch