secpod

TRANSFORMATION STUDY

# Vulnerability Management Transformation for the World's Biggest Online Betting Exchange.

www.secpod.com

# Introduction
# Replacing Qualys with Saner CVEM

## THE CASE IN POINT

Despite using a well-known vulnerability management solution, Betfair discovered that 30–40% of its endpoints were not being patched, a massive security risk hidden behind manual tagging processes and limited vulnerability visibility.

Their existing tool, Qualys, had slower scan times, legacy risk prioritization methods, a smaller proprietary vulnerability database, and required devices to be manually assigned to patching groups, which meant that any untagged machine was effectively invisible to the patching engine. Qualys offered limited automation, and lacked visibility into vulnerability & patching status, creating security blind spots.

This inefficiency left large portions of the infrastructure vulnerable to exploitation, with no real-time insight into what was patched and what wasn't. The operational burden was high, and the risk even higher.

That's when Betfair made a strategic decision to replace Qualys with SecPod Saner CVEM, a unified, automated vulnerability management platform that delivered complete patch coverage, including rapid, continuous vulnerability assessment.

## CHOOSE SANER CVEM

The switch delivered seamless onboarding, real-time vulnerability and patch visibility, and complete endpoint risk remediation.

## BEFORE & AFTER: THE TRANSFORMATION

| COMPARING FACTORS | WITH QUALYS (BEFORE) | WITH SANER CVEM (AFTER) |
|---|---|---|
| Vulnerability Detection | Slower scans, periodic updates | 5-minute scans, continuous updates |
| Integration between VM & PM | Minimal | Seamless & Unified |
| VM database size | Smaller, proprietary database | 190,000+ security checks (largest in industry) |
| Patch Coverage | 60-70% of devices | 100% coverage |
| Device Onboarding | Manual tagging needed | Fully automated |
| Visibility | Unclear patch status | Real-time actionable dashboard for continuous tracking |
| Operational Effort | High manual effort | Minimal intervention |
| Security Posture | Unpatched endpoints left vulnerable | Every device protected |

# Why Qualys Fell Short

## 1. Siloed approach to vulnerability and patch management

- Manual correlation required between detected vulnerabilities and available patches
- No automatic remediation mapping, meaning IT teams had to research and validate patch applicability manually
- Increased risk of delayed remediation and incomplete fixes due to disconnect between detection & action

## 2. Limited vulnerability intelligence

- Vulnerability assessments were not real-time and relied on less frequent database updates
- Assessments were periodic rather than continuous, creating windows of undetected exposure
- Without real-time detection, emerging vulnerabilities often went unnoticed until the next scheduled scan

## 3. Manual, Tag-Based Patching Process

- Required IT teams to manually assign tags to devices before patching
- Devices without tags remained unpatched indefinitely
- High risk of security gaps and compliance failures

## 4. No Automated Device Allocation

- New devices weren't automatically assigned to patching groups
- Many devices sat unassigned, missing critical security updates

## 5. Rigid Patching Cycles

- No flexibility for teams like Customer Support, who needed controlled patching schedules
- Lack of customization meant teams couldn't align patching with business operations

## 6. High Operational Overhead

- Routine tasks such as tagging devices, assigning patch cycles, and managing patch groups were manual and repetitive
- Manual processes slowed down overall security operations

## 7. Poor Visibility and Reporting

- IT teams had no clear view of which devices were patched and which were not
- Difficult to track, audit, and optimize patching workflows
- Inability to get detailed insights on patch metrics

# How Saner CVEM transformed the vulnerability management process

Saner CVEM offered a proactive and comprehensive approach to vulnerability management. By detecting and assessing vulnerabilities continuously, the platform ensured that the patches were deployed and applied in a timely manner. It allowed them to remediate vulnerabilities quickly and helping them implement a continuous vulnerability management strategy that can adapt to changing needs.

### Faster Detection and Assessment
High-speed 5-minute scans powered by the world's largest vulnerability database to assess vulnerabilities rapidly

### Continuous Visbility
Unified dashboard for instant tracking of vulnerability and patch status across all devices

### Automated Patching Policy
Devices automatically onboarded and assigned to cycles

### 100% Endpoint Targeting
No device is left unpatched

### Custom Patch Scheduling
Teams like Customer Support get controlled patching timelines

### Detailed Patch Metrics
Track detailed insights into patching metrics with auto-generated reports and an inbuilt audit log

### Easy Security Compliance
Unified view of patch compliance to address deviations from compliance standards

# Key Benefits

- Clarity on types of Vulnerabilities
- Low Overheads
- Zero Patch Failures
- Hands Free Automation
- Operational Flexibility
- No Business Downtime
- Faster Remediation
- Stronger Security Posture

# Testimonial

*"It is a pretty easy-to-use tool when it comes to automation. You don't have to go through hundreds of options or hundreds of menus to be able to dig that patching task. I can quickly start my day, look at the cyber hygiene score, and ensure it is up to the expected mark. I clearly know what needs to be addressed and can quickly remediate it. It is much easier. I can get the patching job done in just a few clicks."*

***- Tech Support Manager***

TRANSFORMATION STUDY

SecPod is a leading cybersecurity technology company committed to preventing cyberattacks through proactive security. Its mission is to secure computing infrastructure by enabling preventive security posture.

At the core of SecPod's offerings is the Saner Platform - a suite of solutions that help organizations establish a strong security posture to preempt cyber threats against endpoints, servers, network and cloud infrastructure, as well as cloud workloads. With its cutting-edge and comprehensive solutions, SecPod empowers organizations to stay ahead of evolving threats and build a resilient security framework.

Visit us: www.secpod.com

secpod