CASE STUDY

LARGE EUROPEAN MEDICAL TECHNOLOGY COMPANY OVERCOMES PATCH MANAGEMENT COMPLEXITIES ACROSS 18,000 DEVICES TO ACCELERATE RISK REDUCTION AND TRANSFORM SECURITY POSTURE

Profile

The company pioneers breakthroughs in healthcare. With more than 50,000 employees across more than 70 countries, it offers an impressive portfolio of products and services, including medical imaging, laboratory diagnostics, point-of-care testing, healthcare IT, digital solutions, and automation, including clinical specialties.

secpod

CHALLENGE

Siloed approach to patching vulnerabilities leading to poor visibility into risk

The company's IT team took small steps to patch endpoints and servers using siloed tools such MS Update Manager, Ivanti Patch Manager & MS WSUS. They used Qualys Agent & Vurious (client's own scanning tool) for vulnerability scanning and prioritization. This was a risk-averse approach, and the outcomes did not meet expectations. The team was cutting corners due to the legacy approach to patch management, resulting in a surge of vulnerabilities.

The paradox of this approach to patch management is that although the existing tools detected the vulnerabilities, they could not patch them in their entirety and did not have the speed to fix them within a stipulated time frame. They were also not able to get clarity on their software inventory, especially license optimization.

With more than 8000 devices running on Windows and Linux, the tools could not roll back patches in case of failure, had unfriendly dashboards, could not patch third-party applications, and couldn't reboot themselves. Moreover, the licenses were costly.

Patching and tracking system updates to mitigate risks became daunting tasks. These circumstances made the team decide to break the continuity of the existing patch management processes for better upkeep of their technology infrastructure.

THE SOLUTION

SANER CVEM

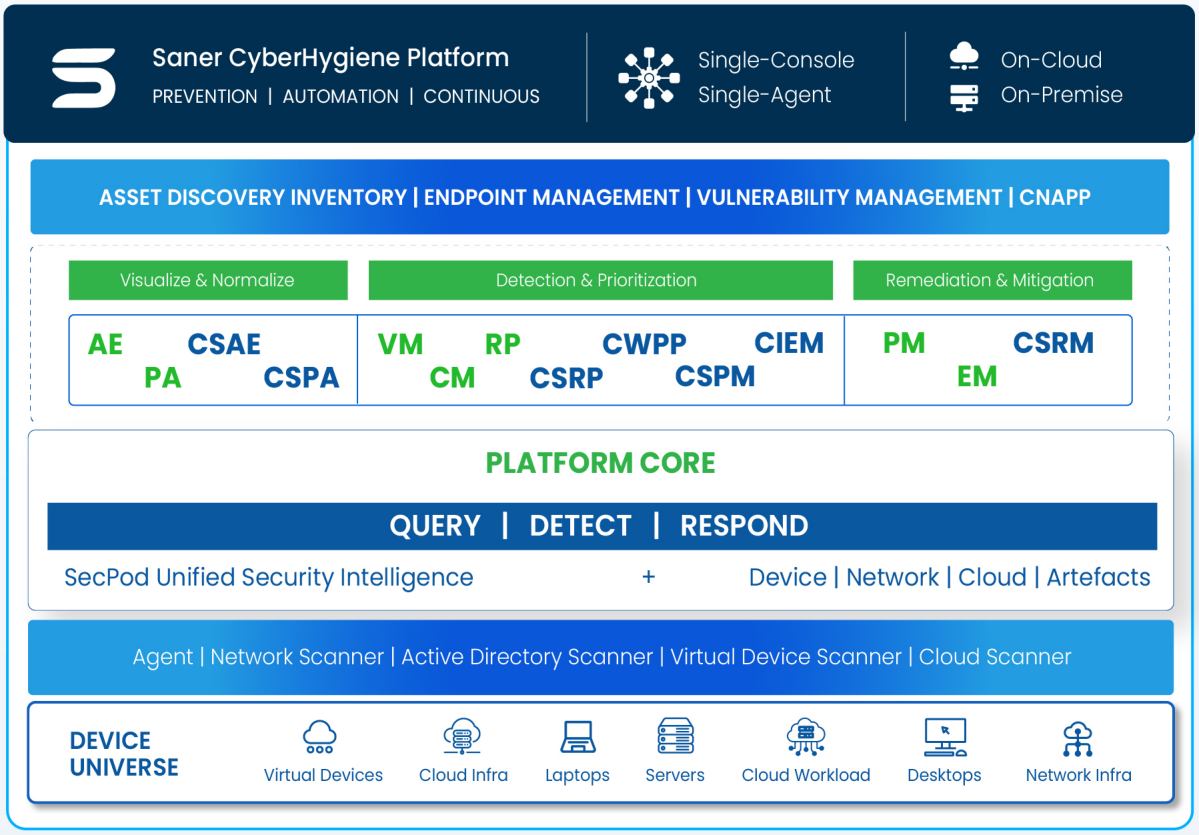
To automate the patch management process across operating systems & third-party applications

Saner CVEM's patch management module ensured a centralized perspective to enable better focus and insight into patch management. The shift to Saner CVEM granted the team the profound power to manage patches and the foresight to tackle any emerging vulnerabilities.

The platform helped identify and focus on the patching gaps across third-party applications running on Windows and Linux. Saner CVEM's patch management module was integrated into its existing vulnerability scanning, detection, and prioritization tools to accomplish its risk reduction goals. The asset inventory module tracked IT assets and software licenses to help with asset use, cost control, and license optimization.

SANER CVEM FOR RISK REDUCTION

Saner CVEM, with its comprehensive coverage and patching of vulnerabilities helped the IT team to advance and accelerate their vulnerability management program.



Note: The client has opted exclusively for the Asset Exposure (AE), Vulnerability Management (VM), and Patch Management (PM) modules.

ASSET EXPOSURE MODULE

To provide detail and context to the catalog of endpoint assets

Ensured continuous visibility and control over IT infrastructure, enabling better control over IT assets. They were able to discover rarely used and outdated applications, track software licenses, and continuously evaluate the use of assets. ***Know more about AE module.***

VULNERABILITY MANAGEMENT

To holistically scan and detect vulnerabilities

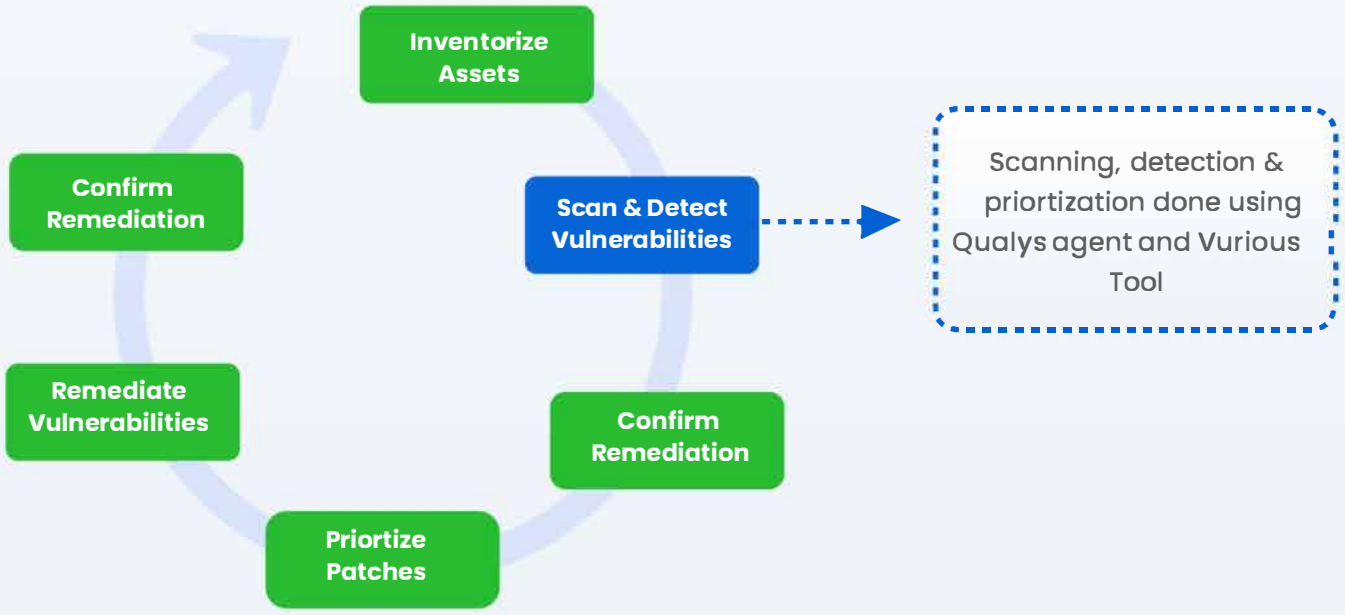
Comprehensive, proactive, continuous scans across every endpoint and server, assessed the status of vulnerabilities, the level of risk tolerance, the level of threat represented by each exposure, and vulnerabilities that need immediate fixes. ***Know more about VM module***

PATCH MANAGEMENT

To speed up patch deployment and remediate risks

Automated end-to-end patch management from scanning, prioritization, download, and testing to scheduled deployment ensured faster deployment cycles across every deployed device, eliminating manual interventions. ***Know more about PM module.***

SANER CVEM PATCHING CYCLE TO SPEED UP REMEDIATION



OUTCOMES

- Patch endpoints at speed and scale and gain clarity on patch compliance status
- Create reports on the patching status of the network
- Experienced comprehensive visibility of endpoints and license management
- Reduced vulnerabilities by 90% across 18000 devices

ABOUT SECPOD

SecPod is a leading cybersecurity technology company committed to preventing cyberattacks through proactive security. Its mission is to secure every connected computing device across modern enterprises by delivering preventive, automated, and intelligent cybersecurity.

At the core of SecPod's offerings is the Saner Platform - a suite of solutions that help organizations establish a strong security posture and prevent cyberattacks before they strike.

The platform includes:
Cloud Security– An AI-fortified Cloud-Native Application Protection Platform (CNAPP) that delivers continuous visibility, security compliance, and risk mitigation for cloud environments.

Vulnerability & Exposure Management – A Continuous Vulnerability and Exposure Management (CVEM) solution that delivers continuous visibility, identifies, assesses, and remediates vulnerabilities across enterprise devices and network infrastructure.

Endpoint and Patch Management – A Continuous Risk Remediation solution that minimizes the attack surface by eliminating potential risks across the IT infrastructure.

With its suite of cutting-edge and comprehensive solutions, SecPod empowers organizations to stay ahead of evolving threats and build a resilient security framework.

GLOBAL FOOTPRINT

Bengaluru, India

California, United States of America

Ho Chi Minh City, Vietnam

Warszawa, Poland

CLIENT TESTIMONIAL

Before Saner CVEM, patching and vulnerability management consumed a significant portion of our team's time and attention. Today, those processes run seamlessly in the background. The platform has brought consistency, confidence, and clarity to how we manage risk across our environment. With reliable automation and visibility into vulnerabilities, our team is no longer stuck reacting, we're able to work proactively on strategic security initiatives. Saner CVEM is helping us strengthen our security posture without increasing operational overhead.

- IT Team

For enquiries, contact us at:

Email: info@secpod.com
Website: www.secpod.com