Profile

With a global footprint spanning India, the United States, United Kingdom, Brazil, and Australia, this multinational pharmaceutical enterprise operates across seven business units and manages multiple endpoints and servers. The company's infrastructure covers diverse operating systems, including multiple Linux and Windows variants, as well as complex firewall and network configurations.

Introduction

The global pharmaceutical company faced persistent challenges in vulnerability detection and remediation. Its existing setup, which involved agentless periodic scanning via a top cybersecurity solution, created significant blind spots and operational delays. The absence of continuous visibility and credible proof-of-concept (PoC) evidence created friction between IT and security teams and led to delayed remediation.

The core concern was growing false positives, nearly 30%, and lack of actionable insights. These inefficiencies led the company to reevaluate its vulnerability management program and search for a solution that could bring accuracy, automation, and better collaboration.

CASE STUDY

REDUCING FALSE POSITIVES AND STREAMLINING RISK MANAGEMENT FOR A GLOBAL PHARMACEUTICAL COMPANY

THE PROBLEM

Prior to adopting Saner CVEM, the pharmaceutical company faced multiple issues that obstructed its security objectives:

Manual Risk Validation and Remediation

Vulnerability data required extensive manual cleanup and validation before any action could be taken.

Limited Visibility into Ownership and Risk Prioritization

The team lacked clarity on who was responsible for remediation, which led to inefficiencies and miscommunication.

High Volume of False Positives

Over 30% of the vulnerabilities flagged by their earlier tool were inaccurate, sparking frequent conflicts between infrastructure and security teams.

No Proof of Evidence for Vulnerabilities

Without a verifiable record of vulnerabilities, remediation efforts were often stalled due to lack of consensus.

Credential Access Barriers

Agentless scanning demanded super-admin credentials across systems, something the security leadership did not permit.

Compliance Gaps

Without continuous and reliable vulnerability assessments, meeting standards like HIPAA, GDPR, and ISO was challenging.

The company realized that its current approach was not scalable or reliable, prompting the need for a more comprehensive platform with stronger remediation alignment and risk accuracy.

THE SOLUTION

Saner CVEM replaced the pharmaceutical company's previous setup with a unified, agent-based and agentless vulnerability and risk management framework. Its features directly addressed the organization's requirements for proof-backed scanning, ownership clarity, and compliance readiness.

The solution involved five key components:

VULNERABILITY MANAGEMENT

Saner CVEM introduced continuous scanning across servers, endpoints, and network devices.

- **Reduced false positives** by offering verifiable PoC evidence for each vulnerability.
- Introduced **ownership tagging** to map systems to the responsible teams, improving accountability and communication.
- **Enabled categorization of vulnerabilities** by OS and applications, streamlining remediation workflows.

RISK PRIORITIZATION

Risk context and exploitability scores allowed the team to focus efforts where they mattered most.

- **Built custom dashboards** for ownership groups across internal units such as JXP, business-critical applications, and internet-facing workloads.
- Simplified issue resolution by providing clear, **visualized data on existing vulnerabilities** and their impact.
- Used **RACI matrices to track responsibility** and progress, helping align IT and InfoSec teams effectively.

COMPLIANCE SUPPORT

With Saner CVEM, the company could now confidently meet global regulatory requirements.

- Enabled **periodic vulnerability assessments** required under GDPR.
- Provided **structured audit trails** and remediation logs necessary for ISO and HIPAA evaluations.
- **Identified vulnerabilities in both infrastructure and applications,** as mandated by global pharma compliance frameworks.

OPERATIONAL EFFICIENCY

Saner CVEM helped eliminate redundant manual steps and gave InfoSec teams a strategic edge.

- **Reduced time spent filtering inaccurate alerts** and allowed faster coordination with application owners.
- Enabled **data-driven decision-making** for security stakeholders across all seven business units.
- Improved collaboration between infrastructure and security teams through **tagging and centralized visibility.**

EVALUATION AND PROCUREMENT FIT

Saner CVEM outperformed alternatives during internal evaluations.

- **Addressed all purchase criteria:** on-prem compatibility, accurate scanning, actionable PoC evidence, and cost feasibility.
- Delivered value through a successful **proof-of-concept exercise,** which aligned with both operational needs and management expectations.

RESULTS

Since adopting Saner CVEM, the pharmaceutical company has made measurable strides in security and operational control.

RISK REDUCTION

- Reduced false positives from **30% to near-zero** through accurate validation and evidence-based scanning.
- **Improved detection and classification** of both OS-level and application-specific vulnerabilities.

OPERATIONAL SAVINGS

- **Eliminated extensive manual effort** previously spent validating risk data.
- Streamlined inter-team workflows by **assigning ownership tags and shared dashboards.**

COMPLIANCE READINESS

- Met GDPR, ISO, and HIPAA audit requirements through **consistent vulnerability assessment and reporting.**
- **Delivered periodic application** and infrastructure scans aligned with regulatory guidelines.

COLLABORATION GAINS

- **Improved alignment** between InfoSec and Infra teams through visibility and tagging.
- Replaced friction with evidence-based discussions, **improving trust and resolution speed.**

CATEGORY COMPARISON

Category	Before Saner CVEM	After Saner CVEM
VULNERABILITY MANAGEMENT	Agentless scanning with high false positives.	Continuous, PoC-backed scanning with deep and persistent visibility.
RISK PRIORITIZATION	Manual analysis and rating.	Context-aware risk models and ownership mapping.
SECURITY VISIBILITY	No clear mapping of systems or responsibility.	Dashboard-based ownership and RACI matrix.
COMPLIANCE	Periodic scans without audit-ready data.	Regulatory-aligned reporting for GDPR, ISO, and HIPAA.
COLLABORATION	Frequent conflicts between security and infra teams.	Centralized dashboards with tagging for faster resolution.
FALSE POSITIVES	30% of vulnerabilities misclassified.	Nearly zero false positives with proof-based validation.
PATCH MANAGEMENT	Managed outside the platform via SCCM and other tools.	Vulnerability data shared with patch teams for better targeting.

ABOUT SECPOD

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 preemptively block cyber threats.

The platform includes:
SANER CLOUD – An AI-fortified Cloud-Native Application Protection Platform (CNAPP) that delivers continuous visibility, security compliance, and risk mitigation for cloud environments.
SANER CVEM – A Continuous Vulnerability and Exposure Management (CVEM) solution that delivers continuous visibility, identifies, assesses, and remediates vulnerabilities across enterprise devices and network 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.

CLIENT TESTIMONIALS

"Saner CVEM helped us gain clarity and control over our vulnerability data. The false positives we dealt with earlier are no longer an issue. With ownership tagging and evidence for every observation, our remediation cycles have become faster and less contentious. Saner CVEM has helped us scale security across all seven business units with greater confidence."

- InfoSec Team, Global Pharmaceutical Company

INDIA
Ground Floor, Tower B,
Subramanya Arcade, No. 12,
Bannerghatta Road,
Bangalore, Karnataka,
560029, India.

UNITED STATES OF AMERICA
SecPod Technologies, Inc.
303 Twin Dolphin Drive,
6th Floor Redwood City,
California, 94065,
United States of America.

For enquiries, contact us at:

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