Profile

A globally distributed enterprise operating across 60+ countries and multiple business units, with an endpoint footprint of over 200,000+ devices. Its heterogeneous IT environment supports technology, consulting, and business services and is globally governed, requiring centralized visibility and strong operational control.

secpod

CASE STUDY

ACHIEVING ENTERPRISE-SCALE ENDPOINT SECURITY AND COMPLIANCE ACROSS 200,000+ DEVICES

CHALLENGE

Managing endpoint security and compliance at this scale had become increasingly difficult and resource intensive.

The customer faced multiple, compounding challenges:

- Limited consolidated visibility across a very large and distributed endpoint estate
- Multiple point tools used independently for vulnerability assessment, compliance checks, patching, and endpoint controls
- Heavy manual effort required to correlate findings and drive remediation across tools
- A rapidly growing vulnerability backlog, with remediation unable to keep pace
- Inability to consistently meet compliance objectives, particularly those aligned to CIS benchmarks

In addition, with distributed and end customer specific project teams, the global enterprise had a challenge over software hygiene at the endpoint level:

- Difficulty identifying unsigned applications across the environment
- Lack of effective mechanisms to detect and eliminate unauthorized software
- Increased risk from unmanaged and non-compliant applications operating outside defined security policies

These issues not only increased security risk but also created significant audit and operational overhead.

THE NEED

The customer concluded that the root cause was not a lack of tools, but a lack of unified visibility, correlation, and enforceable controls across endpoints.

They required a solution that could:

- Discover and normalize all endpoint assets
- Identify vulnerabilities, misconfigurations, unsigned applications, and unauthorized software in a single continuous scan
- Enforce endpoint policies at scale, not just report violations
- Reduce dependency on manual intervention

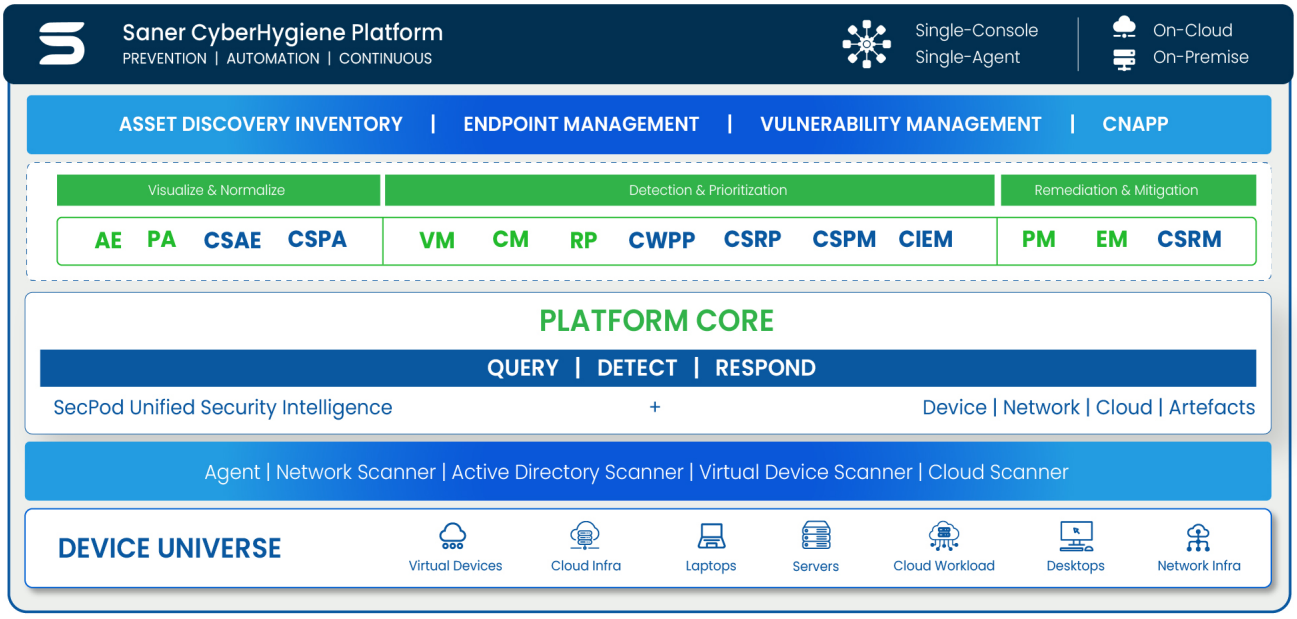
THE SOLUTION

The customer deployed SecPod as a unified endpoint exposure and control platform.
Know more about Saner CVEM.

The following modules were implemented:

- **Asset Exposure Management:** Continuous discovery and normalization of all endpoint assets
- **Vulnerability Management:** Identification, prioritization, and remediation of vulnerabilities
- **Compliance Management:** Detection and correction of CIS-aligned configuration drift
- **Patch Management:** Automated OS and third-party patching
- **Endpoint Management:** Identification and elimination of unsigned and unauthorized applications, enabling enforceable software hygiene policies

All capabilities operated from single pane of glass, single platform powered by SecPod's own unified security intelligence (a large database of more than 200,000+ vulnerability checks) eliminating silos between detection to remediation.



PHASE	WHAT SECPOD DID	ACTIONS TAKEN	OUTCOME
Asset discovery & normalization	Built an asset inventory of 200,000+endpoints	Continuous scans, normalize assets, resolve duplicates, map owners	Single source of truth of IT environment
Endpoint readiness	Ensure all endpoints are reachable & manageable	Agent rollout/ agent verification, connectivity checks, ensure manageability at scale	Endpoints ready for centralized control & automation
Group assets	Established ownership and remediation timelines	Group endpoints by region/business unit, assign SLAs	Clear ownership /accountability with remediation timelines
Automated remediation	Executed patches at scale by replacing manual interventions	Automated OS and third-party patching, policy enforcement	Faster remediation and reduced manual effort
Reporting	Build audit ready reports	Automate weekly reports, SLA tracking,	Continuous CIS compliance & reduced manual reporting

MEASURABLE OUTCOMES

- 95% achievement of defined compliance goals within six months, covering:
  i. Vulnerability reduction
  ii. Elimination of unsigned applications
  iii. Removal of unauthorized software
  iv. Remediation of CIS-relevant configuration drift
- Significant reduction in vulnerability backlog
- Major reduction in manual effort across security and IT teams
- Consistent, auditable endpoint posture across 200,000+ devices
- Clear path toward zero-touch vulnerability and endpoint compliance management

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 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.

GLOBAL FOOTPRINT

Bengaluru, India
Ho Chi Minh City, Vietnam
Warszawa, Poland
California, United States of America

www.secpod.com