



A SanerNow Solution for Regulatory
Compliance & Configuration Hardening

Improve Asset Visibility, Reduce Endpoint Risks & Meet Regulatory Needs

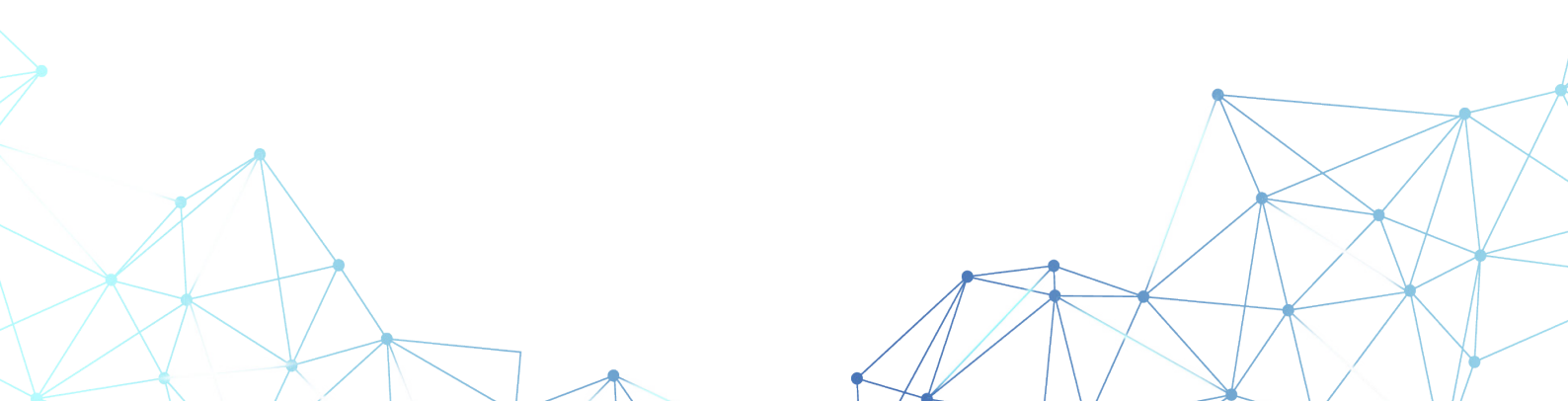
Get Actionable, Customizable Reports. Reduce Attack Surface. Stay Audit-ready.

With the regulatory landscape getting more complex, it's a no-brainer for organizations to strengthen their compliance activities. This isn't that easy, as many of them are still stuck managing their security operations using siloed tools. Launching a counter-offensive on vulnerabilities using these tools to achieve compliance is a next-to-impossible tussle. They sow enough doubts in their ability to understand the distinct world of vulnerabilities and be on the front lines to face the tough reality of managing vulnerabilities across every layer of the infrastructure.

The existential threat of vulnerabilities isn't going to decrease, and security operations must modernize and can't go into hibernation or remain unstable. Organizations need a comprehensive and demonstrable compliance management program driven by an integrated platform to meet changing regulatory standards. However, security teams are still straddling multiple questions on fundamental matters on how to achieve compliance.

These questions arise due to the manual and resource-intensive processes of siloed tools, limited visibility of assets, complex compliance requirements, problems in prioritizing vulnerabilities, lack of an integrated platform, inability to keep abreast with threats due to lack of continuous threat intel feeds, and challenges in getting audit ready customizable reports. These discrepancies and doubts that arise due to siloed tools can be fixed with SecPod's compliance management solution.

SecPod's SanerNow ensures the IT infrastructure is audit-ready, assures compliance, and reduces the attack surface. An integrated vulnerability platform, the platform is an effective lever to maintain compliance. It brings together the best practices of end-to-end compliance management, from detection, prioritization, and remediation to meet global or regional regulatory need.



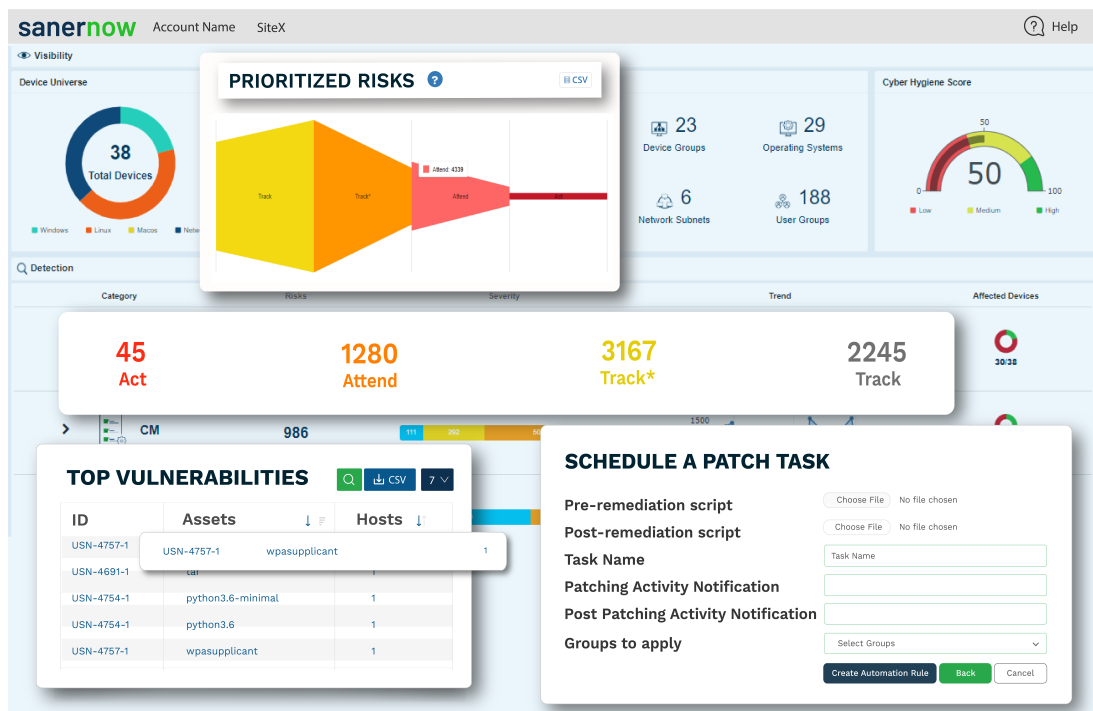
Attain Compliance Integrity at Speed

The compliance management solution has been impressing IT teams with its integrated capabilities to meet regulatory needs. It can obliterate vulnerabilities, streamline security operations, and identify and close gaps in compliance management. The solution is a strategic fit for your security modernization initiatives as it can scale at speed to meet business needs and transformation objectives.

With its proactive and fully automated approach, the solution can continuously verify the compliance integrity of the IT infrastructure environment from end-user computing, data centers, software platforms, operating systems, and cloud workloads.

Far ahead of siloed tools, it has all the necessary controls to drive enterprise-grade compliance management initiatives across hybrid IT environments.

IT teams can now respond and recover from growing vulnerabilities, capitalize on security investments, and derisk the vulnerability challenge across the IT infrastructure. They will be able to stay current with evolving regulations by getting a holistic view of IT inventory, running compliance scans, detecting anomalies, deviations, misconfigurations, and outliers, prioritizing & remediating vulnerabilities, and through audit-ready reports.



Enhance Control and Maintain Compliance

- ✓ Accurately detect global and local IT assets to get a single-pane-of-glass visibility with quick and real-time scans for comprehensive inventory views and asset transparency
- ✓ Discover rarely used and outdated assets or applications to enable decisions on IT asset usage, cost control, and license optimization
- ✓ Drive regular scans to detect any changes in software and hardware
- ✓ Ensure proactive, continuous, automated real-time detection and tracking of assets through a unified cloud-based console
- ✓ Detect malicious software or hardware and block them
- ✓ Automate tracking of OS and third-party applications and drill down into the details of each instance
- ✓ Comprehensive assessment of IT infrastructure and identification of devices different than others using machine learning, statistical analysis, and deviation computation methods
- ✓ Mitigate risks with comprehensive scans based on SecPod's largest built-in vulnerability database with 175,000+ software vulnerability checks
- ✓ Lightweight agent-based scanner which can scan and detect vulnerabilities in 5 minutes



Enhance Control and Maintain Compliance

- ✓ Perform accurate vulnerability detection and prioritization with insights on vulnerabilities based on severity level, exploitability level and isolate high-risk ones.
- ✓ Easily deploy patches across firmware, Windows, Linux, macOS, including 450+ applications
- ✓ Patch support within 24 hours from all supported vendors using an integrated patch manager
- ✓ Detect non-compliant devices by identifying faulty system configurations with fast compliance scans
- ✓ Monitor remote devices easily and simplify compliance reporting
- ✓ Drive compliance risk assessments and get insights on risk remediation
- ✓ Customize compliance policies on available system configurations
- ✓ Convert compliance updates into customizable reports



One Platform. One Agent.

The platform is an ideal choice for attack surface management. With the explosion in distributed IT computing environments, the attack surface is rising. IT teams find it hard to gain a strong footing by keeping track of these assets and who is using them. By using the platform, IT teams can overcome the challenges of legacy tools, which are slow, manual, and error-prone. It works at speed and scale to discover, identify, and prioritize risks across public-facing assets, whether on-prem or cloud workloads.

Scan

Intelligent scanner capable of 5-minute lightning-speed scans. Continuous, on-demand, real-time scans can be scheduled without consuming excessive bandwidth or network resources.

Visualize

Gain 360-degree clarity on software asset exposure, including rarely used/outdated software & its licenses, get unparalleled visibility, monitoring, and access anytime from anywhere with a unified cloud-based console, and track software usage metrics.

Normalize

Discover vulnerable processes making outbound connections, unusual command execution, disabled BitLocker in systems, abnormal events, installation of any unfamiliar applications, and map it with software bill of materials.

Detect

Finds vulnerabilities that can cause high-fidelity attacks. Provides exploitability levels of vulnerabilities, including CVSS information. Ensures near-zero false positives.

Prioritize

Understand and evaluate millions of vulnerabilities to enable mitigation efforts. Prioritizes risk based on exploitability, business impact, and vulnerability data analysis. Gives exhaustive visibility of risks.

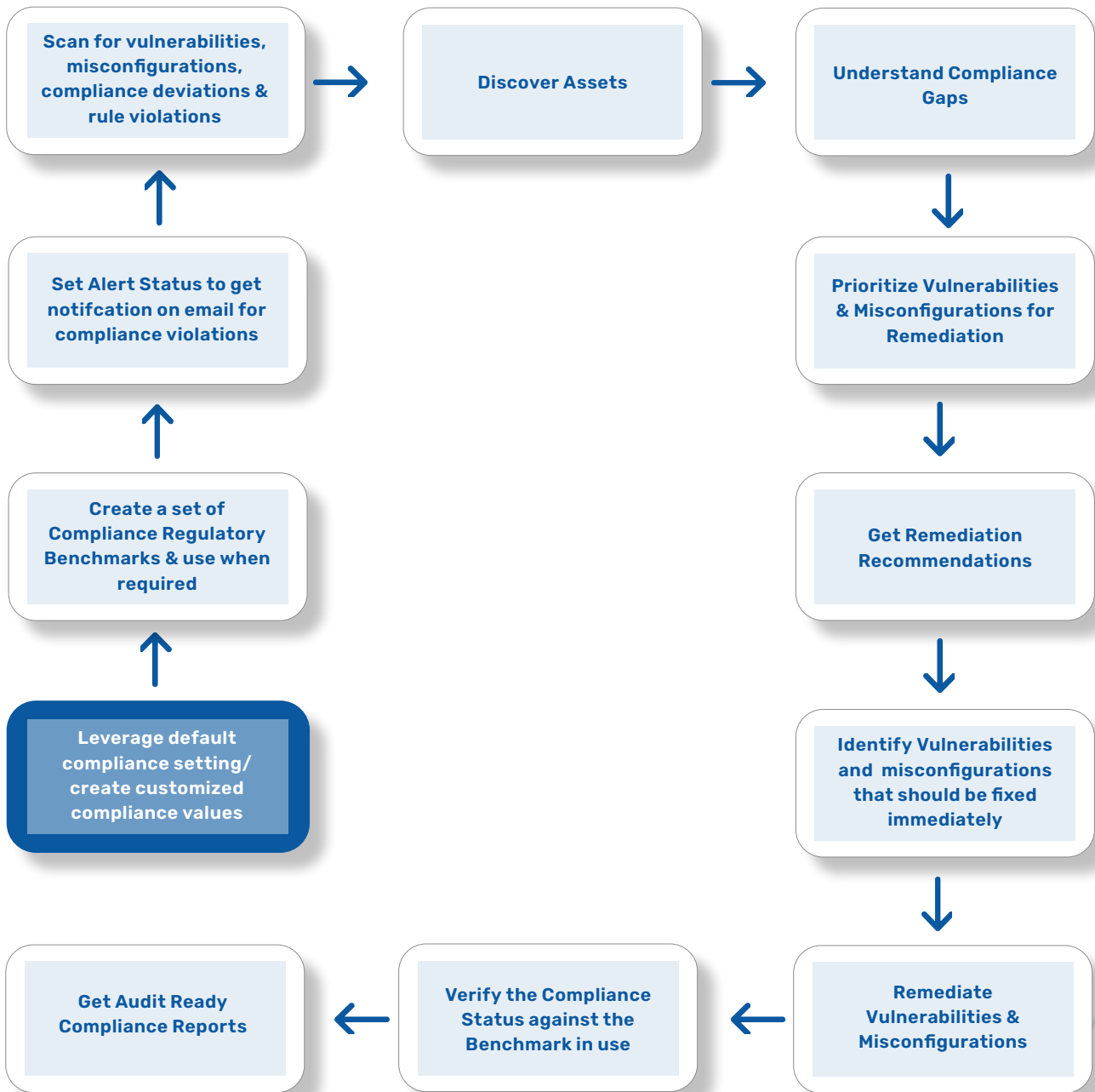
Remediate

Integrated remediation engine to deploy patches across distributed devices and fix vulnerabilities and misconfigurations in Win, MacOS & Linux. Roll-back feature for error-prone patches. Latest vendor patch updates in 48 hours, including third-party & firmware patches. Ensures endpoint health by applying strong security controls, monitoring endpoint settings & configurations. Blocks malicious applications, install & uninstall software, system tuning, blocks rogue devices, & fixes security deviations and anomalies.

Comply

Compliance manager to identify missing system configurations, monitor remote devices, simplify reporting, and ensure continuous compliance scans to fulfill regulatory needs. Run continuous compliance scans, detect non-compliant devices, run compliance risk assessments, and customize compliance policies.

Solution Workflow to Realize Value



Integrated Automated Platform for Security Governance, Risk Management

The compliance management solution helps to reconcile regulatory objectives even more deeply. The platform can ensure astute governance of the vulnerability enclave in the IT infrastructure. With its integrated approach, the solution can overcome the complexities and challenges of siloed systems, which can be circuitous in its approach leading to errors, inconsistencies, and non-compliance.

By fully automating the compliance process, it can automate repetitive tasks and processes, resulting in improved accuracy and consistency

with its standardized workflows. There is improved visibility to compliance activities, this includes, prioritizing vulnerabilities & misconfigurations, monitoring remediation progress, and taking corrective actions, when needed.

Moreover, compliance activities can be managed through a centralized platform and can also be customized to meet changing regulatory requirements.



Security Governance

Evaluate gaps in Security Posture, establish structure & expectations in vulnerability management, align cyber risks with enterprise security goals, monitor/measure/report/improve vulnerability management programs



Security Risk Management

Continuously identify vulnerability risks, analyze the materialization of risks/scale of impact, prioritize risks based on their level of impact, exploitability & business context



Security Operations

Proactive Scanning, Detection, prioritization & remediation of vulnerabilities & misconfigurations, security intelligence feed for accurate detection, manage loss & alerts, and refine security posture continuously

Achieve Compliance with Ease

- » Operate in Multiple jurisdictions or Industry Sectors
- » Consolidate & Simplify Compliance Requirements
- » Automate Compliance with no upfront Investments
- » Collaborate/co-ordinate across departments/functions
- » Leverage best practises in Compliance Management
- » Get Custom Audit Ready Reports
- » Meet any Global or Regional Compliance Requirement

Modules in the Solution Stack



Asset Exposure Module

Ensure continuous visibility and maximize control over IT asset infrastructure by managing software and hardware assets in real time.

- » Track software usage metrics & automatically track asset movements in the network
- » Runs real-time, live asset scans on enterprise devices to gain a comprehensive 360-degree view of inventory with complete transparency
- » Track rarely used & update applications, including software licenses, to optimize asset use
- » Manage vulnerable assets and blacklist malicious and outdated apps

Posture Anomaly Management Module

Assess the network to discover deviations or aberrations, spot anomalies in the network from unusual services & processes, abnormal events in event logs, unwanted ports, unsigned applications, unusually executed commands, and hidden risks.

- » Get intelligent insights on hidden security loopholes in the network and act on these insights to prevent attacks
- » Assess the IT infrastructure and identify the devices that are different from others
- » Get instant remediation measures to fix anomalies
- » Discover attack vectors in the network and reduce risk exposures

Vulnerability Management Module

Operates through a lightweight single agent, which also acts as the single point of management to orchestrate the entire end-to-end process.

- » Continuous, periodic scanning using the world's only automated, high-speed scanner to detect vulnerabilities in just 5 minutes.
- » All scans based on the continuously updated SecPod's world's largest vulnerability & threat intelligence feed
- » Unified cloud console to manage vulnerabilities in decentralized, hybrid IT environments

Compliance Management Module

Regulate devices for PCI-DSS, HIPPA, ISO, NIST, RBI, SEBI, or any other compliance standard with the help of the compliance manager to address configuration drifts.

- » Run compliance checks & detect non-compliance devices.
- » Monitor remote devices & enforce custom industry compliance policies.
- » Ensure the IT environment is audit-ready.
- » Get customized, insightful reports to meet regulatory needs

SSVC-based Vulnerability Risk Prioritization Management Module

Rapidly prioritizes risk and can handle millions of vulnerabilities with ease. Get exhaustive visibility into risk to reduce exploitable attack surface.

- » Automates risk prioritization in real-time by combining SSVC framework with enhanced exploit prediction scoring system, & ML algorithms, & MITRE ATT&CK mapping capabilities
- » Gain decisive insights into prioritizing risks & improve security posture
- » Customize risk prioritization & configure it into based on org structure to calculate business impact

Patch Management Module

Easily deploys patches across distributed devices, remediates vulnerabilities, fixes misconfigurations, & offers a unified view of patching tasks.

- » Continuous, customizable patch scans to find missing patches.
- » Deploys patches across Win, MacOS & Linux and third-party applications.
- » Pre-tested, ready for deployment patches ready within 24 hours.
- » Rollback feature for any error-prone patches.
- » Prioritize patch deployment. dashboards

Endpoint Management Module

Ensure every endpoint across the decentralized, distributed environment functions in peak capacities. Go beyond patching and strengthen endpoint security posture through comprehensive security checks.

- » Monitor more than 100 endpoint health controls in real-time.
- » Configure security settings & manage software licenses.
- » Automate security control activities across major OS platforms.
- » Deploy software & monitor system health.
- » Evade threats by blocking malicious applications.

How the Solution Controls help in Achieving Compliance

SanerNow Controls	Security Control Implementation	PCI DSS Controls	HIPPA Controls	NIST Controls	CSF Controls	SOC 2 Controls
Hardware & Software Roster Maintenance, including BOM	<ul style="list-style-type: none"> » IT asset inventory visibility » Establish and maintain a Software Inventory 			✓	✓	
Find Unwanted Devices in the Network	Find Unauthorized/ Unwanted Devices				✓	✓
Automated Vulnerability Management, Patch Management & Remediation	Continuous Vulnerability Management and Patch Management	✓		✓	✓	✓
Centrally Manage Software Deployment, Configure Software, Device Use Control	Install/Uninstall Security Software, Software Configuration, enable Software Features, Manage Software, Misconfigurations	✓		✓	✓	✓
Security Policy Compliance	Create, Customize, and Institutionalize Security Policies for Compliance	✓	✓	✓		✓
Risk Mitigation to Acceptable Limits						✓

Overcome Vulnerabilities & Misconfigurations. Meet any Compliance Need.



Automated compliance management is critical to modernize compliance workflows. This can be effective risk assessments, evaluating security controls, or taking remedial actions to fix security violations. It ensures a rule-based approach to drive the entire end to end compliance management processes by automatically tracking any outstanding compliance tasks and alerting security teams based on preset rules.

The solution, with its high speed proactive, automated, high-speed scanning capabilities, offers a single source of truth for compliance programs, tracking all compliance activities in one place, ensuring accurate data for internal audits.

The platform helps to keep track of internal IT systems and controls to verify conformity to industry regulations through continuous monitoring, simplifying the process of collecting evidence to demonstrate adhere to standards and rules, and by seamlessly integrating with enterprise SOCs.

The solution can enable the implementation of an end-to-end vulnerability management program while adhering to compliance frameworks with ease. By integrating vulnerability management and compliance, SanerNow provides a risk-based approach to stay ahead of new threats and regulatory requirements and maintain the trust of customers and stakeholders.

About SecPod

SecPod is a cyber security technology company. We prevent cyberattacks. We do everything to prevent attacks on the computing environment. Our product helps implement cyber hygiene measures, so attackers have a tough time piercing through. Our SanerNow Cyber Hygiene Platform provides continuous visibility to the computing environment, identifies vulnerabilities and misconfigurations, mitigates loopholes to eliminate attack surface, and helps automate these routines. Our product philosophy is offering simplicity and automation to make the job of security administrators slightly better.

Visit us- www.secpod.com

Write to us- info@secpod.com

Connect with us



United States of America

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

India

SecPod Technologies Pvt. Ltd.
Ground Floor, Tower B,
Subramanya Arcade, No. 12,
Bannerghatta Road,
Bangalore, Karnataka,
560029, India.

Copyright 2024, SecPod. All rights reserved. No part of this document may be reproduced, stored in a retrieval system, transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the express written permission from SecPod. The information contained herein is subject to change without notice. All other trademarks mentioned herein are the property of their respective owners.