secpod

A SanerNow Solution for Asset Discovery and Normalization

Track, Monitor, and Manage Software & Hardware Assets and Reduce Attack Surface

www.secpod.com

Effectively Manage Vulnerable Assets. Eliminate Security Anomalies.

To sustain the pace of business growth & fuel value creation, organizations are looking at rapidly expanding their IT environments. Competitive dynamics are furthering the pace of this transformation, be it to increase revenue, lower operating costs, improve CSATs, or improve employee productivity. The speed and scale of this transformation can enlarge the attack surface due to an expanded IT estate. This is a serious concern and can compound the complexity of day-to-day security operations.

Here are a few.

Inability to Determine the Inventory of Assets

This can lead to no records of assets and their information, which can be problematic when they are ported across locations for various reasons. IT teams will face difficulties in knowing the assets they already have, where they are located currently, & their current license/warranty status.

Identify any changes in Hard-ware and Software

Difficulty in continuous asset scans to detect any deviations in hardware or software, including their usage metrics, through a centralized console for comprehensive views and transparency.

Increase in Security Deviations

Inability to secure large IT environments due to lack of comprehensive security posture visualization tools for discovering attack vectors and security loopholes. IT teams find it difficult to detect security weakness, and outliers in devices and track optimal functioning of security controls.

Reduced Compliance and Security

This arises due to a lack of customized reports and the inability to track IT asset discovery metrics. Security risks can increase because of Shadow IT, leading to inefficiencies and an inability to implement policies and procedures to stop the use of unauthorized IT resources.

Assess the Device Network for Security Gaps

IT teams find it hard to manage both visibility and continuously assess the network for any anomalies, such as deviations, aberrations, unusual processes/services, unnecessary ports, unsigned apps, unusually executed commands, or any other security loopholes that can become an obvious security risk.

IT teams can easily manage large asset portfolios, monitor device security across different locations, and overcome improper management, operational inefficiencies, or audit risks by using the continuous asset discovery and IT standardization solution from SecPod. It is a transformative solution with which IT teams can implement a robust asset tracking system and fully automated, high-speed continuous scans to establish a set of processes and procedures for asset security and maintenance.

Gain Max Visibility of IT Inventory and Manage Security Anomalies

- Track, monitor, and manage software and hardware assets in real-time
- Run real-time, live asset scans on devices to gain a comprehensive view of inventory
- Get software metrics such as rarely used or outdated apps, track software licenses to enable strategic decisions on IT asset usage, cost control, and license optimization
- Cloud-based console for end-to-end asset visibility and monitoring
- Automated and customizable asset reports for audit-readiness
- Track any changes or deviations in hardware or software inventory
- Insightful dashboards to display inventory data
- Track software usage metrics
- Automatically track and manage asset movements, including newly added or uninstalled hardware or software
- Detect the presence and entry of any malicious or vulnerable assets
- Easily track and manage licenses of OSs, third-party applications, and hardware
- Discover aberrations, deviations, and outliers in IT environment to uncover risks

Gain Max Visibility of IT Inventory and Manage Security Anomalies

- ✓ Spot anomalies from unusual services & processes, abnormal events in event logs, unwanted ports, unsigned applications, unusually executed commands, etc.
- ✓ Detect deviations in IT infrastructure and gain intelligent insights to find unnoticed security loopholes
- ✓ Assess IT infrastructure and identify the devices that are different than others and remediate the anomaly instantly
- ✓ Discover the obvious attack vectors in the network and implement more effective security measures
- ✓ Discover the obvious attack vectors in the network and implement more effective security measures
- ✓ Verify and whitelist devices and configurations in your environment
- ✓ Analyze security controls and find any malfunction in them
- ✓ Examine your security posture with insightful reports

One Platform. One Agent

The risk-based continuous asset discovery and IT standardization solution forms the foundation to establish a strong and reliable security posture. It empowers IT teams to discover endpoints, servers, or data centers continuously and automatically across a distributed and decentralized IT environment.

IT teams can gain clarity in real time and manage and secure these assets to make them highly accessible and available. With the help of insightful dashboards, IT teams can track and analyze attack vectors and ensure continuous compliance by detecting the presence of malicious assets, applications, or users. It is a platform with multiple capabilities driven by a single agent.

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.

Detect

Find changes in software or hardware, track IT asset lifecycle in real-time, recognize any anomalies and identify any vulnerable assets.

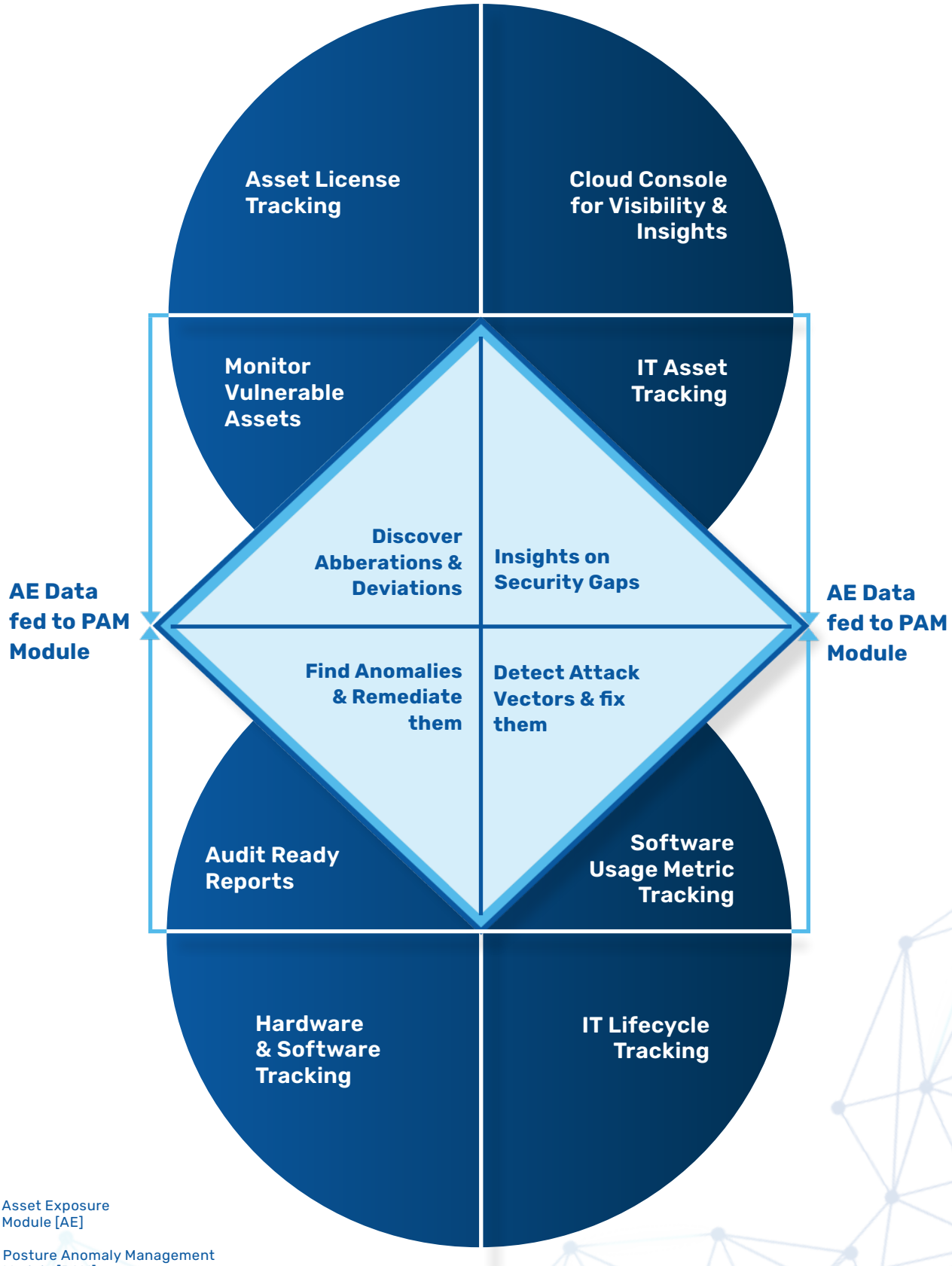
Visualize

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.

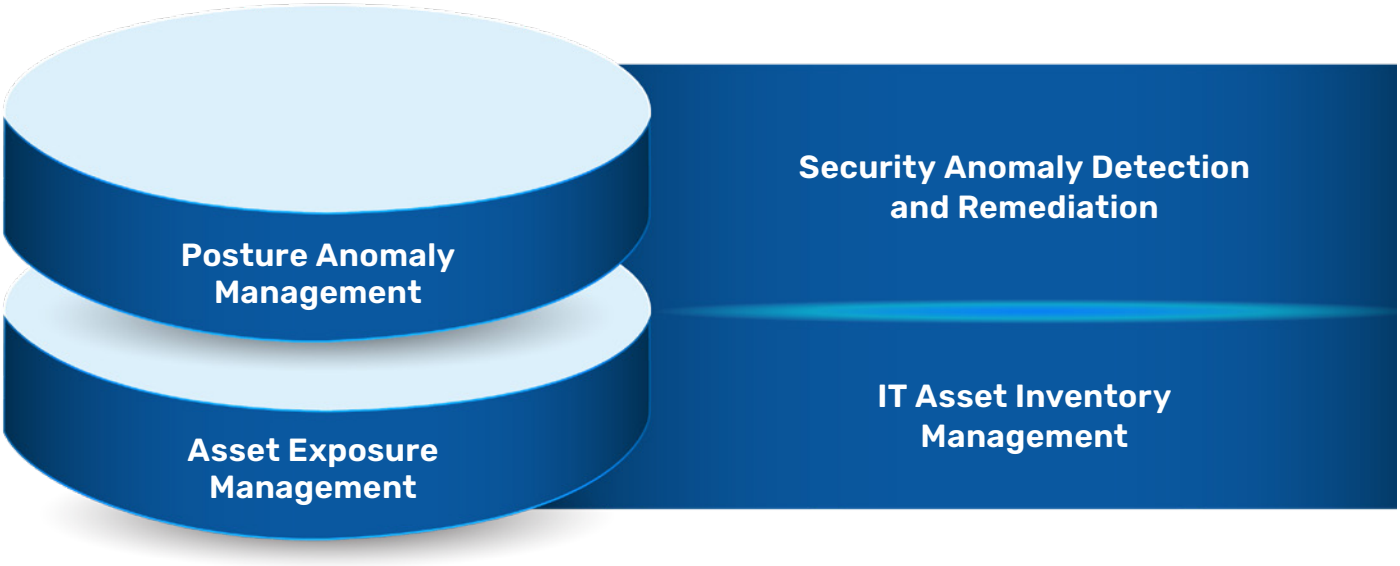
Normalize

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

Solution Workflow to Realize Value



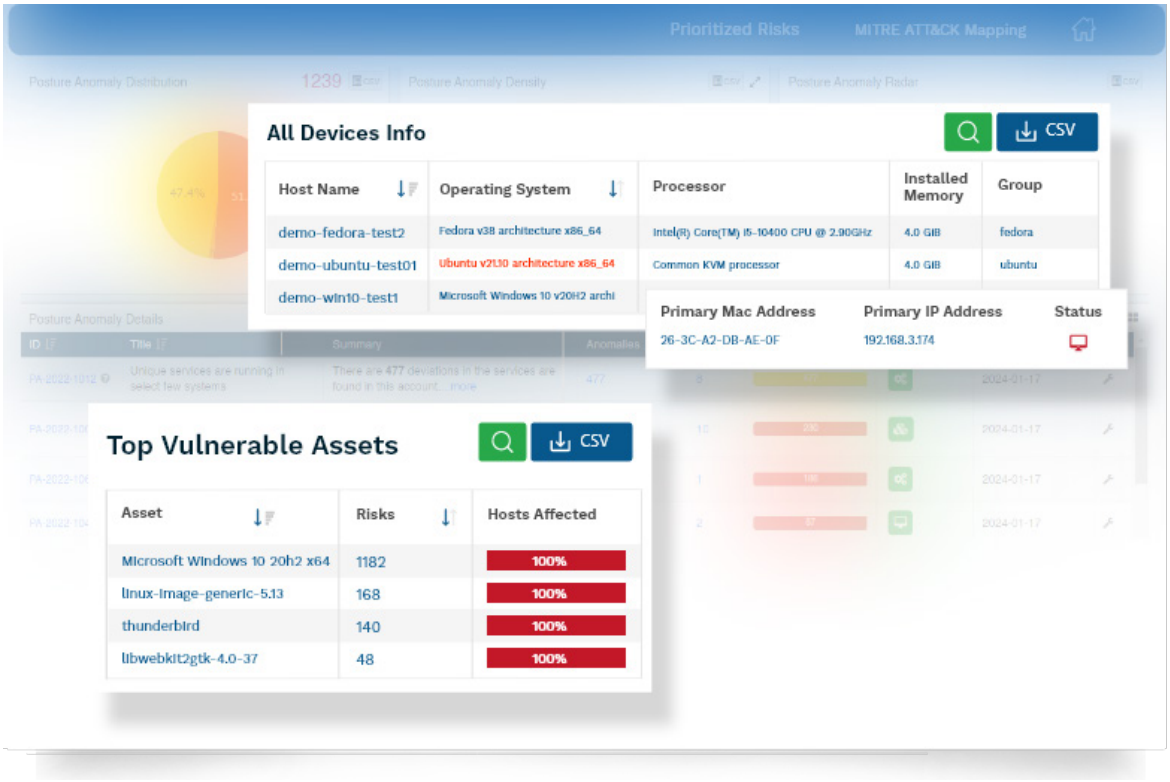
SanerNow Modules in the Solution Stack



01 Asset Exposure Module

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

- Discover shadow IT, unauthorized applications, end-of-life and end-of-support software
- 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
- Build customizable asset reports

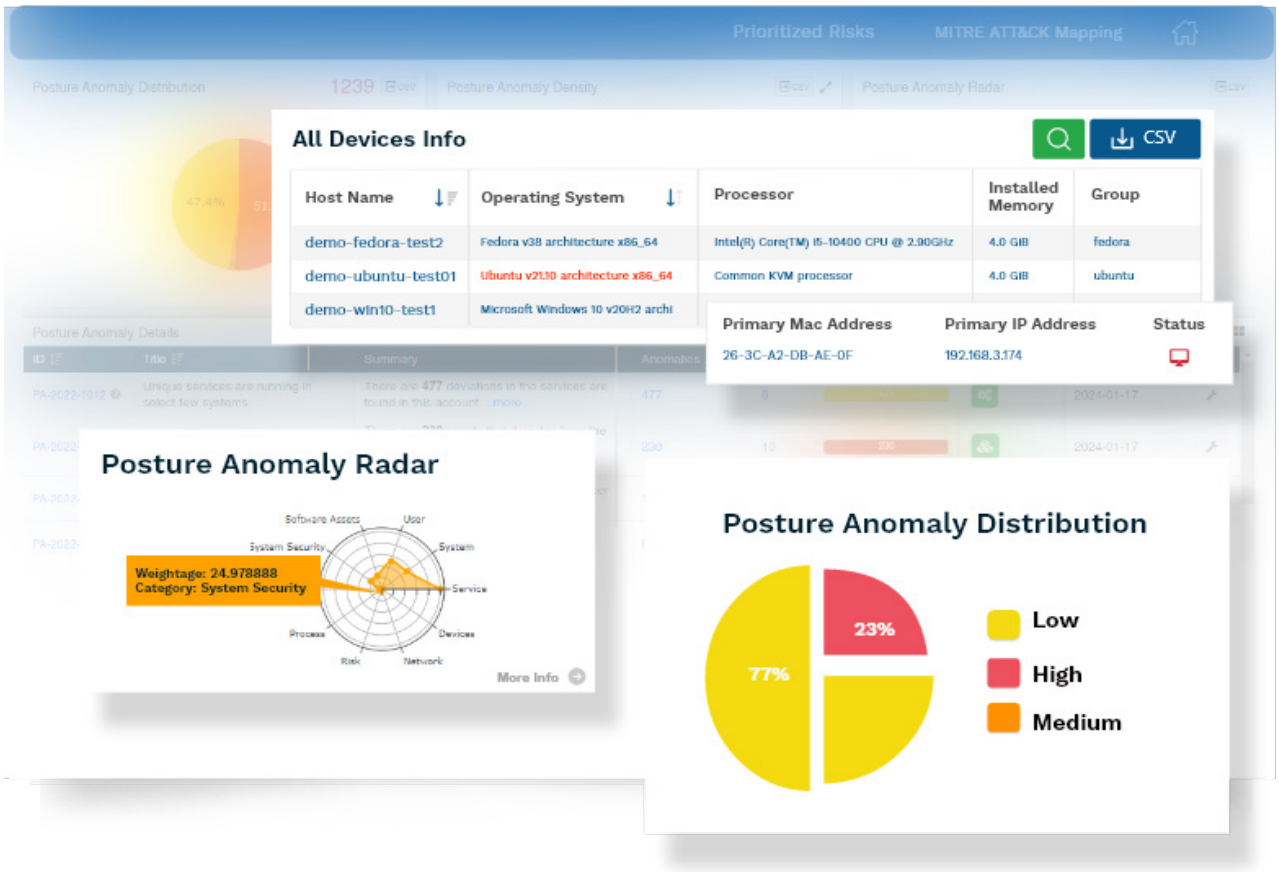


02 Posture Anomaly Management Module

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.

- Perform daily automated scans to discover anomalies & prioritize them
- Execute outlier analysis to test security posture
- Analyze security controls for optimal functioning
- Identify unwanted ports, processes, services, applications and devices
- Use more than 75+ anomaly computation rules to get insights on security posture
- Assess deviations based on statistical algorithms, machine learning and deviation computations

- Get intelligent insightful visualization on hidden security loopholes in the network and act on these insights to prevent attacks
- Evaluate the IT infrastructure and identify the devices that are different from others
- Remediate anomalies instantly
- Discover attack vectors in the network and reduce risk exposures



Maximize Asset Inventory Visibility. Remediate Security Anomalies.

Getting a firm grip on your IT inventory is critical to ensure the hardware and software assets are used in the most efficient manner. By categorizing assets, IT teams will be able to locate and monitor them for audits. They will gain clarity on the optimal functioning or obsoleteness of assets due to lack of updates or replacements. By mapping the assets to location, type, current version, or condition, etc. They can establish efficiency across enterprise IT infrastructure to quickly resolve any asset issues.

With the power of proactive and automated, high-speed scanning capabilities, the time taken to detect assets is extremely short and happens in 5 minutes. The solution not only gives clarity of every asset present in the network, the asset data derived from the scan can also used to identify security anomalies, outliers or aberrations in the IT environment. This helps in enabling a proactive security strategy to strengthen compliance measures and mitigate attack risks.

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