SanerNow CPAM

Get a Bird's Eye View of Your IT Infrastructure, Spot the Obvious Posture Anomalies, and Uncover the Unexplored Risk Exposures and Mitigate them

Due to a lack of sufficient awareness of their IT infrastructure, organizations tend to overlook the most obvious outliers, aberrations, and deviations present in their network, which later become the prime cause of a cyberattack. For instance, anonymous logins, insecure permissions and unwanted network open ports; poorly configured WiFi settings; usage of unapproved VPN software, gaming applications, and cloud sharing applications; publicly discoverable data shares, and by passed user access controls are some of the most obvious risk exposures organizations tend to miss out and attackers easily exploit.

For IT security teams to build an unbreachable security posture and prevent massive cyber-attacks in today's era, it is imperative to obtain deeper insight into the IT infrastructure and uncover the outliers and anomalies that pave way to cyberattacks. Modern IT security teams need a solution that can holistically and deeply assess the IT infrastructure and provide impeccable insights to strengthen cyber resilience and combat cyberattacks.

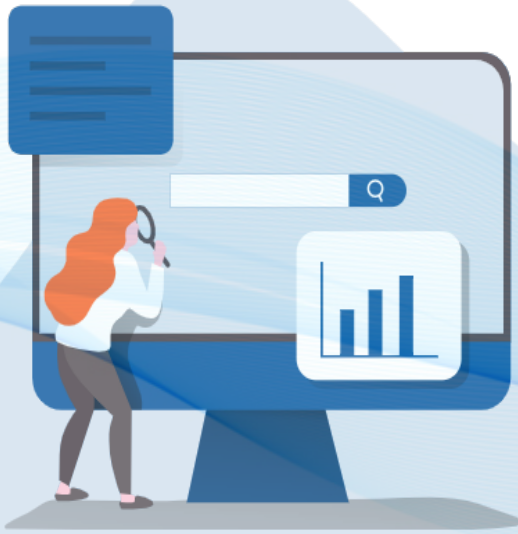
secpod

SanerNow CPAM

Visualize your IT Landscape Like Never Before with SecPod SanerNow Continuous Posture Anomaly Management

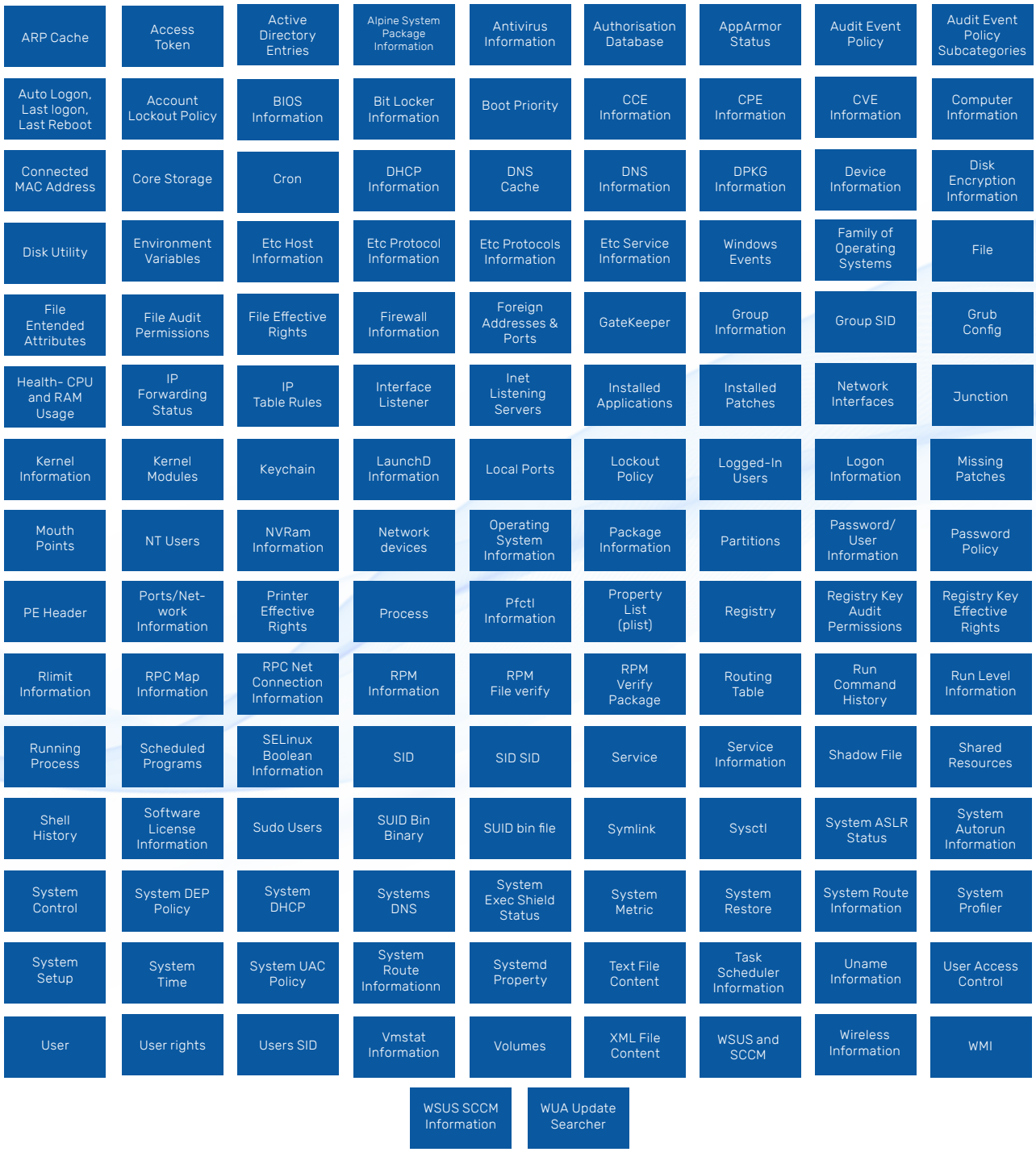
SecPod SanerNow CPAM provides visibility to your IT infrastructure in a way you have never seen before. By collectively monitoring 100s of device parameters and 1000s of artifacts, SanerNow CPAM discovers Posture Anomalies including the outliers, aberrations, and deviations present in your network. To uncover these anomalies and potential risks, SanerNow CPAM uses statistical analysis, machine learning, and deviation computation methods.

With intelligent insights and holistic awareness of your network, you get clarity over what's in your IT environment, detect any abnormalities or issues, and act upon them immediately. You can identify the devices that are incorrectly configured, that have a unique posture, and are configured differently from others. By discovering and managing these anomalies early, you can minimize the risk exposure and gain significant mileage in your cyber defense journey. The SanerNow CPAM will redefine cyberattack prevention and enable IT security teams to stay resilient to threatening security mishaps.

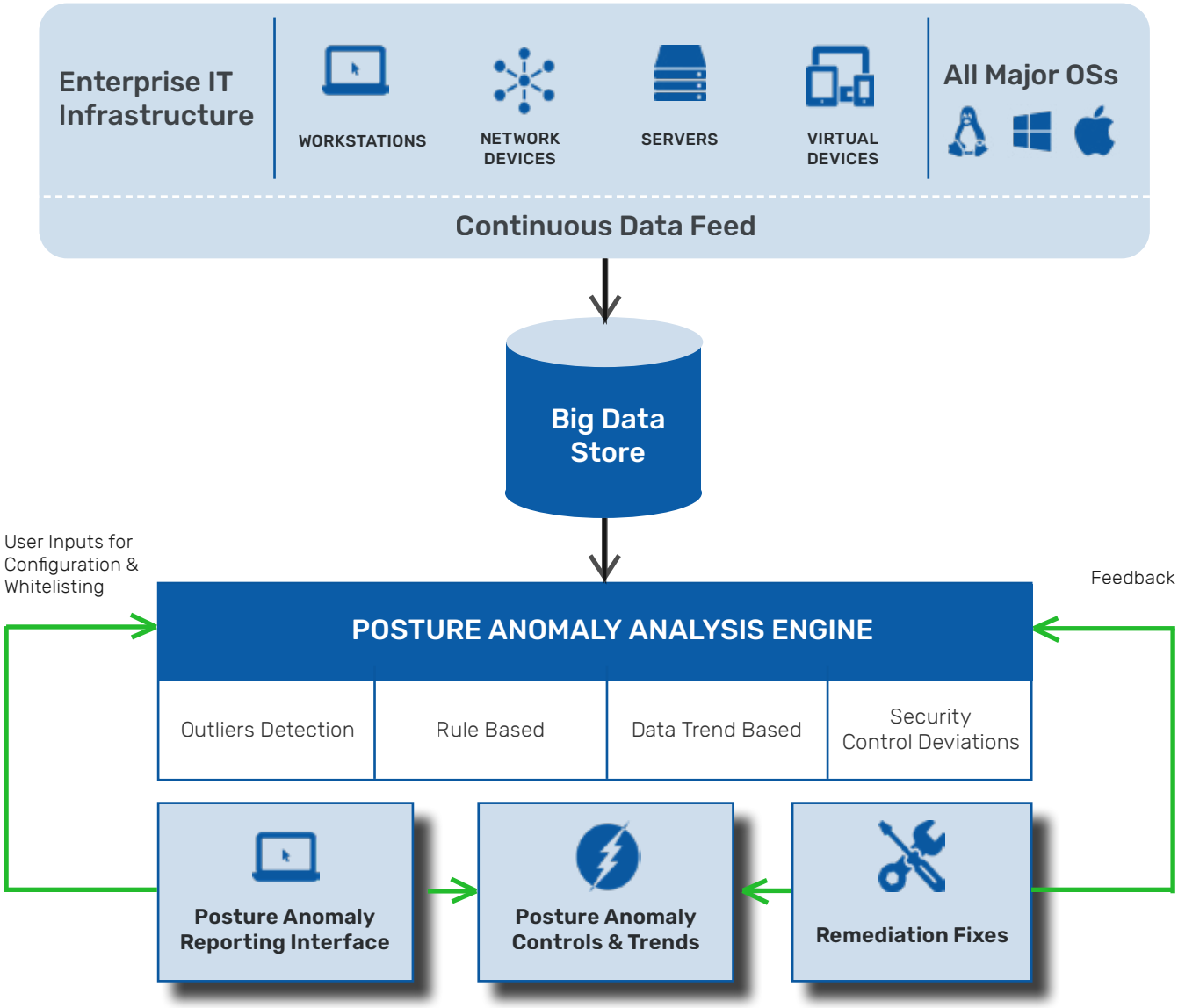


secpod

Insights You can Gain From SanerNow Continuous Posture Anomaly Management



How SanerNow Takes Control of Posture Anomalies?



Analyze your IT holistically to Uncover Obvious Attack Vectors

Leverage Machine Learning, Statistical Analysis, & Deviation Computation Methods to Identify Anomaly Loopholes

SanerNow Continuous Posture Anomaly Management analyzes the IT infrastructure and identifies anomalous devices that are different from others. Machine learning, statistical analysis, and deviation computation are used to comprehend differentiation factors and detect security posture anomalies. SanerNow also provides the necessary remediation measures to fix the anomaly instantly to help you build a solid cyberattack prevention foundation in your network.

Gain Rapid Security Mileage by Enforcing the Most Obvious Cyberhygiene Measures

Go a step beyond viewing your IT infrastructure only in the surface and start inspecting them with a bird's eye view. SanerNow CPAM holistically assess your network to discover any deviations or aberrations that might lead to a potential attack. Discover a plethora of anomalies in your network from unusual services & processes, abnormal events in event logs, unwanted ports, unsigned applications, unusually executed commands, and much more hidden risks that threaten your organization's security.

Utilize comprehensive and insightful intelligence to improve operational efficiency

Most of the times, the reason for a cyberattack could be an unnoticed change in your IT environment. By identifying the most significant and noticeable deviations in your IT infrastructure, SanerNow CPAM provides intelligent insights which otherwise would have remained an unseen security loophole in the network. With intelligent insights, you can act upon these obvious security risks and prevent a wide range of cyberattacks even before implementing other security measures.

Manage your IT security measures with confidence and eliminate uncertainties

Stay aware of the security risks that were once hidden with a holistic view of your IT infrastructure. SanerNow CPAM allows you to discover the obvious attack vectors in the network and implement more effective security measures that will reduce risk exposures significantly. Along with managing vulnerabilities, misconfigurations, and other security risks, you now have control over the security posture anomalies that could have unleashed massive attacks.

SanerNow Continuous Posture Anomaly Management to Redefine Cyberattack Prevention

Machine Learn Your IT Collectively and Identify Aberrations Through Statistical Analysis

Using Machine Learning concepts and Statistical Analysis, SanerNow CPAM collectively assesses your IT infrastructure and discovers outliers or aberrations in the network. For instance, SanerNow Identifies unfamiliar and unique applications that are installed, unusual services and processes that are running, atypical kernel versions, kernel modules or kernel parameters, irregular IP mapping, abnormal events, oddly executed commands, unwanted outbound connections to network ports, strange entries in task scheduler, autorun configurations, uncommon environment variables, and much more hidden risks in your IT network.

Declutter your IT Infrastructure, Eliminate the Unnecessary Assets and Control Your SBOM (Software Bill of Material)

Let only known-good assets reside in your IT infrastructure and eliminate the unwanted ones. SanerNow CPAM allows you to identify the unwanted applications, services, processes, and network ports; inspect scheduled tasks, run level programs and environmental variables; detect the number of VPN tools used in the network, discover cloud applications and file transfer apps, apps from unknown publishers, and unsigned executables. By discovering all these outliers, you can easily declutter your IT infrastructure, allow only the essential assets, and manage your SBOM (Software Bill of Material).

Get a Microscopic View of Your IT and Discover the Unknown Security Risks

Explore and learn about your environment in a way you haven't seen before, and be surprised by what you find. Track the changes in IP, host, and MAC addresses; analyze why so many VPN client applications are in use; find out the aberration in firewall configurations in specific systems; identify why a signed application is unapproved in certain systems; discover inactive users and different user privileges, and a lot of obvious hidden risks, and safeguard your network from a potential cyberattack.

Monitor Security Controls and Identify Deviations in Functioning

Security controls are essential to be up and always running to protect the network from security mishaps. With SanerNow CPAM, ensure Endpoint Protection Software is always functioning, WiFi security configuration is analyzed and strengthened, user identity is configured properly, BitLocker is enabled, DEP/ASLR/SELinux enabled for threat protection, Device Firewall settings are appropriately configured, Gate Keeper and UEFI boot is enabled, Time synchronization issue is detected, and Device shares are determined. By ensuring all these Security Controls are functioning without deviation, you establish a robust security posture in your network.

Out-of-box Capabilities of SanerNow Continuous Posture Anomaly Management

Run Daily automated Scans and Discover Anomalies

SanerNow Continuous Posture Anomaly Management allows you to run daily scans to discover the anomalies in the IT infrastructure. You can schedule and automate these scans according to your organization's requirements.

Analyze array of Security Controls and Spot Deviations

From disabled firewall, poorly configured WiFi security, enabled autologon, outdates OSs and software, to disabled BitLocker, analyze an array of security controls and spot the deviation in the settings that will harm the security posture.

Get Deeper Visibility and Fetch Intelligent Insights of your IT

Get deep visibility to over 2000+ device parameters across your enterprise computing infrastructure. Fetch insightful information about your organization's security posture with over 75+ anomaly computation rules.

Prioritize the Anomalies based on Confidence Score

SanerNow analyses the discovered anomalies and determines a confidence score to prioritize the anomalies that needs immediate attention. Through this, you can remediate the high-priority anomalies quickly and reduce risk exposure to a large extent.

Identify Anomalous Posture through Statistical Anomaly Computation

Spot anomalous configurations and behavioural changes like vulnerable processes making outbound connection, unusual command execution, atypical firewall configuration, and much more by performing statistical anomaly computation.

Remediate all Anomalies with Built-in-actions

SanerNow provides an array of built-in-actions to remediate the discovered anomalies. You can also create your own detection rules to identify the anomalies and remediate them instantly from the same console to secure your IT environment.

Whitelist Necessary IT and Make it Known Good

Upon getting holistic visibility over your IT infrastructure, verify and whitelist the devices and configurations in your environment by assessing various parameters. Identify the posture anomalies and make your IT known-good.

Examine your Security Posture with Insightful Dashboard and Reports

Understand your organization's security posture through insightful visualizations. Perform outlier analysis of the gathered data and uncover interesting posture facts. Generate posture anomaly report and utilize 100s of report APIs to create custom visibility.

Experience Continuous Posture Anomaly Management

START FREE TRIAL

About SecPod

SecPod is a cyber security technology company. We prevent cyberattacks. We do everything to prevent attacks on computing environment. Our product helps implement cyber hygiene measures, so attackers have tough time piercing through.

Our SanerNow CyberHygiene platform provides continuous visibility to computing environment, identifies vulnerabilities and misconfigurations, mitigate 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.

Contact Us

Email us on:
info@secpod.com

www.secpod.com