secpod

Saner Continuous Vulnerability and Exposure Management Technical Brief

Saner Continuous Vulnerability & Exposure Management Technical Brief

Cyberattacks are becoming more complex, costly, challenging, and hard to identify and stop in recent years. Attackers are coming up with numerous ways to invade the network, threatening the organizations' security and reputation. And the post-pandemic era has also bought massive changes to the digital landscape, widening the whole attack surface. However, the most crucial cyberattack prevention process, vulnerability management, has remained the same for over two decades. Traditional vulnerability management requires immense advancements to deal with the modern attack surface and prevent cyberattacks at a larger scale.

It is big-time we understand the need to add a spin to the conventional vulnerability management process and reinvent an advanced solution that will help achieve continuous security posture.

The Need to Reinvent Vulnerability Management

Conventional vulnerability management solutions still rely on multiple-point solutions to orchestrate different steps in vulnerability management. It leaves a huge security gap between steps, making the entire process cumbersome and challenging. These traditional tools also lack the capability to remediate vulnerabilities. They also overlook other crucial security risks, as they are focused solely on software vulnerabilities. These tools also overlook other crucial security risks, as they are focused solely on software vulnerabilities.

Understandably, massive security breaches like ransomware and malware attacks are due to vulnerabilities prevalent in the network. However, numerous security breaches can happen due to various risk exposures prevalent in our network. Starting from a poorly configured setting, security misconfiguration, unavailability of antivirus, deviation in security controls, lack of visibility over scheduled tasks, unwanted ports, hidden assets, to malicious applications and devices, these security risks are as threatening as the vulnerabilities and are unavoidable for enterprises operating at scale.

Thus, you need an advanced vulnerability and exposure management solution that automatically manages different security risks, including vulner-abilities and exposures, from a centralized console to minimize the attack surface effectively.

But are the traditional vulnerability management tools equipped with these advancements is a question we need to ask ourselves.
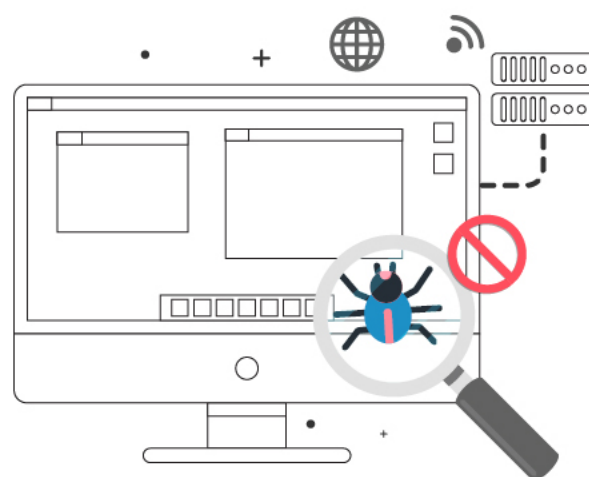
Challenges of Managing Vulnerabilities, Exposures and Other Security Risks with Conventional Vulnerability Management

Siloed Applications

Traditional vulnerability management relies on multiple tools from gaining visibility over the IT infrastructure, identifying vulnerabilities, misconfigurations, and other risk exposures, and mitigating them with relevant remediation controls. The siloed interfaces create chaos, making it hard for security teams to gain control over the risk exposure. They also create delays between different steps, leading to huge security gaps in your vulnerability and exposure management program.

Lack of Deeper Insights into the IT infrastructure

IT security teams do not have deeper visibility over the IT infrastructure. Traditional tools typically provide limited view to hardware and software details with insufficient actionable insights. As a result, IT security teams overlook the most obvious attack vectors that can lead to massive security breaches.

Slow and Ineffective Scanners

As the horizon of exposures and vulnerabilities expand, conventional scanners lack the intelligence to detect them. Many conventional vulnerability and exposure scanners already take hours or sometimes weeks to discover the commonly known vulnerabilities or exposures. The time taken to discover all risks, including vulnerabilities, will be even longer with these traditional scanners.The scanning process also tends to choke network bandwidth apart from the delay.

Unable to keep up with the volume of vulnerabilities

Tens of thousands of security risks are discovered every year, and the volume of vulnerabilities released in the NVD database is mammoth. The year 2023 ended with a total of 31,279 vulnerabilities, 18% more than the previous year. These are just vulnerabilities, with other security risks not being accounted for. Security teams face numerous challenges in keeping up with the increased volume of vulnerabilities.

To add to this, the number of security risks in the network is also huge.

Not Managing vulnerabilities beyond CVEs

All CVEs are vulnerabilities, but not all vulnerabilities have a CVE number. More than 40% of vulnerabilities do not have a CVE identifier assigned. As we rethink the definition of vulnerability, we should look at the other security risk exposures as discussed above. Misconfigurations, asset exposures, posture anomalies, etc, may go under the radar. Many vulnerability and exposure management software focuses only on vulnerabilities with CVEs, which leaves organizations using them under huge risks.

Poor clarity on what to remediate first

According to a **study** by ESG, 43% of security admins have challenges understanding which vulnerability to remediate first. After detecting a huge pile of vulnerabilities and risks, it is critical to identify and remediate the high-risk ones to minimize attacks. Traditional vulnerability management tools lack the right techniques to prioritize vulnerabilities and risks based on severity and business impact.

Delay in patching and remediating vulnerabilities

With new vulnerabilities being discovered every passing day, security teams have difficulty keeping a tab on patching them. Many conventional programs rely on a different tool to patch the vulnerabilities and face hiccups in integrating the vulnerability data and executing the patching process.

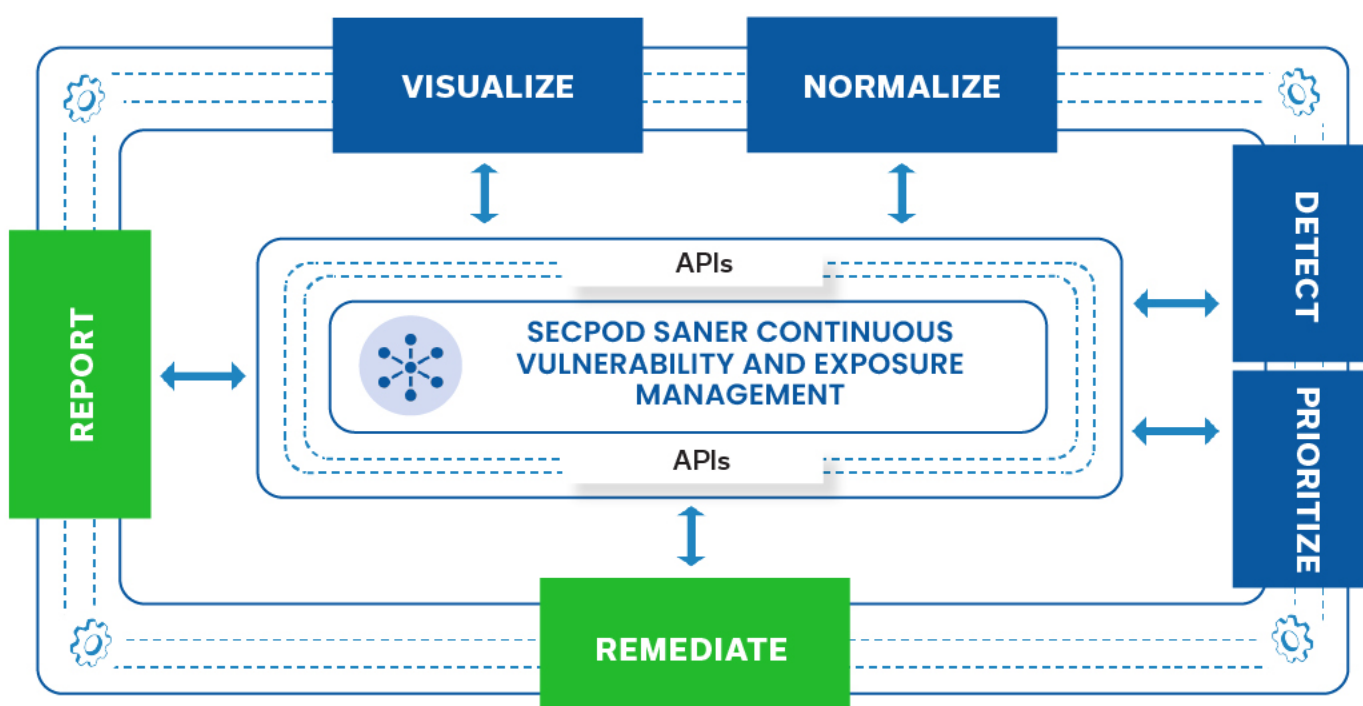## Lack of remediation controls beyond patching

Patching is not the only remediation measure to fix vulnerabilities and other security risk exposures. As the horizon of vulnerabilities and security risks expands, numerous remediation controls are needed to fix different types of vulnerabilities. Traditional vulnerability management tools lack these controls and restrict security teams from going beyond patching to fix other risk exposures.

Unable to align vulnerability and exposure management goals with security compliance

Popular industry compliance standards like HIPAA, PCI, NIST, and ISO propose numerous system hardening controls and vulnerability management measures to tighten security. Many conventional vulnerability management tools in the market are not equipped with sufficient features to align with these security benchmarks. Thus, security teams rely on different tools to enforce security compliance, making it a challenging goal to achieve.

The Saner's Continuous Vulnerability and Exposure Management to Manage Vulnerabilities and Beyond

SecPod Saner CVEM provides a continuous, automated, advanced Vulnerability Management solution built for the modern IT security landscape. Saner CVEM reinvents vulnerability management with deeper and holistic visibility to IT environment, a broader approach to vulnerabilities, rapid scanning techniques, vast and accurate security checks, natively built solutions, and end-to-end automation from a truly integrated platform. We enable IT Security Teams to go beyond traditional vulnerability management practices and automatically detect and remediate vulnerabilities and different security risks from a single centralized console.

VISUALIZE   NORMALIZE

APIs

SECPOD SANER CONTINUOUS VULNERABILITY AND EXPOSURE MANAGEMENT

APIs

REPORT   DETECT   PRIORITIZE   REMEDIATE

With Saner CVEM, you can detect and manage vulnerability and other security risks from a centralized cloud-based console and a single, lightweight, multifunctional agent. Saner CVEM is powered by our homegrown, world's largest, vulnerability intelligence library with 160,000+ security checks. Saner CVEM runs the industry's fastest scans to discover IT assets, vulnerabilities, misconfigurations, missing patches, deviation in security controls, posture anomalies, and other security risk exposures. Along with patching, it also provides the necessary remediation fixes to mitigate them all and helps you combat cyberattacks faster than ever.

Under the Hood of Saner CVEM's Technology

Saner CVEM's backend technology is built with a robust Query, Detect, and Response Model, homegrown world's largest Security Intelligence Feed, powerful Analytics & Correlation Engine, and intelligent Radars to support operations on a wide range of devices and multiple operating systems including Windows, Mac, and Linux platforms.
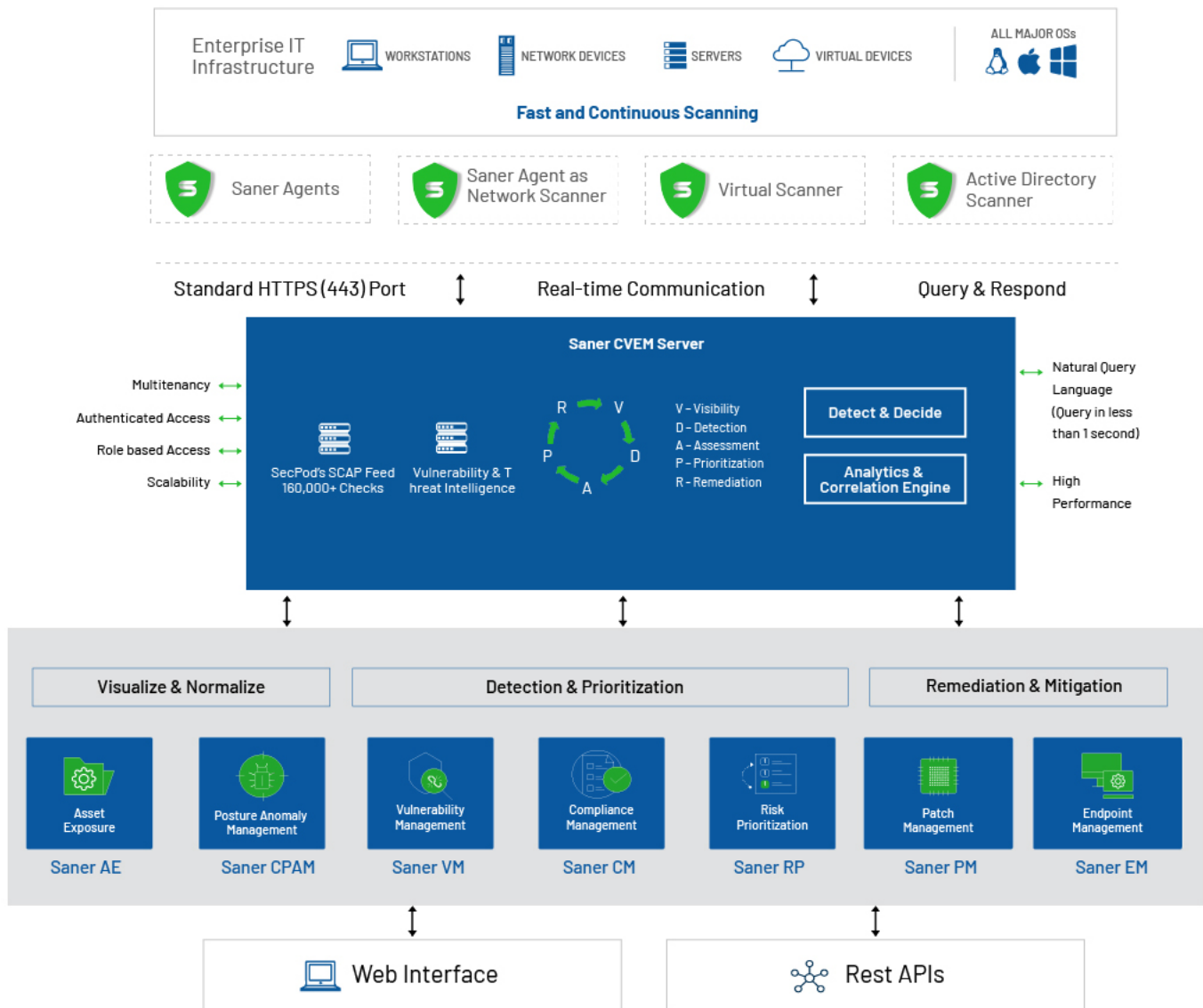
Query, Detect, and Respond

Saner CVEM allows IT security teams to perform real-time, on-demand actions to keep IT security in check. Saner CVEM provides instant visibility over what's happening across your IT infrastructure and provides you with the necessary capabilities to act upon them through its intuitive console.

Saner CVEM provides hundreds of prebuilt queries to detect various security risks in the network, including vulnerabilities on all IP-enabled devices, misconfigurations across operating systems, missing patches, password aging, screen lockout, bit locker status, firewall status, CPU utilization, unwanted programs, wireless security status, sensitive security data like social security numbers, credit card stored in clear texts, antivirus status, status of systems which are running more than seven days, disk space less than 100MB, windows registry values, user information in desktops, installation of malicious applications and devices, and more.

Saner CVEM platform provides an innovative metadata model to support instant searches using unstructured natural language queries. Along with prebuilt checks, you can also create customized checks to detect everything within your IT infrastructure.

The architecture also provides a built-in search to query almost anything in the IT network. With this, you can get details in the network based on IP address, MAC address, system name, hostname, and more.

Security Automation in Saner CVEM's Powerful Architecture

Saner CVEM hosts the world's largest security intelligence feed and vulnerability threat intelligence feed to provide continuous and automated security updates to the Saner CVEM Server.

Security Intelligence feed

Saner CVEM is powered by its homegrown world's largest vulnerability intelligence feed with more than 160,000 security checks. The SCAP repository offers a natural language-based search interface to extract security information. After continuous research and analysis, all the latest vulnerability updates are fed into the homegrown security intelligence feed every day. The security intelligence feed is automatically synced with the SanerNow server to enable continuous discovery of vulnerabilities in the IT network.

The security research team at SecPod continuously works on getting the latest vulnerability and security updates, including CVE, OVAL, CPE, CCE, CWE, CVSS score, severity range, exploit potential, and relevant patch fixes.

- Additionally, SecPod provides **SVE (SecPod Vulnerability Enumeration)** information for those vulnerabilities that are acknowledged by vendors but still lack complete CVE information on common publicly available CVE databases.

- Saner CVEM's native **CRE (Common Remediation Enumeration)** technology maps all the discovered vulnerabilities with remediation enumeration data to patch vulnerabilities and misconfigurations on time.

- Saner CVEM's **ERI (Extended Remediation Information)** technology provides patch information, prerequisites for the patching activity, and evolution of patches over time to aid the complex vulnerability remediation process.

- Saner CVEM's **XCCDF(Extensible Configuration Checklist Description Format)** provides information for benchmarks like HIPAA, PCI, ISO, NIST & SOC 2 to achieve compliance. SanerNow also provides remediation patches to harden configurations.

- Saner CVEM's **SQRL (SecPod's Query & Response Language)** provides a wide range of prebuilt detection and response scripts to manage vulnerabilities and security risks in the IT infrastructure.

Vulnerability Threat Intelligence Feed

Saner CVEM's Vulnerability threat intelligence feed consists of the Malware Vulnerability Enumeration (MVE) data. Saner CVEM maps the detected vulnerabilities with **MVE (Malware Vulnerability Enumeration)** data to identify the vulnerabilities causing high-fidelity attacks. With this, Saner CVEM showcases the threatening vulnerabilities causing dangerous attacks and alerts the IT security teams to remediate them instantly.

Powerful Analytics and Correlation Engine (ANCOR)

Saner CVEM's ANCOR is scalable analytics and correlation engine that operates on multiple sets of data to perform methodical investigations. The data set include vulnerability information, IT asset exposures, missing patches, deviation in security controls, endpoint security metrics, and security posture anomalies. ANCOR correlates all these data to uncover the network's vulnerability and security risk exposure.

Ancor enables detection, assessment, prioritization, remediation, reporting of vulnerabilities & security risks from a single centralized console by analysing data from devices and correlating it with the homegrown security intelligence.

SanerNow Radars

Agent

The smart, lightweight, multifunctional agent must be installed on the endpoints to implement the continuous vulnerability and exposure management tasks. The agents receive the tasks from the Server and silently execute them on the devices without interrupting the users. With Saner CVEM, you can,

- Scan the entire virtual and physical infrastructure
- Establish a live communication channel between the agents installed on the devices and the Server to perform real-time, on-demand queries and responses
- Run active directory scan
- Perform network scan
- Customize the agent-server sync time according to your organization's requirements
- Manage remediation tasks and execute a wide range of actions

Agent as Network Scanner

The powerful agent also takes up the role of a network scanner to scan other devices in the network, saving additional costs over purchasing new hardware. The agents can be configured to scan the entire network to detect vulnerabilities across your IT infrastructure. The agent performs network scanning without consuming excessive bandwidth and system resources. Different scan profiles can be configured to suit your organization's needs.

Agent as an Active Directory (AD) Scanner

The powerful agent also takes up the role of an AD scanner to configure users and devices available in the network. This activity also works without consuming excessive bandwidth and system resources.

Features & Benefits of SanerNow Architecture

Robust, Natively Built, and Truly Integrated Solution

Saner CVEM Cyberhygiene platform is built completely in-house to provide a truly integrated solution. All security tasks can be easily performed from a single place without having to juggle different tools.

Real-Time Communication with Distributed Devices

Saner CVEM allows you to talk and respond to your devices anytime and anywhere in real-time. You can run on-demand operations and establish real-time communication with your organizational devices.

High-Performance Scalable Architecture

The platform is highly scalable with a Big Data architecture, efficiently supporting the management of a large number of devices through a single server without performance degradation.

Multi-tenant Support with Segregated User Data

Efficiently manages multiple business units and system users with a single server. Neatly segregates business users' data and offers the ability to create various user roles with defined access rights to manage different areas of a corporate network.

Rapid, Continuous, and Automated Operations

With Saner CVEM, you can run the industry's fastest scans in less than 5 minutes and automate all security tasks end-to-end and achieve continuous operations.

Leverage cloud or on-premises solution as per requirement

Saner CVEM supports operations on both cloud and on-premises variants. You can opt for either of the ones which suit your business needs.

Easy Setup and Onboarding

Saner CVEM can be set up in less than 30 minutes, and you can kick start your operations in no time. Saner CVEM offers multiple modes to deploy agents seamlessly across your network.

Seamless Integration and Interoperability

The flexible architecture of the platform allows integration with various systems. The REST APIs enable access to all collected data from endpoints and supports search queries.

Provides Multi-factor Authentication

The platform provides multi-factor authentication to protect the Saner CVEM account and add an extra layer of security.

Operates on a lightweight Agent

Saner CVEM platform work on a single, lightweight, multifunctional agent which weighs less than 20MB and execute all the tasks. The agent also takes up the role of network scanner and saves cost on integrating additional hardware.

Supports Natural Language Search Queries

The innovative metadata model of the platform supports instant searches using unstructured natural language queries. Saner CVEM understands it all and provides valuable insights to our customers.

Protects BYOD, Remote Office, and Transient Devices

Ensures security of organizations' devices across perimeter limits. Provides efficient protection and control of transient, remote, and BYOD devices from a centralized console.

Leverage Machine Learning to deep learn IT

Saner CVEM analyses various parameters in the network and uses machine learning concepts to provide deep insights into the IT infrastructure and discover outliers.

Rule & Trend based Analysis to Discover Anomalies

Saner CVEM uses rule and trend-based analysis where it collects some parameters over a period to spot any aberrations or abnormalities in regular pattern.

Deviation Computations of Standard Configurations

Saner CVEM uses 40+ checks to assess if configurations are set differently from others. Through this it identifies the deviated configurations that needs to be looked upon immediately.

Unique Capabilities of Saner CVEM Platform

Saner CVEM CyberHygiene Platform comes with a ton of unique capabilities to make vulnerability management a seamless task. A few of the capabilities include:

- Truly integrated solution for IT asset visibility, vulnerability detection, and remediation
- Manage vulnerabilities and various security risks including misconfigurations, IT asset exposure, missing patches, deviation in security controls, and posture anomalies
- Manages and prioritizes security risks based upon business context, exploitability, automatability and other critical factors through its inbuilt advanced vulnerability intelligence
- Remediate vulnerabilities and security risks with various remediation controls including patching
- Perform real-time data analysis and correlation at the platform with instant visibility & control
- Leverage the continuously updated, world's largest security intelligence Library with 160,00+ checks
- A single, light-weight, multifunctional agent to achieve cybersecurity prevention goals
- Supported by BigData architecture for speed, scalability, and high-volume data analysis
- Multi-tenant and multiuser system model
- Provides single sign-on and multi-factor authentication
- Offers Role based access control
- Integration with Active Directory to replace organizational hierarchy
- Seamless device discovery and onboarding
- Catering to both SaaS and on-premise deployment requirements
- Get Visibility from 198 probes and get to know 1470 attributes on your environment
- Apply 100s of responses to fix issues
- Support for cloud and on-premise deployment
- Support for air-gapped networks
- Easily scalable to manage millions of devices
- Quick product setup in less than 30 minutes
- Distributed and hub and spoke model for network scanning utilizing agents to perform discovery and vulnerability scanning
- Seamless multi-platform support, covering 30+ operating systems
- Perform unlimited scanning and use configure unlimited scanners
- Intelligence Driven Cyber-hygiene Score

Saner CVEM Advanced Vulnerability Management Key Features and Highlights in Detail

Gain Complete Visibility and Control Over Your IT Asset Exposure

Run regular IT asset scans and monitor your hardware and software inventory details in real-time. Saner CVEM allows you to get complete visibility over your IT asset inventory and gain complete control over them.

- Automate, schedule, and run continuous IT asset scans
- Identify managed and unmanaged IT assets
- Get complete visibility over IT asset inventory, hardware, and software
- Get up-to-date information on Devices, Services, Processes and Open Ports
- Get information on the devices based on OS distributions, device types, and manufacturer details
- Discover Shadow IT assets
- Monitor crucial device details like IP address, CPU, RAM, Disk details, and other system specs
- View application details like version, publisher, patch, executable, installed devices, and host name
- Detect outdated End of life, End of Support software
- Discover rarely used applications in your network
- Harness device tagging to customize your filters and classify endpoints with a granular level of customization
- Manage hardware, software, and OS licenses
- Blacklist and whitelist applications and tighten security
- Build asset inventory reports and alerts
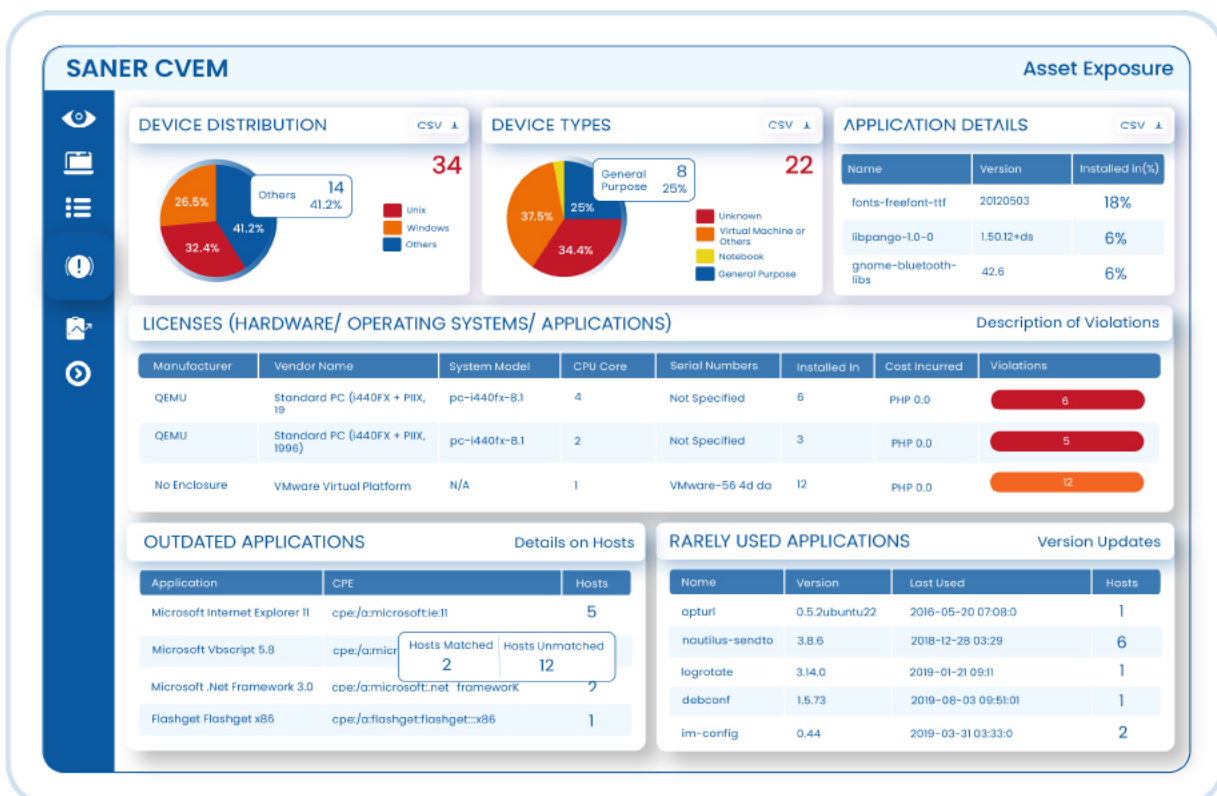
Declutter your IT Infrastructure, Eliminate the hidden uncertainties

Saner CVEM PAM uncovers amazing insights about your IT infrastructure and provides holistic visibility like you have never seen before.

Saner CVEM analyses 100s of system probes, and 1000s of system attributes to find posture anomalies that threaten IT security. In addition, it provides built-in actions that can fix anomalies quickly from the same console.

- Get deep visibility to over 2000 device metrics across your enterprise computing infrastructure
- Perform daily automated anomaly scans to discover posture anomalies
- Get insightful information about your organization's security posture with over 75+ anomaly computation rules
- Perform statistical anomaly computation to identify anomalous posture within an organization's devices
- Outlier analysis of the gathered data to uncover interesting and insightful posture facts
- Whitelist your environment across many parameters and identify anomalies to make your IT known-good
- Analyse an array of security controls, learn deviations to the expected behavior
- Know the confidence score to prioritize the anomalies
- Remediate all anomalies identified with an array of built-in actions
- Understand security posture with insightful visualizations to learn and remediate anomalies
- Create your own anomaly detection rules and respond to aberrations with integrated actions
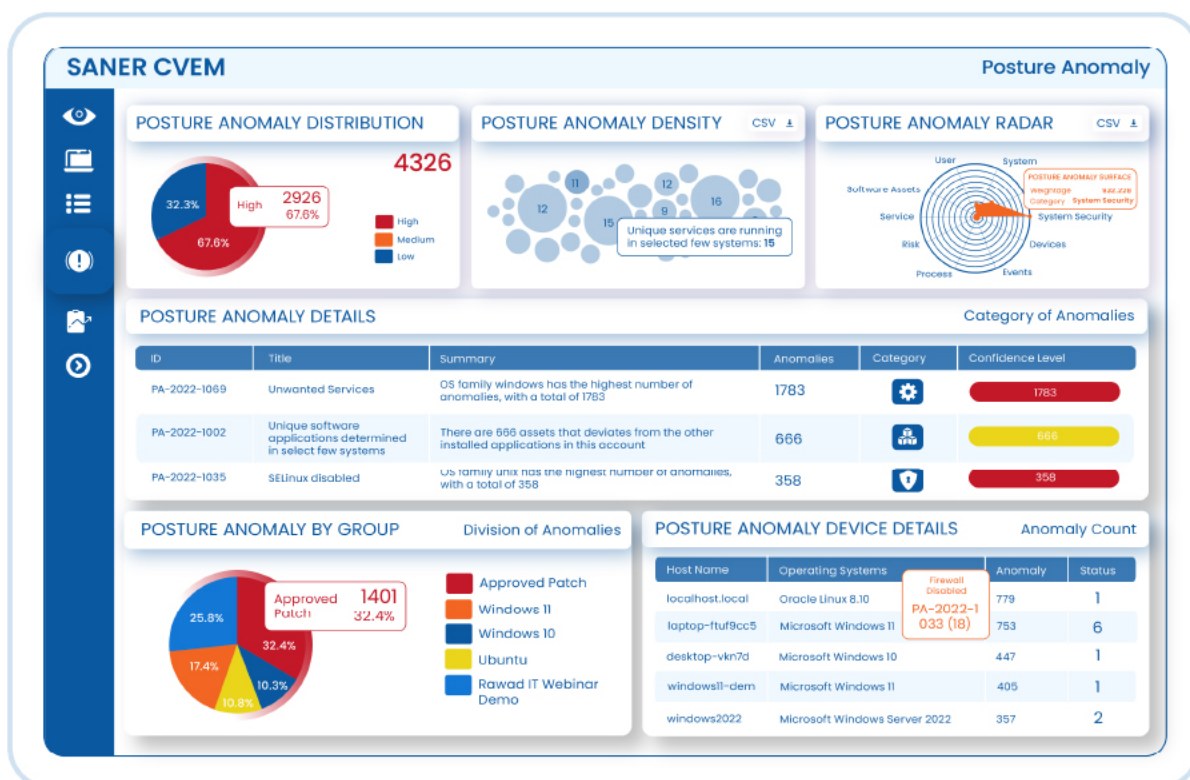
Run Rapid, Continuous, and Automated Vulnerability and Exposure Scans

Scan your network devices in your perimeter, internal network, and cloud environments anywhere and anytime from a single console. You can detect detailed insights into the vulnerabilities and security risks in your network and manage your attack surface. Saner CVEM separates scanning and reporting, allowing you to run deep scans. You can later use the prebuilt vulnerability reports or custom create according to your requirement.

- Run industry's fastest vulnerability and exposre scans across thousands of devices in less than 5 minutes without consuming excessive bandwidth and system resources
- Automate and schedule daily scans to reduce the complexity of performing individual or on-demand scans
- Gain continuous visibility over your IT asset infrastructure
- Perform continuous scan across all network devices and endpoints and identify risk exposures
- Detect vulnerability details based on OS, groups, devices, and age, and gain 360-degree visibility over them
- Fetch the latest insights on the day-to-day vulnerabilities from Saner CVEM's homegrown security database and detect them immediately in your network
- Perform Agent based and Network Scanner based detection
- Configure existing agents as network scanner and save cost spent on additional hardware
- Distributed network scanning to efficiently use network bandwidth and system resources
- Scan external network perimeter and internal scanning with a single solution
- Scan assets behind the firewall and outside the perimeter
- Scan by individual IP, range of IP or multiple subnets by a single scanner
- Cloud native scanning for perimeter less world
- Gain information on vulnerability trends to track data for a period of time
- Configure scan schedule and set parameters as per your requirement
- Leverage 100's of dashboard APIs to build visibility to vulnerability
- Leverage 100s of reporting APIs to create custom visibility
- Integrate with other security tools accessing vulnerability findings through REST API
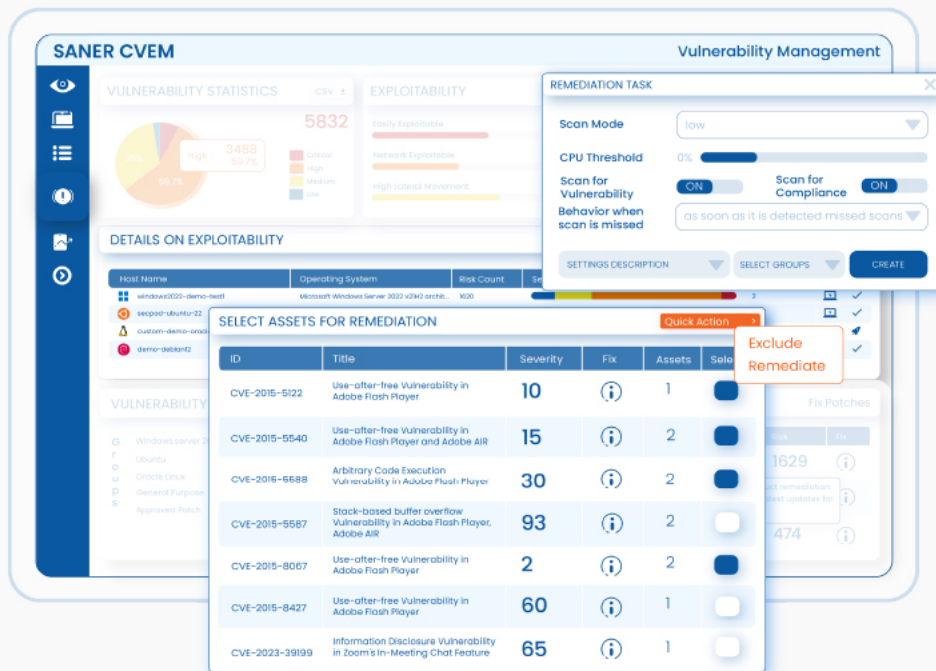
Comprehensive Security Coverage and Accurate Detection

SecPod has built the world's largest security intelligence feed with more than 175,000+ vulnerability checks with more than a decade of research. You can detect vulnerabilities and exposures accurately in your network with nearly zero false positives.

- Saner CVEM's world's largest homegrown database is updated everyday with the latest vulnerability information by our in-house security team
- With the comprehensive checks, achieve 100% detection accuracy with near-zero false positives
- SCAP and OVAL compliant database to provide you with top-notch detection coverage
- Provides multi-level scanning for vulnerabilities, missing patches, and other risk exposures based on several criteria to ensure accurate detection
- Detect vulnerabilities beyond CVEs and manage other risk exposures
- Bundled with intelligent security checks to discover vulnerabilities beyond CVEs
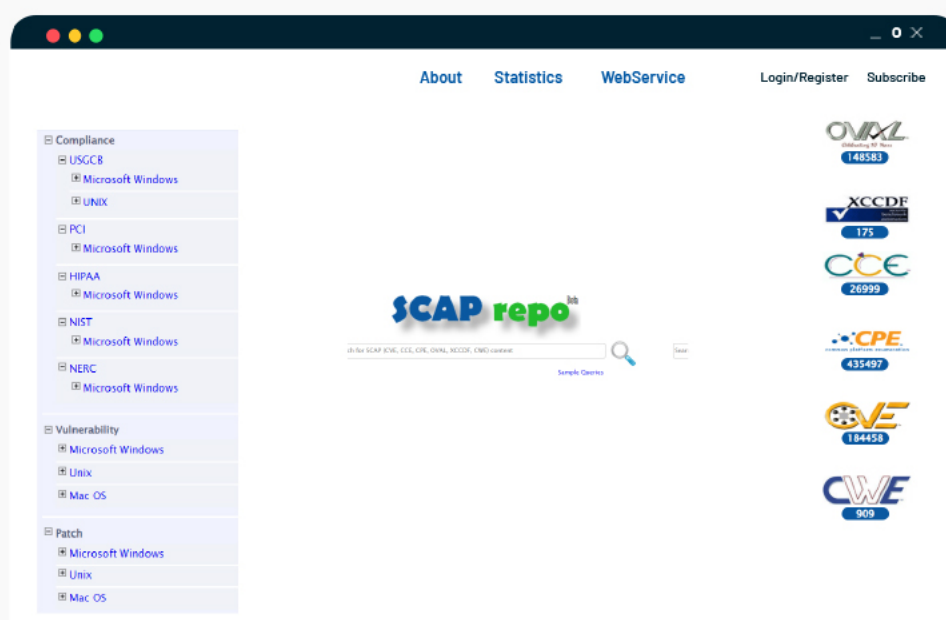
Intact Risk Prioritization

Saner CVEM Risk Prioritization assesses security risks thoroughly in-house vulnerability and threat intelligence, implements an enhanced Exploit Prediction Scoring System (EPSS) and SecPod's unique risk categorization algorithm to help you plan remediation smartly.

- Comprehensive Risk Prioritization model based on SSVC, vulnerability intelligence, machine learning based exploit prediction, kill-chain validation, business context, data analysis and moreGain vulnerability insight and risk analysis for each vulnerability
- Natively integrated vulnerability scanner for accurate and faster detection of vulnerabilities, eliminating the need for external vulnerability ingestion.and the number of vulnerable assets
- Natively integrated remediation engine to rollout fixes to effectively eliminate vulnerabilities.
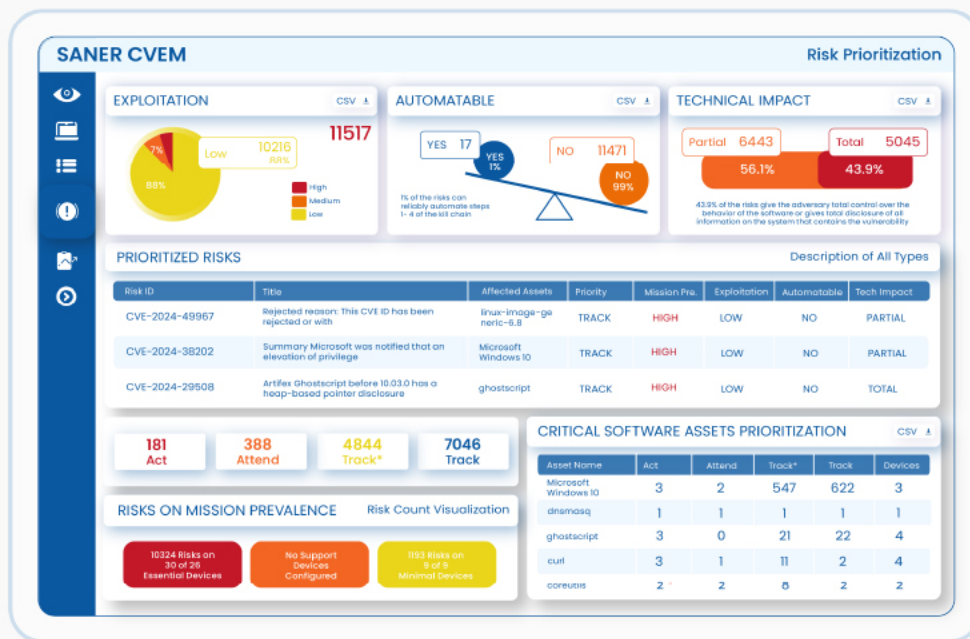

Integrated Patching for Faster Remediation

Saner CVEM provides integrated patch management to remediate vulnerabilities on time and prevent attacks.

- Provides accurate and immediate patch information for all the detected security risks
- Cross-platform Operating systems and third-party patches support to remediate vulnerabilities in a heterogeneous environment
- Continuous & automated scanning to detect missing security and non-security patches
- Automate end-to-end patching from scanning to deployment, achieve zero-touch patching
- Rapid support to the latest patches within 24Hrs to aid in faster remediation
- Single click window to fix all critical and high-profile exploitable vulnerabilities
- Test patches in test environment and approve them before taking it to the production environment
- Supports patching for firmware updates
- Provides the roll-back option to prevent errors from faulty patches
- Searches based on CVEs and other security exploitability indexes to mitigate vulnerability

- Intact patch prioritization based on severity
- Cloud based solution for easy and remote patching for all devices
- Set patch compliance goals and rollout patches
- Customize remediation procedure and execute pre and post deployment scripts
- Apply patches/fixes through custom scripts
- Schedule patching with multiple controls
- Perform on-demand patching
- Specify remediation time window
- Control and manage device reboots, integrated through patching jobs
- Deliver messages to end user about patching activity
- Understand 14 different patching status, apart from success/failure
- Achieve seamless patching within and outside the network perimeter
- Ready-to-use patch compliance report
- Report on device and asset patch compliance, by groups, sites and across the organization
- Assess the impact of patching with insightful Patching Impact Report
- Leverage 100s of reporting APIs to create custom visibility
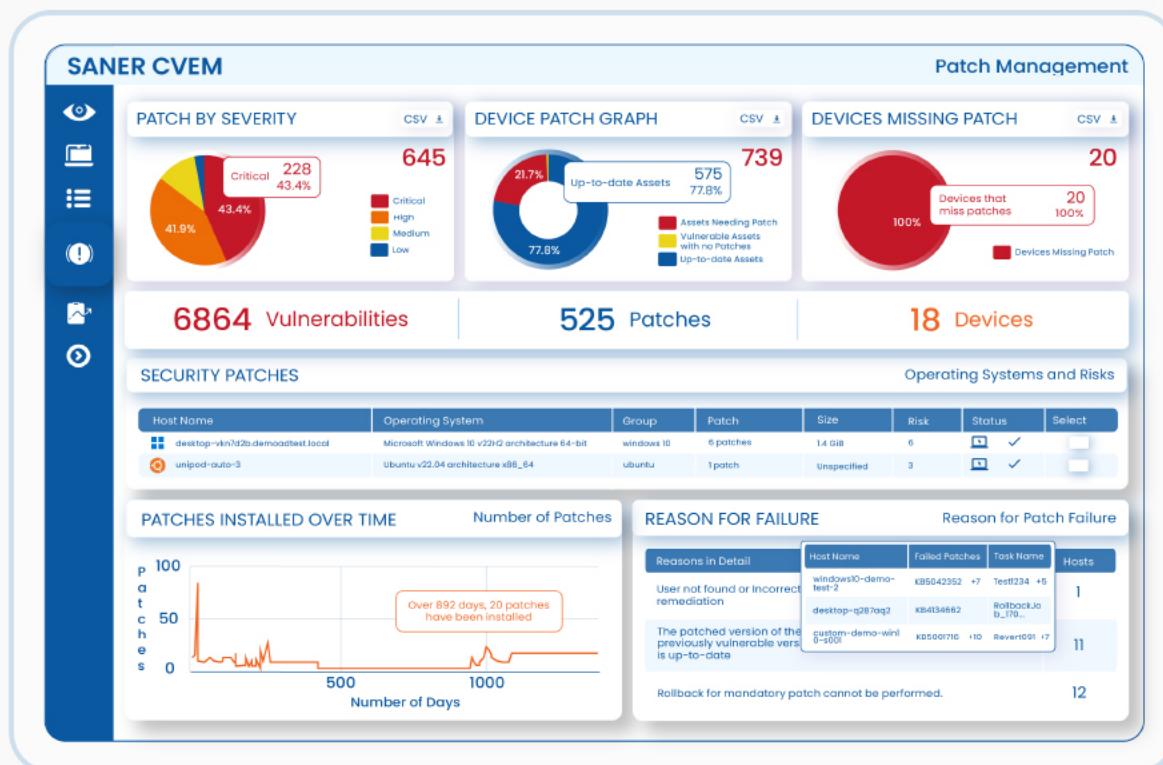
Harden System Configuration and Achieve Compliance with Major Industry Security Benchmarks

Saner CVEM supports compliance management for all major security benchmarks like HIPAA, PCI, NIST, and ISO. Saner CVEM allows you to easily align your vulnerability and exposure management goals with security compliance and strengthen your security posture.

- Run compliance scans and identify deviations in settings and misconfigurations across your network
- Perform Device Hardening/ System Hardening/ Misconfiguration assessment
- Continuous and automated scanning for misconfigurations in 1 minute
- Scan from an up-to-date database of over 20,000 misconfigurations
- Achieve 100% detection accuracy with near-zero false positives
- Coverage for endpoints, applications, databases, servers, and network devices
- Customize and create security policies according to your requirement
- Technical risk assessment for NIST 800-53, NIST 800-171, CIS, DISA STIG
- Adhere to industry compliance benchmarks like HIPPA, PCI, and SOC-II
- Built-in mitigation scripts to fix all misconfigurations, no coding or scripting required
- Mitigate compliance deviations to achieve 100% compliance
- Create automation rules and achieve continuous compliance
- Detailed insights and risk analysis for each misconfiguration
- Severity rating and grouping for all misconfigurations
- Know how to mitigate each misconfiguration and prioritize remediation
- 100's of dashboard APIs to build visibility to misconfiguration
- Configure agents as network scanners to detect misconfigurations across the network
- Distributed network scanning to efficiently use network bandwidth and system resources
- Scan external network perimeter and internal scanning with a single solution
- Scan assets behind the firewall and outside the perimeter
- Cloud native scanning for perimeter less world
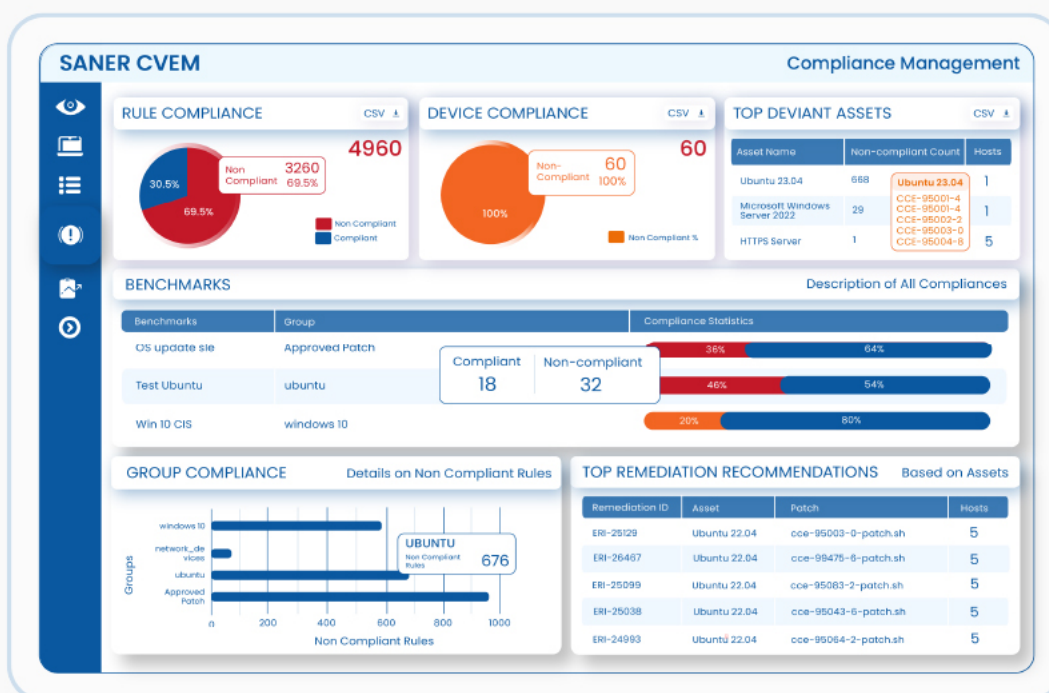
Go Beyond Patching and Apply Various Security Controls

Saner CVEM enables you to go beyond patching with numerous remediation methods and endpoint controls to manage other risk exposures.

- Gain complete visibility over endpoints with 100's of built-in checks
- Track anti-virus status
- Track system event logs
- Discover sensitive data
- Remote system health monitoring
- Gain visibility to networks, subnets, and network settings
- Schedule visibility alerts based on event occurrence
- Multi-platform endpoint management supporting Windows, Linux, and Mac OS
- Software deployment and inventory management covering applications for Windows, Linux, and Mac OS
- Track and uninstall unwanted software applications
- Upload custom applications and deploy
- Deploy software applications silently and with additional command line options
- Configure installation rules to ensure systems have only authorized applications
- Block unwanted applications on individual systems or group of devices
- Block devices on individual system or group of devices
- Stop or start services and processes
- System Tune-up to clean unwanted files, registry, browsing history, and download locations
- Apply network settings across group of devices
- Quarantine or isolate a system to a separate network
- Execute custom scripts
- Edit system registry, kernel settings
- Schedule and edit start-up programs and cron jobs
- Apply security settings, kernel parameters, firewall settings
- Reboot or shutdown systems
- Perform file operations like search, edit, and delete
- Schedule jobs to run periodically
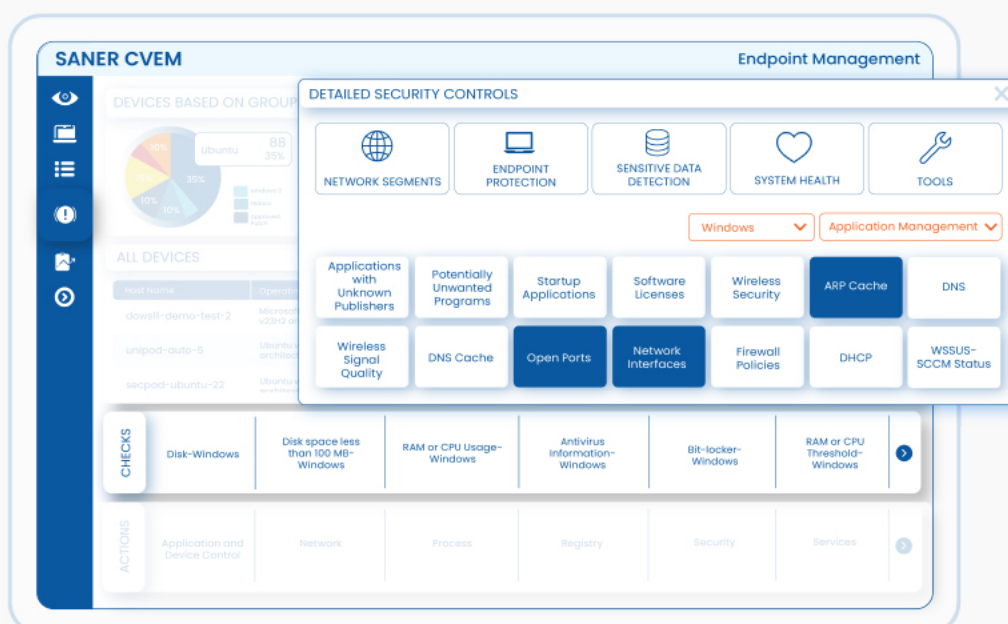
Build Query and Responses to Fix Deviations in Endpoint Activities

Saner CVEM provides an array of query and response checks to get complete visibility over endpoint activities and fix any deviations.

- Build queries to get instant visibility to endpoint activities
- Build queries from a list of 198 probes and 1470 attributes on any device
- Run queries periodically to get up-to-date information
- Cascade multiple queries into one single query job through AND and OR operations
- Assign severity level to categorise query results
- Define the scope of query execution to a device, or group of systems
- Build responses to fix deviations and aberrations seen in query results
- Build responses from a list of 100s of response statements across any device
- Track response status and ensure fixes for posture anomalies
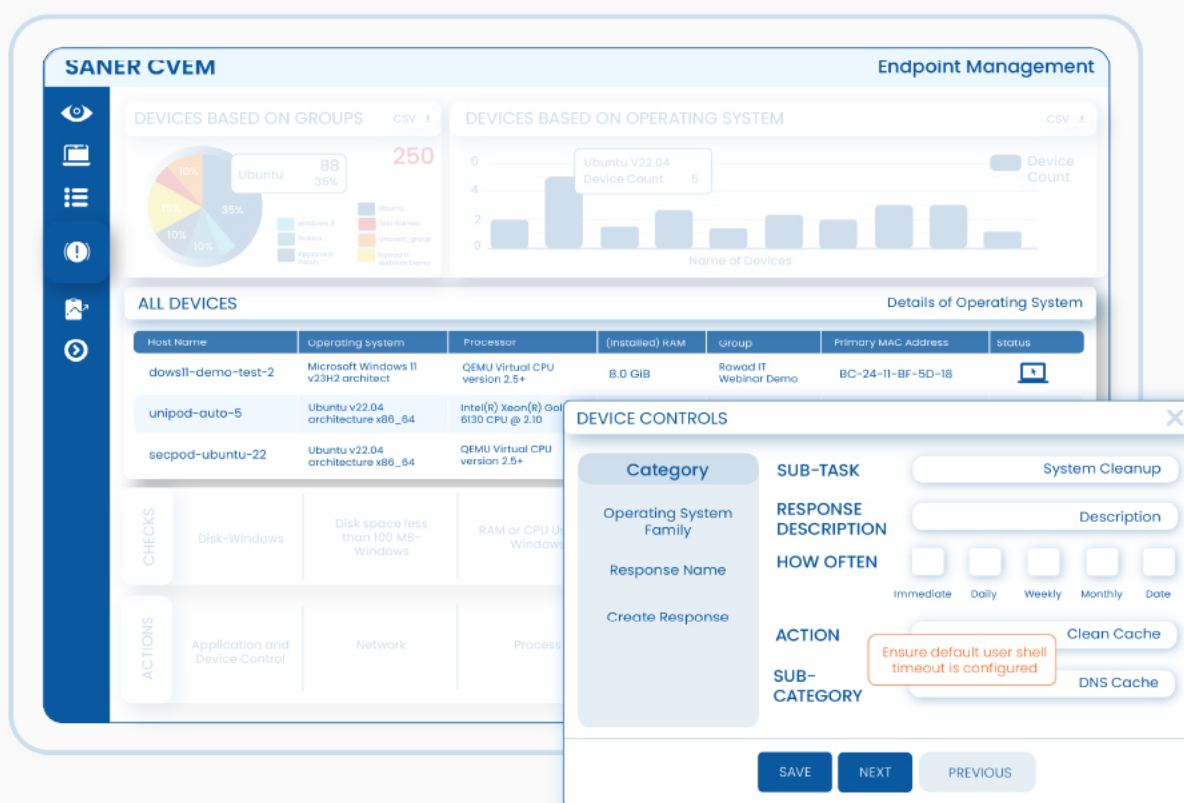
Customizable, Insightful Reports and Alerts

Saner CVEM provides out-of-box in-built reports to help you analyze various metrics.

- 100s of prebuilt reports with insightful information represented in understandable graphs and tables
- Organizational compliance reporting out of the box for compliance policies
- Customize and create new reports with hundreds of APIs
- Schedule and automate these reports and receive them in your mailbox
- Risk-assessment report to provide a complete view of security risks in the network
- Patching impact report to understand the impact of patches in the network
- Canned reports for all modules
- Generate reports for regulatory compliance benchmarks
- Schedule reports for backup and mail reports in PDF format
- Export reports to PDF, CSV
- Create different custom reports based on different stake-holder needs
- 1000s of Report API for custom report generation
- Schedule e-mail-based alerts for 100s of events
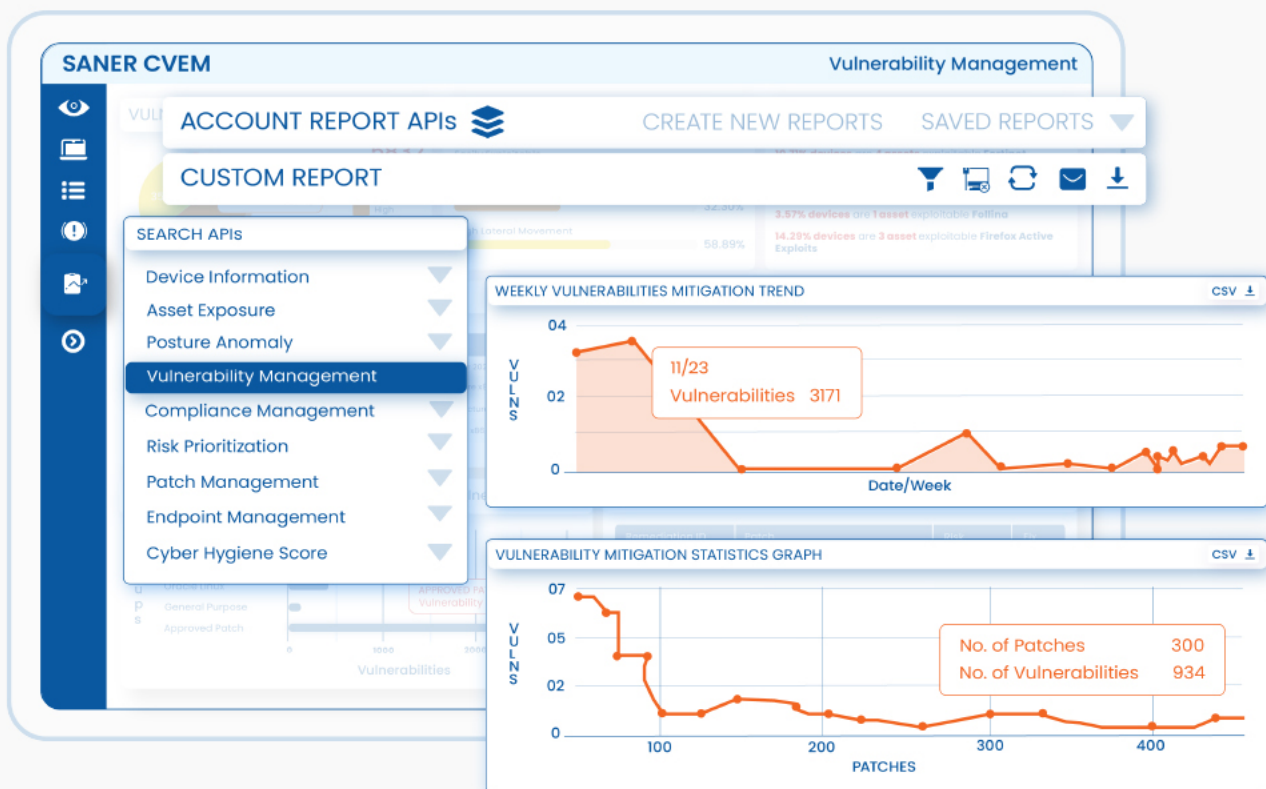
Intelligence Driven Cyber-Hygiene Scores

Quantify your cybersecurity posture and eliminate risk rapidly with intelligence-driven, natively-developed cyber hygiene scoring framework.

- Hygiene scores are categorized as low with the range of 0-40, Good 40-80 and better 80-100.
- Achieve the best possible score of 99.6 percentile and stay at the top of cyber-hygiene game.
- Know where your organization stands internally through local score.
- Pin-point Different Security Risks in your Devices.
- Demonstrate cyber readiness and measure cyber defense with ease.
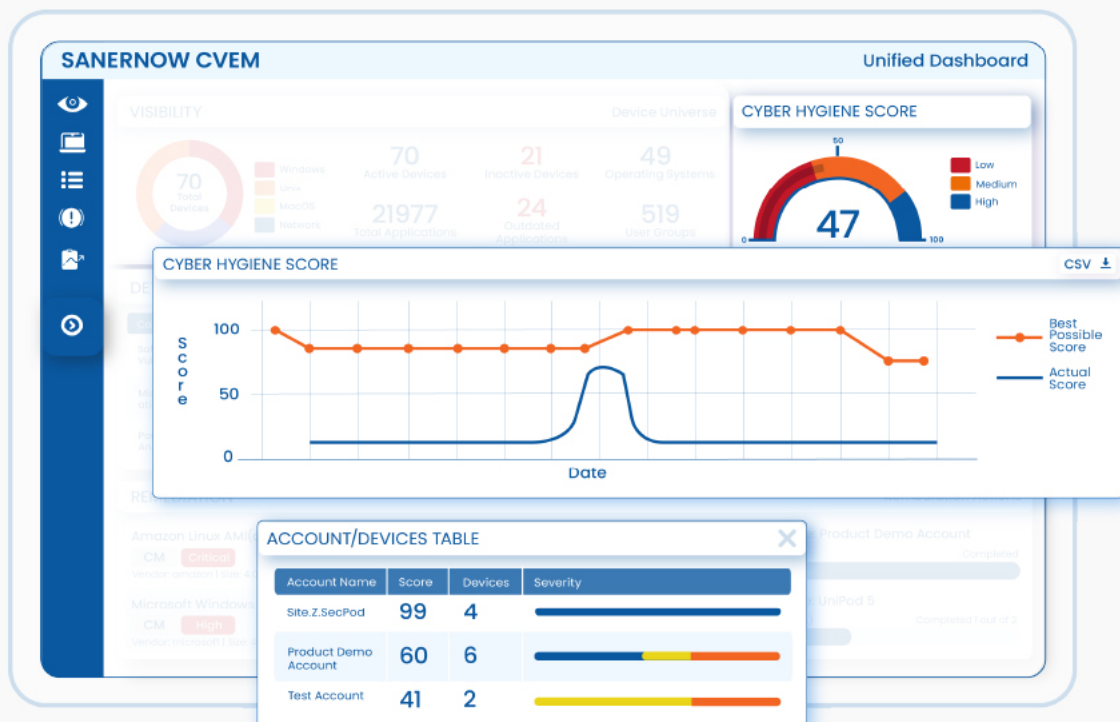
Saner CVEM's New-age Continuous Vulnerability and Exposure Management for the Modern Security Landscape

For more than two decades, the definition of vulnerability has been straightforward, "a weakness or flaw or error in devices." And even today, many security teams have a fragile approach to vulnerability and exposure management with a lack of clarity over remediation.

With massive changes in the security landscape today, we need to rethink vulnerability and exposure management to bring potential enhancements to managing risks. SecPod Saner Continuous Vulnerability & Exposure Management innovates a new paradigm to discover and remediate vulnerabilities and different security risks in an IT network.

With Saner CVEM, you can gain control over IT assets, detect and remediate vulnerabilities, apply patches on all operating systems and 450+ third-party applications, abide by security compliance benchmarks like HIPAA, PCI, ISO, and NIST, identify and fix security misconfigurations, implement strong security controls, fix security anomalies, and achieve all of it from a single centralized console. Using SanerNow, you can manage vulnerabilities, exposures and beyond and establish a new regime to manage security risks.

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.

Contact Us

Email us on:
info@secpod.com

www.secpod.com