Join Forces with
SecPod's OEM Program

Build a Disruptive Vulnerability Management Offering for your Customers

www.secpod.com

The Existing Vulnerability Management Landscape

The threat landscape is changing unimaginably. With thousands of new vulnerabilities and the growing complexity of digital environments, the sheer volume of attacks isn't going to stop.

Businesses are going to be more bullish about their growth, and this, again, will lead to more security challenges. Let us look at a few:

- Managing vulnerabilities associated with critical infrastructure components
- Handling increase in scale and complexity in infrastructure
- Meeting regulatory compliance
- Integration of vulnerability management with SOC services
- Deep dive analysis of vulnerabilities to correlate with threats and events

These challenges define and notch up a huge portion of time and resources in an organization's run-up to strengthen its security posture. Though obviously tied to these reasons, companies also need to take a hard look at the most exploited vulnerabilities in recent years to understand this landscape more deeply.

These vulnerabilities leave their imprint & mark as it is the doorway for an attack.

Here are a few vulnerabilities, that have caused havoc:

- **Log4Shell**

This vulnerability affects Apache's Log4j library and allows an attacker to take full control of the system

» FortiOS

This vulnerability affects Fortinet SSL VPNs and allows an attacker to expose SSL VPN credentials

» Injection Remote Code Execution

This vulnerability affects the Atlassian Confluence server and allows an attacker to execute code remotely

» ProxyLogon

This vulnerability affects Microsoft Exchange & allows attacker to run code remotely

» ZeroLogon

This vulnerability affects Microsoft Windows and allows an attacker to gain administrative access to a domain controller

The patterns of attacks due to these vulnerabilities can show up in big ways, though most organizations use vulnerability management tools. These tools are siloed and don't seem to work.

The number of companies affected by WannaCry has only grown to 53%, and CISA has mentioned the importance of reducing the trends in system weakness due to misconfigurations.

With thousands of new vulnerabilities and the growing complexity of digital environments, the sheer volume of attacks isn't going to stop.

Most vulnerability management tools are siloed & don't seem to fix these vulnerabilities.

IT & Security teams across the world are fed up. They need a change. They want to explore new practices to fix these vulnerabilities & misconfigurations.

Vulnerability Management- The Backbone of Zero-Trust Security

Before we move ahead to discuss the disruptions needed in the vulnerability management space, here is a brief on vulnerability management's implications for Zero Trust security.

Why is this needed?

» Zero Trust security is imperative for the success of any security program

» It's a mix of security solutions, where each component enables a defense-in-depth approach across the enterprise to provide a hardened environment

Vulnerability management forms the backbone of such an approach by focusing on infrastructure security. It focuses on remediating vulnerabilities & misconfigurations from endpoints, servers, data centers, cloud workloads, and applications. Before the attackers can find them.

Are the Current Vulnerability Management Tools Truly Enabling Zero Trust

However, the tools that exist in the market deserve some scrutiny. Most of them are siloed & offer a fuzzy implementation of end-to-end implementation of vulnerability management. They are mostly focused on "certain kinds" of vulnerabilities, such as software vulnerabilities, removing aspects such as security control weakness, misconfigurations, etc., out of the equation.

These tools also lack key features, such as:

» Poor IT infrastructure visibility, integrated remediation, inability to prioritize risks
» Lack of automation, continuous scans
» Cumbersome deployments, multiple agents
» Higher false positives.

It's hard to argue on two points:

» Without a continuous, automated, integrated platform, companies will witness a steep decline in the efficiencies of SecOps, leaving their security posture in jeopardy
» And if they do not deal with their burgeoning number of vulnerabilities, they risk what they precisely fear, a huge number of exploits, leaving them disgruntled

This challenge is an opportunity for you in the vulnerability management market space. It's time you step in with the answer. It's time you step in with the answer.

The tools that exist in the market deserve some scrutiny.

Tools also lack key features such as poor IT infrastructure visibility, integrated remediation, inability to prioritize risks, lack of automation, continuous scans, cumbersome deployments, multiple agents, higher false positives, etc.

The Time is Ripe. Go for an OEM Partnership with SecPod

Here is why you must explore the OEM partner business model with SecPod.

» First, vulnerability management is largely a high-ticket market space

» This can be a powerful alliance that is at the start of the value chain and holds immense potential for you to enter the vulnerability management market

» Gives you the power to disrupt the market with the right answers for IT and security teams

Let us understand this partnership and how it can help you to stand apart in the market.

By partnering with SecPod, you can develop a globally acclaimed, fully automated, integrated, continuous vulnerability exposure management solution under your brand by white labeling the SanerNow SDK and penetrate a new market segment without investing heavily in new product development.

By partnering with SecPod, you can develop a globally acclaimed, fully automated, integrated, continuous vulnerability exposure management solution under your brand by white labeling the SanerNow SDK and penetrate a new market segment without investing heavily in new product development.

Partnership with SecPod Key Advantages

Provides you with the window to unleash your creativity and compartmentalize the solution of your choice based on your customer needs:

- You will be able to repackage multiple modular components to offer the precise functionality your customer needs
- Helps you to move away from traditional sales and marketing strategies to drive revenue
- Focus on well-defined value propositions to solve specific security pain points of your customers
- Ensure perfect product-market fit combined with performance that can strongly resonate with your customers
- Leverage SecPod 's technology expertise and customer success support for better UX and consistent quality
- Utilize SecPod's strengths to drive top-line revenue

By forging an alliance with SecPod, you can focus on well-defined value propositions to solve specific security pain points of your customers. If you are thinking of establishing dominance in the vulnerability management market space, SecPod can help you develop the perfect product-market fit combined with performance that can strongly resonate with your customers.

The marketing of the product remains entirely in your realm to drive its market success, while SecPod stays in the background to give you the technology expertise and customer success support for better user experience and consistent quality. This allows you to leverage our strengths to drive your top-line revenue.

More Benefits of Partnering with SecPod

✓ REDUCE TIME TO MARKET

Embed vulnerability management, patch management, IT asset exposure, security controls, and compliance management capabilities to your existing solution within a matter of days. This helps you to quickly validate the product with the necessary improvements.

✓ FLEXIBLE LICENSING MODELS

Quickly meet customer demands with our licensing models that let you choose between our APIs and SDKs to integrate with your solution.

✓ ONBOARDING & TECHNICAL SUPPORT

We provide you with extensive support during onboarding and assist you in the SDK integration process. You also get developer access to the platform, API reference guides, code samples, and technical support on any queries during solution development. NFR (Not for Resale) license access along with Level 3 support during the integration period, along with access to engineering resources for any enhancements or issue resolution.

✓ PARTNER STRATEGICALLY TO DRIVE BUSINESS

We can align with your strategic business goals by providing our in-house end-to-end capabilities from design, development, and support. This helps you leverage our expertise to the full extent possible while maintaining a high level of proficiency across the customer journey.

✓ SAVE COSTS ON INNOVATION

Conceptualize innovative solutions faster & offer game-changing disruptions to the market at lower costs. Design & engineer products with the existing capabilities of SanerNow SDK, which is built over years of R&D efforts of SecPod's engineering team. This helps you to save innovation costs & developmental overheads to create your own IP. You can also get visibility into our future SDK roadmap.

✓ EXPAND PRODUCT PORTFOLIO

Get guidance from our engineering team for design, development, lifecycle management, and support to develop a robust product. Get the right service, support, and technology to differentiate your product, increase its potential for success, and serve your customers better. You will quickly expand your product offerings with no obstacles.

✓ GET A GREATER RETURN ON INVESTMENT

Generate better value by offering competitive products to force higher profit margins. You will also be able to experience shorter product life cycles and faster product updates. Reduce your total cost of developing a product from scratch, including that of resources and other operational overheads.

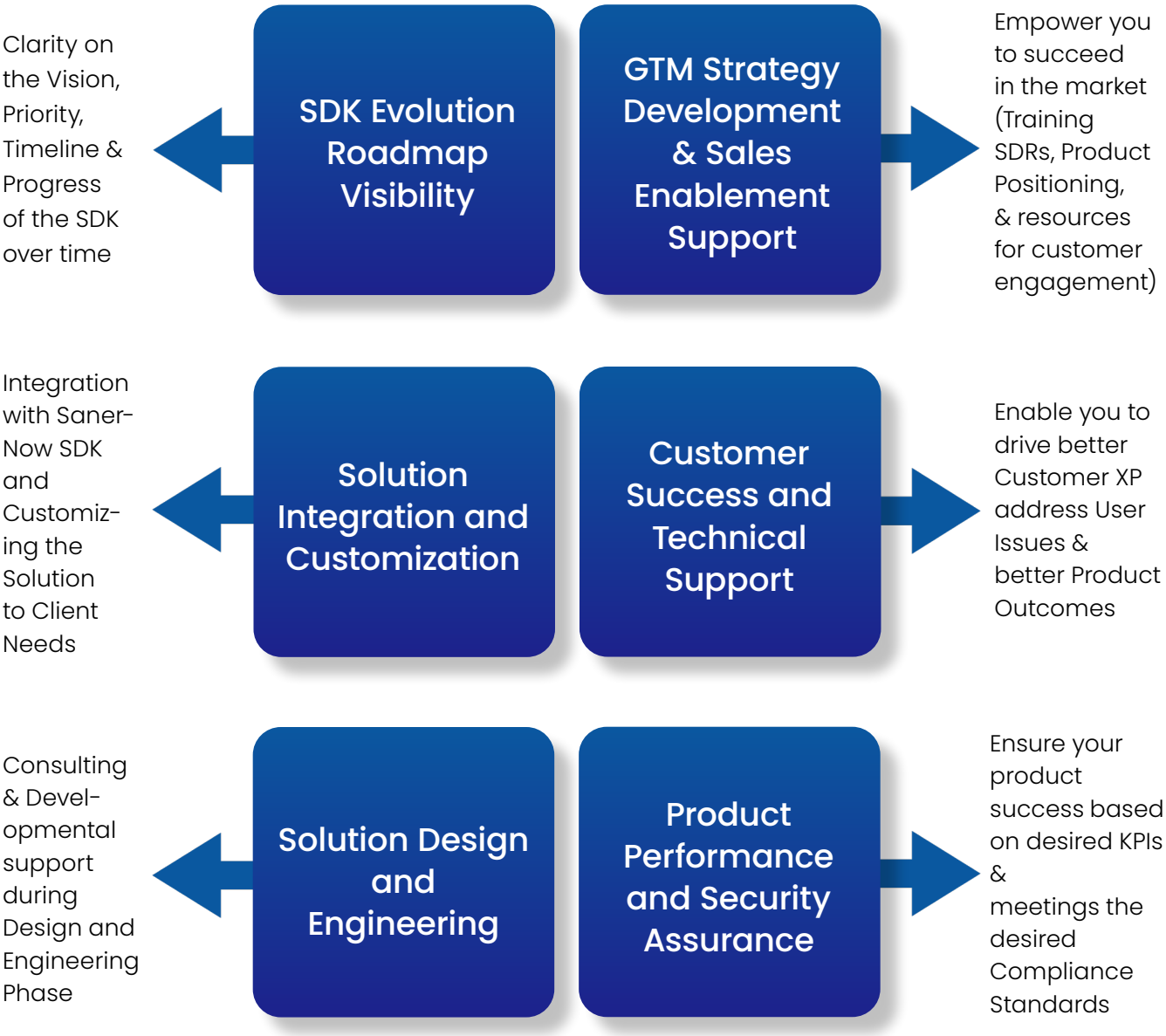
✓ REDUCE BUSINESS RISKS

By collaborating with us, you can mitigate all possible risks associated with development, product quality and regulatory compliance. You do not need any additional technology investments. SanerNow SDK offers advanced vulnerability management features that might be too expensive to develop in-house.
This access empowers you to stay ahead of industry trends and innovate continuously with no business risk.

✓ SUCCESS IN THE MARKET

You will be able to create a well-defined value proposition, address the specific pain points of customers, establish your dominance in the industry segment, scale your business and establish brand credibility. You will also have access to SecPod's marketing expertise to fine-tune your GTM strategy, including marketing/sales collaterals.

Your Gains from the OEM Partnership Program



SanerNow SDK – Your Technology Disruption Enabler is Here

The SanerNow SDK is radically different. Here is why.

- A new technology that can tip the industry upside down
- Simple to adopt, easy to use, and affordable
- Combine various use cases into outputs of greater value
- Disrupts the way your security ecosystem works by improving efficiencies, reducing operational costs & resource overheads
- Helps you to create new markets and discover new categories of customers

You can refine the SDK and use it to develop unique products for specific use cases and reshape the way the world perceives vulnerability management.

There is also a good reason to think that the pace of innovation will increase as you improvize the form and function of your product using the SDK to expand its disruptive influences on new industry realms.

We promise you the SDK will help you change the way the world looks at vulnerability management by offering new levels of value for a cost three times lower than current market leaders. The SDK is a result of a long and arduous process endured by our engineering team since 2008 to transform their body of knowledge into building a disruptive and intuitive technology by leveraging their assortment of expertise and experimentation.

You can refine the SDK and use it to develop unique products for specific use cases and reshape the way the world perceives vulnerability management.

SanerNow SDK Capabilities

Rapid, Continuous & Automated Operations

Provides the industry's fastest scans to discover vulnerabilities in less than 5 minutes and automates security tasks to achieve continuous operations, from scanning, detecting, prioritizing, and remediating the vulnerabilities.

Seamless Integration and Interoperablity

Flexible architecture for integration with various systems. REST APIs enable access to collected data from endpoints and support search queries and SDK for tighter integration of SecPod's technologies in your application.

Multi-tenant Support with Segregated User Data

Multi-tenant support to manage multiple business units and system users with a single server for vulnerability management. With neatly segregated business users' data, you can create various user roles with defined access rights to manage different areas of a corporate network.

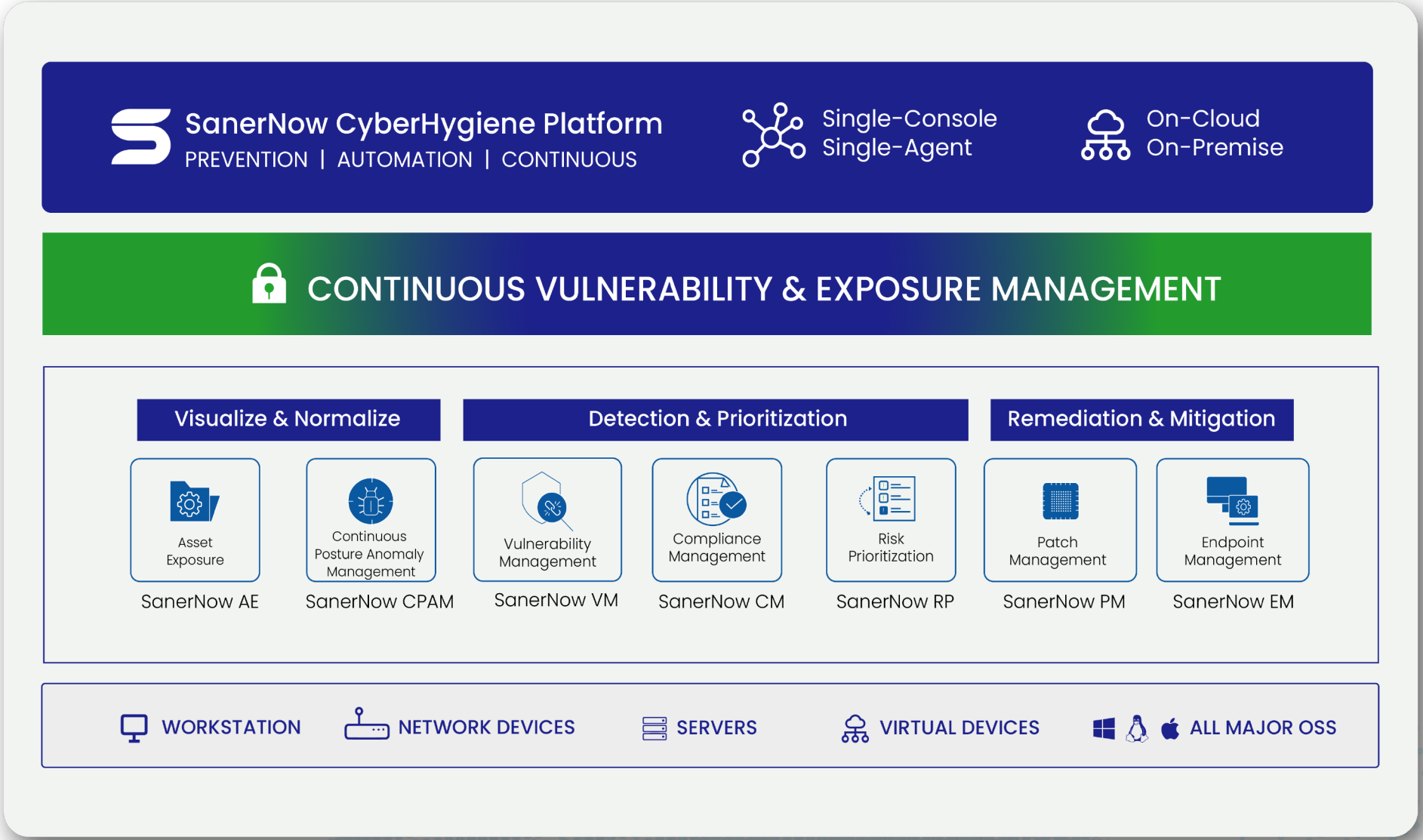
High Performance Scalable Architecture

Develop a highly scalable solution with a Big Data architecture. The architecture efficiently supports the management of a large number of devices.

Operates on a Light-weight Agent

Single, lightweight, multifunctional agent that weighs less than 15MB to execute the tasks. The agent also takes up the role of network scanner and saves costs on integrating additional hardware. You can also choose to embed SecPod's technology into their own agent through SDKs to prevent the installation of the additional agent.

Actioning SanerNow Features to take on Vulnerabilities



Feature-rich SDK Modules that You Can Use

Vulnerability Management

Perimeter-less cloud-based vulnerability management for hybrid IT environments using a cloud-based console. Scans and detects vulnerabilities in 5 minutes. Schedule and automate vulnerability scans. Detect vulnerabilities causing high-fidelity attacks. Powered by industry-renowned SecPod SCAP feed with over 175,000 vulnerability checks.

Patch Management

Patches on all major OSs and 450+ third-party apps. Get the latest patches from all supported vendors in under 24 hours. All patches are pre-tested and ready for deployment. Create automation rules and execute faster patching across network. Continuous and customizable patch scans to find missing patches. Effortless rollback for an error-prone software patch.

Compliance Management

Run compliance scans & address configuration drift. Align with global & regional compliance regulations. Customize compliance policies based on available system configurations. Convert compliance status into insightful reports. Drive compliance risk assessments to remediate risks.

Risk Prioritization

Harness the power of CISA SSVC risk prioritization framework to prioritize risks. Reduce exploitable attack surface. Leverage a good mix of exploitability, vulnerability intelligence, business impact, and context to categorize risks. Gain decisive insights into security risks. Configure and customize prioritization based on business needs.

Posture Anomaly Management

Discovers the aberrations, deviations, risks, and outliers by assessing devices using statistical analysis, machine learning, and deviation computations. Discover attack vectors in the network and implement security measures to reduce risk exposures.

Endpoint Management

Monitor and assess 100+ endpoint health controls in real time. Install or uninstall software, block apps or processes, start or stop a service, configure settings, apply security controls, automate all security control activities across all major OS platforms, Get instant visibility over security risks, & automate day-to-day endpoint management.

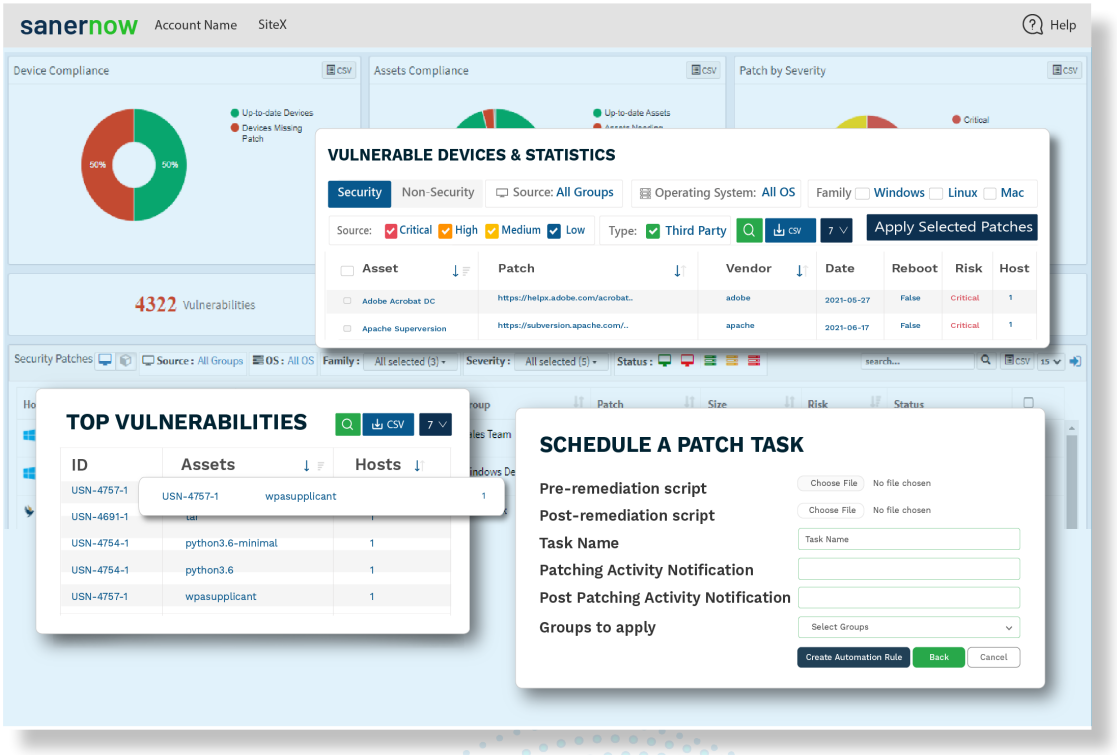
Asset Exposure

Track, monitor, and manage software and hardware assets in real time. Detect rarely used applications, blacklist software, and software license tracking. Track software usage metrics, monitor and manage vulnerable assets, manage asset license details, and manage the IT

The Many Product Possibilities to help you Succeed

Your product development team has it easy with the SanerNow SDK. They can create a product for various use cases and integrate it with the SDK. The kit is developed to customize the modules it offers and make the entire product development process more efficient and seamless.

The SDK also includes code, APIs, libraries, developmental tools, code samples, documentation, practices, and rules on how to use it effectively to maximize the impact of the product. Here is a detail overview on the SDK use cases and how you integrate the SDK with your application to create a new product.



The Many Product Possibilities to help you Succeed

Product Use Case 1

Anti-Virus

- Malware protection
- Prevention & detection
- Quarantine and remediation
- Protection from removable devices
- Offer multiple layers of protection
- Patch management

Product Use Case 2

Security Operations Centre

- Vulnerability scanning
- Vulnerability management
- Risk Prioritization
- Asset Management
- Vulnerability remediation
- Malware prevention
- Patch management
- Compliance management

Product Use Case 3

Breach and Attack Simulation

- Vulnerability scanning
- Vulnerability management
- Risk Prioritization
- Real-time vulnerability alerts
- Security posture validation
- Threat intelligence integration
- Asset management
- Patch Management

Integration Using Rest APIs

SanerNow Platform

Types of Scanners that can be installed in your Client's System

- Endpoint/Server Vulnerability Scanner
- Network Vulnerability Scanner
- Active Directory Vulnerability Scanner
- Virtual Device Vulnerability Scanner
- Cloud Scanner

SanerNow SDK

Integrate Your Application

The Many Product Possibilities to help you Succeed

Product Use Case 4

Endpoint Security

- Asset discovery
- Anomaly management
- Vulnerability management
- Patch management
- Endpoint management
- Malware Prevention
- Device Control
- Device Monitoring
- Device Configuration
- Manage Patches and Updates
- Block Malicious Apps and Devices

Product Use Case 5

ITSM

- Vulnerability Management
- Patch Management
- Asset Management
- Posture anomaly management

Product Use Case 6

SIEM

- Compliance management
- Vulnerability management
- Detect Misconfigurations
- Prevent asset compromise
- Detect malicious devices
- Threat intelligence integration
- Identify system deviations

Integration Using Rest APIs

SanerNow Platform

Types of Scanners that can be installed in your Client's System

- Endpoint/Server Vulnerability Scanner
- Network Vulnerability Scanner
- Active Directory Vulnerability Scanner
- Virtual Device Vulnerability Scanner
- Cloud Scanner

SanerNow SDK

Integrate Your Application

Let’s have a Conversation to Explore the Possibilities

Connect with us. We will be glad to help.

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.