secpod

STEP BY STEP GUIDE TO BUILD AN Attack Surface Management Program

www.secpod.com

Introduction

Traditional Vulnerability & Exposure Management is Not Good Enough !

With traditional vulnerability and expousre management severely struggling to cope with rapidly mutating and evolving cyber-attacks, there's a desperate need to reinvent the existing process. With no scope for risks beyond software vulnerabilities, traditional vulnerability adn exposure management restricts itself by only looking at software vulnerabilities. Adding to it is the lack of any real visibility into IT assets, further limiting any meaningful actions an IT admin can take.

System admins, IT, security teams, and CISOs are still struggling with siloed solutions & multiple consoles to combat the evolving vulnerability and threat landscape. With the lack of integrated remediation, the vulnerability management process becomes lengthy and skewed. Moreover, due to the absence of automation, vulnerability management becomes a monthly or yearly cyclic process instead of a continuous one. Continuous Vulnerability and Exposure Management is the new way forward, and with the right tools, you can develop and practice CVEM that provides a whole slew of benefits over traditional VM or EM.

How is CVEM Different from Traditional Vulnerability Management ?

Continuous Vulnerability and Exposure Management integrates vulnerability and exposure detection, assessment, and remediation into a unified, continuous process while increasing the scope of detection of threats by covering various other security risks beyond software vulnerabilities like misconfigurations, missing configurations, and security anomalies.

Continuous Vulnerability and Exposure Management incorporates the weakness perspective, an aggressive way of actively searching for security risk that could pose a potential threat to the IT infrastructure. By keeping continuity, automation, and an expanded scope of detection at its core, CVEM allows for effective and smooth attack surface management and threat exposure reduction.

It ensures that your vulnerability & exposure management is a continuous process that can patch, prevent, and protect you from cyberattacks. It encompasses all the features of vulnerability & exposure management within itself and provides additional enrichment and oomph for the better.

Traditional Vulnerability Management	Continuous Vulnerability & Exposure Management
Siloed Interfaces & multiple-point solution approach	Unified Single-solution approach to visibility, detection, assessment, prioritization & remediation
Rely on a separate tool for remediation	Integrated & seamless patch management capability for timely remediation
Discover only CVEs or software vulnerabilities	Detect vulnerability, misconfigurations, asset exposures, missing critical security patches, & security posture anomalies within a single console
Lack of remediation controls to fix security risk exposures	Remediation controls beyond patching to fix the vulnerability and other security exposures
Manual methods & irregular processes	Built for automation, achieving continuous compliance
Irregular scans and no clarity on real-time risk posture	Continuous scan and up-to-date risk posture assessment
Prolonged Patch Management Lifecycle taking months to complete	Rapid, continuous and automated patch management lifecycle
Lack of capabilities to build queries to detect and respond to security risks	Build custom queries to detect security risks and deploy instant response
OS and device-specific support	Heterogeneous and device-agnostic support
Multiple Agents	Single, light-weight, multifunctional agent
Lack of API support & eco-system integration	Native API support & eco-system integration
Ineffective Attack Surface Management	Rapid and effective Attack Surface Management
Lack of weakness perspective for cyberattack prevention	Weakness perspective incorporated into managing security risks
Segregated security and IT Goals	Unified security and IT Goals

Step by Step Guide to Build a Continuous Vulnerability & Exposure Management Program

01 Discovery of IT Assets for Complete Visibility

The first and critical step in continous vulnerability and exposure management is the discovery of all IT assets, including routers, switches, and other network devices.

WHAT IS IT?

A thorough inventory and tracking of ALL the devices in a network. Cyberattackers often exploit forgotten and outdated devices in a network. And you can't protect what you

can't see, and missing out on even one device can be devastating. So, having complete visibility is critical to ensure all points of entry are covered and it is an integral part of a continuous vulnerability exposure management program and helps you understand your organization's security posture.

HOW TO DO IT?

Discovery of IT assets is usually done by performing a complete check of all the devices in your network. Typically, the discovery is performed with an inventory tool that can scan the entirety of the organization and detects IT assets like routers, servers, switches, workstations, and other network devices. Accurate asset inventorying tools are recommended.

WHY DO WE NEED IT?

- You can't protect something if you do not know whether it exists or not.
- Discovering assets ensures that all the network components are covered under a protective umbrella, and no devices are left behind in the IT infrastructure. It ensures that threat actors do not exploit the weakness in the devices.
- With complete visibility, you can monitor the performance and the condition of assets which in turn will improve the longevity of the devices.

Figure 01- An unified dashboard that provides an eagle view into the network and all the devices within it.

02 Quantifying your Organizational Security Posture

All the assets and network devices constitute your organization's attack surface and the next step of continuous vulnerability and exposure management is to measure it.

WHAT IS IT?

It is the quantification of your organization's attack surface by evaluating every device and the risk associated with them. Measuring the attack surface allows you to find and pinpoint weak links and the most critical devices in your network as well. Further, visualizing the attack surface as a number has many advantages, and it also helps simplify and speed up the vulnerability management process.

HOW TO DO IT?

It is usually done by using a data-driven tool that can collect vulnerability and risk information, comprehend and assess it based on a quantification algorithm to help transform the attack surface into a number. The tool must evaluate a device's security posture holistically to give a clear picture of the security posture.

WHY DO WE NEED IT?

- Putting a number on your attack surface makes it easier to understand the infrastructure's exposures. Further, this allows you to make laser-focused remediation decisions.
- The difference in the score allows you to check the effectiveness of your mitigation strategies, which will help you fine-tune and improve it.
- A single score also allows you to communicate risk with stakeholders easily instead of thousand-page reports that are difficult to understand.

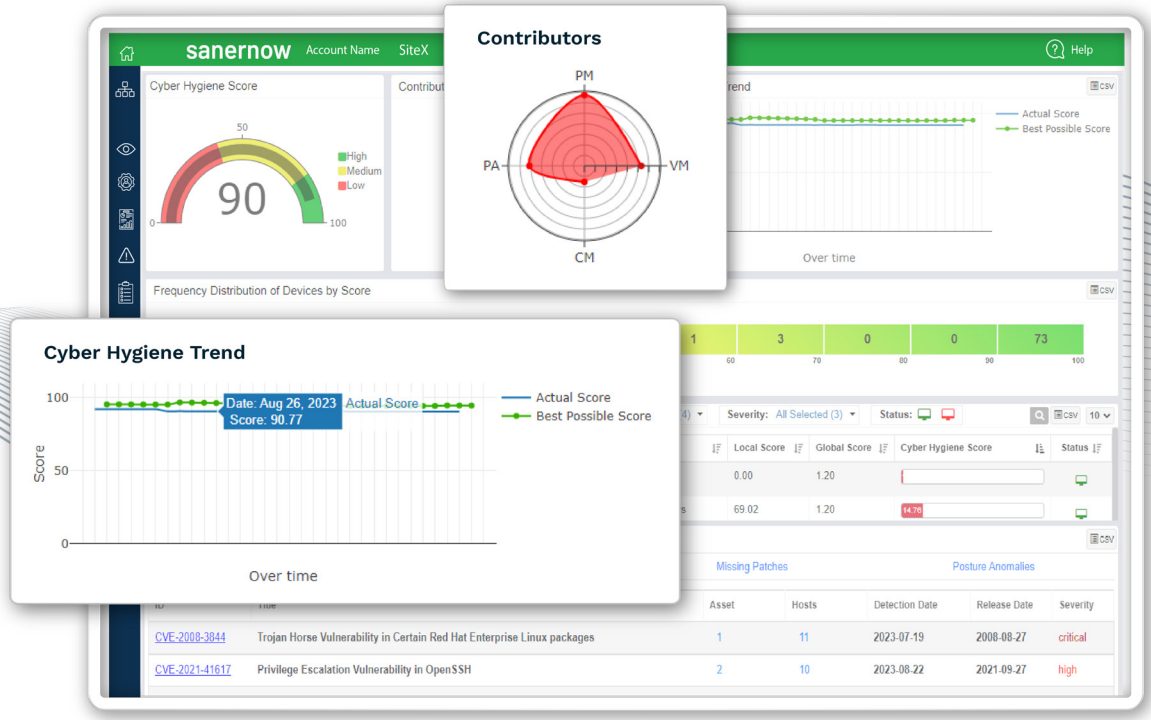


Figure 02- Quantified cybersecurity posture in SanerNow dashboard.

03 Normalization of IT Infrastructure from Posture Anomalies

The next critical step in continuous vulnerability and exposure management is normalizing your IT network from posture anomalies that threaten your IT security. Posture anomalies are deviations from the known good in your network and are some of the easiest ways for a hacker to get into your network.

WHAT IS IT?

Detection and mitigation of posture anomalies in your IT network to declutter IT assets for efficient vulnerability management. Posture anomalies might not look like security risks at first glance, but threat actors try to find the weakest link in your network. So it's critical to ensure they are accurately detected and normalized to ensure there are no loopholes a hacker can take advantage of. Cyberattackers can take advantage of ineffective user access controls or guest logins to get inside your network and try to exploit other lurking vulnerabilities.

HOW TO DO IT?

Normalizing your IT network starts by detecting posture anomalies using a posture anomaly scanner. By scanning for posture anomalies like anonymous and guest logins, unusual applications and services, bypassed user access controls, etc., and fixing them. While improving your organization's security posture, normalizing your devices also provides more control over them and helps reduce the chance of vulnerabilities being exposed.

WHY DO WE NEED IT?

- Sometimes, the most obvious attack vectors are hiding in plain sight. And without holistic visibility, a hacker might exploit them. Further, IT assets are supposed to work a certain way; if they deviate from the known good, it is a security risk, and it's important to eliminate the risk.
- Unused assets are an unnecessary expense for your organization and can simply bloat your IT infrastructure.
- Managing posture anomalies makes vulnerability management easier by eliminating the unnecessary and normalizing your IT.

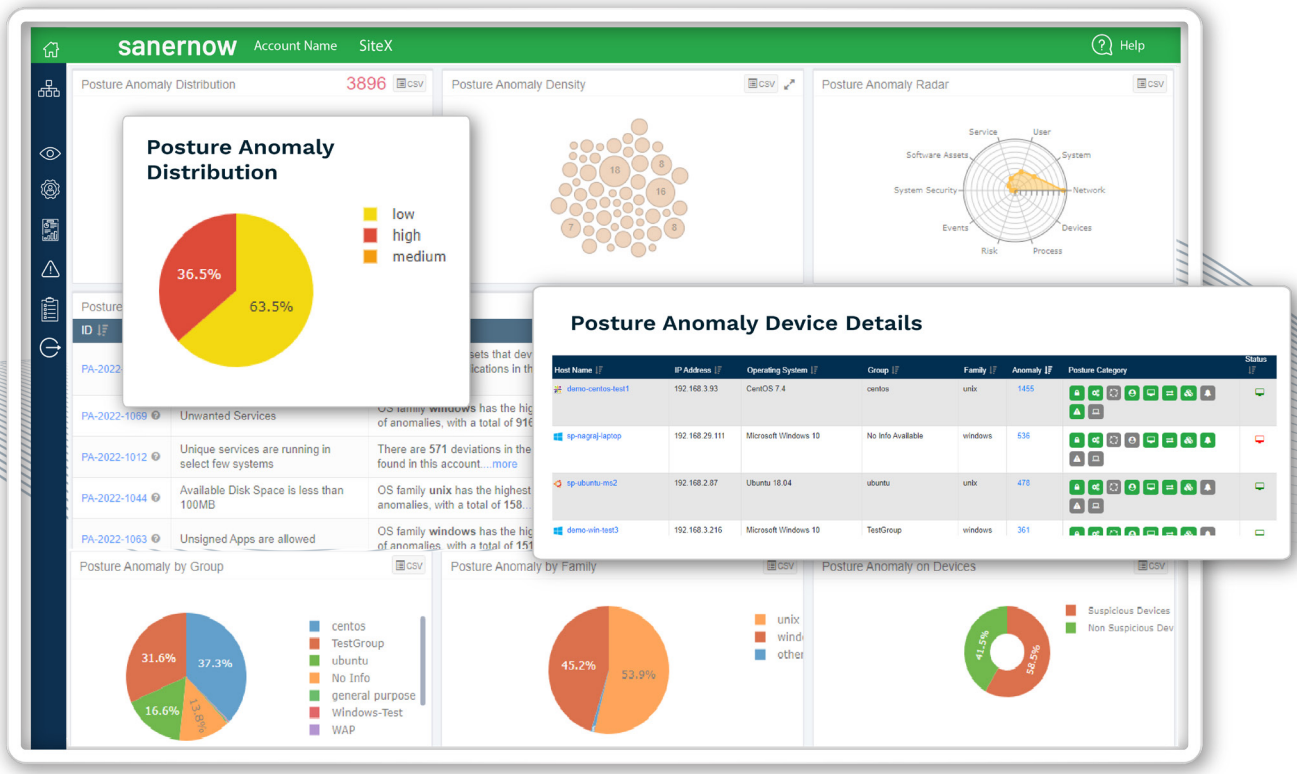


Figure 03- Posture Anomaly detection, distribution, and density in a single dashboard in SanerNow.

04 Identification of Risks Beyond Software Vulnerabilities

After discovering assets and endpoints, the next important step in continuous vulnerability and exposure management is identifying and detecting vulnerabilities, exposures & security risks.

WHAT IS IT?

Identification of vulnerabilities, exposures and other risks with vulnerability scans. It is usually performed by an inbuilt scanner powered by an extensive database that has a wide coverage of vulnerabilities. Software vulnerabilities and exposures are the tip of the iceberg when it comes to security risks. And nowadays, hackers exploit other security risks like misconfigurations, posture anomalies, asset exposures, and security deviations to breach your network.

HOW TO DO IT?

- Assets are scanned and checked to find out any vulnerabilities, exposures and security risks. It is typically performed by collecting information regarding the software and frameworks in the devices.
- Not stopping at vulnerabilities, identifying misconfigurations, security anomalies, and deviations ensures you are considering all the potential attack points for remediation.
- By using an advanced vulnerability scanner that can quickly and accurately detect the aforementioned security risks without false positives.

WHY DO WE NEED IT?

- Know what you must fix!!
- ONLY by identifying vulnerabilities, exposures and security risks accurately can you prioritize and mitigate them efficiently.
- Most compliance policies mandate regular vulnerability scans.

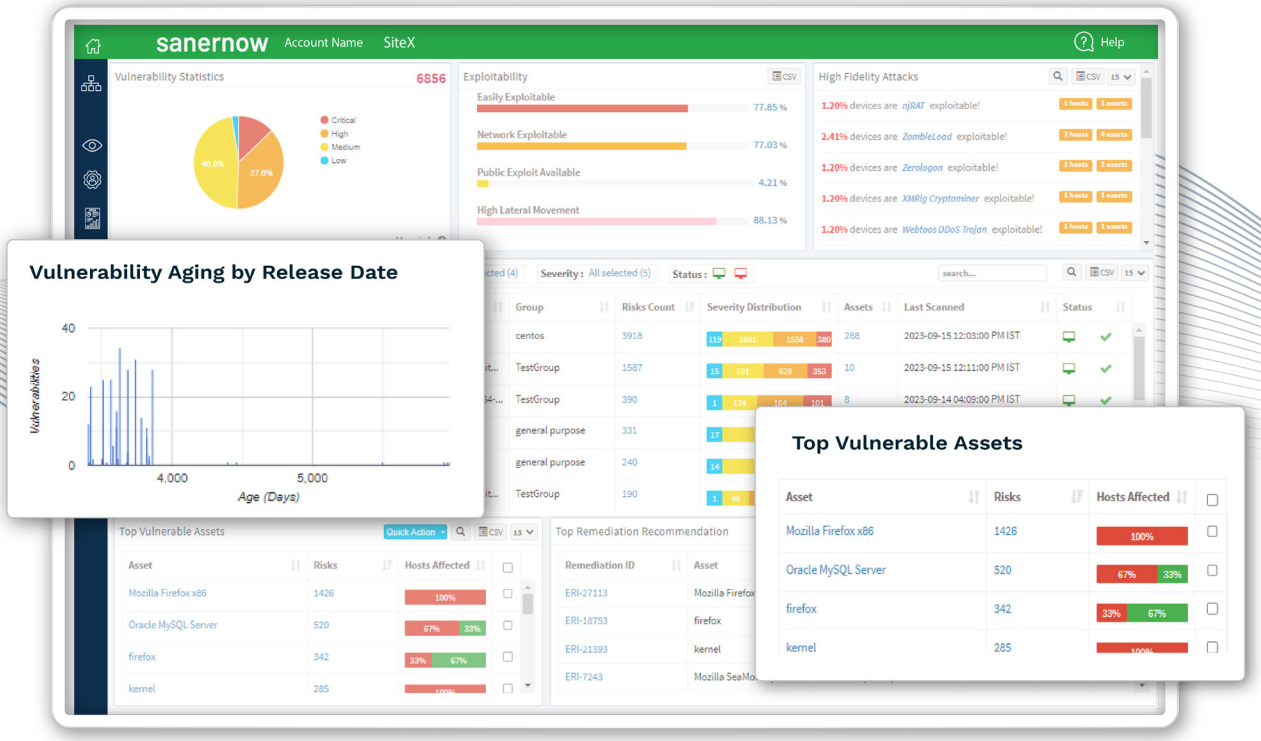


Figure 04- Comprehensive scans of all the devices in the network to identify and detect vulnerabilities in the same dashboard in SanerNow.

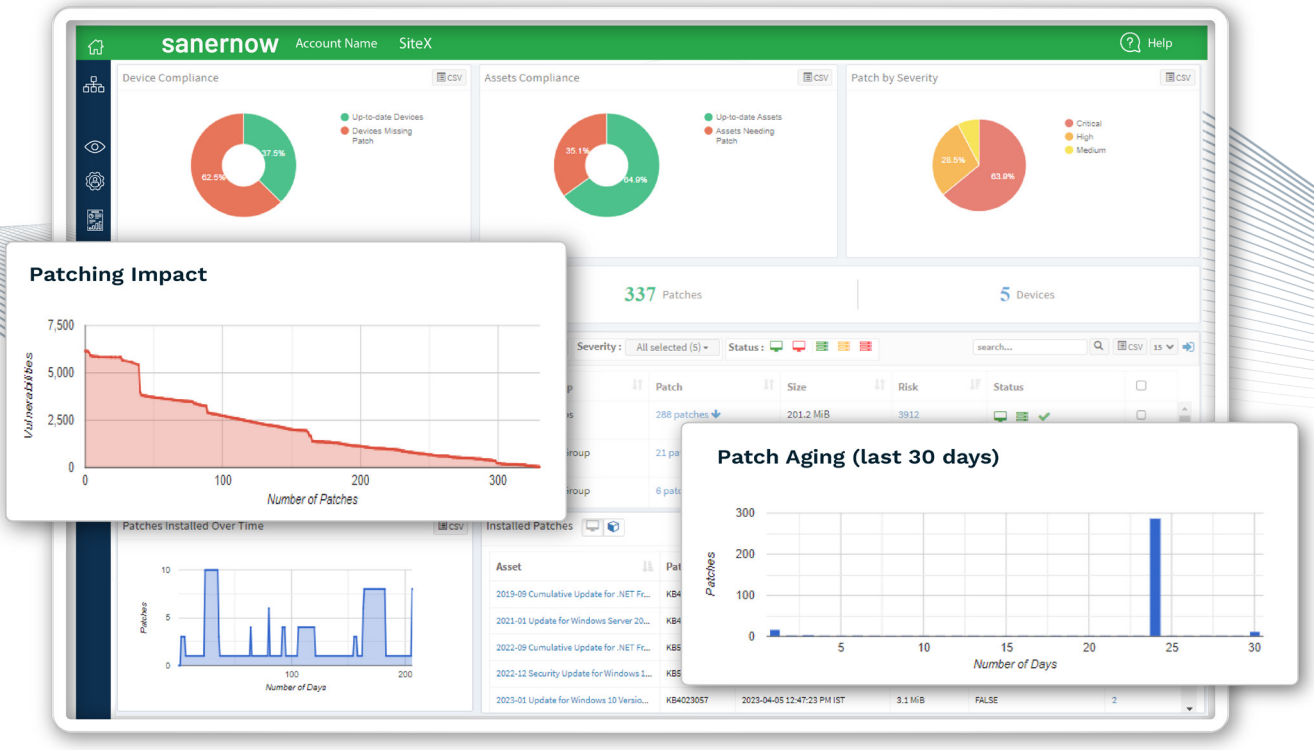


Figure 05- SanerNow scans also detect misconfigurations in the devices within the network that can cause harm.

05 Assessment of Detected Vulnerabilities & Risks

The next step of continuous vulnerability and exposure management is the assessment of the detected vulnerabilities and other security risks.

WHAT IS IT?

Understanding vulnerabilities and exposures and their potential risk by systematically and continuously monitoring the devices is the next step in continuous vulnerability and exposure management. A medium-risk vulnerability might have exploit kits in the wild, making it very dangerous, or a high-risk vulnerability might be in a rarely used application making it practically ineffective. So, detecting security risks isn't enough to stop cyberattacks and it is critical to assess the detected vulnerabilities before directly jumping into mitigation.

HOW TO DO IT?

Using a unified console that can provide an overview of the detected vulnerabilities or exposures and correlate with publicly available information. Ideally, a vulnerability scanning tool that has a large and actively updated database, with information on exploitation and high-fidelity attacks should be used. Assessing security risks effectively allows you to speed up vulnerability remediation and improve overall security posture.

WHY DO WE NEED IT?

- Assessment of vulnerabilities and exposures allows IT and security teams to gauge the risk and respond accordingly. By assigning severity scores to these vulnerabilities, you can plan and prioritize the remediation.
- With a single unified console, it becomes easier to monitor and assess the vulnerabilities and security risks, and insightful, concise reports add value to it.

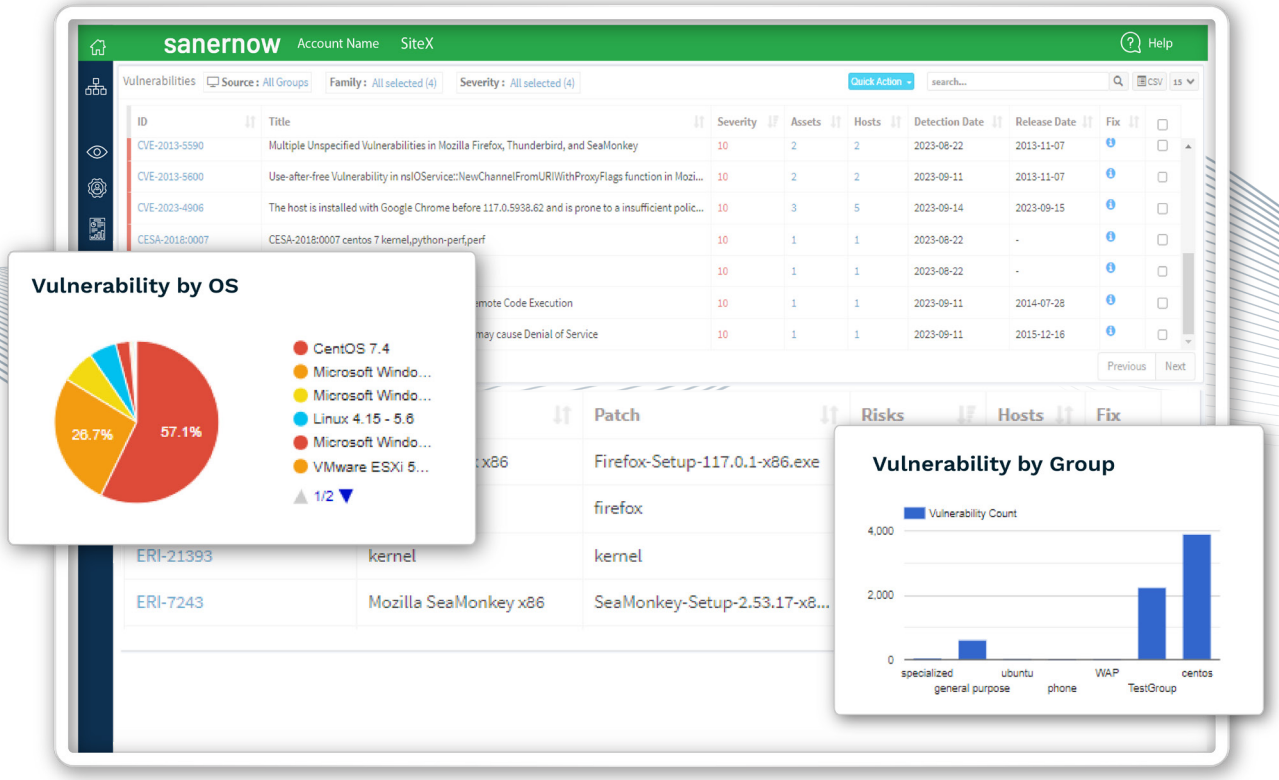


Figure 06- Assessment of vulnerabilities by assigning severity scores to detected vulnerabilities in SanerNow.

06 Intelligent Prioritization of Risks & Vulnerabilities beyond CVSS

Vulnerabilities and exposures might be significant in numbers, and not all vulnerabilities require the same effort to remediate. While all vulnerabilities need your attention, some require large amounts of time and provide little value in protecting your network. Mitigating the most dangerous threats is key in effective attack surface management.

WHAT IS IT?

Efficient sorting of risks and vulnerabilities based on criticality and other metrics to “choose what to remediate first” With CVEM, prioritization is automatic, and your time and resources can be spent elsewhere. With business context, exploitability, and other factors in mind, risk-based vulnerability prioritization allows you to remediate risks in devices that matter most and rapidly reduce your attack surface.

HOW TO DO IT?

An efficient method of prioritizing vulnerabilities must be followed, dividing the weakness into critical, high, medium, and low. This ensures that the most critical ones are patched first and prevent attackers from abusing them. Risk prioritization tools that collect and compute different data can help you prioritize remediation, but it is recommended to use a unified tool that can perform all the steps of vulnerability or exposure management.

WHY DO WE NEED IT?

- Older vulnerabilities with new exploits can be dangerous, and with a dynamic severity score in place, you can smartly prioritize vulnerabilities, exposures and security risks to mitigate risks better.
- With existing available data about vulnerabilities like public-available-exploits and historical attack info, dangerous vulnerabilities should be given more importance.

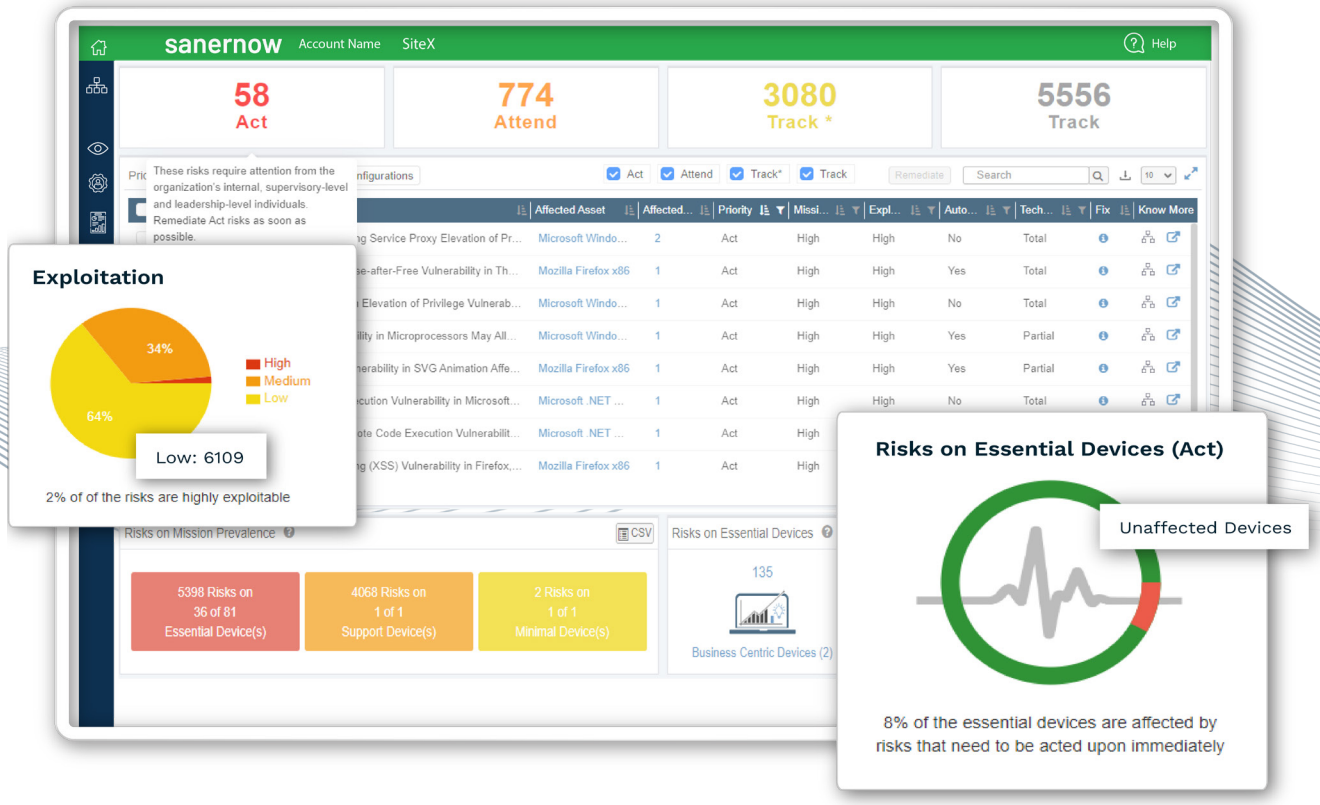


Figure 07- Vulnerability prioritization by classifying them based on severity and risk. Risks are typically categorized based on the assets within a device.

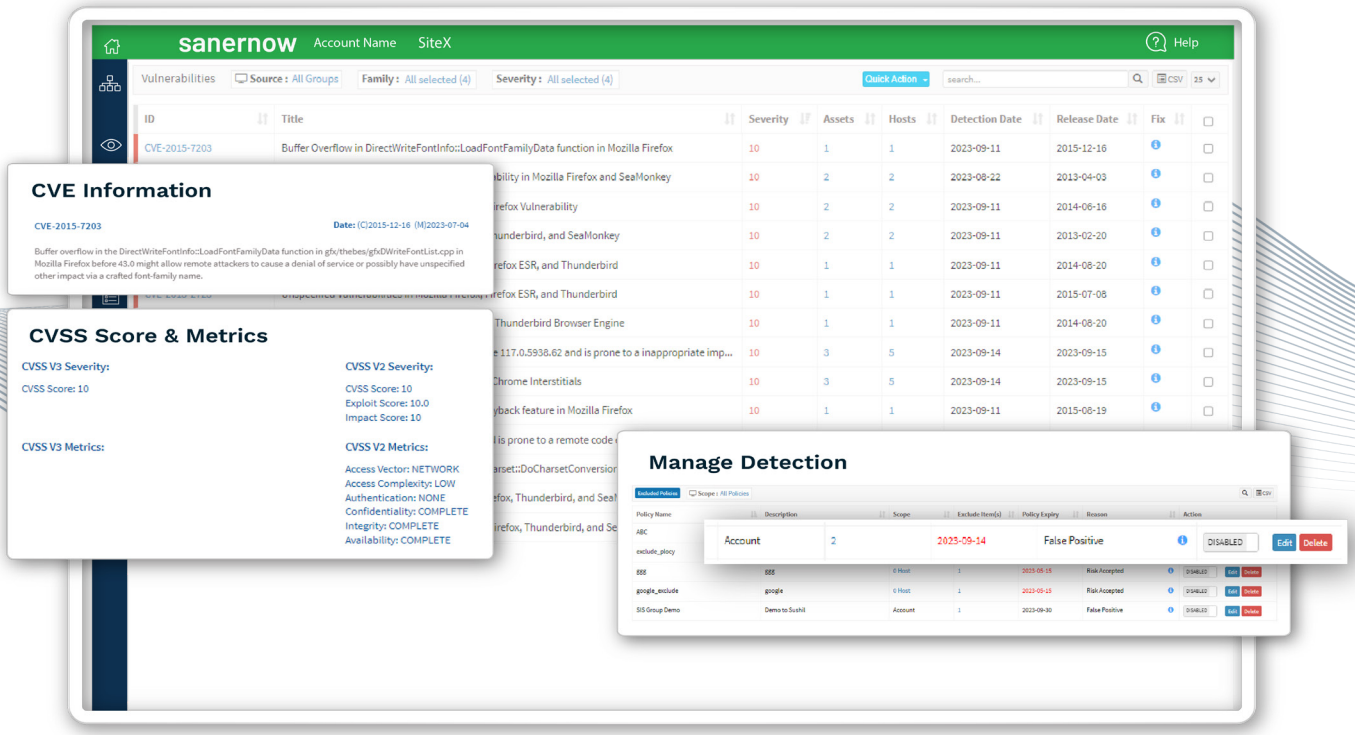


Figure 08- Vulnerability information along with severity classification in SanerNow. This information and its classification are helpful in efficiently remediating vulnerabilities.

07 Instant Mitigation of Vulnerabilities with Integrated Remediation

The most crucial step of a continuous vulnerability and exposure management program is smartly remediating the detected vulnerabilities.

WHAT IS IT?

It is the process of remediating vulnerabilities, exposures and other security risks by fully fixing or patching them while maintaining compliance and following regulatory policies. And it becomes the most critical step in vulnerability management. Security risks typically have patches or mitigations and it is critical to apply them immediately to ensure a cyber attacker doesn't get through your network.

HOW TO DO IT?

Usually done by using a patching tool that can download and apply the latest patches. Along with patching, additional security controls can be used to isolate, quarantine, and

remove other security risks which can't be patched. It is critical to keep workarounds in mind since they are just temporary fixes and are not remediation. As always, it is recommended to use a unified single tool that can perform both scanning and remediation.

WHY DO WE NEED IT?

- Only remediation can ensure security risks are mitigated and the devices are in their best shape for productivity.
- With additional remediation controls that go beyond patching, you can significantly reduce the attack surface and secure your network from impending cyberattacks.
- With integrated remediation in a natively built platform, detected vulnerabilities or exposures can be instantly remediated, so the vulnerability management process becomes faster and more efficient.

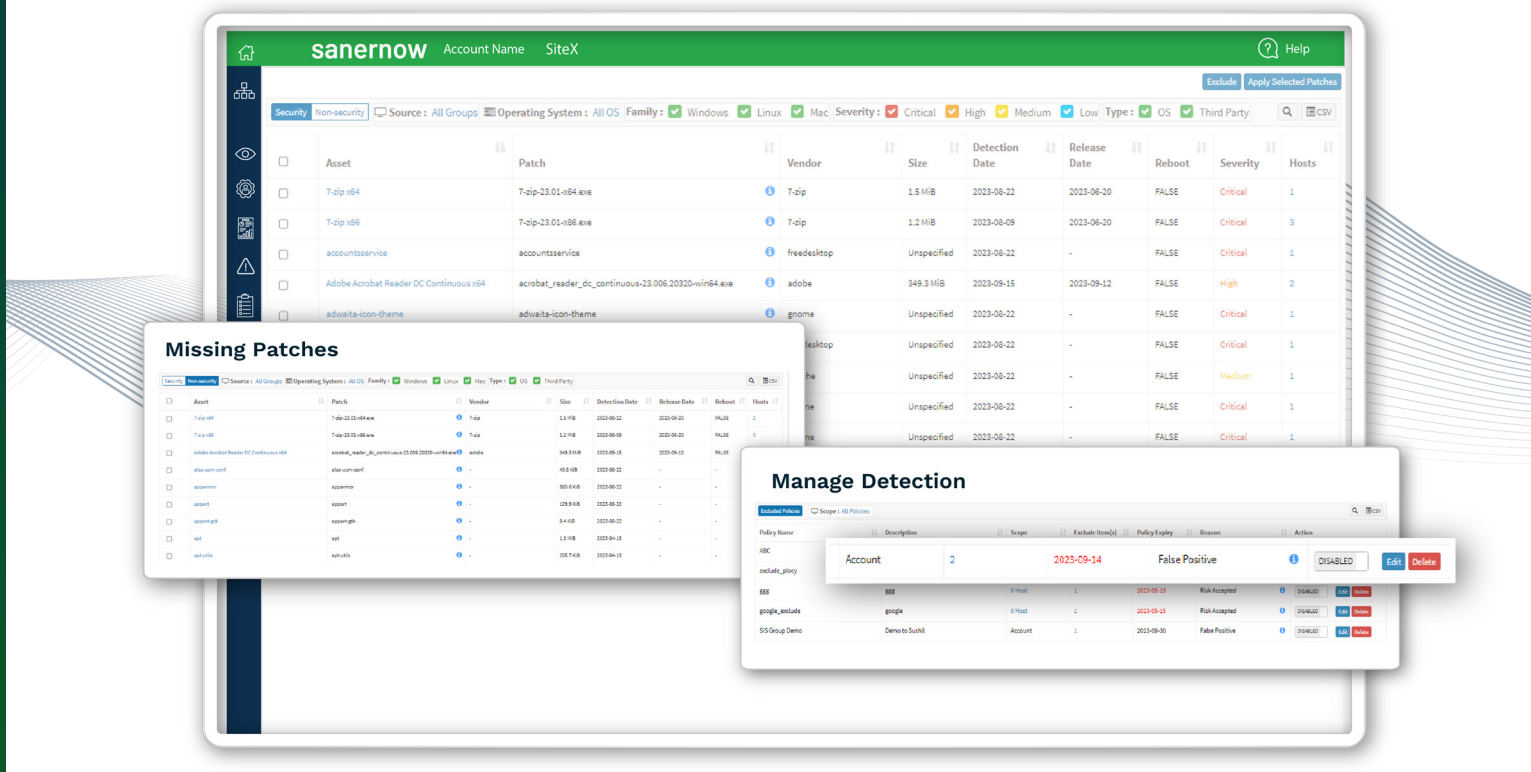


Figure 09- Integrated remediation of vulnerabilities from a single console, which can be sorted based on risk for efficient risk mitigation.

The Use Cases & Advantages of Continuous Vulnerability and Exposure Management

Continuous Vulnerability & Exposure management not only improves the capabilities of traditional vulnerability management but also brings in some key differentiators and added advantages. CVEM allows for an effective and simpler way to manage your attack surface.

Biggest Advantages of Continuous Vulnerability and Exposure Management:

• Demonstrate Continuous Compliance with Industry Guidelines

Often achieving compliance with industry guidelines falls under the responsibility of IT and Security teams, and it becomes difficult to do it along with vulnerability or exposure management effectively. With continuous vulnerability and exposure management aligned to fix misconfigurations and harden your systems, the task of achieving continuous compliance becomes easier.

• 95%+ Patch Compliance

Detecting missing patches and applying them themselves might be a Herculean task with traditional or exposure vulnerability management. But continuous vulnerability and exposure management allows you to achieve 95%+ patch compliance and become compliant with your organization's or industry's regulatory controls.

• Reduce Vulnerability Count by 90% in Three Weeks

Speed is the biggest differentiator in CVEM, & with all the steps of vulnerability or exposure management being streamlined, the entire process becomes significantly faster compared to its traditional counterpart. With that in mind, it is easy to estimate a reduction of 90% of the vulnerability count within the first three weeks of instating it.

• Continuous Asset Visibility

Another advantage of CVEM is continuous asset visibility. With continuous monitoring of the IT network, continuous vulnerability and exposure management ensures you always have visibility over any changes in your IT assets as well.

• Actions to Critical and Zero-day Vulnerability in Less than 48hr

Continuous Vulnerability and Exposure Management allows you to take actions quickly and effectively and quick response is a must to combat critical and zero-day vulnerability. With no room for error and not a lot of time to apply fixes, instantly taking the right actions can only be performed with CVEM's streamlined process.

• Establish Controlled, Known-good IT in a Month and Maintain It

Vulnerability and exposure management should be a continuous repetitive process, & establishing a controlled and monitored IT network with sporadic scanning of traditional vulnerability management is not easy. But with CVEM's continuous, automated, & streamlined process, maintaining a known good IT with minimal security risks is a reality.

Here are the Critical Use Cases of Continuous Vulnerability and Exposure Management:

• Monitor Your IT Assets in Real-time

With continuous & deep real-time visibility into your IT assets, you can monitor and track every hardware and software in your organization from a unified console. You can also detect and manage asset exposures and maintain your IT assets with ease.

- **Discover and Eliminate Anomalies, and Normalize IT**

With holistic visibility into your IT assets, it gets easier to eliminate posture anomalies and outliers that could potentially harm your organization. Further, it also reduces the potential points of attack in your organization and provides an additional layer of security to your organization.

- **Detect, Assess, and Prioritize Vulnerabilities and Exposures**

Continuous and automated scanning of vulnerabilities allows you to keep them in check and easily detect, assess, and prioritize vulnerabilities in one dashboard, further simplifying the entire process.

- **Harden System Configurations and Achieve Compliance**

Be it NIST, HIPAA, PCI, or more, continuous vulnerability and exposure management can effectively harden your organization's devices based on the regulations. As a result, you can achieve continuous compliance and align compliance with IT security goals.

- **Remediate Vulnerabilities and Mitigate Threats with Integrated Patching**

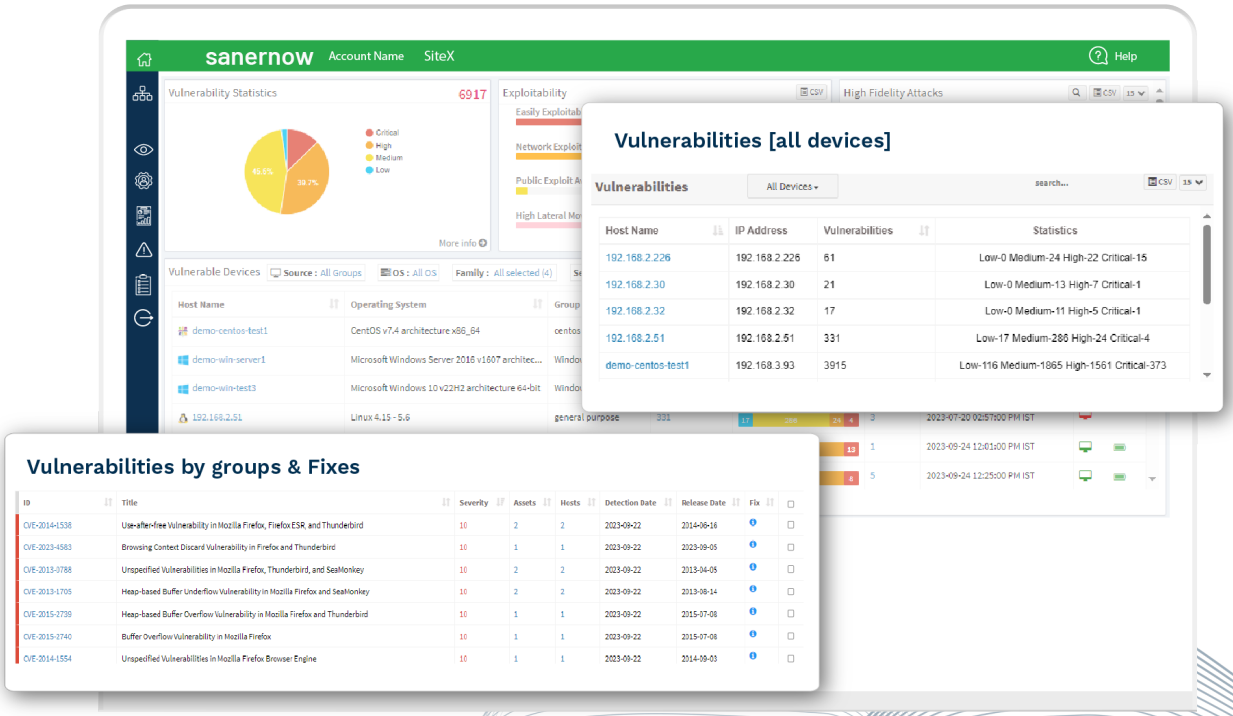
Reducing risk rapidly and efficiently is critical in ensuring your organization's attack surface is minimized. Further, with integrated patch management, the entire process of remediation speeds up as well.

- **Go Beyond Patching with Remediation Controls to Mitigate Security Risks**

While patches work for software vulnerabilities and exposures, other security risks need remediation controls like application blocking and quarantining, blacklisting, and more to mitigate the potential risk originating from it effectively.

Automate End-to-End Vulnerability Management

When the entire process of vulnerability management is performed in a streamlined way, ideally with a single tool, automating it becomes easy. Further, automation also allows for a more rigorous security posture and significantly reduces the chance of a cyber attacker breaching the network.

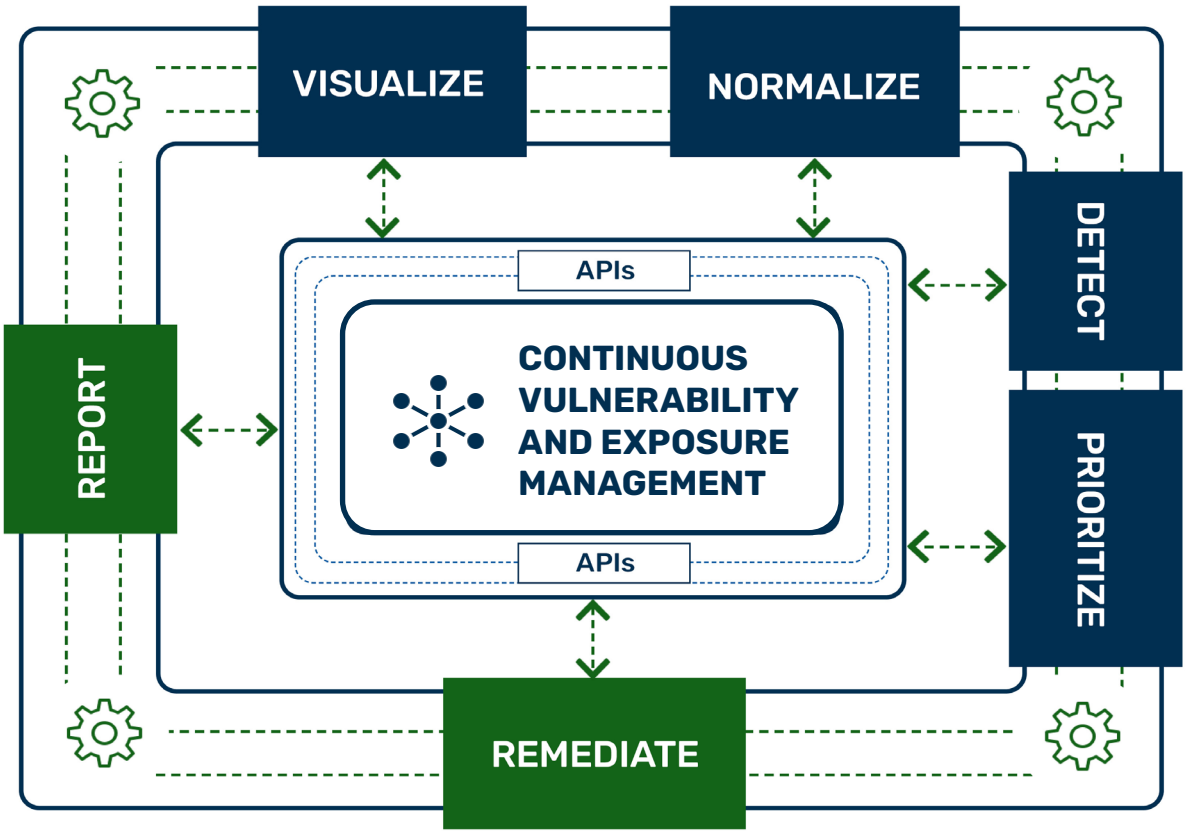


Building a Robust Security Risk & Compliance Posture with SanerNow CVEM

SecPod's SanerNow is an Continuous Vulnerability & Exposure Management platform that can scan quickly to learn about assets, vulnerabilities, posture anomalies, misconfigurations, and other security risks, apply fixes to mitigate them, and help automate that into a continuous routine.

SanerNow goes beyond traditional vulnerability and exposure management and provides an advanced solution by providing natively built, truly integrated tools on one platform to manage vulnerabilities and security risks.

Built upon the Continuous Vulnerability and Exposure Management architecture of Visualize, Normalize, Detect, Prioritize, Remediate, and Report, SanerNow is the single end-to-end continuous vulnerability and exposure management tool that can replace your vulnerability management stack entirely.



SanerNow helps you achieve continuous security risk and compliance posture by eliminating attack surfaces to keep the threat actors at bay and keep your organization's network safe by preventing cyberattacks.

WITH SANERNOW, YOU CAN:

01 Take control over your IT asset exposure

02 Quantify your organization's cyber hygiene and get a laser-focused view of your IT infrastructure

03 Get holistic visibility of your organization and discover and eliminate posture anomalies

04 Continuously and quickly scan and detect vulnerabilities for real-time protection with the world's largest vulnerability database with over 160000+ checks and the fastest 5 minutes scans.

05 Precisely assess risk exposures and prioritize vulnerabilities based on severity and risk for efficient remediation

06 Instantly remediate vulnerabilities with integrated patch management for better attack surface management

07 Enforce security controls beyond patching to strengthen and harden your network

08 Completely automate the vulnerability or exposure management process from start to finish

09 Generate smart and audit-ready reports with actionable insights

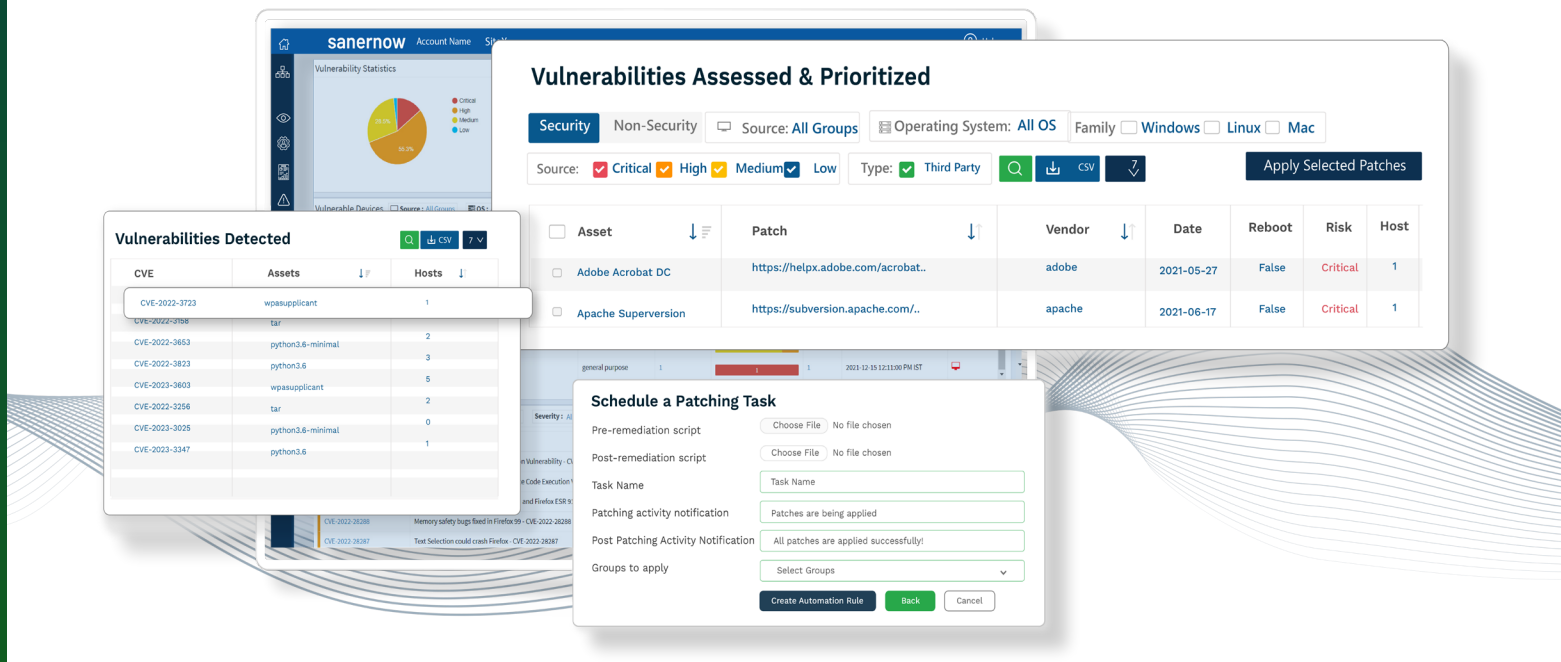
Closing Thoughts

Knowledge is power, and in the modern digitized world of computers, the statement is more relevant than ever. Every organization collects and stores data and confidential company assets and secrets. Everything we do on the internet leaves a digital footprint, and someone somewhere is ready to pay for this data or, worse, steal it. So, information becomes very valuable, and protecting the data becomes even more critical.

Every attack originates from a weakness, so by finding the source of a potential risk, you can prevent impending cyberattacks!

Beyond just vulnerabilities and exposures, system misconfigurations and deviations are weaknesses that can have a devastating effect on your organization if neglected. An advanced vulnerability managementcontinuous vulnerability and exposure management program helps ensure that your organization's assets are safe, sound, and secure in your absence.

Preventing cyber-attacks is more important, as a strong defense is better than a weak solution.



We are SecPod, and We Prevent Cyber-attacks.

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, & helps automate these routines. Our product philosophy is offering simplicity & automation to make the job of security administrators slightly better.

Contact Us

Email Us on:
info@secpod.com

www.secpod.com