Make Cyber Hygiene Your Topmost Priority

SANERNOW

Cyber Hygiene Orchestration and Automation Platform

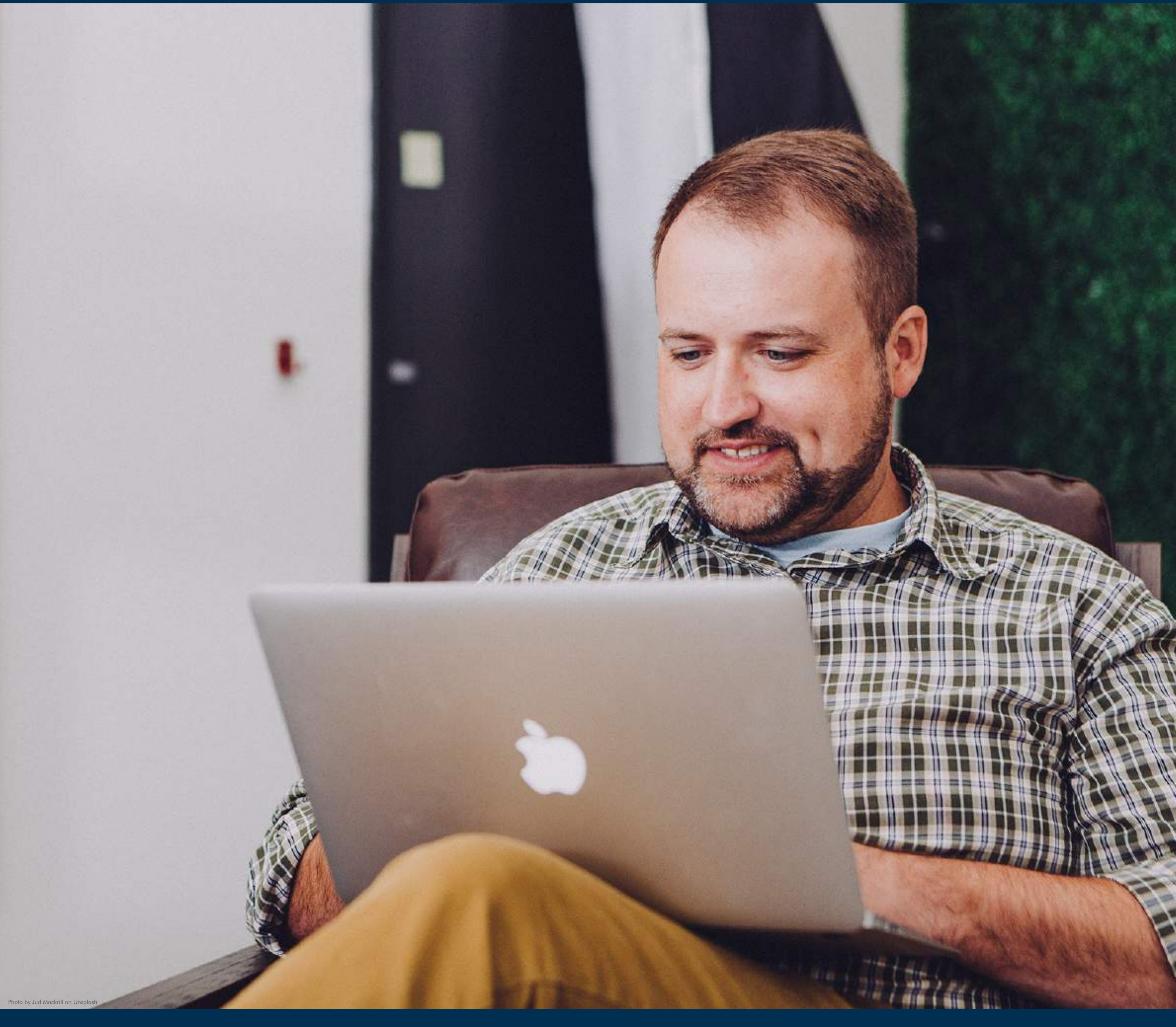


Photo by Jud Mackrill on Unsplash

Most cyber attacks target endpoints and create major headaches for enterprise IT security teams. While there are many available tools, there is little security. A cyber security platform that combines risk assessment with risk mitigation is a core requirement.

ALL ENDPOINTS ARE VULNERABLE. Endpoints & applications are the main target and biggest security headache for enterprises. The presence of vulnerabilities within an endpoint system (Operating System and applications) can be exploited by hackers to gain access to valuable data, manipulate transactions, and cause serious disruption to business operations.

90% of organisations allow employees to access data from personal devices, which are hard to monitor, and can have a variety of security risks.

18000 vulnerabilities were added to the NIST database in 2018. 30-40 are added every day, making security a painful moving target.

30-120 days are typically needed for organizations to fix vulnerabilities discovered during annual security audits.

INTRODUCING SANERNOW - CYBERHYGIENE ORCHESTRATION & AUTOMATION PLATFORM

SecPod's SanerNow platform provides the fastest, easiest and most affordable way to assess risks and detect threats in an enterprise. SanerNow provides continuous visibility into IT assets, performs a continuous vulnerability assessment, and helps remediate vulnerabilities through integrated patching. IT security teams can now reduce the cyber-attack surface and prevent attacks through SanerNow's cyber-hygiene automation platform.

SanerNow provides integrated risk assessment and risk mitigation. It provides a daily automated process for detecting and mitigating endpoint security issues. SanerNow performs daily scans to identify vulnerabilities and misconfigurations across **your endpoints in less than 5 minutes.** With integrated patch management, SanerNow helps ensure your devices are fully protected from malware and ransomware exploits.

- ☑ Discover vulnerabilities and missing patches automatically and deploy patches at scale across all assets located on-premise, in the cloud, and at remote locations.
- ☑ SanerNow provides tools to unify security operations from assessment to mitigation, detection to response, all on a single platform, eliminating the need for multiple point solutions.
- ☑ With over 100,000 vulnerability checks and 400-500 config checks per OS, SecPod provides the world's largest SCAP library for discovering and patching vulnerabilities.

> *"SecPod's SanerNow platform helps our customers get and stay compliant with many of today's standard frameworks. By monitoring for vulnerabilities, compliance misconfigurations and threat indicators, it allows us to focus on our customers' most critical risks. The included instructions help take the guesswork out of how to keep an organization secure."*
>
> ***- John Riley, COO, SACTECH***

SANERNOW BENEFITS

- **Achieve security effectiveness** by automating risk assessment and mitigation activities. Reduce the attack surface and prevent attacks. Gain visibility into your IT assets through a single pane of glass and continuously monitor to avoid attacks.

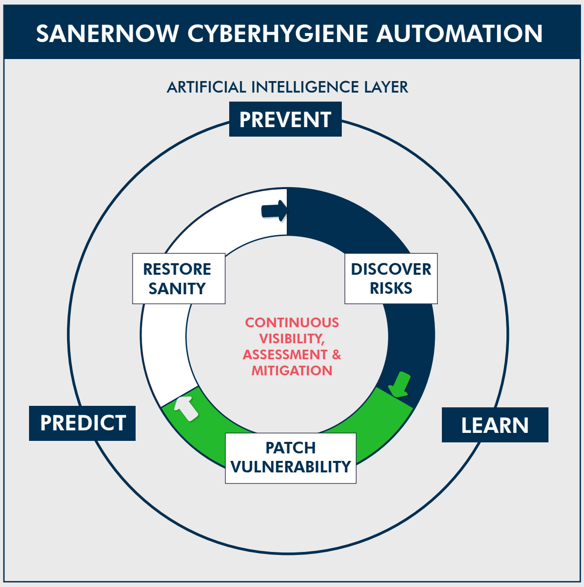
- **Reduce complexity** by eliminating the need to work with multiple point products. SanerNow provides multiple tools in a single, easy to deploy console.

- **Boost productivity** by automating routine checks and tasks. SanerNow is light on system and network resources and ensures security is not impacting productivity.

- **Reduce operating costs** by investing in one platform to address multiple cyber security use cases and remove vendor onboarding and management complexities.

GOING BEYOND THE TRADITIONAL WAY OF PATCHING VULNERABILITIES

New vulnerabilities are being identified at an alarming rate. 40-50 new vulnerabilities are added to the vulnerability database each day. Every day we hear about multiple high-profile attacks exploiting weaknesses.


SANERNOW CYBERHYGIENE AUTOMATION
ARTIFICIAL INTELLIGENCE LAYER
PREVENT
RESTORE SANITY
DISCOVER RISKS
CONTINUOUS VISIBILITY, ASSESSMENT & MITIGATION
PREDICT
LEARN
PATCH VULNERABILITY

SecPod is the first to come up with this framework. The SanerNow platform is built on the core principles of cyberhygiene management and uses a library of more than 100,000 security protocols to automate continuous vulnerability assessment and patch management for enterprises.

93% of cyber attacks across industries can be prevented with proper cyberhygiene.

SANERNOW FEATURES

- **Detect and mitigate vulnerabilities** within seconds with SanerNow's agent-based architecture. With over 100,000 vulnerability checks and 400-500 config checks per OS, SanerNow provides the world's largest library for discovering and patching endpoint vulnerabilities.

- **Perform daily automated vulnerability scanning** to identify risks and prioritize remediation before attackers exploit vulnerabilities.

- **Understand and mitigate risks and potential threats** before they are exploited. Stay current with daily updates on vulnerability and threat intelligence.

- **Automate patch management** with a centralized approach covering heterogeneous operating systems and third-party applications. Fix misconfigurations and firmware issues to achieve desired patch compliance across all IT assets.

- **Easily deploy agents** across Windows, Linux, and Mac endpoints. SanerNow's agent-based architecture is resource efficient and scalable.

- **Continually monitor** the security posture of endpoints. Automatically create and distribute reports and notifications to stay current on risk and compliance across the enterprise.

LIST OF FEATURES

Risk Assessment

- Achieve continuous visibility into IT assets.
- Perform daily, automated scans for vulnerabilities.
- Detect policy violations across operating systems and applications.
- Identify rogue, blacklisted and end-of-life applications.
- Detect software mis-configurations and default configuration errors.
- Detect end-of life or end-of-support applications.
- Update outdated firmware/drivers.
- Identify unwanted services, processes and network listeners.
- Detect suspicious registry entries, anonymous or guest users, anonymous shares, weak encryption ciphers and 100s of other potential threats.

Risk Mitigation

- Patch operating systems covering Windows, Linux and Mac OS X environments.
- Patch 100s of third-party applications.
- Update outdated firmware/drivers.
- Prioritize patching with severity indicators and patch to address specific vulnerability.
- Automate patching to a daily routine with rules.
- Patch production servers through workflows.
- Rollback failed patches.
- Use an array of controls to reboot and execute additional tasks.
- Remove unwanted and rogue applications.
- White-list or black-list applications and devices.
- Clean-up registry keys and values.
- Control services, processes and daemons.
- Execute scripts and run tools.

SANERNOW CYBERHYGIENE ORCHESTRATION & AUTOMATION PLATFORM

Your platform for endpoint security and management - a platform that hosts tools to cover endpoint security and management requirements.

One Platform, Endless Possibilities

Query, Analyze, Detect, Prevent, Respond, Automate

- Vulnerability Management
- Patch Management
- Asset Management
- Compliance Management
- Endpoint Management
- Threat Detection and Response

REQUEST A DEMO

Detailed platform documentation: https://www.sanernow.com/documentation/

ABOUT SECPOD

SecPod is leading provider of endpoint security and management solutions. SecPod (Security Podium, incarnated as SecPod) has created revolutionary SanerNow platform and tools that are used by MSPs and enterprises worldwide. SecPod also licenses security technology to top security vendors through its SCAP Content Professional Feed.

secpod

USA OFFICE

303 Twin Dolphin Drive,
6th Floor Redwood City,
California, 94065

INDIA OFFICE

1354, 9th Cross, 33rd Main,
JP Nagar I Phase, Bangalore,
KA, India - 560078

For enquiries, contact us at:
Email: info@secpod.com | **Tech Support:** support@secpod.com
Phone: (+1) 918 625 3023 (US) | (+91) 80 4121 4020 (IN)

www.secpod.com