SanerNow

Your platform for managing and securing endpoints

Many Products, No Security

So many products: Organizations invest in multiple products, many with overlapping capabilities. And investments are huge when considering the cost of products, maintenance, professional services, training and vendor management.

Yet so little security: Ransomware and other malware exploits are always in the news. Attackers exploit endpoints after penetrating perimeter and anti-virus protection. Unpatched endpoints are insecure and easily compromised. Current results illustrate a fundamental shortcoming in how security is being approached.

A platform-centric approach with applicable, effective tools is needed to transform endpoint management and security.

Bring saneness to your endpoint security and systems management with SanerNow, a cloud-delivered solution.

SanerNow…

Your Platform for Managing and Securing Systems

SanerNow's "platform with an agent and apps" model addresses a sweeping range of endpoint security and management challenges. It offers many apps, each addressing a specific security scenario.

- VULNERABILITY MANAGEMENT
- PATCH MANAGEMENT
- COMPLIANCE MANAGEMENT
- ASSET MANAGEMENT
- ENDPOINT MANAGEMENT
- THREAT DETECTION & RESPONSE

One platform, multiple use cases: Simplify IT security and management. Reduce costs.

WHY SanerNow?

BENEFITS

- ☑ Single platform, multiple use cases
- ☑ Simplify endpoint security and systems management
- ☑ Reduce up to 60% of IT product investment
- ☑ Deploy in minutes for immediate results

FEATURES

- ☑ Continuous monitoring
- ☑ Self-healing
- ☑ Scans in less than 5 minutes across thousands of endpoints
- ☑ Seamless scalability — scale agents up or down as needed
- ☑ Architected for multi-tenancy, role-based access
- ☑ Agents support Microsoft Windows, Linux and Mac OS X
- ☑ High-performance, search results in less than a second

How does SanerNow Work?

SanerNow Queries and Monitors Endpoints, Analyzes the Security Posture, and Responds to Bring Endpoints to an Approved State

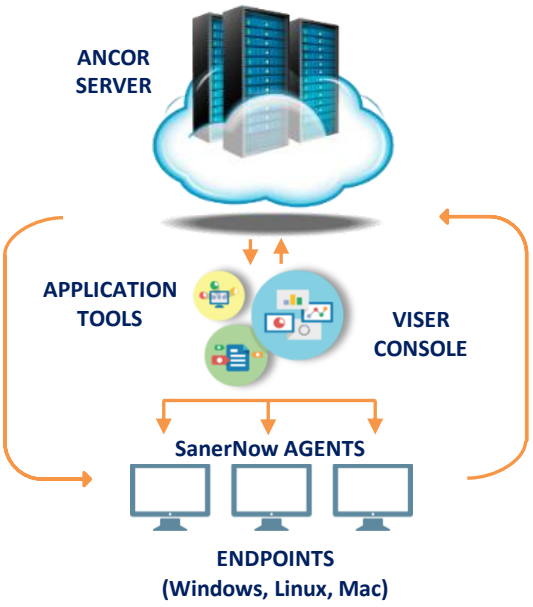
SanerNow's platform-centric approach is designed on the same principles as that of an operating system. The core ('kernel') performs the analytical computations required to detect aberrations and deviations. The 'shell' provides the ability to query, monitor and make changes. The 'user/application layer' helps transform these computations to support various use cases.

SanerNow is built with these four primary concepts:

- Query the system to get visibility
- Monitor for changes and aberrations as they occur
- Analyze the system for risks and threats
- Respond to fix the issues

SanerNow Deployment

A Single Platform for Comprehensive Endpoint Security and Systems Management



Ancor Server

The ANCOR (Analytics and Correlation) server houses vulnerability and threat intelligence, information collected from endpoints, and correlates the two to identify issues, risks and threats. The Ancor server also helps manage endpoint devices.

Viser Management Console

A web-based management console helps you monitor and manage endpoints.

SanerNow Agent

A light-weight agent is installed on all endpoints (Microsoft Windows, Linux and Mac OS X), it scans endpoints, and interacts with servers to accomplish tasks.

SanerNow Use Cases

Empower Yourself to Take Proactive Action to Protect Against Threats

Vulnerability Management

- ☑ Get continuous risk assessment without impacting system or network resources
- ☑ Gain insight into the security posture and align the enterprise with the security policies of the organization
- ☑ Automatically remediate risks

Patch Management

- ☑ Identify and roll out patches automatically
- ☑ Keep all major operating systems (Windows, Linux and Mac OS X) as well as third-party applications up-to-date
- ☑ Detect and fix configuration deviations, such as password polices and encryption strength

Compliance Management

- ☑ Achieve compliance to regulatory standards
  - PCI, HIPAA, NIST 800-171, NIST 800-53
  - Custom configuration standards
- ☑ Fix compliance deviations automatically to ensure that your organization is continuously compliant

Asset Management

- ☑ Track software and hardware assets
- ☑ Track new installations and changes to configuration settings
- ☑ Manage and optimize software licenses and costs
- ☑ Blacklist rogue applications that show up in the inventory

Endpoint Management

- ☑ Get visibility into the status of endpoint systems, with 100s of built-in checks
- ☑ Gather network details and map of devices
- ☑ Search for the presence of sensitive data, such as credit card information, social security numbers, etc.
- ☑ Deploy software, block applications and devices

Threat Detection & Response

- ☑ Detect Indicators of Attack (IoA) and Indicators of Compromise (IoC)
- ☑ Run queries to check for abnormal behavior or unusual network activity that is symptomatic of an attack
- ☑ Stop on-going attacks by blocking applications, killing processes, cleaning up startup folders

Request a demo: **info@secpod.com**

ABOUT SecPod

SecPod is an endpoint security and systems management technology company. Founded in 2008 and headquartered in Bangalore with operations in USA, SecPod creates cutting edge products to manage and secure endpoints.

Contact Us
Enquiry: info@secpod.com
Technical Support: support@secpod.com
Phone: +91 080 4121 4020

USA
303 Twin Dolphin Drive, 6th Floor
Redwood City, California, 94065
United States of America
Phone: +1 918 625 3023

INDIA
1354, 9th Cross, 33rd Main
JP Nagar, I Phase
Bangalore - 560078
Karnataka, India
Phone: +91 080 4121 4020