# Many Products, No Security

A WHITEPAPER

on

A Cost Effective, Single Platform Approach to Security and Endpoint Management

secpod

# Introduction

"We have many products, but very little security." This is a typical complaint when securing and managing an IT environment. Organizations invest in many products with overbearing features and overlapping functionality. Yet, environments are still difficult to manage. And they are still subject to attacks and exploitation.

The footprint of most products expands with new releases and functionality. This leads to a bloated feature set, which increases complexity and training requirements. In addition, a whole cottage industry has been created to provide user certifications to assert that a person is qualified to use a product.

Relying on more and more vendors increases the burden of procurement, installation and training. At the same time costs are unreasonably increased. Yet security and system management issues remain.

Compared to a decade ago, building a computing infrastructure is now a speedy activity, thanks to virtualization and cloud technology. But IT management and security products haven't kept pace. We can quickly provision a computing infrastructure but struggle to secure it.

Just as a computing infrastructure can be provisioned, a similar approach is needed for IT management and security. A platform of tools, rather than many point products, would more effectively handle tasks. With task specific tools it would no longer be necessary to absorb the cost of product features that aren't applicable or useful. Installation and training burden would nearly be eliminated. And with proper tools, security and system management concerns would be resolved.

SecPod has built its SanerNow platform and toolset with these fundamental benefits:

- Tools for security and system management tasks
- Self-provision tools from the cloud
- Pay only for actual use of tools
- Eliminate risk, try out tools to ensure they meet requirements
- Keep things simple, no training classes or certifications required

This white paper discusses challenges with managing and securing infrastructures. Using a platform of tools for specific tasks addresses many of the limitations.

# Challenges

## Problem #1: So Many Products

Organizations invest in multiple products, train employees, and manage activities, yet don't achieve security goals. IT environments and endpoints are still vulnerable to attacks and exploits.

Despite the availability of different point solutions, many questions remain.

- Why do vulnerabilities still exist when we have had vulnerability scanners for decades?
- Why do attacks almost always use an unpatched vulnerability in systems?
- Why isn't patching a top priority? Why do people believe patching is hard? Why do people ignore or take several months to roll out a patch?
- Investments in vulnerability management, patch management, compliance management, GRC solutions, endpoint management, EDR, asset management, and RMM are huge, but why is there so little value?
- Why are there so many endpoint agents?
- Why aren't tools and processes simple and intuitive? Why does it take weeks to deploy products, buy professional support, and pass certifications, only to get stuck in a workflow/ticketing rut?

Many products have complicated and feature-rich functionality, but only address a single security challenge. For each use case, a new product with overbearing capabilities is created. Though meant to simplify life and to secure the environment, the embedded complexity in many tools leads to their limited usefulness.

## Problem #2: Containing Cost

Whether using a CapEx or OpEx model, purchasing multiple products with overlapping capabilities creates excessive cost. Generally, organizations are paying for unused functionality and CIOs/CISOs deal with many vendors, absorbing much of their time.

Typically, organizations invest in:

- Products
- Professional Services
- Maintenance and upgrades
- Training and certification
- Vendor and contract management

Multiple vendors and multiple products contribute to unreasonable upfront and on-going costs.

## Problem #3: Ineffective IT Management and Security

Today, some of the most critical IT issues deal with compromised endpoints. Ransomware and other malware attacks are continually in news headlines. Attackers are able to easily bypass perimeter protection systems and create major damage in just a few minutes. The frequency of these security breaches and exploits illustrate a fundamental shortcoming in how security is being approached. The following points highlight the issue.

- 60% of malware is undetected, demonstrating the ineffectiveness of anti-malware solutions.
- 90% of successful attacks occur because of vulnerabilities and misconfigurations.
- Nearly all endpoints have critical vulnerabilities (frequently in the 100's) due to not having appropriate patches applied.
- Endpoint configurations don't adhere to organizational guidelines and many businesses struggle to meet regulatory requirements.
- There is a general lack of visibility into and control of endpoints.

All too often, an organization doesn't have a clear view of their security posture and risk of being exploited.

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

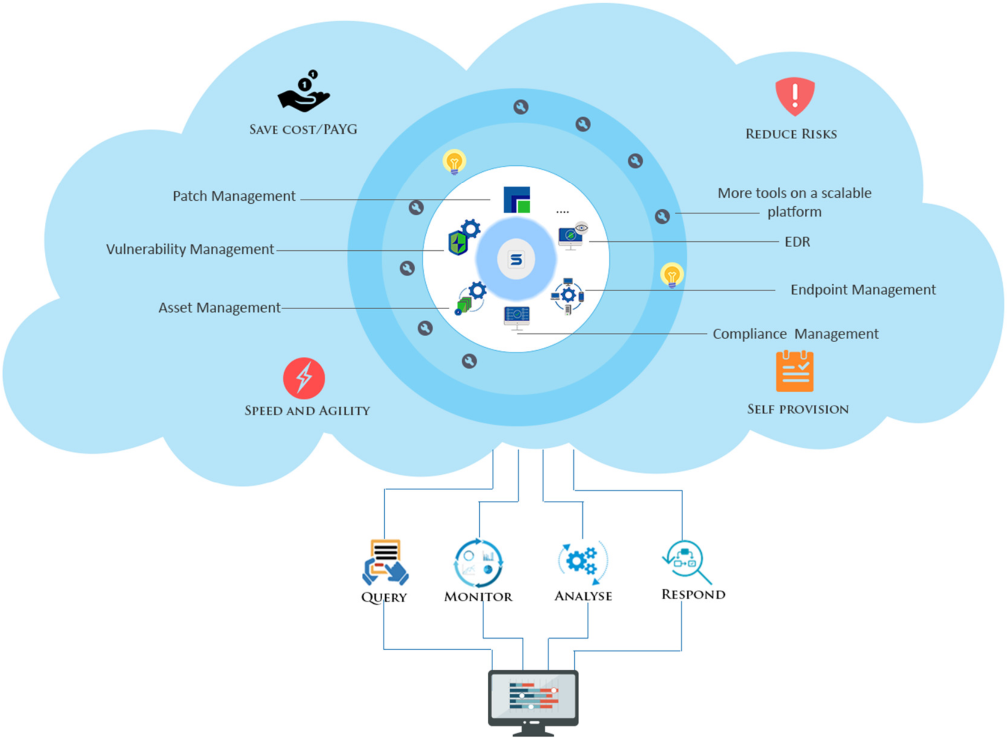
## SanerNow: A Platform for Managing & Securing Endpoints

SanerNow is a platform for endpoint security and management — a platform that hosts numerous tools to cover various endpoint security and management requirements. SanerNow queries your systems to find aberrations, and helps your systems retain normality.

SanerNow is provided as Software as a Service (SaaS). With no capital expenditure, a pay-as-you-go model allows payment for only services used, based on the number of endpoints being serviced. Having tools to address multiple use cases within one platform helps reduce up to 60% of the investment in endpoint security and management.

The following concepts are embodied within the SanerNow platform and tools.

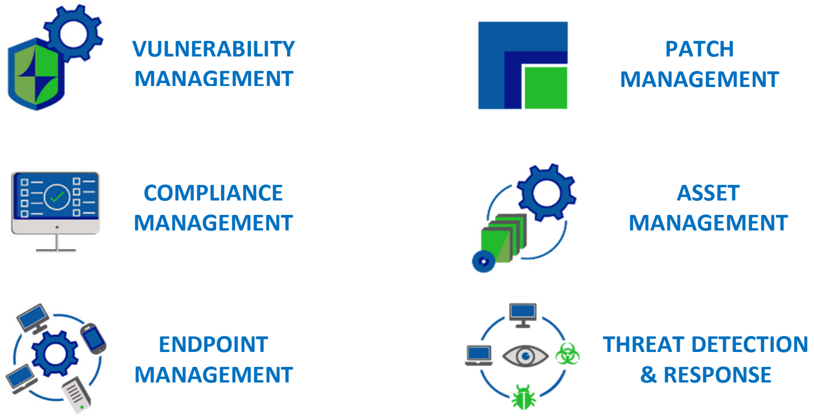
- Self-provision tools from the cloud, as needed, for specific use cases
- Pay for actual usage and avoid lengthy product procurement process
- Eliminate risk, try out tools to ensure they meet requirements
- Be usable, without the need for training or massive product documentation
- Effectively address endpoint security and management tasks



## SanerNow: Business Cases

SanerNow addresses the following business cases:

- Vulnerability Management – Continuously assess risks, automated to a daily routine.
- Patch Management – Apply operating system and third-party application patches for Windows, Linux and Mac OS X.
- Compliance Management – Comply with regulatory standards benchmarks and achieve continuous compliance (PCI, HIPAA, NIST 800-53, NIST 800-171).
- Asset Management – Discover and manage assets.
- Endpoint Management – Manage endpoints and ensure their well-being.
- Endpoint Threat Detection and Response – Detect and Respond to Indicators of Attack (IoA) and Indicators of Compromise (IoC).



SanerNow is continuously updated to add new use cases. Currently in the labs are:

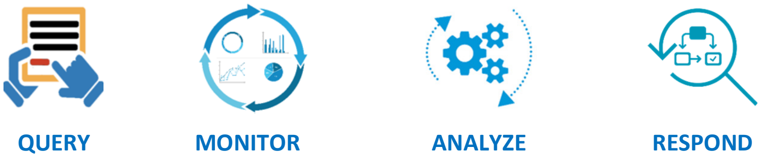
- File Integrity Monitoring
- Remote Desktop Sharing
- Data Discovery, Data Classification, Data Loss Prevention, Device Encryption
- Mobile Device Security

# SanerNow: Query, Monitor, Analyze, Respond

Typically, system management requires the functionality of 'querying, monitoring, analyzing and responding,' whether the system is simple or has multiple components that interact with each other.

SanerNow is fundamentally built with these 4 capabilities,

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



# SanerNow Platform: Ancor

Ancor is a scalable analytics and correlation engine. It works with the SanerNow agent that resides on endpoint devices to collect and transmit data to the Ancor server. Ancor correlates the data from agents on endpoint devices with compliance standards and best practices, and vulnerability and threat intelligence to provide real-time endpoint management and protection capabilities.

Key platform features include:

- **Continuous monitoring:** System controls
- **"Principle of Self-Healing"**
  - Detect and fix vulnerabilities
  - Identify unwanted/unused assets and uninstall them
  - Monitor the anti-virus program status, and start it if it is not running
  - Detect IoC/IoAs and respond to the threats
- **Speed:** Deploy SanerNow in minutes, scan 1000s of endpoints in less than 5 minutes
- **Scalability**
- **Multi-tenancy, multi-user and role-based access**
- **High-performance:** Retrieve search results in less than a second
- Agents: Support for **Windows, Linux and Mac OS X**

# Benefits

## Effective IT management and security

SanerNow is a platform with a variety of tools for managing and securing endpoints. It addresses security issues, whether it is fixing vulnerabilities, achieving configuration compliance, or killing a threat chain, etc. This is in contrast to the many products that merely report.

## Reduced cost and reduced risk

SanerNow is offered as SaaS (Software as a Service). With no capital expenditure, the pay-as-you-go model allows payment for only tools that are being used. And since SanerNow tools are self-provisioned, they can be evaluated to ensure they meet specific use cases. This avoids the risk of investing in products that may not satisfy requirements or work properly. Using tools from one platform rather than multiple products can also reduce overall endpoint management and security costs by up to 60%.

## Ease of use; peace of mind

SanerNow is built for quick deployment and ease of use. Once agents are deployed, most value is realized in less than 5 minutes, irrespective of the number of deployed endpoints. Extensive training is not required to use SanerNow and its tools for managing and securing endpoints.

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. © 2018 SecPod is a registered trademark of SecPod Technologies Pvt. Ltd.

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

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