secpod

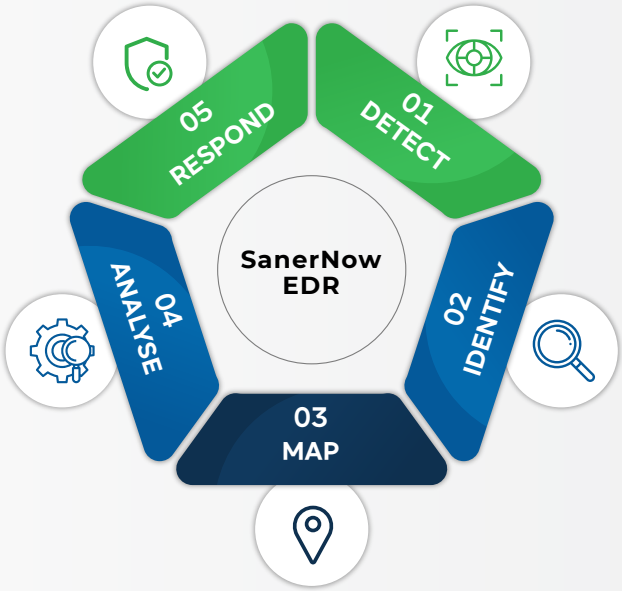
SANERNOW

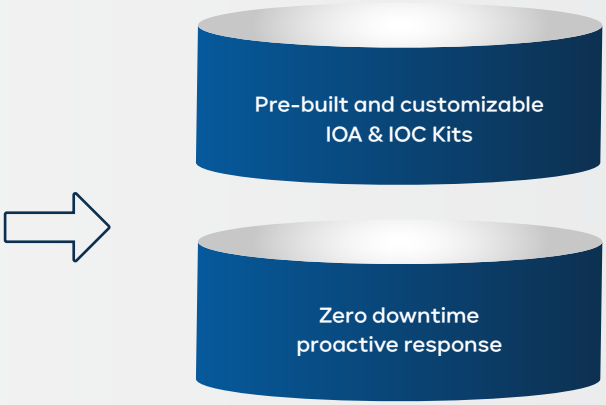
ENDPOINT DETECTION & RESPONSE

Part of Industry's First Integrated and Automated SanerNow Cyberhygiene Platform

www.secpod.com

Detect and eliminate threats instantly. Seal-off attacks at the door.





As of 2020, cyber-attacks have reached a high level of sophistication. It takes, on average, 280 days to identify and contain a data breach. This kind of a lag in resolution time can give a threat actor ample time for lateral movement through the network. For instance, a ransomware attack can cost businesses, on average, approximately $713,000 per incident.

Continuous scrutiny is critical to ensure timely detection and prevention of cyber threats. However, the ever-increasing number of nodes and endpoints that need to be monitored can result in increased threat exposure and several false positives, with resulting issues and gaps in accurately detecting the upstream and downstream impact of potential threats.

Nipping a threat in the bud requires a proactive strategy to identify and eliminate threats. A strong security posture requires the ability to rapidly respond to attacks with minimal delays to protect your business.

SecPod SanerNow Endpoint Detection & Response (EDR)

SanerNow Endpoint Detection and Response protects your business by providing a suite of integrated tools to prevent cyber-attacks and strengthen your security posture. Provided both on-cloud and on-premise as an integrated console, with smart, multi-functional agents, it helps detect, identify, and map indicators of attacks (IoA) and indicators of compromise (IoC) and helps predict and prevent attack events.

Any deviations from expected settings or configurations are checked and flagged by the smart agents for evidence of attack or compromise, triggering alerts through the console with proactive and preventive remediation measures, where necessary.

The pre-built IoA and IoC kits from SanerNow detect and isolate systems with indications of attack or compromise, and also allow you to define additional checks based on available settings.

SanerNow EDR also offers rapid and effective execution of the response plan to isolate any compromised endpoints, preventing the spread of an attack. SanerNow EDR is integrated with SanerNow Cyberhygiene Platform TM that includes vulnerability management as well as other risk assessment and remediation tools to reduce your organization's threat exposure across your heterogeneous OS endpoints (extends supports to OS types like Windows, MAC and Linux).

Actively thwart cyber-attacks with SanerNow Endpoint Detection and Response

Improve security and resilience with real-time and on-demand threat hunting

Detect, identify and take down threat vectors swiftly with SanerNow's real-time and on-demand threat hunting.

Trigger speedy and zero-downtime responses to threats

Close the gap between threat detection and response. Respond instantly to incidents of breach or compromise to prevent and contain the spread of attacks and secure your business.

Discover imminent threats with ongoing system behavior tracking

Monitor deviations in your endpoint behaviour, including settings or configurations to detect and respond to attack indicators in real-time.

Gain seamless visibility and control to secure your globally distributed endpoints

Get a single-pane-of-glass view across your endpoints mapping all potential threats and historic responses with SanerNow's centralized cloud-based console.

Rapidly detect, analyze, and respond to cyber-attacks in real-time

Indicators of attacks (IOA) for immediate detection of an attack

Set indicators of attack using our pre-made and customizable IOA kits. SanerNow constantly scans for these indicators in your networks and instantly raises a red flag whenever the attack conditions are triggered.

Indicators of compromise (IOC) for quickly isolating affected devices

Apart from identifying new or impending threats or attacks, SanerNow also detects devices that have been compromised by ransomware like WannaCry, CryptoLocker, Fantom, EternalRocks Worm, BadRabbit, etc. Rapidly scan and isolate any affected endpoints to prevent attacks from spreading.

Additional control with customizable checks

Go beyond pre-defined checks for threat detection to include additional detection events to gain better control based on your internally designed incident response plans.

Zero-day response to threats with comprehensive coverage

Use SanerNow to instantly trigger incident responses to secure your network. Proactively mitigate threats and evade attacks by sealing off security gaps.

Auditable, detailed incident summaries of all detection and response activities

View detailed information of all detections and responses performed by SanerNow – when indicators were triggered, affected devices, risk level, response status, etc. to get an overview of all your incident detection and response activities.

Extensive reporting and audit logs

Get auto-generated reports based on detection and response metrics like detected attacks, monitored devices, threat responses, and more. A detailed audit log keeps a record of all admin actions performed in a network, allowing you to track data related to users and actions on the SanerNow console.

About **SecPod**

SecPod is an endpoint management, security, risk, and compliance technology company. SecPod (Security Podium, incarnated as SecPod) has created the 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.

The SanerNow **Platform**

SecPod SanerNow is a cyberhygiene platform that automates and orchestrates measures to safeguard your enterprise devices from cyber attacks. The major applications of SanerNow includes:

- Patch Management,
- Vulnerability Management,
- Asset Management,
- Endpoint Management,
- Compliance Management

Talk to **Sales**

For enquiries on pricing

Email us on: info@secpod.com
Call us at: India - (+91) 80 4121 4020 / USA - (+1) 918 625 3023