SECHARD

Cyber Hygiene Platform

One Platform. Total Resilience.

Automate cyber hygiene, eliminate blind spots, and secure your entire infrastructure with the SecHard platform.

Cyber Hygiene is Not Optional. It's Your Foundation.

5x Organizations without basic hygiene controls are five times more likely to suffer a data breach.(1)

82% Of data breaches are caused by preventable issues like system misconfigurations or human error.(2)

98% Of all cyber-attacks can be stopped with the consistent application of basic security hygiene.(5)

60% Of enterprises still lack real-time visibility into their digital assets, leaving them exposed.(3)

Common Security Challenges

Visibility Gaps

Inability to see across all IT, OT, and cloud environments.

Privilege Misuse

Limited control and visibility over who accesses critical systems.

Manual Processes

Security tasks are manual, slow, and prone to human error.

Weak Hardening

Security policies are inconsistent and difficult to enforce everywhere.

Fragmented Reporting

Vulnerability data is siloed across different tools and systems.

Default Windows Server configuration has only 21% CIS Benchmark compliance.

sales@sechard.com

www.sechard.com

The Solution: SecHard Cyber Hygiene Platform

Cybersecurity Asset Management

Automatically discover, inventory, and monitor every device and piece of software. Eliminate blind spots completely.

Continuous Hygiene Monitoring

Track compliance, configuration changes, and overall hygiene posture in a single, real-time dashboard for immediate insights.

Security Hardening

Automate the enforcement of security benchmarks like CIS and STIG. Turn policy into action and ensure consistent configuration across all systems.

SECHARD
Cyber Hygiene Platform

Risk Scoring

Quantify your cyber hygiene posture by scoring risks across the enterprise (Risk = Impact × Likelihood). Transform raw data into clear, actionable security metrics.

Privileged Access Control (PAM/TACACS+)

Centralize and secure access to network infrastructure with full session recording, audit-ready logs, and granular visibility.

Vulnerability Center

Continuously assess, enrich, and prioritize vulnerabilities from built-in and third-party scanners to proactively shrink your attack surface.

CIS Community Defense Model v2.0

CIS Safeguards vs MITRE ATT&CK

Figure 1: CDM v2.0 attack pattern analysis

Top 5 Attacks	CIS Safeguards can defend against XX% of ATT&CK (Sub-)Techniques
Malware	94%
Ransomware	92%
Web Application Hacking	98%
Insider Privilege and Misuse	90%
Targeted Intrusions	95%

All percentages are based on ATT&CK (sub-)techniques assigned to an ATT&CK mitigation.

Supported Products

More than 250+ products

Windows Server · Windows 10 · Windows 11 · macOS · kubernetes · ORACLE Linux · APACHE HTTP SERVER PROJECT · ORACLE DATABASE · Exchange · Office · aws · CHECK POINT · paloalto NETWORKS · cisco · HUAWEI · DELL · hp

5 Stars | 100% Recommend

Gartner Peer Insights™

SecHard In-App Protection

Sources: (1) Gartner, Security Operations Trends, 2022, (2) Ponemon Institute, Cost of a Data Breach Report, 2023, (3) IBM, SOAR and Automation Impact Study, 2023, (5) Microsoft Security Insider, 2023