SECHARD

Automated Security Hardening & Remediation

Automated, standardized hardening that elevates CIS benchmarks from **21% to 95%+**, quadruples cyber resilience, and automates compliance across servers, networks, cloud, and 200+ assets.

Challenges

Insecure Configurations

According to Center for Internet Security (CIS), the default Windows Server Benchmark scores stand at a mere 21%.

Ever-Evolving Threat Landscape

To maintain a proactive stance against emerging threats, the cybersecurity team must continuously assess and configure critical systems.

Complexity and Talent Shortage

According to CIS, in a medium-sized organization, approximately 1 million security hardening checks need to be performed. It's a complex, error-prone, time-intensive process requiring expertise when done manually.

Regulatory Compliance Adherence

Numerous regulations mandate the implementation of security hardening measures in systems. The ongoing execution of these checks is a time-intensive endeavor.



Solutions

Automated Security Hardening & Remediation

Effortlessly elevating and automating security hardening scores from 21% to an impressive 95% or more, it simultaneously boosts cyber resilience fourfold.

Continuous Monitoring and Risk Scoring

Maintaining continuous surveillance on system configurations and implementing security hardening policies in accordance with the determined security baseline by performing asset risk scoring.

Flawless Security Hardening Process

The automated security hardening process is standardized based on global authorities, quality control tests have been performed many times, it is consistent and free from human error.

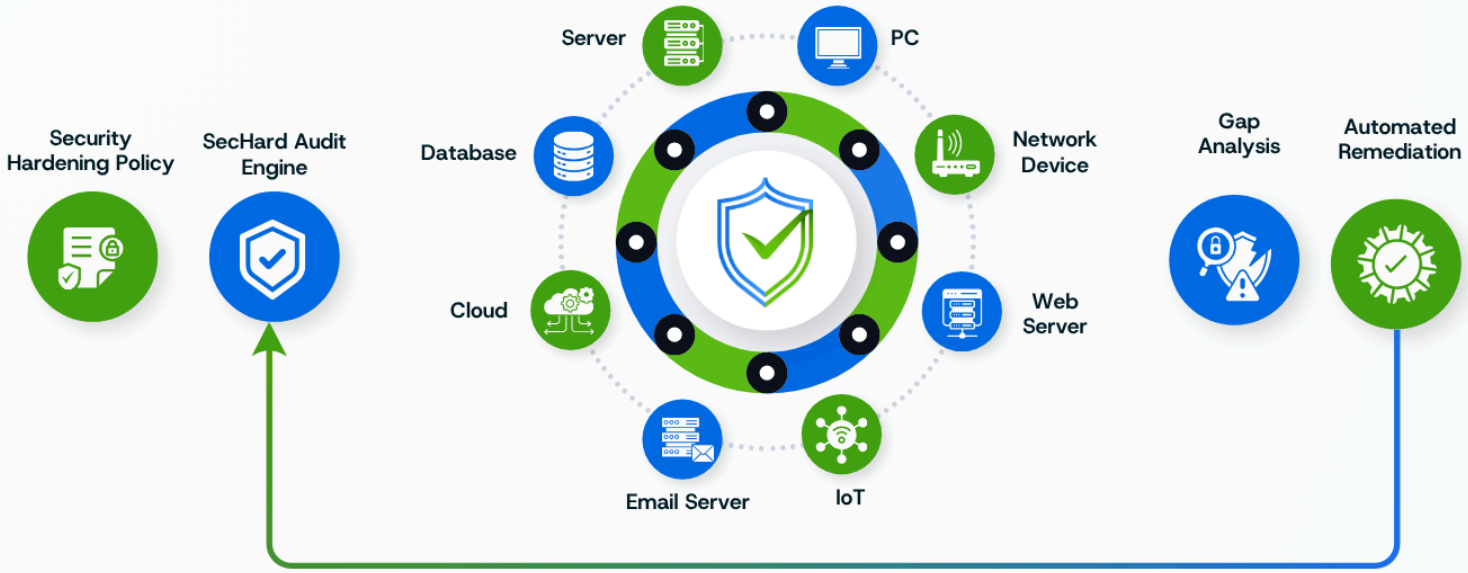
SecHard Compliance Suite

Supporting a wide array of regulations, including NIST CSF, CIS, CMMC, DISA-STIG, ISO 27001, SOX, GDPR, Turkish DTO, and KSA ECC. Creating gap reports and automated enforcement measures to achieve regulatory compliance.

sales@sechard.com

www.sechard.com

SECHARD



- CIS Certified
- DISA-STIG
- CBDDO (The Presidency of Republic of Türkiye, Digital Transformation Office)
- Custom Security Baseline

CIS Benchmark vs MITRE ATT&CK

Top Cyber-Attacks

Malware	67%
Ransomware	74%
Web Application Hacking	41%
Insider Privilege and Misuse	64%
Targeted Intrusions	59%
Combined Attack Types	83%

CIS Microsoft Windows 10 v1.11.0 Benchmark

CIS Microsoft Windows 10 v1.11.0 Benchmark can defend against XX% of ATT&CK (Sub-)Techniques

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