



Is Manual Security Hardening Draining Your Resources?

Automate Your Way to 95%+ Compliance!




Are your IT and security teams bogged down with the painstaking process of manual security hardening? We get it. Ensuring every server, client, and network device meets stringent security benchmarks can feel like an endless task. Consider this:

- A default Windows Server typically scores a mere **21% on CIS benchmarks**, leaving significant security gaps.
- For a medium-sized organization, this can translate to performing approximately **1 million** security hardening checks manually!
- This process is not only **time-intensive** but also complex, error-prone, and demands specialized expertise.



The SecHard Solution: Automation and Complete Zero Trust

Stop firefighting and start fortifying! SecHard's Security Hardening module is designed to:

- 
- Effortlessly elevate your security hardening scores from as low as 21% to an **impressive 95%** or more.
 - Boost your cyber resilience fourfold through automated configuration and remediation.
 - Generate comprehensive gap analysis reports in minutes, not days.
 - Apply automated remediations in seconds with a single click, eliminating risks associated with manual changes and freeing your experts.

One of our clients with approximately 2500 assets saw their security hardening gap report generated in just one hour, with all remediations completed in a few weeks thanks to SecHard's automation!




Why Choose **SecHard** for Security Hardening?

- **Rapid Audits & Remediation:** The industry's first security hardening audit with automated, risk-free remediation.
- **Wide Support:** Covers servers, PCs, network devices, databases, cloud, IoT, and more.
- **Achieve Compliance:** Seamlessly meet requirements for NIST CSF, CIS, CMMC, DISA-STIG, ISO 27001, GDPR, and many others.
- **Unmatched ROI:** Significantly reduce costs and complexity associated with manual hardening.

Why **React to Attacks** When You Can Eliminate Risks Before They Start?

Most cybersecurity solutions react after an attack – detecting threats, blocking intrusions, and responding to breaches. But by the time they activate, damage may already be done. The SecHard platform takes a different approach, focusing on proactive cyber hygiene. We don't just detect threats; we eliminate the risks before they become threats, by hardening systems, enforcing compliance, and reducing attack surfaces.

**SECHARD**
Complete Zero Trust

Dashboard

Resource

PAM

TACACS

Security Zone

Hardening Zone

Security Zone

Vulnerability Zone

Connection Zone

Multi Resource Conf

Backup & Restore

Records

Mac Addresses

Ports

Alarms

Maps

Management

User Management

Asset Management

Task Management

Hardening Zone

Search Name

Switch

Cisco

Cisco IOS Ser

Standart Benchmark v4.0.1

	1.01 Enable aaa new-model	1.01 Set the hostname	1.02 Set the ip domain name	1.02 Enable aaa authentication login	1.03 Set no interface tunnel	1.03 Set modulus to greater than or equal to 2048 for crypto key generate rsa	1.03 Enable aaa authentication enable default	1.04 Set seconds for ip ssh timeout	1.04 Set ip verify unicast source reachable-via	1.05 Set maximum value for ip ssh authentication-retries	1.05 Set login authentication for line tty	1.06 Set version 2 for ip ssh version	1.06 Set login authentication for line vty	1.07 Set aaa accounting to log all privileged use commands using commands 15	1.08 Set aaa accounting connection	1.09 Set aaa accounting exec	1.10 Set aaa accounting network	1.11 Set aaa accounting system	2.01 Set ip access-list extended to Forbid Private Source Addresses from External Networks	2.01 Set no cdp run	2.01 Set privilege 1 for local users	2.02 Set transport input ssh for line vty connections	2.02 Set no ip bootp server	2.02 Set inbound ip access-group on the External Interface	2.03 Set no service dhcp	2.03 Set no exec for line aux 0	2.04 Create access-list for use with line vty	2.04 Set no ip identid	2.05 Set access-class for line vty	2.05 Set service tcp-keepalives-in	2.06 Set exec-timeout to less than or equal to 10 minutes for line aux 0	2.06 Set service tcp-keepalives-out	2.07 Set no service pad	
F1 Switch - 172.16.0.2	✓	✓	✓	✓	✓	▲	▲	▲	—	▲	—	▲	▲	✓	▲	✓	▲	✓	▲	✓	▲	—	▲	▲	—	▲	—	—	—	▲	✓	—	✓	✓
F1 Switch - 172.16.0.26	✓	✓	✓	✓	✓	▲	▲	▲	—	▲	—	▲	▲	✓	▲	✓	▲	✓	▲	▲	▲	—	▲	▲	—	▲	—	—	—	✓	✓	—	✓	✓
F1 Switch - 10-3N16-1	✓	✓	✓	✓	✓	▲	✓	▲	—	▲	—	▲	✓	✓	▲	✓	▲	▲	▲	▲	▲	—	▲	✓	—	✓	—	—	▲	✓	—	✓	✓	
Cisco Intercity Dudulu Servisler 2960	✓	✓	✓	✓	✓	✓	✓	▲	—	▲	—	✓	✓	▲	▲	▲	▲	▲	▲	▲	✓	—	▲	▲	—	▲	—	—	▲	✓	—	✓	✓	
Cisco Akyacht 2960 2	▲	✓	✓	—	✓	▲	—	▲	—	▲	—	✓	—	—	—	—	—	—	▲	✓	▲	✓	—	▲	▲	—	▲	—	—	▲	▲	—	▲	✓
F1 Switch - 172.16.0.14	✓	✓	✓	✓	✓	▲	▲	▲	—	▲	—	▲	▲	✓	▲	✓	▲	✓	▲	✓	▲	—	▲	▲	—	▲	—	—	✓	✓	—	✓	✓	

Powered by **SecHard** / 3

Prevent, Protect, Comply

Before Threats
Even Emerge

SecHard Advantage

- ✓ **Prevention Over Reaction**
 - Harden systems before threats arise
- ✓ **Compliance-Driven Security**
 - Ensure regulatory adherence at scale
- ✓ **Seamless Integration**
 - Works with existing security platforms
- ✓ **Automated Risk Mitigation**
 - Reduce attack surfaces effortlessly

Why Wait for an Attack? **Secure Your Infrastructure Now.**

Most cybersecurity solutions react during or after an attack—detecting threats, blocking intrusions, and responding to breaches. But by the time they activate, the damage may already be done. SecHard takes a different approach.

We don't just detect threats—we eliminate the risks before they become threats. Through system hardening, security configuration management, risk assessment, and access control, we fortify your infrastructure from the inside out. Our platform ensures your systems are resilient, compliant, and impenetrable, minimizing the need for reactive security measures.



SECHARD
Complete Zero Trust

A True Platformized Security Approach

Security today isn't just about isolated tools—it's about platformization. SecHard integrates seamlessly into your security ecosystem, complementing solutions like Palo Alto, Trellix, and Symantec. While they focus on attack detection and response, we focus on proactive risk elimination. The result? A holistic security strategy that enhances resilience, strengthens compliance, and gives your organization the ultimate defense against evolving threats.



sales@sechard.com



www.sechard.com

SecHard Zero Trust Orchestrator



The SecHard Zero Trust Orchestrator is a multi-module software designed as a comprehensive platform for implementing Zero Trust Architecture and facilitating compliance with the Executive Office of Presidential memorandum (M-22-09), NIST SP 800-207, and Gartner Adaptive Security Architecture.

It also supports compliance with CBDDO compliance, CIS V7.1, CIS V8, CMMC Compliance, HIPAA compliance, ISO 27001, ISO 27002, NIST 800-171r2, NIST 800-207A, NIST 800-210, NIST 800-53r5, PCI DSS, SOX Compliance, GDPR, KSA SAMA, KSA ECC, Egypt Financial Cyber Security Framework Digital v1 compliance. SecHard Zero Trust Orchestrator is built on the principles of zero-trust security, which means it treats all devices and users as untrusted and verifies every access request before granting access.

SecHard Zero Trust Orchestrator modules, such as Security Hardening, Privileged Access Manager, Asset Manager, Vulnerability Manager, Risk Manager, Device Manager, Performance Monitor, Key Manager, TACACS+ Server, and Syslog Server, work together seamlessly within this platform to provide a comprehensive set of tools that facilitate compliance with industry standards and promote excellent cyber hygiene across your environment.

Contact us today to learn more
about how Sechard can help you
achieve your cybersecurity goals!



SECHARD

Complete Zero Trust

Did you like this content?



Double
Tap



Leave
a Comment



Share
with friends



Save it
for Later

+ Follow



sales@sechard.com



www.sechard.com