



Cybersecurity Asset and Risk Management

Why visibility and context are everything



www.sechard.com



sales@sechard.com



The Visibility Gap: A top security threat

As enterprises expand across on-prem, cloud, and remote infrastructures, the number of connected assets has grown exponentially. Without a centralized asset inventory, security teams operate in the dark, missing misconfigured servers, unmanaged devices, and unauthorized applications.

But visibility alone is not enough.



sales@sechard.com



www.sechard.com





From Discovery to Actionable Insight

Effective risk management requires linking assets to risk scores, contextual data, and remediation pathways. This means knowing not just what is vulnerable, but why it matters. For example, whether it is a critical server supporting financial operations or a forgotten device exposing your internal network.

That is where traditional CMDBs and spreadsheets fall short.



sales@sechard.com



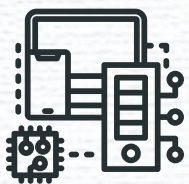
www.sechard.com





SecHard: A Unified Platform for Asset and Risk Management

SecHard's integrated approach brings together asset discovery, risk calculation, vulnerability detection, and automated hardening in one agentless platform:



Comprehensive Asset Discovery

Automatically detects devices, applications, servers, IoT, OT, and more, whether they are online now or newly added tomorrow.



Context-Aware Risk Scoring

SecHard combines technical data such as vulnerabilities, hardening status, and privilege level with business risk inputs from GRC systems to create a true real-world risk score.



Real-Time Configuration Management

Monitor system integrity, track unauthorized changes, and automatically enforce baseline security policies.



Seamless Integration with GRC Tools

Import and export risk data to ensure that SecHard is not another silo but a central part of your risk governance architecture.



Automated Remediation

Do not just detect risks. Eliminate them with automated patching, hardening, and access controls.

Why it matters?

When risk is calculated based only on technical severity, high-value business systems may be overlooked, or minor issues may be exaggerated. SecHard aligns cybersecurity risk with operational impact, helping security leaders focus on what truly matters.


Ready to See Everything?

With SecHard, asset and risk management becomes more than a checklist. It becomes a strategic function that drives resilience, compliance, and security ROI.

Schedule a demo to discover how SecHard can transform your asset visibility and risk posture into a unified, automated, and intelligent process.

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

Most cybersecurity solutions react after an attack—but why wait? SecHard eliminates 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 ident | 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 |
|--|---------------------------|-----------------------|-----------------------------|--------------------------------------|------------------------------|---|---|-------------------------------------|---|--|--|---------------------------------------|--|--|------------------------------------|------------------------------|---------------------------------|--------------------------------|--|---------------------|--------------------------------------|---|-----------------------------|--|--------------------------|---------------------------------|---|----------------------|------------------------------------|------------------------------------|--|
| F1 Switch - 172.16.0.2 | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| F1 Switch - 172.16.0.26 | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| F1 Switch - 10 - 3N16-1 | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Cisco Intercity Dudullu Servisler 2960 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Cisco Akyacht 2960 2 | ✗ | ✓ | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| F1 Switch - 172.16.0.14 | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✓ |

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.



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.

SecHard Cyber Hygiene Platform

One Platform. All Hygiene. Total Resilience.

SecHard delivers a unified cybersecurity platform that operationalizes holistic cyber hygiene. The platform automates essential practices like asset visibility, configuration management, vulnerability assessment, hardening, and access control—all from a single, integrated solution.

The SecHard Cyber Hygiene Platform is a multi-module software designed to build foundational security and resilience from within your environment. It facilitates compliance with a wide range of industry standards and frameworks, including 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.

The platform's modules work together seamlessly to provide a comprehensive set of tools for strengthening your security posture. These modules include: Security Hardening, Privileged Access Manager, Asset Manager, Vulnerability Manager, Risk Manager, Device Manager, Performance Monitor, Key Manager, TACACS+ Server, and Syslog Server.

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



sales@sechard.com



www.sechard.com



Did you like this content?



Double
Tap



Leave
a Comment



Share
with friends



Save it
for Later

+ Follow



sales@sechard.com



www.sechard.com