SECHARD

Top 10 Vulnerability Management Metrics

sales@sechard.com

www.sechard.com

SECHARD

Total Number of Discovered Vulnerabilities

1

A simple count of all new vulnerabilities detected across the environment (e.g., via vulnerability scans, penetration tests, or threat intelligence feeds).

Provides a high-level view of the security posture and scanning coverage. A persistent increase could indicate newly introduced systems, poor patching practices, or the rollout of new scanning tools with better detection capabilities.

Vulnerability Severity Distribution

2

The classification of vulnerabilities by criticality (e.g., Critical/High/Medium/Low), often aligned with frameworks such as CVSS (Common Vulnerability Scoring System).

Helps prioritize remediation efforts. If the critical or high-severity category grows or remains unaddressed, that's a clear sign of elevated risk.

sales@sechard.com

www.sechard.com

SECHARD

Mean Time to Remediate (MTTR)

3

The average time it takes to fix or mitigate a vulnerability from the moment it is discovered.

Represents how quickly teams address security weaknesses. Short MTTRs generally indicate a mature patching and remediation process, while longer MTTRs could signal resource constraints or workflow inefficiencies.

Mean Time to Detect (MTTD)

4

How long it takes on average for the organization to detect a vulnerability after it has been introduced into the environment.

Highlights detection capability and the thoroughness/timeliness of scanning. A lower MTTD means you're discovering issues before attackers can exploit them.

sales@sechard.com

www.sechard.com

SECHARD

Patch Compliance Rate

5

The percentage of systems or applications that are fully patched against known vulnerabilities.

Gauges how effectively and consistently teams are applying security fixes. It is often used in conjunction with organizational patching policies or service-level agreements (SLAs).

Vulnerability Recurrence Rate

6

The frequency at which a previously remediated vulnerability reappears on the same systems.

Recurring vulnerabilities often indicate issues with the patch management process (e.g., incorrect configurations, untested rollbacks, or incomplete fixes). A higher recurrence rate suggests a breakdown in the remediation workflow.

sales@sechard.com

www.sechard.com

SECHARD

Remediation SLA Compliance

7

The ratio or percentage of vulnerabilities remediated within a defined SLA (e.g., critical vulnerabilities fixed within 7 days).

Measures whether teams are meeting organizational or regulatory deadlines for addressing vulnerabilities. Low compliance can expose the organization to increased risk or potential noncompliance penalties.

Open Vulnerabilities Over Time (Aging Analysis)

8

Tracks how long vulnerabilities remain open before they are fixed or mitigated, often broken down by severity.

Highlights backlogs and identifies systemic delays. This metric can be represented in various ways—for instance, how many critical vulns remain open for more than 30 days, 60 days, etc.

sales@sechard.com

www.sechard.com

SECHARD

False Positive Rate

9

The proportion of identified vulnerabilities that turn out to be non-issues or cannot be reproduced.

A high false positive rate wastes analysts' time and can reduce trust in the scanning process. Monitoring this rate helps teams fine-tune scanning tools and reporting processes.

Coverage Metrics (Scan Depth & Frequency)

10

An assessment of how many assets or application components are being scanned, how often they're scanned, and how thoroughly each system is tested.

Even the best vulnerability detection and remediation processes will miss issues if not applied thoroughly across all assets. Coverage metrics help gauge whether critical systems or networks are under-scanned or neglected.

sales@sechard.com

www.sechard.com

Are you ready to elevate your organization’s security posture, streamline compliance, and take the guesswork out of vulnerability management?

Look no further than SecHard—a comprehensive security platform designed to empower security and IT teams with powerful automated scanning, intuitive dashboards, and actionable threat intelligence.

SecHard cuts through complexity to pinpoint critical risks fast, so you can protect your business from today’s most sophisticated cyber threats.

SECHARD

sales@sechard.com

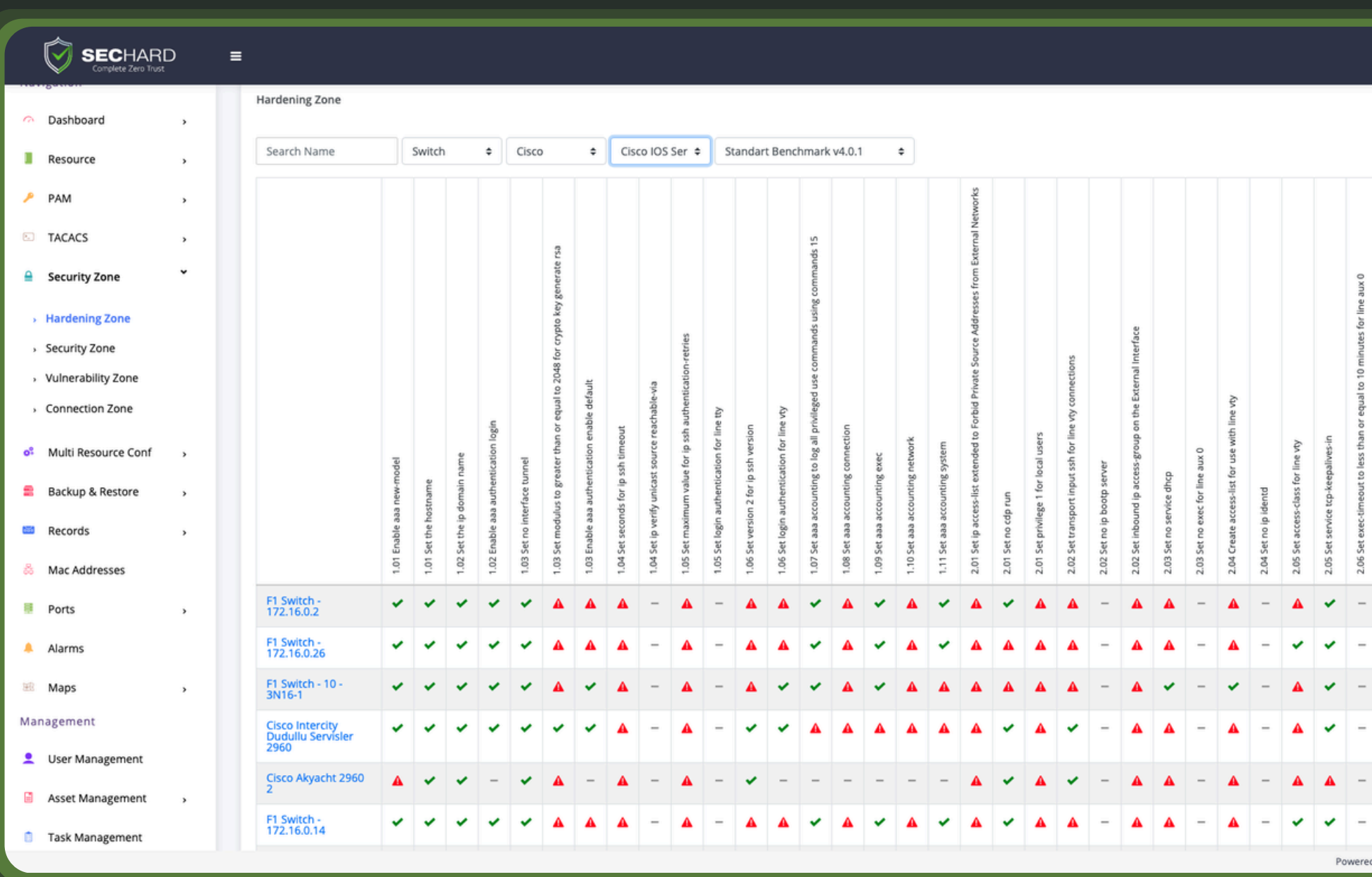
www.sechard.com

www.sechard.com

SECHARD

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.



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

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

SecHard Zero Trust Orchestrator is a multi-module software for implementing Zero Trust Architecture designed to facilitate 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 to provide a comprehensive set of tools that facilitate compliance with industry standards.

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

sales@sechard.com

www.sechard.com

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