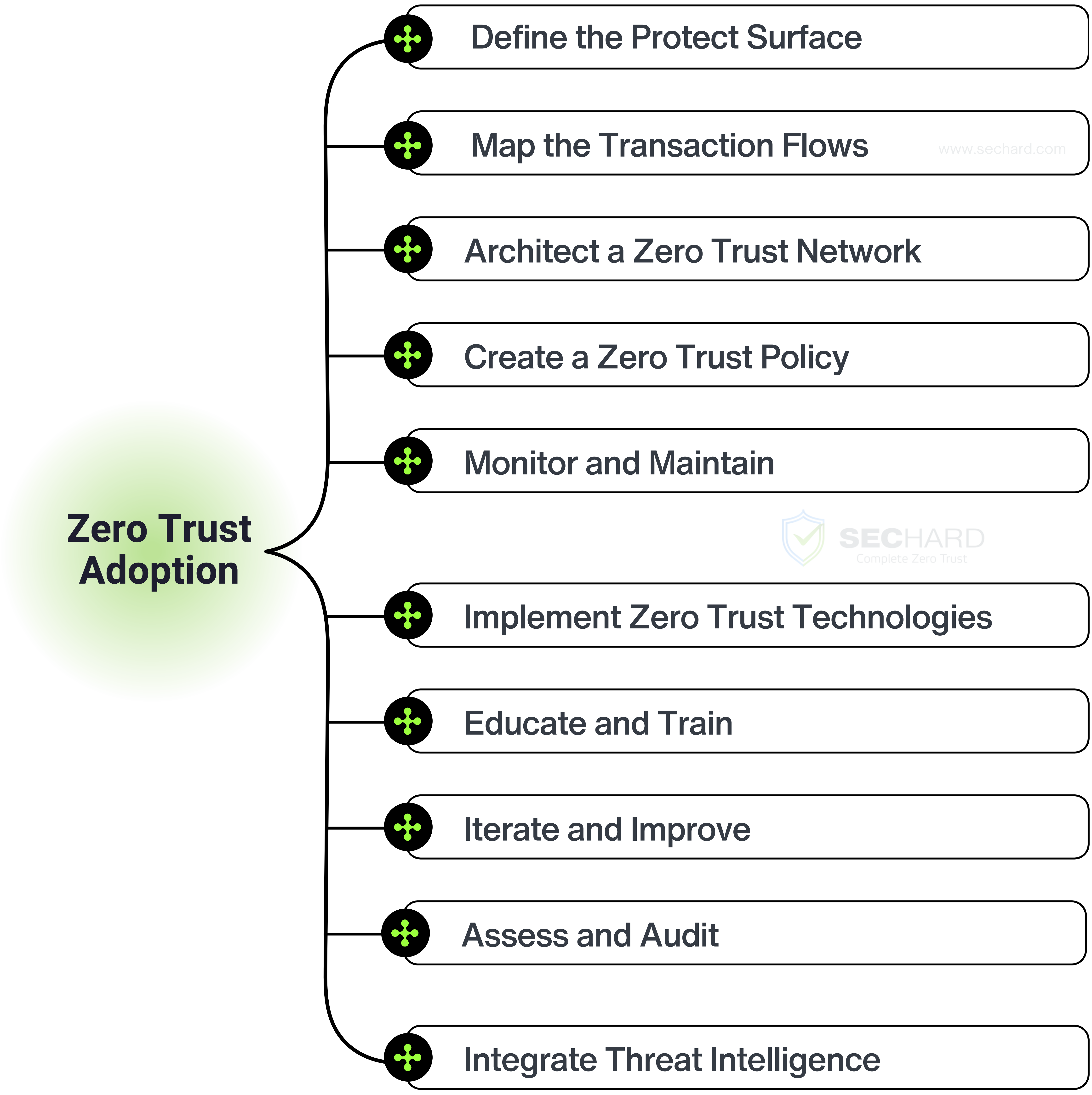
Zero Trust Adoption Framework



Zero Trust Adoption

- Define the Protect Surface
- Map the Transaction Flows
- Architect a Zero Trust Network
- Create a Zero Trust Policy
- Monitor and Maintain
- Implement Zero Trust Technologies
- Educate and Train
- Iterate and Improve
- Assess and Audit
- Integrate Threat Intelligence

Define the Protect Surface

1 Catalog and classify all critical data, assets, applications, and services (DAAS)

2 Determine which resources are most valuable and sensitive.

3 Assess the potential impact of a breach on these resources.

4 Prioritize protection efforts based on risk and importance.

Map the Transaction Flows

1 Document how data flows across the network and between resources.

2 Identify authorized users, devices, and services for each transaction.

3 Understand dependencies and interactions among various network components.

4 Establish baseline patterns for normal network behavior.

Architect a Zero Trust Network

1. Design network segmentation to isolate critical resources and minimize lateral movement.
2. Implement micro-segmentation to create secure zones within the network.
3. Apply network controls such as firewalls, gateways, and access lists.
4. Ensure encryption of data in transit and at rest.

Create a Zero Trust Policy

1. Develop policies that enforce least-privilege access based on user, device, and application context.
2. Incorporate risk assessments into access decisions.
3. Define clear rules for granting, denying, and revoking access.
4. Regularly update policies to adapt to changing security requirements.

Monitor and Maintain

1. Continuously monitor network activity for signs of unauthorized access or anomalies.
2. Use security information and event management (SIEM) tools for real-time analysis.
3. Implement automated responses to detected threats.
4. Conduct periodic reviews to ensure policies and controls remain effective.

Implement Zero Trust Technologies

1. Deploy multi-factor authentication (MFA) to verify user identities.
2. Use identity and access management (IAM) solutions for access control.
3. Utilize endpoint detection and response (EDR) tools for device security.
4. Leverage software-defined perimeter (SDP) technologies for secure access.

Educate and Train

1. Provide comprehensive training on Zero Trust principles and best practices.
2. Conduct regular security awareness programs for all stakeholders.
3. Simulate phishing and social engineering attacks to test awareness.
4. Offer specialized training for IT and security teams on Zero Trust technologies.

Iterate and Improve

1. Continuously evaluate the effectiveness of the Zero Trust implementation.
2. Gather feedback from users and stakeholders to identify areas for improvement.
3. Stay informed about emerging threats and security trends.
4. Adjust strategies and technologies to address evolving challenges.

Assess and Audit

1 Conduct regular security assessments to identify vulnerabilities.

2 Perform audits to ensure compliance with Zero Trust policies and standards.

3 Use penetration testing to evaluate the resilience of the Zero Trust architecture.

4 Review access logs and incident reports for insights into security posture.

Integrate Threat Intelligence

1 Incorporate real-time threat intelligence feeds into the Zero Trust framework.

2 Analyze global and industry-specific threats to anticipate potential risks.

3 Use threat intelligence to inform policy decisions and response strategies.

4 Collaborate with external security organizations and communities for shared intelligence.

Zero Trust Principles for the C-suite

(Zero Trust is a strategy and architecture based on three principles)

SECHARD
Complete Zero Trust

Principle	Technical Description	Business Description
Verify explicitly	Always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies.	This principle requires users to verify who they are, using more than one method, so that compromised accounts gained by hackers aren't allowed to access your data and apps. This approach also requires devices to be recognized as being allowed to access the environment and, ideally, to be managed and healthy (not compromised by malware).
Use least privileged access	Limit user access with just-in-time and just-enough-access (JIT/JEA), risk-based adaptive policies, and data protection to help secure both data and productivity.	This principle limits the blast radius of a potential breach so that if an account is compromised, the potential damage is limited. For accounts with greater privileges, such as administrator accounts, this involves using capabilities that limit how much access these accounts have and when they have access. It also involves using higher-levels of risk-based authentication policies for these accounts. This principle also involves identifying and protecting sensitive data. For example, a document folder associated with a sensitive project should only include access permissions for the team members who need it. These protections together limit how much damage can be caused by a compromised user account.
Assume breach	Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses.	This principle assumes the likelihood that an attacker will gain access to an account, identity, endpoint, application, API, or other asset. This principle also involves implementing tools for ongoing threat detection and rapid response. Ideally these tools have access to signals integrated across your environment and can take automated actions, such as disabling an account, to reduce the damage as soon as possible.

*Source: Microsoft

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 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

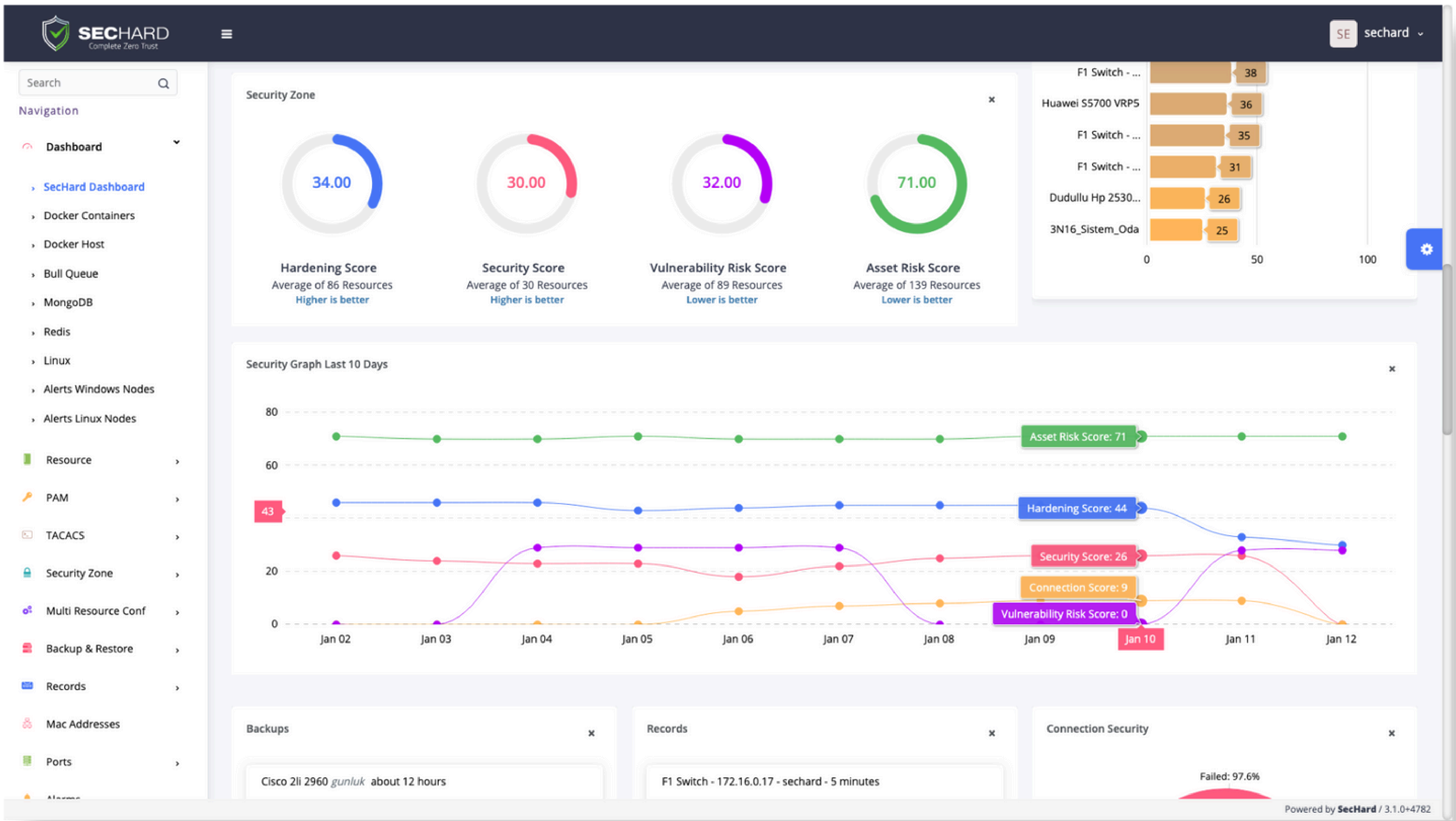
SecHard Zero Trust Orchestrator is a multi-module software for implementing Zero Trust Architecture designed to facilitate compliance with the Executive Office of Presidential memorandum (M-22-09), NIST SP 800-207, and Gartner Adaptive Security Architecture. It also supports compliance with CBDDO compliance, 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

SecHard provides automated security hardening auditing, scoring, and remediation for servers, clients, network devices, applications, databases, and more.

According to CIS, in order to have a secure operating system, it is necessary to change approximately four hundred security settings on a Microsoft Windows Server running with the default settings. There are most probably hundreds of missing security settings on the computer that you have. In an enterprise network with hundreds or thousands of IT assets, reporting and remediating all these deficiencies can be an operation that will take years for IT teams.

With SecHard, enterprises can easily add their own, unique controls and run them on thousands of different assets. In this way, special audit and automatic remediations can be produced for both common and non-common technologies such as Operating Systems, Network Devices, Applications, IoT, SCADA, Swift, POS and many more.



Cisco 2li 2960 *gunluk* about 12 hours

F1 Switch - 172.16.0.17 - sechard - 5 minutes

sales@sechard.com

SECHARD
Complete Zero Trust

Contact us ▪ Get Started ▪ Contact us ▪ Get Started

SecHard Zero Trust Orchestrator

SECHARD
Complete Zero Trust

Are you struggling to keep up with the latest cybersecurity standards and guidelines? Do you want to ensure your enterprise network complies with NIST SP 800-207? Look no further than Sechard.

With SecHard Zero Trust Orchestrator, you can easily implement the guidelines and best practices of NIST SP 800-207, the Executive Office of Presidential memorandum (M-22-09), and Gartner Adaptive Security Architecture, ensuring your enterprise network is secure and compliant.

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