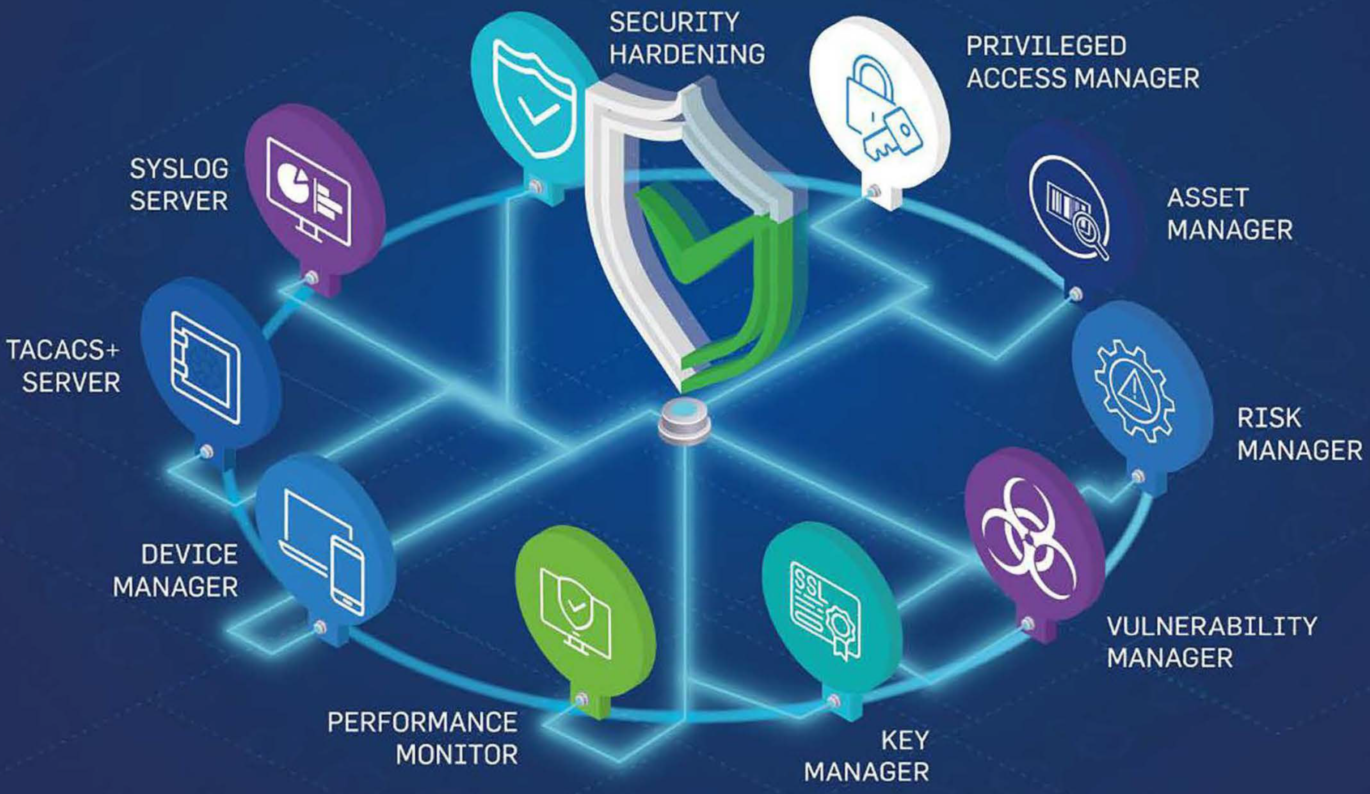
SECHARD



ZERO TRUST ORCHESTRATOR

RPM TECHNOLOGY

www.rpmtechnology.co.uk

SECHARD
Complete Zero Trust

Complete Zero Trust is now possible

www.rpmtechnology.co.uk

PRODU

RPM TECHNOLOGY

Complete Zero Trust

INTRODUCTION

Creating a useful strategy and managing operations to ensure Information Security puts a strain on you while it also puts an immense pressure on your Information Technology and Security Teams. Luckily, the Zero Trust Architecture (ZTA) documents published by institutions like NIST guide us and shed light on achieving our goal. Our game-changing product SecHard, simplifies these complex processes with its integrated approach and gives you complete Zero Trust (ZT). In addition to providing time and cost advantages, it also alleviates the workload of your Information Security Experts.

> *"ZT is the term for the evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. ZTA uses zero trust principles to plan industrial and enterprise infrastructure and workflows. ZT assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned). Authentication and authorization (both subject and device) are discrete functions that are performed before a session to an enterprise resource is established."* [1]

ZTA requires Protection Visibility Control (PVC) in five areas: People, Workload, Network Device, User Device and Data. SecHard is the unique integrated solution that provides PVC in these five areas.

Organizations need to implement comprehensive information security and resilient practices for ZT to be effective. When balanced with existing cybersecurity policies and guidance, identity and access management, continuous monitoring, and security hardening (best practices), ZTA can protect against common threats and improve organizations' security posture by using a managed risk approach.

The importance of ZTA in cybersecurity has been recognized by the USA and its implementation has been made mandatory for all US Federal agencies with the memorandum published [2] by Executive Office of the President on January 26, 2022.

The hardest part of the implementation and management of ZTA is security hardening. According to the Center for Internet Security (CIS) hundreds of setting changes are required on thousands of devices. SecHard's security hardening module generates gap analysis reports within minutes according to the industry standards and makes automatic remediations for them within seconds.

Before SecHard, in order to put ZTA into practice, there was a need for buying and managing a variety of products. Those times are left behind us. SecHard brings you peace of mind thanks to holistic approach and automated remediation features.

SecHard meets all requirements of Zero Trust Architecture on a single platform.

PRODUCT OVERVIEW

SECURITY HARDENING	PAM	ASSET MANAGER	VULNERABILITY MANAGER	KEY MANAGER
RISK MANAGER	DEVICE MANAGER	PERFORMANCE MONITOR	TACACS+ SERVER	SYSLOG SERVER

[1] (1): NIST Special Publication 800-207, Zero Trust Architecture, P:4

[2] (2): https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

SECURITY HARDENING

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.

For the remediation process, experienced specialists and an extremely large amount of time is required. Some critical changes can also have unexpected consequences that could lead to a disaster. SecHard automatically performs the necessary security remediations in seconds with a single click, eliminating all the risks related to change without the need for a mastery-depth knowledge.

SecHard is one of the products with the highest return on investment in the field of information security.

CASE STUDY

One of our customers has approximately 2500 assets. They had difficulties in managing their security hardening processes to get compliant with several regulations.

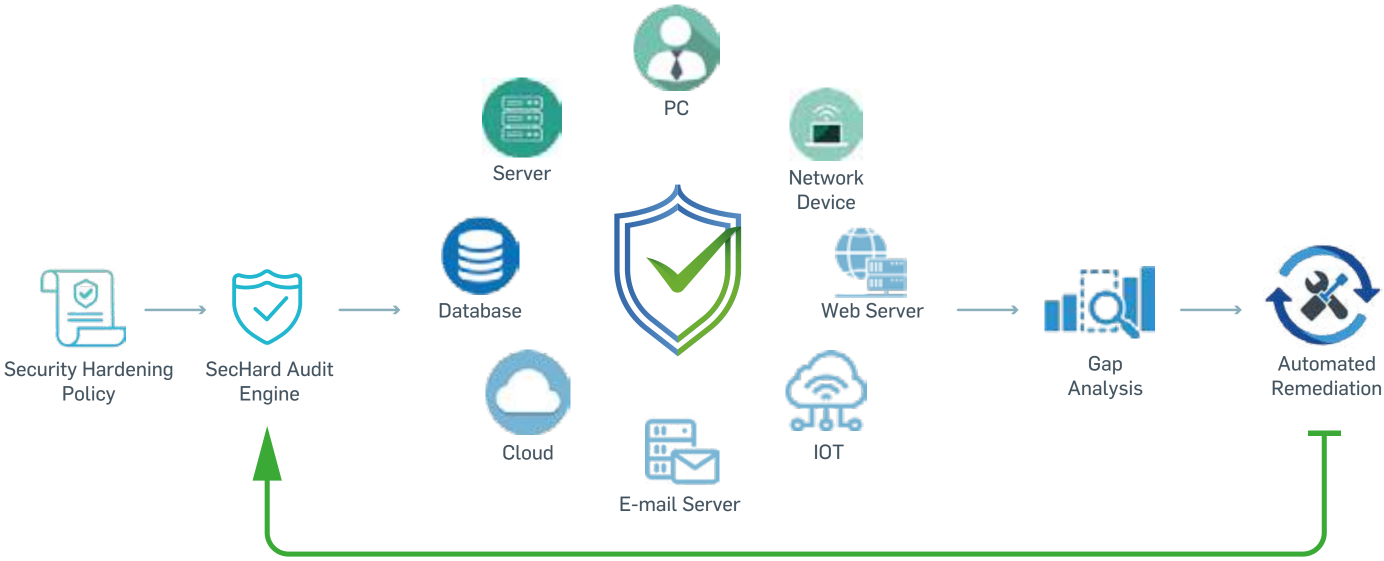
SecHard created the security hardening gap report in just an hour.

All the hardening remediation operations were completed in a few weeks with SecHard's automatic remediation feature.

Ultra-fast audit and remediation

KEY BENEFITS

- Industry's first Security Hardening audit with automated remediation
- Detailed security scoring
- Wide device and platform support
- Remediation with NO RISK
- Unmatched Return on Investment



PRIVILEGED ACCESS MANAGER

The most important PVC in ZTA is People. Studies have found that 77% of data leaks are caused by privilege abuse[3], which proves the importance of this control. Due to the difficulty of identity management, many different types of threats can arise ranging from espionage to ransomware.

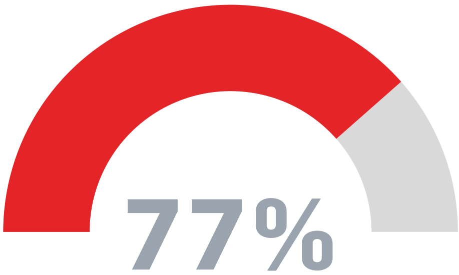
Unlike a traditional PAM product, SecHard offers a PAM solution that integrates with other PVC areas recommended by the ZTA. SecHard not only gives privilege access to the right person, but also performs the recommended PVCs that are required for the ZTA on all the network devices used in the connection, and on the computer that makes the connection. In this way, the computers whose hardening or security scores produced by SecHard are below the acceptable security level can be restricted from authorized access or risk warnings can be generated. SecHard can automatically discover and login new assets, perform automatic security hardening scoring, and remediate predefined hardening settings fully automatic.

This does not mean SecHard does not have traditional PAM features. Like all other PAM products, SecHard has a password vault. It can enable the accesses such as RDP, VNC, SSH, and Telnet without knowing the password and can record all the sessions both in video and text format.

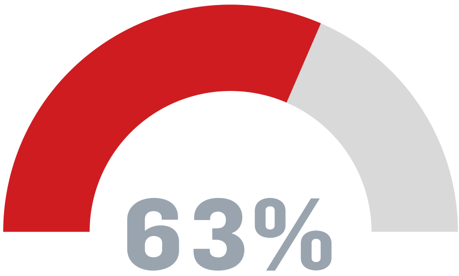
Do you already have a PAM product? Don't worry. SecHard can integrate with third party PAM products and it can score their security hardening, as well.

KEY BENEFITS

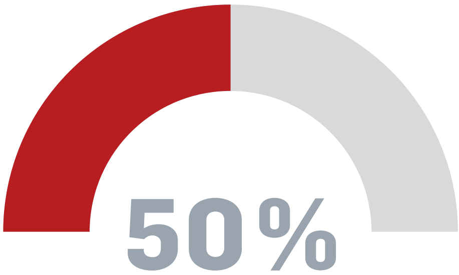
- Advanced password vault
- RDP, VNC, SSH, Telnet session recording and OCR support
- Third party PAM Integration
- 2FA Authentication
- Reduce costs and complexity



data leaks caused by privilege abuse[3]



data leaks caused by personal[4]



data leaks caused by system admin[5]

(3)(4)(5): Verizon 2021 Data Breach Investigations Report, P:44

ASSET MANAGER

Managing assets is always a challenge. Changes are happening on existing assets almost every day and new assets are being added to the environment. These endless changes take away the visibility. Companies that do not have enough information about assets cannot perform information security risk analysis correctly.

SecHard solves the asset management problem with full automation. Thanks to its auto discovery feature SecHard can detect new and changing assets, it automatically and securely accesses the assets using the features of the PAM module and automatically generates various security scores including security hardening.

The SecHard Asset Manager module enables the management and reporting of hardware, hardware components (CPU, RAM, disc, etc.) and software inventory (operating systems, installed software, running services etc.). Assets that do not have an IP address such as keyboards and monitors, can be managed by SecHard. All hardware and software can be assigned to people, units, or locations. It monitors the warranty and license periods of hardware and software, the running services on computers, generates alarms for critical services, and can automatically restart a service that unexpectedly stopped.

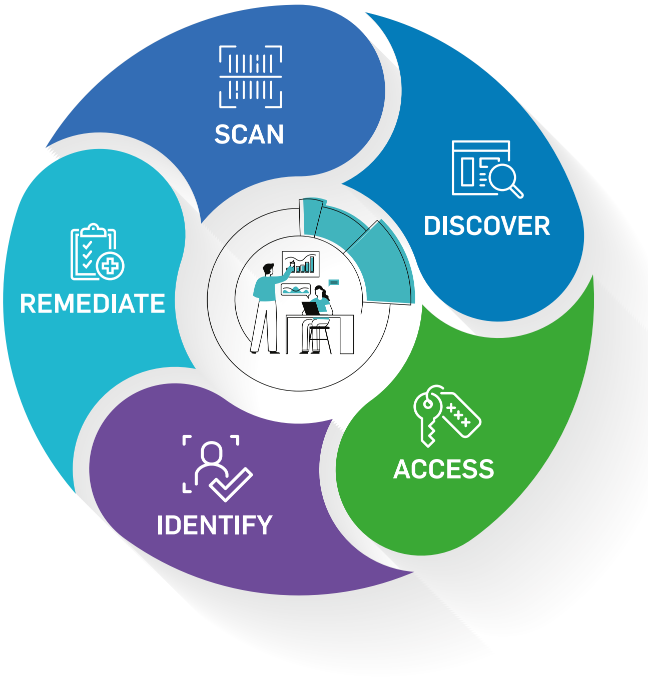
The Asset Manager module also makes it possible to save risk scores to assets and/or asset groups, generated by the organization's information security department, which will be used by the risk manager module. SecHard can also import risk scores from GRC products.

SecHard Asset Manager module has been developed in accordance with the NIST Cybersecurity Framework and Gartner Adaptive Security Architecture and it provides powerful risk-aware asset management.

KEY BENEFITS

- Automated asset discovery
- Automated security scoring for new assets
- Security baseline enforcement
- Hardware and software inventory management
- GRC and CMDB integration

SecHard Asset Management Process



RISK MANAGER

The biggest problem that the industry has not been able to respond to is the inability to holistically score and manage business risks along with technical risks. In every ISO27001 Information Security Management System (ISMS) compliance analysis, business risks are scored but doomed to live in an Excel cell. In fact, these scores are not actually used anywhere.

SecHard combines business and technical risks and calculate real world risk scores. It measures and scores the technical security risks of assets or asset groups with its own security hardening, vulnerability management, and asset management modules.

Security risk scored by information security teams for ISO 27001 ISMS and similar regulations can be added to SecHard's Asset Management Module. Besides, technical scores and business scores can be integrated by SecHard risk algorithm, which determines the real world risk score.

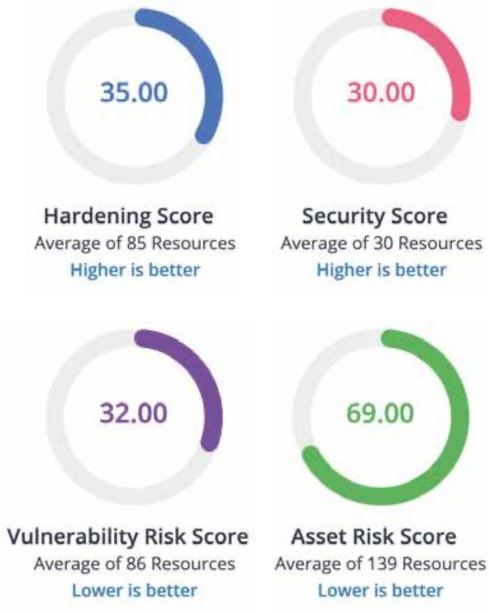
SecHard has the security hardening remediation feature to reduce technical risk scores after determining the real world risk score. At the same time, thanks to the Trellix (McAfee Enterprise) integration, SecHard makes it possible for conventional security software to provide instant security by automatically triggering hardened Endpoint Security, DLP, EDR and TIE configurations for assets above the acceptable risk level.

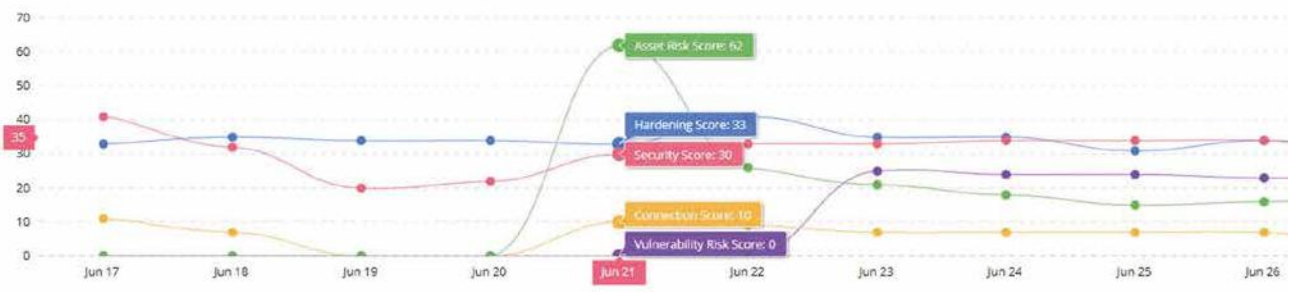
In large enterprises Governance, Risk and Compliance (GRC) products are used to manage risks. SecHard can associate SecHard assets with asset groups in GRC and automatically takes asset or asset group risk scores from the GRC. Thanks to this integration, asset and asset groups scores can be automatically imported from the GRC and necessary security controls can be automatically operated by SecHard according to the risk level.

KEY BENEFITS

- Hardening, security and vulnerability risk scoring
- Asset-based risk management
- Real world risk scoring
- GRC integration
- Immediate security with Trellix (McAfee Enterprise) integration

Security Zone





Security Graph Last 10 Days

VULNERABILITY MANAGER

One of the most primary principles of information security is to detect and manage vulnerabilities. SecHard operates the vulnerability detection and management processes for all IT assets without creating any risks thanks to the passive scanning method.

SecHard collects detailed information about assets and their software using the asset manager and device manager modules. Vulnerabilities on operating systems can be reported by queries sent to the National Vulnerability Database (NVD). The risk levels of the detected vulnerabilities are shown in the CVSS standard and SecHard reports whether there is a public exploit that uses these vulnerabilities. SecHard also redirects you to articles published by vendors for detailed information about vulnerabilities.

SecHard can import scores generated by third-party vulnerability scanning tools and include them in the risk management process. SecHard is also able to send vulnerability scores to third parties.

KEY BENEFITS

- Passive vulnerability scanning
- CVSS based risk scoring
- Integration with third parties
- Public exploit availability
- Detailed reports and alarms

PERFORMANCE MONITOR

Availability is as important as privacy and integrity in the information security equation. According to the ZTA, performance and availability are two factors that should be monitored considering security controls and risk management.

SecHard provides integrated performance and availability monitoring for both servers and network devices. This integrated architecture makes it possible to monitor servers and network devices data coming through VMI, Nod and SNMP exporters via an advanced dashboard. SecHard's customizable dashboards show real-time information to monitoring teams.

It is impossible to monitor hundreds of assets with the human eye from screens in large networks. SecHard monitors critical assets on behalf of monitoring teams. It can generate alarms, send e-mails, and run trigger predefined actions when thresholds are exceeded. In addition, SecHard stores performance data historically and simplifies the capacity planning.

The SecHard performance monitor tool provides monitoring services for all types of devices and software with IP addresses such as desktops, servers, databases, web services, smtp services, ip cameras, network printers, routers, switches etc.

KEY BENEFITS

- Wide device support
- Advanced alarms and automatic actions
- Intelligent and customizable dashboards
- Bandwidth monitoring for network devices
- Historical reporting

KEY MANAGER

One of the biggest problems for companies is the fact that most of the time, they are unaware about certificates in their own environment. In addition to this, they do not know the expiration dates of the certificates that they know of, and that they should renew before their expiration dates. Most importantly, there is a chance of unsecure certificates that the companies have under their environment.

SecHard auto-discovers the certificates in companies' environment, reports the expiration dates of these certificates, and it can automatically renew some of these certificates through well-known certificate authorities. In addition, it can do security checks to existing certificates.

SecHard uses port scan method to discover the certificates. It scans web application ports manually or continuously in environment and generate certificate inventory.

SecHard continuously analyzes configuration vulnerabilities and checks expiration date of certificates. It reports and sends notification to certificate admins. You always be aware of weaknesses and never forget the expiration date of certificates.

Thanks to global certificate authority integration, SecHard provides certification life cycle, and it renews your certificates before they expire.

SecHard revokes control with openSSL. Removed or blocked certificates by CA can be detected and a notification regarding the status are sent to users every 24 hours.

During the analyzation phase, certificates are controlled with public key size. Key size which is less than 1024 certification is reported.

Certification vulnerability control is done according to NVD and MITRE datasheet every 24 hours and time frame is managed by user.

Certification list and certification vulnerability report are exported with CVS format.

KEY BENEFITS

- Certification vulnerability control
- Certification expiration date
- Certification life cycle management
- Certification visibility and report

DEVICE MANAGER

Configuration security is an important element in the ZTA. SecHard performs security hardening checks with great success and speed. Beyond the security hardening, configuration and device management tasks are also performed by SecHard.

Configuration backup and restore operations of network devices can be done centrally by SecHard. In addition to security configurations, SecHard can automatically manage and monitor all configuration changes on the assets it manages. SecHard also sends configuration changes on multiple devices.

For network devices, the number of ports and their status, the details of the traffic passing through the ports, CPU and RAM usage are monitored by SecHard. Alarms can be triggered when critical events occur. Operational tasks such as creating a VLAN on network devices can be easily performed through the SecHard user interface with a few clicks without the need to know the CLI commands.

In order for network devices to be able to remediate vulnerabilities previously detected by SecHard, their firmware can be upgraded through the SecHard user interface.

Making port security settings is vital to prevent attacks such as ARP Spoofing, STP Manipulation and DHCP Starvation that can be made due to insecure configuration of network devices. SecHard checks whether the port security settings have been made correctly or not. Network devices with missing port security configurations can be automatically remediated with SecHard. It can also disable ports that are not used for a certain period of time and assign them to a passive VLAN.

Thanks to these features, it provides security for network devices even in areas untouched by global security hardening authorities and regulations.

KEY BENEFITS

- Configuration backup and restore
- Change management
- Role-based management
- Multiple device configuration
- Continuous monitoring and reporting

TACACS+ SERVER

Probably the most important of the PVCs recommended by the ZTA is People. Microsoft Active Directory provides a centralized account management service for Microsoft Windows systems, but *nix systems and network devices are not so lucky. These systems, which do not have a central account management, come with their local accounts and passwords. Center for Internet Security (CIS) strongly recommends restricting local accounts and implementing centralized account management.

SecHard TACACS+ module can perform central authentication and authorization for *nix systems and network devices. It provides efficient management of all devices with a single account. In addition, SecHard TACACS+ server provides Single Sign On (SSO) facility with Microsoft Active Directory integration.

Implementing TACACS+ configurations on multiple *nix systems and network devices is a difficult and time-consuming operation. SecHard provides automated implementation to enforce required configuration on network devices and servers within minutes.

SecHard TACACS+ has detailed authorization and monitoring beyond authentication with AAA support. Thus, detailed role management is possible. All events are logged and these logs are guaranteed to remain unchanged with timestamps.

KEY BENEFITS

- AAA support
- Microsoft Active Directory integration
- Single Sign-On
- Automated TACACS+ configuration on multiple devices
- SIEM and third parties integration

SYSLOG SERVER

In ZTA it is necessary to monitor continuously, log events and trigger alarms for critical events. SecHard has a comprehensive Syslog module that can provide all necessary tasks recommended by ZTA.

SecHard Syslog Server supports Secure (TLS) Syslog to collect logs securely from devices that support sending secure Syslog messages. Additionally, the collected event logs store with a time stamp.

All Syslog events can be forwarded to third parties such as SIEM, SOAR, log management software in CEF or Syslog format.

KEY BENEFITS

- Quick deployment
- Realtime log monitoring
- Advanced reporting and alarm
- Event forwarding for third parties
- Customizable dashboards

SUMMARY

With its holistic approach, SecHard is a game changer which can comprehensively fulfill the requirements of Executive Office of the President Memorandum (M-22-09), NIST SP 800-207 Zero Trust Architecture publication. It can automatically perform the NIST Cybersecurity Framework functions and the recommended processes by the Gartner Adaptive Security Architecture by eliminating the need for experts.

Thanks to its automated security analysis and remediation, provides dramatic cost savings as it eliminates the need for experienced information security engineers. SecHard provides significant return on investment (ROI) tens of times higher than other information security products.

This incredible technology works agentless without requiring any changes in your environment and installation only takes an hour. It has bidirectional API support to have easy integration with third parties.

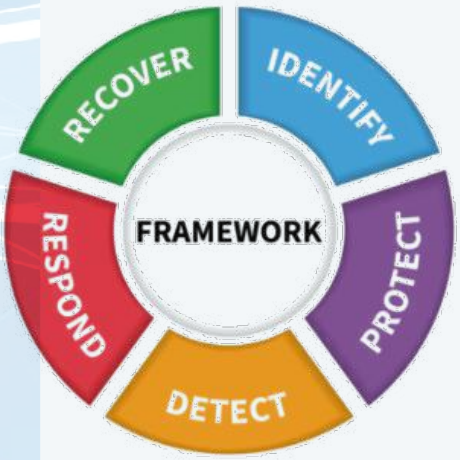


Figure 1

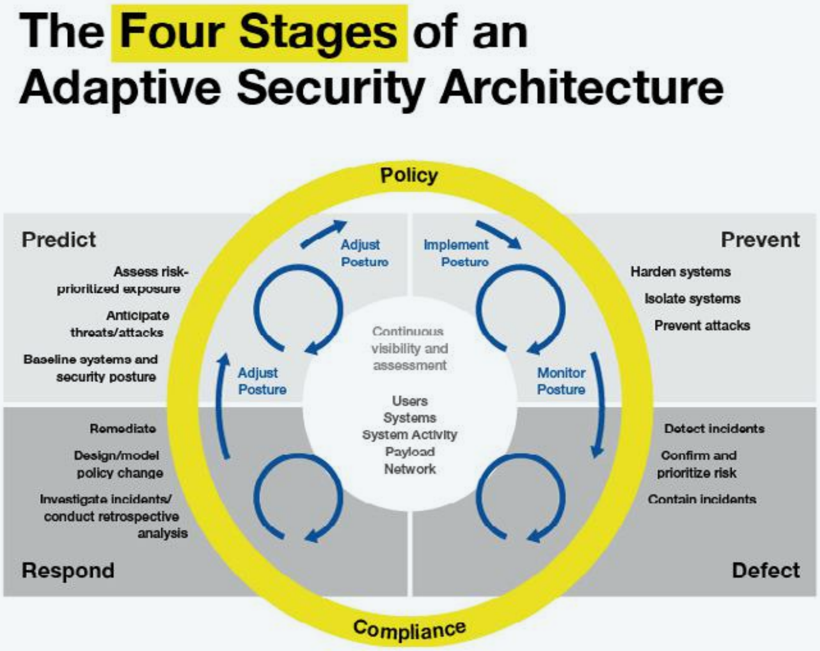

The Four Stages of an Adaptive Security Architecture
Policy
Predict
Assess risk-prioritized exposure
Anticipate threats/attacks
Baseline systems and security posture
Prevent
Harden systems
Isolate systems
Prevent attacks
Adjust Posture
Implement Posture
Adjust Posture
Monitor Posture
Continuous visibility and assessment
Users
Systems
System Activity
Payload
Network
Remediate
Design/model policy change
Investigate incidents/ conduct retrospective analysis
Respond
Detect incidents
Confirm and prioritize risk
Contain incidents
Defect
Compliance

Figure 2

LICENSING

SecHard provides the complete Zero Trust in one platform with an extremely simplified licensing model. It counts only servers, network devices, and client computers in terms of licensing. Unlimited number of users can connect to all modules, including PAM. SecHard, which is sold with an annual subscription license, also offers a purchase advantage with multi-year subscription.

Figure 1: https://www.nist.gov/cyberframework
Figure 2: https://www.gartner.com/smarterwithgartner/build-adaptive-security-architecture-into-your-organization

SECHARD

Complete Zero Trust

RPM TECHNOLOGY

www.rpmtechnology.co.uk