SECHARD

Privileged Access Manager

Consolidated, agentless PAM that helps you adopt Zero Trust in hours, eliminate privilege abuse, and simplify compliance across complex, hybrid environments.

Challenges

Zero Trust Adoption

According to Gartner, more than 50% of organizations implementing ZT will fail to realize the benefits.

Complexity of IT Environments

Managing privileged access across diverse platforms and technologies is overwhelming.

Data Breaches

According to Verizon DBIR 2021 Report, 77% of data leaks caused by privilege abuse. The average cost of data loss is $4.45M .

Compliance and Regulation

Meeting industry-specific regulations and compliance standards can be complex.



Solutions

Implementing Zero Trust Architecture

Empowers organizations to transition to a zero-trust architecture within just 2 hours.

Reducing the Risk of Data Leakage

Reduces the risk of data leakage by more than 80%.

PAM + TACACS + RADIUS

Consolidated privilege management for Windows systems, Linux and Mac OS, network devices, and many other systems.

Compliance Support

Easy compliance with Zero Trust, NIST CSF, NIST 800-53, NIST 800-171, PCI-DSS, SOX, GDPR, KSA ECC, and more.

Possessing a cybersecurity product does not ensure complete security

Cybersecurity is more than just a product; it's a refined process chain that demands expertise. At SecHard, we specialize in constructing a robust framework integrating people, processes, and cutting-edge technologies. With industry best practices at our core, we ensure your organization's security. Choose SecHard for comprehensive cybersecurity solutions that go beyond products, providing you peace of mind in the digital realm.

Enhance your knowledge by downloading our PAM Best Practices Guide at your convenience...

Scan me

Why SecHard

More Secure | Wide-range Coverage | Consolidated PAM

1

Secure by Design

SecHard runs on secure, hardened, and restricted Docker containers. Common and Personal Password Vaults are not accessible and isolated.

2

Agentless, Compact, and Enterprise Ready

SecHard is a virtual appliance. Multiple node clustering is available for free to have high availability.

3

PAM for Everything

SecHard offers free Tacacs and Radius servers to cover linux systems and network devices.

4

Risk Aware

SecHard has a risk engine to calculate cybersecurity risks for the IT environment such as high-risk assets may automatically require a second authentication or approval.

Key Functions

- Central and Private Password Vaults
- Session Management and Recording
- Active Directory Bridging
- Just in Time Access
- Command Blocking
- AD Dynamic Group Mapping

Supported Protocols

RDP / VNC / SSH / Telnet

5 Stars | 100% Recommend

Gartner Peer Insights™

Privileged Access Management