System Hardening

Secure-by-design service to minimize cyber threats to your critical operating systems

System Hardening offer

System Hardening is a service from Schneider Electric that reduces overall cybersecurity risk by reducing a system's attack surface.

The hardening process aims to mitigate attack vendors that result from leveraging software applications, firmware, operating systems, and networks. In the hardening process, configurations are set to allow only the required services, functionality, and access needed to maintain operations.

The System Hardening service that Schneider provides is an industry best practice and aligns with regulatory requirements, as seen in NIST/ IEC 62443. Those standards call for the following actions as baseline controls:

1. **Define** and update hardening guideline documentation.
2. **Deploy** a patch management program and install patches according to the desired frequency.
3. **Disable** unused ports, services, and applications.
4. **Perform** configuration activities for authenticated users and devices.

Key benefits

- **Improved security resiliency.** Reduced attack surfaces decrease the risk of system breaches, unauthorized access (intentionally or unintentionally), and malware.
- **Enhanced system performance.** Fewer necessary programs and less functionality means less risk of operational issues, misconfiguration, etc.
- **Simplified compliance and auditing.** Fewer programs and accounts coupled with a less complex environment make auditing more transparent and straightforward.
- **Improved system and application capabilities.** Often, security patches are packaged with broader updates that deliver new and improved capabilities.

se.com/cybersecurity-services

Life Is On | Schneider Electric

System Hardening service

System Hardening tasks are completed using tools, software, and service elements that support the following tasks:

- **Disabling unused ports and services**
  - Turning off unused ports.
  - Creating firewall policies to enable secure communication across networks.
  - Removing unnecessary applications.
- **Enabling required functionality to maintain operations**
  - Activating essential ports to allow deployment of solutions (i.e., anti-virus software).
  - Deploying secure remote access solutions.
  - Using security patches/updates as needed.
- **Implementing access controls**
  - Enabling authentication and authorization controls (i.e., multi-factor authentication, strong passwords, defined user groups, least privilege, etc.).
    - Reducing system permissions.

Why Schneider Electric?

Schneider Electric has the IT and OT expertise to determine critical functions and services to ensure a secure and functional network. The combination of tools, software, and services associated with the System Hardening service helps customers to regularly evaluate their cybersecurity posture and make the required changes to reduce the attack surface.

44%

of organizations reported a cyber incident involving an IoT or OT device in the past 2 years.

Source: Microsoft

Contact us today to learn more about **System Hardening** and our range of solutions to support your needs for cybersecurity protection across all business types and industries.

se.com/cybersecurity-services

Life Is On Schneider Electric

Schneider Electric Industries SAS
35, rue Joseph Monier - CS 30323
F92506 Rueil-Malmaison Cedex