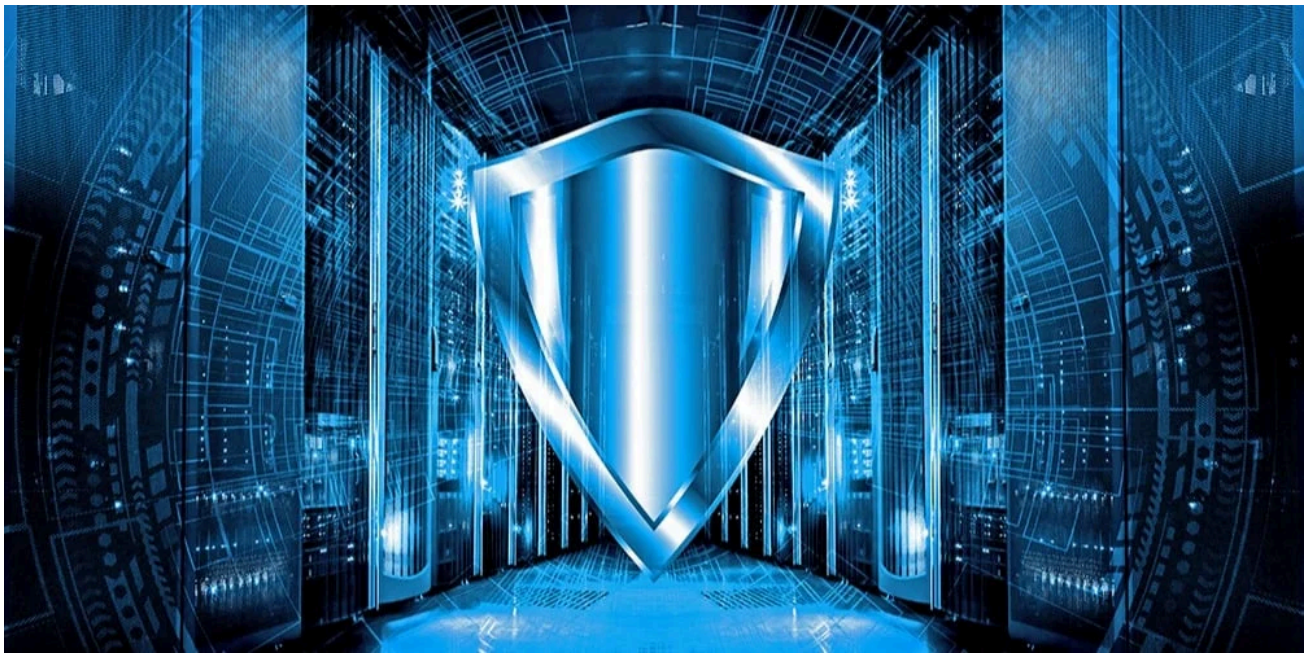
System Hardening: An Easy-to-Understand Overview

Graphic: System hardening is all about protecting your server or workstation.

> *Competitors deterred from engaging the United States and our allies in an armed conflict are using cyberspace operations to steal our technology, disrupt our government and commerce, challenge our democratic processes, and threaten our critical infrastructure.*

As such, many companies supporting and selling servers and workstations to the DoD are turning to advanced system hardening tools and best practices to improve the security of their servers and other computer systems, oftentimes as a prerequisite for doing business with the DoD.

In this blog post, we'll discuss system hardening, its importance, the types of system hardening, how system hardening is achieved, and more. By the end, you should know what steps to take to begin or expand upon your system hardening processes and procedures.



Graphic: System hardening involves reducing a server's or workstation's attack surface.

What does system hardening mean?

System hardening is the process of securing a server or computer system by minimizing its attack surface, or surface of vulnerability, and potential attack vectors. It's a form of cyberattack protection that involves closing system loopholes that cyberattackers frequently use to exploit the system and gain access to users' sensitive data.

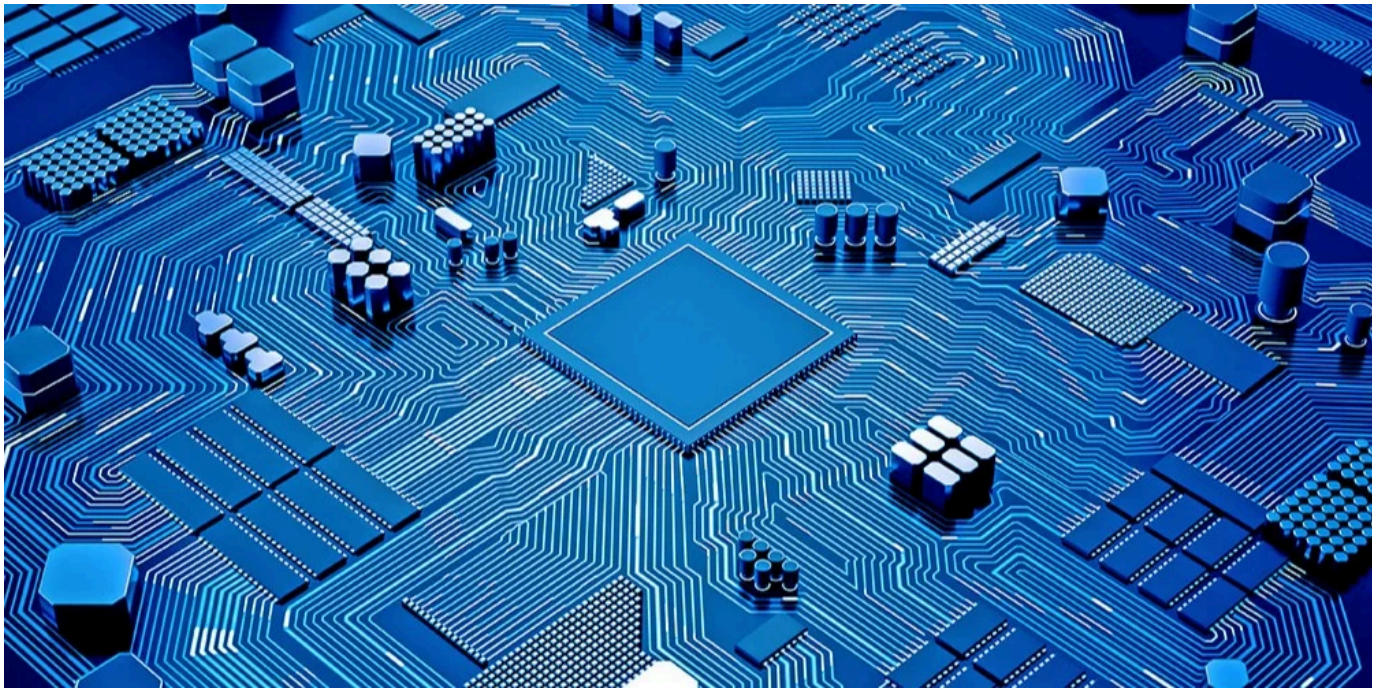
One official definition of system hardening, according to the National Institute of Standards and Technology (NIST), is that it's "a process intended to eliminate a means of attack by patching vulnerabilities and turning off non-essential services."

Part of the system hardening elimination process involves deleting or disabling needless system applications, permissions, ports, user accounts, and other features so that attackers have fewer opportunities to gain access to a mission-critical or critical-infrastructure computer system's sensitive information.

But at its core, system hardening is a method for protecting a system against attacks perpetrated by cybercriminals. It involves securing a computer system's software mainly but also its firmware and other system elements to reduce vulnerabilities and a potential compromise of the entire system.

Now you know why system hardening exists, but you might be wondering about its practical purpose and why businesses and organizations implement system hardening practices.

The basic purpose of implementing system hardening techniques and practices is to simply minimize the number of potential entryways an attacker could use to access your system and to do so from inception. This is oftentimes referred to as following a secure-by-design philosophy.



Graphic: There are a few different types of system hardening, but they're all interrelated.

What are the types of system hardening?

System hardening involves securing not only a computer's software applications, including the operating system, but also its firmware, databases, networks, and other critical elements of a given computer system that an attacker could exploit.

There are five main types of system hardening:

- Server hardening
- Software application hardening
- Operating system hardening

- Database hardening
- Network hardening

It's important to note that the types of system hardening are broad enough to be universal and translate well across different server and computer system configurations; however, the methods and tools used to practically achieve a hardened or secure-by-design state vary widely.

But for now, let's review the purpose of each type of system hardening.

Server hardening

Server hardening is a general system hardening process that involves securing the data, ports, components, functions, and permissions of a server using advanced security measures at the hardware, firmware, and software layers.

These general server security measures include, but are not limited to:

- Keeping a server's operating system patched and updated
- Regularly updating third-party software essential to the operation of the server and removing third-party software that doesn't conform to established cybersecurity standards
- Using strong and more complex passwords and developing strong password policies for users
- Locking user accounts if a certain number of failed login attempts are registered and removing needless accounts
- Disabling USB ports at boot
- Implementing multi-factor authentication
- Using self-encrypting drives or AES encryption to conceal and protect sensitive information
- Using firmware resilience technology, memory encryption, antivirus and firewall protection, and advanced cybersecurity suites specific to your operating system, such as Titanium Linux

Software application hardening

Software application hardening, or just application hardening, involves updating or implementing additional security measures to protect both standard and third-party applications installed on your server.

Unlike server hardening, which focuses more broadly on securing the entire server system by design, application hardening focuses on the server's applications, specifically, including, for example, a spreadsheet program, a web browser, or a custom software application used for a variety of reasons.

At a basic level, application hardening involves updating existing or implementing new application code to further secure a server and implementing additional software-based security measures.

Examples of application hardening include, but are not limited to:

- Patching standard and third-party applications automatically
- Using firewalls
- Using antivirus, malware, and spyware protection applications
- Using software-based data encryption
- Using CPUs that support Intel Software Guard Extensions (SGX)
- Using an application like LastPass to manage and encrypt passwords for improved password storage, organization, and safekeeping
- Establishing an intrusion prevention system (IPS) or intrusion detection system (IDS)

Operating system hardening

Operating system hardening involves patching and implementing advanced security measures to secure a server's operating system (OS). One of the best ways to achieve a hardened state for the operating system is to have updates, patches, and service packs installed automatically.

OS hardening is like application hardening in that the OS is technically a form of software. But unlike application hardening's focus on securing standard and third-party applications, OS hardening secures the base software that gives permissions to those applications to do certain things on your server.

Oftentimes, operating system developers, such as Microsoft and Linux, do a fine and consistent job of releasing OS updates and reminding users to install these updates. These frequent updates - and we've all ignored them - can actually help keep your system secure and resilient to cyberattacks.

Other examples of operating system hardening include:

- Removing unnecessary drivers
- Encrypting the HDD or SSD that stores and hosts your OS
- Enabling and configuring Secure Boot
- Limiting and authenticating system access permissions
- Limiting or eliminating the creation and logging in of user accounts

Database hardening

Database hardening involves securing both the contents of a digital database and the database management system (DBMS), which is the database application users interact with to store and analyze information within a database.

Database hardening mainly involves three processes:

1. Controlling for and limiting user privileges and access
2. Disabling unnecessary database services and functions
3. Securing or encrypting database information and resources

Types of database hardening techniques include:

- Restricting administrators and administrative privileges and functions
- Encrypting in-transit and at-rest database information
- Adhering to a role-based access control (RBAC) policy
- Regularly updating and patching database software, or the DBMS
- Turning off needless database services and functions
- Locking database accounts if suspicious login activity is detected
- Enforcing strong and more complex database passwords

Network hardening

Network hardening involves securing the basic communication infrastructure of multiple servers and computer systems operating within a given network.

Two of the main ways that network hardening is achieved are through establishing an intrusion prevention system or intrusion detection system, which are usually software-based. These applications automatically monitor and report suspicious activity in a given network and help administrators prevent unauthorized access to the network.

Network hardening techniques include properly configuring and securing network firewalls, auditing network rules and network access privileges, disabling certain network protocols and unused or unnecessary network ports, encrypting network traffic, and disabling network services and devices not currently in use or never in use.

Using these techniques in combination with an intrusion prevention or intrusion detection system reduces the network's overall attack surface, and thus, bolsters its resistance to network-based attacks.

Photo: The NIST maintains one of several system hardening standards.

What are some system hardening standards?

Several industry standards and guidelines for system hardening exist. The National Institute of Standards and Technology (NIST), the Computer Information Security (CIS) Center for Internet Security, and Microsoft, for example, all maintain standards for system hardening best practices.

For example, system hardening best practices outlined by the NIST in Special Publication (SP) 800-123, a document focused entirely on system hardening, include:

- Establishing a system security plan
- Patching and updating the OS
- Removing or disabling unnecessary services, applications, and network protocols
- Configuring OS user authentication
- Configuring resource controls appropriately
- Selecting and implementing authentication and encryption technologies

Another example of a system hardening standard is CIS Benchmarks, an expansive collection of more than 100 system hardening configuration guidelines addressing vendor-specific desktops and web browsers, mobile devices, network devices, server operating systems, virtualization platforms, the cloud, and commonly used software applications.

The CIS Center's system hardening standards are accepted by government, business, industry, and academia. Relevant CIS benchmarks are available for download free of charge on the organization’s Free Benchmarks PDFs webpage.

How can I harden my system?

System hardening is a dynamic and variable process. One of the best ways to begin or expand upon the system hardening process is to follow a system hardening checklist or a system hardening standard, such as those published by the NIST or CIS Center.

Generally, how you harden your system depends on your server’s configuration, operating system, software applications, hardware, among other variables.

The system hardening standards and guidelines published by the NIST and CIS Center for Internet Security, for example, discuss system hardening techniques specific to Microsoft Windows, Unix, and Linux.

So, if you're curious about how to begin the system hardening process, reading the NIST's Special Publication 800-123 and the CIS Center for Internet Security's free benchmark PDFs is a good place to start. You can then, if necessary, consult with an experienced cybersecurity professional on how to move forward with implementing these standards' recommended processes and best practices within your business or organization.

There are some common and transferrable system hardening practices of which you should be aware, however. We've put a few best practices in the checklist below.

A good system hardening checklist usually contains the following action items:

1. Have users create strong passwords and change them regularly
2. Remove or disable all superfluous drivers, services, and software
3. Set system updates to install automatically
4. Limit unauthorized or unauthenticated user access to the system
5. Document all errors, warnings, and suspicious activity

Photo: Trenton Systems' 3U BAM Server, a hardened, cyber-resilient rugged server.

Conclusion: Trenton Systems hardens its servers from inception.

Trenton Systems partners with leading cybersecurity companies and is able to make changes to its server hardware, firmware, and software in an effort to further secure, or harden, its servers and workstations.

The 3U BAM Server is our most recent shining example of trusted computing and system hardening. The BAM is secured by Intel PFR, Intel SGX, and Intel TME, and we can even make changes to its ports, further secure its BIOS, among other enhancements, to ensure that your BAM server is as cyber-resilient as possible.

In addition, Star Lab, a Wind River company and Trenton Systems software technology partner, offers the Titanium Security Suite for Linux operating systems. Through our partnership with Star Lab, we can incorporate this suite for customers upon request. We can also incorporate FUTURA Cyber's self-encrypting drive security manager to assist with the management of FIPS 140-2 SEDs.

For more information about acquiring a secure, hardened rugged server or workstation, reach out to us. Our in-house cybersecurity experts and cybersecurity technology partners are here to assist you every step of the way.