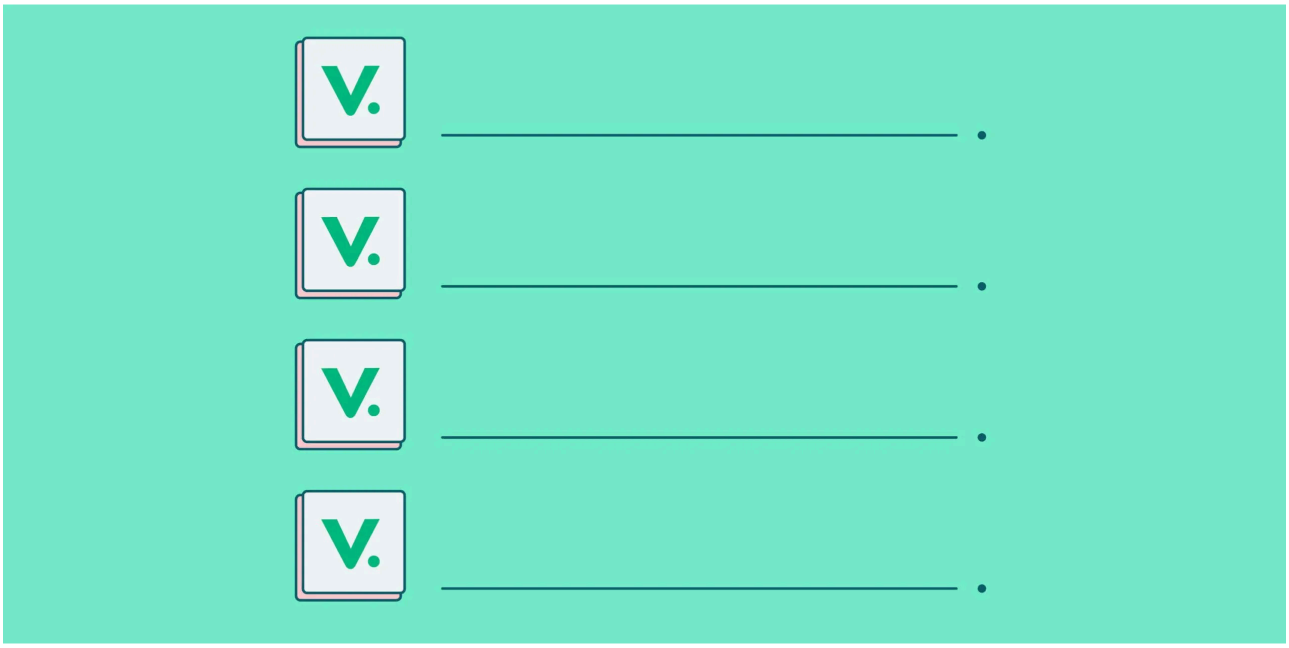
CIS Benchmarks: the ultimate guide

CIS benchmarks help minimize security risk by removing possible attack vectors and shrinking a system’s attack surface. Here's everything you need to know.



System hardening includes a set of best practices, tools, and approaches designed to reduce the vulnerability of technology applications, systems, and infrastructure. System hardening with resources such as CIS Benchmarks minimizes security risk by removing possible attack vectors and shrinking a system’s attack surface.

This blog will explore the fundamentals of CIS benchmarks – what they are and how to implement them for better system hardening.

What you’ll learn

What is system hardening?

The attack surface of a web application includes security vulnerabilities such as unpatched software and firmware, unsafe configuration, insecure logins (i.e., using hardcoded and default passwords), credentials stored in plain text, and inadequate data encryption in transit as well as at rest. System hardening uncovers and fixes these vulnerabilities, thereby reducing and eventually eliminating the attack surface.

The goal is to secure servers or computers by minimizing their attack surface, vulnerability, and potential attack vectors. It eliminates the flaws in the system that cyber attackers can exploit to access sensitive user data.

To make it more difficult for malware and attackers to access your computer environment, you must remove all problematic defaults/configurations, functions, programs, applications, ports, and permissions.

Some types of system hardening include:

- Server hardening
- Operating system hardening
- Database hardening
- Network hardening
- Application hardening

What are CIS Benchmarks?

The Center for Internet Security (CIS) Benchmarks include a set of best practices used to secure a target system's configuration. The Center for Internet Security that designed these benchmarks is a non-profit organization made up of cyber-security professionals and experts from around the world. These guidelines are best practices, consensual security configuration guidelines endorsed by academia, industry, government, and business.

CIS guidelines are considered by many compliance standards—including HIPAA, PCI DSS, SRG, and NIST, to name a few—as the industry standard for hardening systems and hardware.

Why should you use the CIS Benchmarks?

CIS Benchmarks are fundamental to safety and compliance and are among the recommended security configuration and best practices endorsed by industry, academia, and government for configuring a target system. A CIS framework provides a standard way to configure common digital assets, from operating systems to cloud infrastructure. This ensures that the enterprises don't need to reinvent the wheel and provides a clear roadmap to minimize their attack surface.

How do you implement CIS benchmarks?

You can implement CIS Benchmarks using any of the following tools:

- **CIS CSAT:** Free web application ideal for tracking and prioritizing CIS controls implementation.
- **CIS-CAT® Pro:** Helps organizations achieve their cyber security goals and evaluate target system security states.
- **CIS Build Kits:** Automated, scalable tool containing a subset of the recommendations within the CIS Benchmark.
- **CIS-CAT Lite:** Free tool to start implementing CIS frameowkrs quickly.

There are many open-source tools available as well. Among some of the more popular tools for implementing CIS Benchmarks are CIS_benchmarks_audit, Docker Bench for Security, Dockle, and Sebaz.

Introducing Critical CIS Controls

The CIS Controls are a prioritized list of categories that form an in-depth defense set of best practices to mitigate most attacks on systems and networks. These internationally recognized security best practices are created by a group of IT experts. These experts develop the CIS Controls from many sectors, including government, defense, manufacturing, healthcare, and education.

Reduce your attack surface with system hardening

System hardening involves protecting your applications, operating systems, databases, networks, firmware, and other essential components of a computer system that an attacker can exploit. In this section, we'll examine how system hardening can help reduce the attack surface of your computer system.

What is the importance of system hardening?

Hardening is an essential step in increasing your organization's overall security. Hardening standards provide baseline settings and guidelines for organizations to use in hardening their systems. Failure to comply with these standards can have serious consequences, such as a complete organizational breach. In terms of security, system hardening is a necessary antecedent to defensive solutions such as firewalls and EDRs.

No matter how much money has been spent on cyber security technology, if a system has not been appropriately hardened, it is not safe. It will never be safe unless it is configured and maintained in accordance with the best practices. Key compliance frameworks, such as PCI-DSS, HIPAA, and FedRAMP, designate CIS benchmarks as established best practices. It is therefore essential to meet the CIS framework's criteria if your business wants to comply with one or several frameworks.

Establishing a system hardening baseline

To engage in system hardening, the first thing you must do is establish a baseline. This requires a preliminary evaluation of system "hardness" against a best practice framework. A manual or solution-assisted examination of systems and assets is needed to determine how well they comply with the appropriate CIS Benchmarks. The baseline is established based on the results of the first assessment as well as documentation of areas in which the configuration falls short of the benchmark.

How to harden a network

Network hardening is the process of safeguarding the underlying communication infrastructure of various servers and computer systems that are connected to a network.

Network hardening can be accomplished in two ways:

- By constructing an intrusion prevention system
- By constructing an intrusion detection system

Both options are often software-based. These programs automatically monitor networks and report suspicious activity to administrators, preventing unwanted network access.

Protect VM images with CIS hardening

CIS Hardened Images refer to VM images that have been set up in accordance with security standards, based upon the relevant CIS Benchmark. CIS provides virtual images that have been hardened according to the CIS Benchmarks. These are internationally recognized, vendor-agnostic guidelines for secure configuration.

CIS Hardened Images offer users a secure, scalable, and on-demand computing environment. They are offered by all leading cloud computing platforms, including AWS, Azure, GCP, and Oracle Cloud.

The advantages of CIS Hardened Images include:

- Images have been certified to conform with CIS Benchmarks.
- It takes less time and effort than hardening a base image.

CIS Cloud Security Control recommendations

CIS Cloud Security Control recommendations to improve cloud security include:

- Establish and activate monitoring and alerting.
- Take advantage of AWS CloudTrail or Google Cloud's Operations Suite to enable Cloud Control Plane logging.
- Build industry-compliant, secure cloud workloads that follow the recommended hardening standards and best practices.
- Enable robust authentication for every cloud administrative interface, including the web portal and command line.
- Enable cloud storage encryption and other data security precautions.
- Secure cloud-native network access controls in order to restrict network traffic and monitor network activity.
- Implement identity policies based on least privilege for various cloud operational roles.

CIS Benchmarks Levels 1 and 2 recommendations

CIS standards specify two levels of security. These include:

- **Level 1:** Proposes necessary basic security criteria that may be enabled on any system and should result in little or no service disruption or diminished functionality.
- **Level 2**: Level 2 security settings are recommended for areas needing increased security, which may result in some restricted functionality.

CIS also provides resources for configuring systems per STIGs, both on-premises and in the cloud. The CIS STIG Benchmarks and related CIS Hardened Images feature a Level-3 profile that incorporates additional requirements from STIG. If you use the recommendations of a CIS framework and require STIG compliance, you should use the three profiles to fill in gaps between STIGs and the original CIS Benchmark profiles.

Checklist for system hardening

System hardening is a dynamic process that requires a thorough examination of digital assets and the dangers they pose to *your* organization. A good CIS server hardening checklist should include:

-
    - **Conduct a vulnerability assessment of your servers:** This is one of the easiest ways to get started with system hardening.
    - **Follow a system hardening checklist:** This is the next step. Such checklists are available through CIS or NIST. Based on this, you can then make the changes applicable to your environment.

- **Automation:** While system hardening can be a complex process, you can automate part of it. This can be achieved using automated vulnerability scanners to check if any new or updated applications threaten its security. You also take advantage of patch management software to distribute security patches and upgrades to systems and servers automatically.

CIS benchmarks: next steps

Recently, we’ve been witnessing some of the most significant vulnerabilities that have threatened to expose massive amounts of data. We’re not yet where we should be, as far as protecting our online ecosystems against such attacks is concerned. The good news is that you can take advantage of CIS Controls to safeguard your critical assets, even with budget constraints.

The CIS Controls provide uniform cyber security standards across organizations of all sizes, helping them stay protected from the evolving cyber threat landscape. When adequately implemented alongside a mature cyber risk management program, these CIS hardening controls can make it exceptionally difficult for hackers to breach your security landscape.

FAQs

What is the difference between CIS and NIST?

CIS (Center for Internet Security) and NIST (National Institute of Standards and Technology) are both organizations that provide guidance and resources for information security. The main difference between the two is that CIS focuses on enhancing cybersecurity readiness and response, while NIST provides a comprehensive framework for managing cybersecurity risk. CIS provides resources such as benchmark standards and checklists, while NIST offers guidelines, standards, and best practices to help organizations identify, assess, and manage cybersecurity risks. While both organizations offer valuable resources, the choice between them often depends on the specific needs of the organization and the industry in which it operates.

What is the difference between STIG and CIS benchmarks?

The CIS Benchmarks are security configuration guides that are developed and accepted by a consensus of government, business, industry, and academia, and are not tied to any particular vendor. The STIG is a set of configuration standards for DOD IA and IA-enabled devices or systems. It should be noted that cloud environments and operating systems are not secure by default.

Is data recovery part of CIS?

Center for Internet Security (CIS) Control 11, which has been recently updated and renumbered, emphasizes the importance of having backups to ensure the timely and seamless recovery of data in the event of a security breach or misconfiguration.