SmartSuite

Framework / Cybersecurity / CIS Controls

CIS Benchmarks

CIS Benchmarks are consensus-developed secure configuration guides for specific technologies, with Level 1, Level 2 and STIG profiles.



What it is

The CIS Benchmarks are secure configuration guides, developed by the Center for Internet Security (CIS) through a consensus process of cybersecurity professionals and subject matter experts, that tell an organization exactly which settings to apply to harden a specific technology such as an operating system, cloud platform, database, browser or network device. CIS says they cover more than 25 vendor product families, and they are distributed free of charge in PDF format.

CIS, a nonprofit organization, publishes them and develops them with volunteer experts, technology vendors and the CIS Benchmark development team. They are voluntary and not a certification, and they do not bind an organization by law, although audits and contracts often name them.

At a glance

PUBLISHER Center for Internet Security (CIS)	TYPE Guidance	VERSION Versioned per technology; new releases announced monthly
EFFECTIVE Continuously released	DOMAIN Cybersecurity	FAMILY CIS Controls
REGION United States	ADOPTION MODEL Voluntary	IMPLEMENTATION COMPLEXITY Medium

Source: cisecurity.org/cis-benchmarks

Why it matters

- **Prescriptive, platform-specific settings** Each Benchmark targets a single product and version and lists recommendations with the setting, rationale, audit procedure and remediation.
- **Profiles for different risk** Level 1 is a base recommendation that can be implemented fairly promptly, and Level 2 is defense in depth for environments where security is paramount.
- **STIG alignment** Where a DISA STIG exists, a STIG profile provides all the recommendations that are STIG specific.
- **Consensus, not vendor opinion** Benchmarks are developed through a consensus process of cybersecurity professionals and subject matter experts.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports CIS Benchmarks

Benchmark and Profile Selection

Record which CIS Benchmark, version and profile (Level 1, Level 2 or STIG) applies to each platform in scope.

Configuration Baselines

Document the hardened configuration and approved settings per platform, with version history.

Scan Results and Evidence

Attach scan outputs from CIS-CAT Pro or another assessor to each recommendation and platform.

Exceptions and Compensating Controls

Capture each exception with approval, rationale, compensating control and expiry date.

Drift Reviews

Schedule recurring reviews to detect configuration drift and adopt new benchmark versions.

Coverage Reporting

Report conformance, exceptions and remediation status by platform and team on a dashboard.

Common framework mappings

CIS Controls v8.1 | ISO 27001:2022 | ISO 27002:2022 | NIST CSF 2.0 | NIST 800-53 Rev.5 | PCI DSS 4.0.1 | SOC 2 | FedRAMP Rev. 5 | HIPAA (NIST SP 800-66 Rev. 2)

Official resources

CIS Benchmarks Overview

Provides a comprehensive introduction to CIS Benchmarks and their application in cybersecurity.

cisecurity.org/cis-benchmarks

CIS Benchmark Level 1 and Level 2 Details

Defines Level 1 and Level 2 benchmark specifications for secure configurations.

cisecurity.org/benchmark

CIS Benchmarks FAQ

Answers common questions about what the Benchmarks cover, how Level 1 and Level 2 profiles differ, and how to assess against them.

cisecurity.org/cis-benchmarks/cis-benchmarks-faq

CIS Benchmark Scoring Tool

Describes the tool for scoring compliance against CIS Benchmarks.

cisecurity.org/cybersecurity-tools/cis-cat-pro

Frequently asked questions

What are CIS Benchmarks?

Secure configuration guides for specific technologies, developed by the Center for Internet Security through a consensus process of cybersecurity professionals and subject matter experts. Each Benchmark lists the settings to apply to harden one product and version.

What is the difference between Level 1 and Level 2 profiles?

Level 1 is a base recommendation that can be implemented fairly promptly and lowers the attack surface while keeping machines usable. Level 2 is defense in depth for environments where security is paramount and can cause problems if not implemented with care.

What is the STIG profile in a CIS Benchmark?

It provides all the recommendations that are specific to the relevant DISA STIG. It replaced the earlier Level 3 profile, and overlapping Level 1 and Level 2 recommendations appear in it where applicable.

Are CIS Benchmarks free, and are they mandatory?

CIS distributes them free of charge in PDF format. CIS SecureSuite members can also download additional formats via CIS WorkBench and tailor recommendations. They are voluntary and not a certification.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How do CIS Benchmarks relate to the CIS Critical Security Controls?

The Benchmarks provide the platform-specific settings, and the Controls provide the broader program. For example, CIS Controls safeguard 4.1 asks an organization to establish and maintain a secure configuration process, and the Benchmarks supply the configurations.

License included / downloadable: No CIS distributes the Benchmarks free of charge in PDF format from cisecurity.org, and CIS SecureSuite members can download additional formats. The text is not included with the platform.

Full framework page and mappings: smartsuite.com/frameworks/cis-benchmark