Center for Internet Security (CIS) Benchmarks

The Center for Internet Security (CIS) has published a series of benchmarks for Microsoft products and services.

Microsoft and the CIS Benchmarks

The Center for Internet Security (CIS) has published benchmarks for Microsoft products and services including the Microsoft Azure and Microsoft 365 Foundations Benchmarks, the Windows 10 Benchmark, and the Windows Server 2016 Benchmark.

CIS benchmarks are internationally recognized as security standards for defending IT systems and data against cyberattacks. Used by thousands of businesses, they offer prescriptive guidance for establishing a secure baseline configuration. System and application administrators, security specialists, and others who develop solutions using Microsoft products and services can leverage these best practices to assess and improve the security of their applications.

Like all CIS benchmarks, the Microsoft benchmarks were created using a consensus review process based on input from subject matter experts with diverse backgrounds spanning software development, audit and compliance, security research, operations, government, and law. Microsoft was an integral partner in these CIS efforts. For example, Office 365 was tested against the listed services, and the resulting Microsoft 365 Foundations Benchmark covers a broad range of recommendations for setting appropriate security policies that cover account and authentication, data management, application permissions, storage, and other security policy areas.

In addition to the benchmarks for Microsoft products and services, CIS has also published CIS Hardened Images for use on Azure virtual machines configured to meet CIS benchmarks. These include the CIS Hardened Image for Microsoft Windows Server 2016 certified to run on Azure. CIS states that, "All CIS hardened images that are available on the Azure Marketplace are certified to run on Azure. They have been pre-tested for readiness and compatibility with the Azure public cloud, the Microsoft Cloud Platform hosted by service providers through the Cloud OS Network, and on-premise private cloud Windows Server Hyper-V deployments managed by customers."

Microsoft in-scope cloud services

- Azure and Azure Government
  Learn more
- Office and Microsoft 365
  Learn more
- SQL Server
- Windows 10
- Windows Server 2016

Audits, reports, and certificates

Get a complete list of CIS benchmarks for Microsoft products and services.

CIS Azure Foundations Benchmark
Learn more

CIS Microsoft 365 Foundations Benchmark
Learn more

Windows 10 Benchmark
Learn more

Windows Server 2016 Benchmark
Learn more

How to implement

CIS Benchmark for Azure
Get prescriptive guidance for establishing a secure baseline configuration for Azure.
Learn more

Office 365 security best practices
Minimize the potential of a data breach or compromised account by following these best practices.
Learn more

Windows security baselines
Follow these guidelines for effective use of security baselines in your organization.
Learn more

CIS Controls Cloud Companion Guide
"Get guidance on applying security best practices in CIS Controls Version 7 to cloud environments."
Learn more

About CIS Benchmarks

The Center for Internet Security is a nonprofit entity whose mission is to "identify, develop, validate, promote, and sustain best practice solutions for cyberdefense." It draws on the expertise of cybersecurity and IT professionals from government, business, and academia from around the world. To develop standards and best practices, including CIS benchmarks, controls, and hardened images, they follow a consensus decision-making model.

CIS benchmarks are configuration baselines and best practices for securely configuring a system. Each of the guidance recommendations references one or more CIS controls that were developed to help organizations improve their cyberdefense capabilities. CIS controls map to many established standards and regulatory frameworks, including the NIST Cybersecurity Framework (CSF) and NIST SP 800-53, the ISO 27000 series of standards, PCI DSS, HIPAA, and others.

Each benchmark undergoes two phases of consensus review. The first occurs during initial development when experts convene to discuss, create, and test working drafts until they reach consensus on the benchmark. During the second phase, after the benchmark has been published, the consensus team reviews the feedback from the internet community for incorporation into the benchmark.

CIS benchmarks provide two levels of security settings:

- Level 1 recommends essential basic security requirements that can be configured on any system and should cause little or no interruption of service or reduced functionality.
- Level 2 recommends security settings for environments requiring greater security that could result in some reduced functionality.

CIS Hardened Images are securely configured virtual machine images based on CIS Benchmarks hardened to either a Level 1 or Level 2 CIS benchmark profile. Hardening is a process that helps protect against unauthorized access, denial of service, and other cyberthreats by limiting potential weaknesses that make systems vulnerable to cyberattacks..

Frequently asked questions

Will following CIS Benchmark settings ensure the security of my applications?

CIS benchmarks establish the basic level of security for anyone adopting in-scope Microsoft products and services. However, they should not be considered as an exhaustive list of all possible security configurations and architecture but as a starting point. Each organization must still evaluate its specific situation, workloads, and compliance requirements and tailor its environment accordingly.

How often are CIS Benchmarks updated?

The release of revised CIS Benchmarks changes depending on the community of IT professionals who developed it as well as on the release schedule of the technology the benchmark supports. CIS distributes monthly reports that announce new benchmarks as well as updates to existing benchmarks. To receive these, register for the CIS Workbench (it's free) and check **Receive newsletter** in your profile.

Who contributed to the development of Microsoft CIS Benchmarks?

CIS notes that its "Benchmarks are developed through the generous volunteer efforts of subject matter experts, technology vendors, public and private CIS Benchmark community members, and the CIS Benchmark Development team." For example, you'll find a list of Azure contributors on CIS Microsoft Azure Foundations Benchmark v1.0.0 Now Available.

Additional resources

- CIS best practices for securely using Microsoft 365
- Windows 10 security policy settings
- Windows 10 enterprise security