

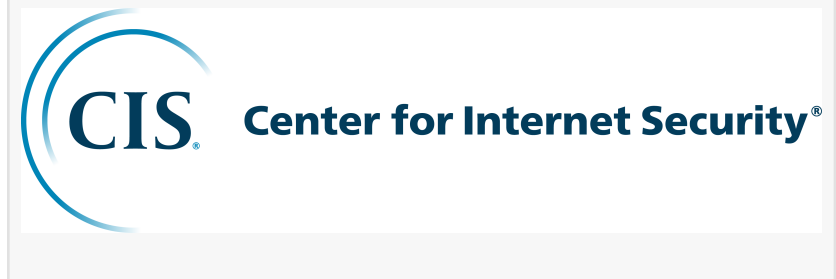
CIS Launches AI MCP Benchmark

New CIS Benchmark helps organizations securely connect AI assistants and agents to data, applications, and online services

CLIFTON PARK, NY, UNITED STATES,
September 16, 2026 /

EINPresswire.com/ -- The Center for Internet Security, Inc. (CIS®) today

announced the release of the [CIS MCP Server Benchmark v1.0.0](#), a consensus-developed set of best practices for securely configuring Model Context Protocol (MCP) servers, which enable AI assistants and agents to connect to data, applications, and other digital tools.



As organizations increasingly deploy AI-powered assistants and agents, securing the systems that manage those connections is becoming increasingly important. The CIS MCP Server Benchmark provides organizations with a vendor-neutral standard for helping protect sensitive data, control access to resources, and reduce security risks.

Developed against the current MCP specification, the Benchmark addresses both local and remote MCP deployments, including gateway and proxy technologies commonly used to secure and manage connections between AI systems and external resources.

CIS Benchmarks are globally recognized, consensus-developed best practices for securely configuring technologies and systems. The CIS MCP Server Benchmark includes 55 prescriptive recommendations across 10 security domains:

1. Governance and Versioning
2. Transport and Connectivity
3. Authentication and Authorization
4. Client (Host) Configuration
5. Server Configuration
6. Data Protection and Privacy
7. Observability and Audit
8. Supply Chain Security
9. Isolation and Execution Safety
10. Resource Limits and Caching

Each recommendation includes a rationale, audit procedure, and remediation guidance to support implementation and assessment.

"As organizations continue adopting AI agents, securing the systems that connect them to enterprise resources is essential," said Erin Haggerty, Director of the Cloud Team at CIS. "The CIS MCP Server Benchmark provides clear, actionable guidance to help organizations deploy MCP securely and reduce risk."

MCP is increasingly being used to connect AI systems to databases, file systems, cloud services, browsers, and other business resources. Because MCP servers often provide access to sensitive systems and data, misconfigurations can create opportunities for unauthorized access, data exposure, tool manipulation, and execution of untrusted code.

The CIS MCP Server Benchmark provides specific, testable recommendations that organizations can use to assess, audit, and strengthen the security of their MCP server deployments. The CIS MCP Server Benchmark v1.0.0 is available for free download.

To learn more, download the Benchmark, or participate in future Benchmark development efforts, visit [CISecurity.org/Benchmarks](https://cisecurity.org/Benchmarks).

###

About CIS:

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation. We are a community-driven nonprofit, responsible for the CIS Critical Security Controls® and CIS Benchmarks®, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud. CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. election offices. To learn more, visit or follow us on X: [@CISecurity](https://twitter.com/CISecurity).

Kelly Wyland

Center for Internet Security

[email us here](#)

Visit us on social media:

[LinkedIn](#)

[Instagram](#)

[Facebook](#)

[YouTube](#)

[X](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/942834622>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.