

AI Security Server



Overview

This guide examines the 15 best solutions for securing AI agents in 2026, spanning enterprise MCP gateways and dedicated security platforms. Security researchers with AI security startup Cyata this week reported finding three vulnerabilities in the Git MCP server maintained by Anthropic, the AI company that created the Model Context Protocol to give AI models and agents a standardized way of accessing external data, tools, and services. Connectivity cloudCloudflare's connectivity cloud delivers 60+ networking, security, and performance services. Find a partnerPowerUP your business - connect with Cloudflare Powered+ partners. Secure AI interactions by controlling data and managing risk across your AI lifecycle. Qualys TotalAI now provides layered discovery of MCP servers across network, host, and supply. Employees are adopting AI tools in every channel that they work, often without the knowledge of security teams. And autonomous agents are connecting to enterprise systems. AI Security and Anomaly Detection is a market focused on providing runtime protection and monitoring for AI applications, particularly those using generative models like large language models (LLMs). These solutions detect and mitigate risks such as prompt injection, hallucinations, toxicity. Microsoft Security Dashboard for AI is a unified security dashboard that helps security leaders understand and address the AI risk in their organization. The dashboard equips leadership with a governance tool that provides clear and comprehensive AI security insights and answers the most pressing.

Article Content

Released: December 2025 Exchange Server Security

We have released Security Updates for Exchange Server SE. Exchange Server 2019 and 2016 ESU updates only.

Released: February 2026 Exchange Server Security

Exchange Server 2016 and 2019 are out of support. Customers who enrolled in the Extended Security Update (ESU) program are eligible to receive

Assess your organization's AI risk with Microsoft

Use the Microsoft Security Dashboard for AI dashboard to discover, assess, and mitigate AI risks across your organization.

Windows Server 2025 security baseline 2602: 10 new

Microsoft released version 2602 of the Security Baseline for Windows Server 2025, approximately eight months after the previous version

Best MCP Gateways and AI Agent Security Tools (2026)

As AI agents evolve from simple chatbots to autonomous systems managing critical business operations, two infrastructure layers have emerged

CISA Warns of Microsoft Exchange Server Vulnerability Exploited in

CISA has issued a fresh warning about a newly disclosed Microsoft Exchange Server vulnerability that is already being exploited in real-world attacks, raising concerns for organizations

ServiceNow Knowledge 2026: AI Control Tower, Action Fabric,

ServiceNow expanded its AI Control Tower with new integrations, observability and governance tools and features to measure the value of AI agents. The company also expanded its

Salt Security: Agentic AI Security, MCP Discovery, and

Salt Security is the only holistic AI security solution for the entire agentic AI lifecycle, from API discovery to posture management to threat protection.

Unified AI Security Platform for Enterprise Protection

Secure every AI interaction across your organization with unified discovery, runtime enforcement, and a defensible audit trail See Discover and inventory every AI application, agent, MCP server, toolchain,

August 2025 Exchange Server Security Updates

Microsoft releases August 2025 Exchange Server Security Updates for vulnerabilities found in Exchange Server SE/2019/2016.

Microsoft Releases New Defender Update for Windows 11, 10, and Server ...

Microsoft has officially rolled out its latest security intelligence update for Microsoft Defender Antivirus, delivering crucial protections for Windows 11, Windows 10, and Windows Server

Extended Security Updates for Windows Server overview

Extended Security Updates for Windows Server help you stay protected after end of support. Learn how to upgrade or migrate to Azure for continued security.

December 2025 Exchange Server Security Updates

Microsoft releases December 2025 Exchange Server Security Updates for vulnerabilities found in Exchange Server SE/2019/2016.

AI Security Suite | Solution for scaling AI adoption | Cloudflare

Secure AI interactions by controlling data and managing risk across your AI lifecycle. Cloudflare AI Security Suite offers a unified platform for securing workforce AI tools and public-facing applications.

spring-projects/spring-authorization-server

Spring Authorization Server has moved to Spring Security 7.0. The 1.5.x branch is the last generation of Spring Authorization Server. See the OSS and Enterprise

How AI Enhances Server Security Protocols

This article explores how AI enhances server security protocols by embedding intelligence into every layer of defense — from threat detection and response to access control, encryption, and...

Critical Microsoft Exchange Server Vulnerability Actively Exploited in ...

Microsoft Exchange Server spoofing flaw, is being actively exploited against on-premises systems before a permanent patch is available.

The MCP Server for Wiz: Smarter AI, Stronger Security

Today, we're excited to announce the launch of the Model Context Protocol (MCP) Server for Wiz, now available in preview for our customers. ...

Kali Linux Enhances AI-driven Penetration Testing with

This setup demonstrates a viable, privacy-preserving alternative to cloud AI assistants for offensive security work. According to the Kali Linux

Anthropic, Microsoft MCP Server Flaws Shine a Light on AI Security ...

Post 1AI agents and MCP servers promise powerful automation, but they also introduce new and unfamiliar attack surfaces. According to recent findings highlighted by Security Boulevard,

OpenClaw Chain Vulnerabilities Expose 245,000 Public AI Agent Servers ...

A chain of four critical vulnerabilities discovered in OpenClaw, one of the fastest-growing open-source platforms for autonomous AI agents, has left an estimated 245,000 publicly accessible

KB5090407

For installation instructions and direct links to the CU package downloads, see the SQL Server 2019 Release Notes. More information Prerequisites To apply this update, you must have

Addressing Exchange Server May 2026 vulnerability CVE-2026-42897

Addressing the vulnerability permanently Microsoft is working on and will release and announce a security update for impacted versions of Exchange Server in the future. Update will be

Microsoft Defender Antivirus on Windows Server

Update antimalware security intelligence To get your regular security intelligence updates, the Windows Update service must be running. If you use an update management service,

MCP Servers Are the New Shadow IT for AI

What are MCP servers, and why are they a security risk? MCP servers act as an integration layer between AI clients and enterprise systems,

KB5090407

To update SQL Server 2019 on Linux to the latest CU, you must first have the Cumulative Update repository configured. Then, update your SQL Server packages by using the appropriate

Best AI Security and Anomaly Detection Reviews 2026

Find the top AI Security and Anomaly Detection with Gartner. Compare and filter by verified product reviews and choose the software that's right for your organization.

Contact Us

For more information, pricing, or custom solutions, please contact us:

Website: <https://www.truhope.co.za>

Email: sales@truhope.co.za

Phone: +27 64 987 3021

Address: 22 Loop Street, Cape Town, 8001, South Africa

This document is for informational purposes only. Specifications subject to change without notice.

