Adam Tas Corridor Energy

Security Issues in AI Server Deployment

Overview

The Cisco and AWS partnership addresses three challenges enterprises face when scaling AI agents: visibility gaps, security bottlenecks, and compliance risks. In this post, we explore how you can overcome AI security challenges through automated scanning and unified governance. The Agent-to-Agent (A2A) Protocol followed in April 2025, enabling autonomous agents to communicate directly without human intervention. As organizations adopt AI capabilities at an unprecedented rate, security teams must proactively gain visibility into AI usage and implement appropriate controls to mitigate risks. Whether you trained the model, fine-tuned it, or connected it to a RAG (Vector DB), that data likely has PII, privacy concerns and other sensitive information in it. Shadow AI refers to the unregulated use of AI technology within organizations, often without official oversight or security measures. In enterprise contexts, these systems often draw on vast stores of internal data: ranging from documents.

Security Issues in AI Server Deployment

KB5087541: May 2026 Security Patch - Windows Server 2022 23H2

KB5087541 is a May 12, 2026 security update for Windows Server 2022 23H2 Edition that addresses critical security vulnerabilities and updates the OS build to 25398.2330. This update

Office 2016/2019 have reached end of support - here's

Security fixes for vulnerabilities that are discovered and that may make devices, apps, or servers more directly exposed to security breaches. Bug

Secure AI Deployment Strategies: From IDEs to Public Model Risks

Whether hosted on-premises or via SaaS, AI models require secure deployment strategies. This article provides insight into threats like model backdoors, IDE-based leakage, and

9 Linux Dedicated Server Hosting Providers , Cherry

Linux dedicated servers give you full control, strong security, and reliable performance for

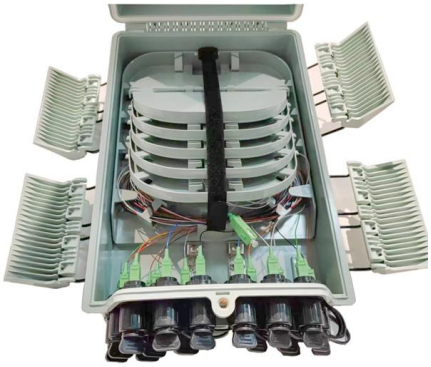
demanding projects. They are a solid choice for running

OneUptime , The Open-Source Observability Platform

OneUptime is an open-source complete observability platform. Monitor websites, APIs, and servers. Get alerts, manage incidents, and keep customers informed

KB5087538: May 2026 Security Update - Windows 10/Server 2019

KB5087538 is a May 2026 security update that addresses multiple vulnerabilities in Windows 10 Version 1809 and Windows Server 2019, including critical security fixes for Windows

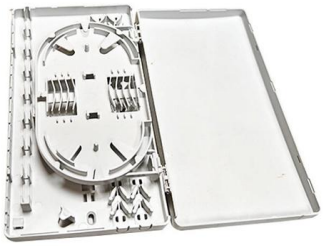


Security Issues in Cloud Computing

In this, we will discuss the overview of cloud computing, its need, and mainly our focus to cover the security issues in Cloud Computing. Let's discuss it

Navigating secure AI deployment: Architecture for

In this article, we'll examine the architectural considerations for deploying AI systems that are both secure and safe. A resilient AI architecture



State of AI trust in 2026: Shifting to the agentic era

AI trust is increasingly viewed as a business enabler rather than a compliance exercise. The state of AI trust today: Scrambling to keep up with the pace of change The AI Trust Maturity

Welcome to Channel Dive , Channel Dive

Welcome to Channel Dive. We're Informa TechTarget's new publication, focused on delivering daily news and analysis for executives at North

Securing AI Agents and MCP Servers: A

This comprehensive guide explores the unique security challenges posed by AI agents and MCP servers, providing practical strategies and

Deploy the Azure MCP Server as a remote MCP server

Deploy the Azure MCP Server over HTTPS as a self-hosted remote server. This setup lets AI agents in Microsoft Foundry and Microsoft Copilot

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

Why Server Security Risks Threaten AI Data Safety

Server security risks can significantly impact AI data safety, disrupting operations and compromising sensitive information. Understanding these risks is crucial to developing

How to Ensure AI Data Security in Enterprise

Discover critical data risks before deploying AI systems: data leakage, poisoning attacks, and quality issues. Learn how to mitigate these

Guidelines for Secure AI Systems Guidelines for Secure Develop

The organization's security policies should be updated to address the specific requirements of AI services, ensuring that all employees and contractors are familiar with them.

Choose your n8n , n8n Docs

Setting up and configuring servers and containers Managing application resources and scaling Securing servers and applications Configuring n8n n8n recommends self-hosting for expert users. Mistakes

Securing AI agents: How AWS and Cisco AI Defense scale MCP and

The Cisco and AWS partnership addresses three challenges enterprises face when scaling AI agents: visibility gaps, security bottlenecks, and compliance risks. In this post, we explore how you

8 Real World Incidents Related to AI

A list of 8 real world incidents related to AI from the past 24 months, highlighting the risk of using and deploying AI without safety and security measures

May 12, 2026--KB5087544 (OS Builds 19045.7291 and 19044.7291)

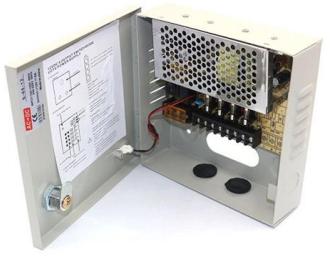
This security update includes fixes and quality improvements that are part of the following updates: April 14, 2026--KB5082200 (OS Builds 19045.7184 and 19044.7184) The following is a

Java

Automate WildFly deployments with Ansible Learn how to automate WildFly deployments using Ansible's middleware collection. Deploy enterprise

Deploy Microsoft Defender endpoint security to Windows devices

For more information about Defender endpoint security for Windows 7 SP1 and Windows Server 2008 R2 devices, see Deploy the Defender endpoint security solution for Windows 7 SP1 and



Azure AI security best practices , Microsoft Learn

This article provides best practices for securing artificial intelligence (AI) workloads specifically in Azure. As organizations adopt AI capabilities at an

Joint Guidance on Deploying AI Systems Securely

The guidance provides best practices for deploying and operating externally developed artificial intelligence (AI) systems and aims to: Improve the confidentiality, integrity, and availability of

Best practices on securing your AI deployment

Discover the crucial role of trust in securing gen AI deployments and learn how

Five Eyes warn agentic AI is too dangerous for rapid rollout

Much of the advice targets developers who deploy AI, but the authors also urge vendors to ensure they test their wares thoroughly and ensure their products "fail-safe by default requiring

Contact Us

For datasheets, pricing, or custom telecom energy solutions, please visit: https://www.koskolong.co.za