# Cisco unveils AI Defense to enhance security for enterprises using AI



Security and networking giant Cisco has unveiled its latest innovation, Cisco AI Defense, designed to enhance the security framework surrounding enterprise applications that leverage artificial intelligence. This launch comes at a time when businesses across various sectors are increasingly integrating AI technologies into their operations, thus facing an array of new security challenges.

As organisations embrace AI, the accompanying risks have become apparent. Traditional security measures often fall short in addressing the complexities introduced by AI systems. The Cisco AI Defense solution aims to bridge this gap by providing enterprises with tools that facilitate the secure development, deployment, and monitoring of AI applications. According to Cisco, this new service is structured to mitigate various risks associated with AI technologies.

The functionality of Cisco AI Defense is focused on two primary domains: the protection of AI application development and deployment, and the ongoing monitoring of AI usage within corporate environments. This includes a robust capability to discern between sanctioned and unsanctioned AI applications operating within both public and private cloud infrastructures. The platform employs automated testing methods to identify potential vulnerabilities, thereby reinforcing security measures.

Cisco AI Defense specifically addresses several cybersecurity threats such as prompt injection, data leakage, and denial-of-service attacks. The solution also provides security teams with essential tools to create and enforce policies aimed at preventing data poisoning and safeguarding sensitive information. One of the critical features of the system is its ability to deliver comprehensive visibility into AI application usage across an enterprise, ensuring compliance through its integration with Cisco’s broader security ecosystem.

In a shift from models that are often bound to specific AI applications, Cisco AI Defense is equipped to support multiple AI frameworks. It is built into the Cisco Security Cloud platform, utilising the company's proprietary machine learning models and threat intelligence to adapt dynamically to the ever-evolving landscape of cybersecurity threats.

Jeetu Patel, Executive Vice President and Chief Product Officer at Cisco, remarked, “Cisco AI Defense combines the unique ability to detect and protect against threats when developing and accessing AI applications without tradeoffs.” This commentary highlights the platform's dual capacity to enhance security while preserving operational efficiency, reflecting Cisco's commitment to addressing the complexities of modern AI deployment.

The introduction of Cisco AI Defense solidifies the company's position as a key player in the cybersecurity domain, particularly at a time when AI is rapidly transforming business practices and creating new avenues for both growth and vulnerability.

Source: [Noah Wire Services](https://www.noahwire.com)

## References

* <https://www.cybersecuritydive.com/spons/enterprises-are-embracing-ai-but-can-they-secure-it/716362/> - This article explains the security challenges associated with AI adoption in enterprises, including the need for visibility, controls, and continuous monitoring, which aligns with the security features of Cisco AI Defense.
* <https://perception-point.io/guides/ai-security/ai-security-risks-frameworks-and-best-practices/> - This guide details AI security risks such as data breaches, unauthorized access, and data manipulation, which are addressed by the security measures in Cisco AI Defense.
* <https://perception-point.io/guides/ai-security/top-6-ai-security-risks-and-how-to-defend-your-organization/> - This article outlines key AI security risks like adversarial attacks, data poisoning, and model theft, which Cisco AI Defense is designed to mitigate.
* <https://www.cybersecuritydive.com/spons/enterprises-are-embracing-ai-but-can-they-secure-it/716362/> - The article discusses the importance of real-time protection and continuous monitoring for AI applications, features that are integral to Cisco AI Defense.
* <https://perception-point.io/guides/ai-security/ai-security-risks-frameworks-and-best-practices/> - This resource emphasizes the need for robust encryption, secure communication protocols, and compliance with data protection regulations, all of which are relevant to the security framework of Cisco AI Defense.
* <https://perception-point.io/guides/ai-security/top-6-ai-security-risks-and-how-to-defend-your-organization/> - The article highlights best practices such as implementing data handling and validation, limiting application permissions, and ensuring diversity in training data, which are aligned with the capabilities of Cisco AI Defense.
* <https://www.cybersecuritydive.com/spons/enterprises-are-embracing-ai-but-can-they-secure-it/716362/> - The article discusses the concept of 'Secure by Design' and protecting AI applications from both traditional and AI-specific attacks, which is a core aspect of Cisco AI Defense.
* <https://perception-point.io/guides/ai-security/ai-security-risks-frameworks-and-best-practices/> - This guide mentions the importance of regular security audits and compliance with data protection regulations, which are essential components of the Cisco AI Defense solution.
* <https://perception-point.io/guides/ai-security/top-6-ai-security-risks-and-how-to-defend-your-organization/> - The article discusses the use of AI-driven security solutions and continuous monitoring, which are key features of Cisco AI Defense in enhancing security and preventing various AI-related threats.
* <https://www.cybersecuritydive.com/spons/enterprises-are-embracing-ai-but-can-they-secure-it/716362/> - The article emphasizes the need for controls to enforce corporate security policies and limit access to confidential data, which is a primary function of Cisco AI Defense.