Competitive Overview

AI Aware

in Tenable Vulnerability Management

Q: What is Tenable AI Aware?

- Tenable AI Aware is a feature within Tenable Vulnerability Management and Tenable Security Center that helps organizations monitor and mitigate the risks associated with the rapid adoption of AI technologies. It leverages advanced detection technologies, including agents, passive network monitoring, dynamic application security testing, and distributed scan engines, to identify unauthorized AI solutions, detect AI vulnerabilities, and illuminate unexpected AI or Large Language Model (LLM) development. AI Aware provides a comprehensive security-first approach to managing AI-related risks by offering deep visibility into AI software, libraries, and browser plugins across an organization's digital ecosystem.

Q: How is Tenable's AI Aware feature different from what's currently available in the market?

- Tenable AI Aware stands out from the competition due to its **multi-layered detection capabilities**, which provide unmatched visibility and control over AI-related risks. While other solutions in the market may focus on specific aspects of AI risk management, Tenable AI Aware offers a more **holistic approach** by combining multiple detection methods and integrating with existing vulnerability management frameworks.
- Unlike competitors that may focus on specific aspects of AI security, Tenable AI Aware offers broad detection capabilities that cover unauthorized AI software, browser plugins, and AI-related vulnerabilities. Leverages Tenable's established vulnerability management platforms, providing a unified approach to managing AI risks alongside other security concerns. Combines data from various detection methods (agents, passive network monitoring, dynamic application security testing, and distributed scan engines) to provide a complete picture of AI-related risks.
- While Tenable AI Aware excels in AI-specific detection, it may not have the same depth of model integrity monitoring and regulatory compliance features as some competitors, like Qualys Total AI. Organizations not already using Tenable's ecosystem may face a learning curve in fully leveraging the capabilities of AI Aware compared to standalone solutions like those from Qualys or Darktrace.

Competitive Analysis

1. *Qualys Total AI*: Web Page

- **Qualys Total AI** is a solution designed to secure AI applications, models, and data across various environments, including on-premises, cloud, and hybrid setups. It focuses on identifying AI vulnerabilities, monitoring AI model integrity, and ensuring compliance with AI-related regulations. Qualys Total AI provides strong capabilities in monitoring AI applications and models, ensuring their integrity, and detecting potential threats. Emphasizes compliance with AI-related regulations, which is critical for organizations in heavily regulated industries. Qualys Total AI benefits from seamless integration with the broader Qualys Cloud Platform, offering a unified security and compliance solution.
- Qualys Total AI's primary focus is on AI applications and models, which may leave gaps in broader ecosystem monitoring, such as detecting unauthorized AI software or browser plugins. While Qualys Total AI is robust in monitoring AI models, it lacks the depth of detection for unauthorized AI solutions, especially at the network and endpoint levels.
- *Tenable AI Aware* offers broader detection capabilities across the entire ecosystem, including unauthorized AI software, browser plugins, and AI-related vulnerabilities in web applications. It also excels in combining data from various detection technologies, providing a more holistic view of AI-related risks. While Qualys focuses more on model integrity and compliance, Tenable AI Aware is stronger in detecting unauthorized AI usage and monitoring broader ecosystem impacts.

2. Other Competitors

- **CrowdStrike**: Web Page
  Focuses on endpoint security and has extended some capabilities to monitor AI-related threats, particularly those originating from malware or advanced persistent threats (APTs) leveraging AI. Strong in endpoint protection and real-time threat intelligence, with capabilities to detect AI-driven malware. Primarily focused on endpoint threats, which may not cover unauthorized AI software and broader AI usage across the network.
- **Darktrace**: Web Page
  Known for its AI-driven cybersecurity platform, Darktrace offers solutions that include detecting AI-based threats and anomalies in network behavior. Exceptional in detecting AI-based anomalies and threats using its own AI algorithms, providing proactive threat detection. While excellent at detecting anomalies, it may lack the specific focus on AI vulnerabilities and unauthorized AI software detection that Tenable AI Aware provides.

- *Tenable AI Aware* provides a more focused approach to AI-specific threats and vulnerabilities compared to CrowdStrike's general endpoint protection and Darktrace's anomaly detection. Tenable's strength lies in its ability to integrate AI threat detection with its existing vulnerability management capabilities, offering a more comprehensive solution for organizations looking to manage AI risks across multiple layers of their IT environment.

Tenable AI Aware positions itself as a robust and comprehensive solution for organizations looking to manage the wide-ranging risks associated with AI technologies. Its strengths lie in its holistic approach, broad detection capabilities, and seamless integration with Tenable's existing security platforms. While competitors like Qualys Total AI and Darktrace offer strong features in specific areas, Tenable AI Aware's ability to cover multiple layers of AI risk makes it a superior choice for organizations seeking a more complete AI risk management solution.