Black Duck Newsroom

Black Duck SCA Introduces AI Model Risk Scanning for Enhanced Software Security Insights

Support now available to identify and manage open source AI models, addressing growing need for comprehensive risk visibility, governance and compliance capabilities

BURLINGTON, Mass., Nov. 12, 2025 /PRNewswire/ -- Black Duck®, a leading global provider of application security solutions, today announced that Black Duck® SCA can now identify and analyze AI models, starting with the 2025.10.0 release. This capability addresses the growing need for enterprises to gain visibility into the usage, licensing and data origins of open source AI models integrated into their software development processes.

As companies increasingly leverage AI models to drive innovation, they face significant challenges in managing these complex components. Black Duck's AI Model Risk Insights capability provides comprehensive visibility into AI model usage across applications, including versions and datasets, even if they are hidden or modified. This ensures that companies have a complete understanding of their AI model landscape, enabling them to enforce their AI policies with confidence.

Key Features and Benefits

- **AI Model Identification and CodePrint Scanning** detects models from repositories like Hugging Face, even if they are not declared in build manifests or are intentionally obfuscated. This feature utilizes proprietary, signature-based scanning to accurately identify model type and version.
- **License Compliance and Metadata Display** identifies model licenses to help ensure compliance with project requirements. This feature introduces a dedicated UI screen displaying model-specific metadata, including model cards and training data insights.
- **Seamless Integration and Scalability** leverages CodePrint scanning and BOM Engine for minimal setup in existing Black Duck workflows. This positions customers for future AI security requirements without workflow disruption.
- **Regulatory Compliance and Governance** helps meet emerging standards like the EU AI Act, the U.S. Executive Order on AI, and industry-specific guidelines. This provides audit-ready reports on AI components, simplifying compliance audits and reducing legal exposure.

"With the introduction of AI model scanning, Black Duck SCA is setting a new standard for software composition analysis," said Jason Schmitt, CEO at Black Duck. "This innovation directly addresses the emerging security challenges of AI adoption, empowering companies to confidently integrate AI models securely while maintaining compliance and regulatory adherence. The capabilities now available through AI Model Risk Insights also represent a significant leap forward in Black Duck's mission to help companies build and deliver secure and compliant software."

AI Model Risk Insights is available as a new licensed feature and is part of Black Duck's ongoing commitment to providing cutting-edge SCA capabilities that address the evolving needs of software development teams.

For more information about Black Duck SCA and its AI model scanning capabilities, please visit our website or read our detailed blog post.

About Black Duck

Black Duck® meets the board-level risks of modern software with True Scale Application Security, ensuring uncompromised trust in software for the regulated, AI-powered world. Only Black Duck solutions free organizations from tradeoffs between speed, accuracy, and compliance at scale while eliminating security, regulatory, and licensing risks. Whether in the cloud or on premises, Black Duck is the only choice for securing mission-critical software everywhere code happens. With Black Duck, security leaders can make smarter decisions and unleash business innovation with confidence. Learn more at www.blackduck.com.

SOURCE Black Duck Software

For further information: Editorial Contact: Liz Samet, Black Duck, 336.414.6753, esamet@blackduck.com

---

Additional assets available online: Video (1)

https://news.blackduck.com/2025-11-12-Black-Duck-SCA-Introduces-AI-Model-Risk-Scanning-for-Enhanced-Software-Security-Insights