Black Duck Newsroom

Black Duck Arms the Defender Against the Wave of AI-Driven Software and Supply Chain Attacks

New Polaris Platform capabilities empower teams to close security testing gaps, withstand the flood of supply chain vulnerabilities, and automate remediation pipelines

BURLINGTON, Mass., June 16, 2026 /PRNewswire/ -- Black Duck®, the leader in AI-powered application security, today announced significant feature enhancements to its Black Duck Polaris™ Platform, engineered to empower organizations to stay ahead of exploits generated by hackers using sophisticated AI models such as Claude Mythos, as well as the flood of vulnerability disclosures and patches expected as open source maintainers scramble to use AI to find and fix vulnerabilities in commonly used supply chain components.

The latest Black Duck innovations equip security teams to detect, prioritize, and remediate vulnerabilities faster than ever before by addressing three core pillars of Mythos readiness: eliminating AST gaps that are easy targets for AI, equipping teams for the AI vulnerability flood, and leveraging AI to minimize the mean time to remediate (MTTR) security risks. Together, these capabilities enable teams to transform their current manual remediation practices into a fast-paced and highly automated VulnOps model, essential to defend against AI-speed cyberattacks.

This urgency is reflected in real-world usage, with Polaris scan volumes increasing more than 100% in the first five months of 2026 as organizations accelerate security testing to keep pace with AI-driven threats.

"The window between vulnerability discovery and exploitation has collapsed, turning software risk into an immediate and potentially existential business risk," said Dipto Chakravarty, Chief Product & Technology Officer at Black Duck. "Black Duck is redefining the application security operating model, enabling organizations to reliably and continuously identify and reduce risk in real time to protect critical assets, maintain resilience, and keep pace with adversaries that move at AI speed."

Closing Visibility Gaps and Enforcing Security at Scale

AI models like Claude Mythos enable attackers to chain together multiple application vulnerabilities into sophisticated exploits in a matter of minutes. Even vulnerabilities considered low severity when viewed in isolation can lead to exploit when chained with other security defects. New capabilities in Polaris help teams eliminate the gaps and inconsistencies in their application security testing, triage, and remediation to prevent vulnerabilities from going undetected:

- **Eliminating application security blind spots.** The proliferation of agentic coding tools is dramatically increasing the volume of code and pace of development. Polaris continuous SCM monitoring and synchronization ensure that every repository and branch is automatically tracked and tested, enabling organizations to uncover shadow AI projects and continuously evaluate them for security and compliance risks.

- **Ensuring the right tests are run at the right time.** Event-driven static (SAST) and software composition analysis (SCA) testing enables teams to automatically trigger scans based on SCM pull requests and

merges based on branch type, with results delivered directly to developers via pull request comments, helping minimize the MTTR.

- **Automating consistent security control enforcement.** The growing volume of code being created by AI significantly increases the vulnerability triage and prioritization backlog. Updated Polaris policies enable teams to automate enforcement of fine-grained security controls in SCM and CI flows, helping ensure vulnerabilities are handled consistently across development projects, preventing code that violates policy from advancing to production, and freeing security teams to focus triage efforts on complex issues that require deeper analysis.

Equipping Teams for the AI Supply Chain Vulnerability Flood

As software component vendors and open-source maintainers scramble to test and patch their products using AI, teams building software with these supply chain components must be prepared for a flood of new vulnerability disclosures, which are expected to top 50,000 in 2026 and could rise to nearly 200,000 by 2028. Several new capabilities in Polaris help teams ensure they have the visibility and rapid response capabilities needed to survive:

- **Eliminating supply chain coverage gaps**. Black Duck Audits reveal that most teams track just 50% of the OSS they use. Untracked and unpatched components are low-hanging fruit for AI-powered cyber-attacks. Polaris fAST SCA now supports full binary and container analysis, as well as source and package manager detection, enabling teams to generate complete and accurate SBOMs for all software they build and deliver.

- **Ensuring exploitable vulnerabilities are fixed first.** Because hackers can now use AI to chain together multiple lower-severity vulnerabilities into attacks, teams need to look beyond CVSS scores when prioritizing remediation. Polaris now combines reachability analysis, enhanced exploitability insights from Black Duck Security Advisories (BDSAs), and CISA Known Exploited Vulnerabilities (KEV) data with CVSS scores to surface the vulnerabilities that pose the greatest real-world threat.

- **Enabling machine-speed VulnOps**. New automated SCA fix pull requests enable teams to fast-track remediation of high-priority vulnerabilities based on reachability, exploitability, and policies, while keeping the human in the loop for review and approval prior to merge. This eliminates the time-consuming manual triage-and-assignment loop while enabling teams to ensure upgrade to a non-vulnerable component version doesn't accidentally break their code.

Streamlining Developer and Security Analyst Workflows with AI

While AI models like Mythos empower skilled security analysts to detect novel vulnerabilities, most security and development teams face the immediate challenge of defending against a wave of AI-powered attacks. Polaris brings AI-enabled AppSec to their DevOps workflows today, with the ability to integrate Black Duck Signal™ agentic AppSec capabilities alongside the deterministic, scalable, compliance-ready analysis of Polaris fAST Static, SCA, and Dynamic:

- **AI False Positive Detection**. As the volume of software and security tests increases with AI, teams can be overwhelmed with issue triage. Polaris AI False Positive Detection lets security analysts delegate the research and deprioritization of false positives to a built-in AI agent, which will leverage insights from the

Black Duck ContextAI™ model. This ensures that false positives never reach development.

- **Polaris issue management MCP server**. Teams using agentic software development tools like Claude Code and GitHub Copilot can now access Polaris scan results, prioritization information, and remediation guidance using Model Context Protocol (MCP), within their custom agentic AI test and fix workflows.
- **Code Sight AI features for IDEs**. The latest release of the Code Sight IDE plug-in enables teams to access LLM-based security analysis (via Black Duck Signal) and apply AI generated code fixes with a single click, so teams can leverage AI to improve the security of their code directly in their existing developer environment.

Together, these capabilities help security and development teams ensure that all the software they deliver is thoroughly tested, they can process the flood of AI-driven vulnerabilities and patches, and their vulnerability triage and remediation is able to stay ahead of hackers using AI to target security defects.

To learn more about the Black Duck Polaris Platform, visit our website, read our detailed blog post, and register for the upcoming webinar.

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:LizSamet, Black Duck, 336.414.6753, esamet@blackduck.com

---

https://news.blackduck.com/2026-06-16-Black-Duck-Arms-the-Defender-Against-the-Wave-of-AI-Driven-Software-and-Supply-Chain-Attacks