Trend Micro: Delivering Open Source Cybersecurity

Company overview

A global leader in cloud and enterprise cybersecurity, Trend Micro helps make the world safe for the exchange of digital information. Fueled by decades of security expertise, global threat research, and continuous innovation, its cybersecurity platform protects 500,000+ organizations and 250+ million individuals across clouds, networks, devices, and endpoints.

Trend Micro's platform delivers central visibility for better, faster issue detection and response. And it provides a powerful range of advanced threat defense techniques optimized for environments like AWS, Microsoft, and Google.

Since 2019, Trend Micro has used Black Duck software composition analysis (SCA) to create and maintain a comprehensive and accurate Software Bill of Materials and to aggregate open source vulnerability management across software repositories.

The challenge: Moving beyond manual maintenance for better vulnerability management

"Before Black Duck®, our open source management process was essentially a manually maintained inventory of third-party apps, primarily open source components," said Fabio Arciniegas, senior cybersecurity architect at Trend Micro. "Each individual Trend Micro product team manually reviewed that list and updated it as needed during their release process. We also utilized an in-house CVE collection process that notified the various product teams of new CVEs based on the inventory."

"The manual nature of the process impacted developer productivity and undermined the reliability of our third-party vulnerability management, especially considering the increasing number of open source security vulnerabilities discovered each year," Arciniegas continued. "We wanted to embrace the 'shifting security testing left' concept fully with an efficient, automated vulnerability management solution that would provide us with a comprehensive Software Bill of Materials (SBOM) that could be automatically and regularly updated."

The solution: Black Duck SCA for open source management

Black Duck is a comprehensive software composition analysis solution that helps organizations manage the security, quality, and license compliance risks that come from using open source and third-party code in applications and containers. Black Duck gives organizations like Trend Micro visibility into third-party code, enabling them to control it across the software supply chain and throughout the application life cycle.

"We conducted testing on several vendors' products noted in analysts' reports as SCA industry leaders," Arciniegas said. "We found that Black Duck surpassed other vendors in terms of accuracy and support for scanning of various file types. We were impressed by the Black Duck Signature Scanner and its ability to analyze more types of files from different package management ecosystems than other vendors."

In a typical Black Duck scan, Black Duck Detect scans source code (including archive formats), a Docker image, or a binary artifact. Once the scan is launched, Black Duck Detect utilizes a set of internal tools (Black Duck Signature Scanner, detectors, and inspectors) to discover open source components. These tools also gather metadata about the code, which includes package manager data and code prints. When that process is complete, Detect sends the metadata to Black Duck in the form of a scan file. A Black Duck server communicates with the Black Duck KnowledgeBase™ and uses the scan file to create a Software Bill of Materials that includes all discovered open source and the associated risk. Black Duck Detect maps the scan file to a project and project version in Black Duck, where the SBOM will be displayed.

The results: Effective monitoring of third-party vulnerabilities

“We’ve found Black Duck very easy to install and to use,” said Arciniegas. “It integrates well into our CI/CD process—which includes Jenkins and GitHub Actions—and has useful APIs to create customized queries. For example, we use a Python script to call the Black Duck API and post results to Slack.”

“With Black Duck, monitoring of third-party vulnerabilities is a required Trend Micro policy in order to release a product. Our product teams must perform Black Duck scans regularly and address discovered vulnerabilities in compliance with corporate policy. Our policy requires that all high or critical vulnerabilities with a CVSS score of seven or higher must be fixed.”

About Black Duck

Black Duck® offers the most comprehensive, powerful, and trusted portfolio of application security solutions in the industry. We have an unmatched track record of helping organizations around the world secure their software quickly, integrate security efficiently in their development environments, and safely innovate with new technologies. As the recognized leaders, experts, and innovators in software security, Black Duck has everything you need to build trust in your software. Learn more at www.blackduck.com.