Real World Experience: Blackboard

Blackboard Results

Automated component vulnerability tracking	Recommends safer component versions	Product up-and-running in one day	Developers get real-time component updates

Bb
Blackboard

NEXUS LIFECYCLE USER

Blackboard gives Sonatype high marks for open source governance at the speed of development

Educational Software | Washington, D.C.

About Blackboard

Blackboard is the world's leading education technology company. They challenge conventional thinking and advance new models of learning in order to reimagine education and make it more accessible, engaging and relevant to the modern day learner and the institutions that serve them. In partnership with leaders in higher education and K-12 as well as corporations and government agencies around the world, their mission is to help every learner achieve their full potential by inspiring lifelong learning. In order to support this mission, Blackboard has an industry-leading security program, dedicated to successfully protecting the integrity of the company's data and products' mission critical availability.

The Challenge

Blackboard has written millions of lines of custom code—and about half of it touches one or more of 100+ open source components, including the likes of Spring, Struts, Hibernate and Tomcat. Assuring those components are free of vulnerabilities is incredibly important to Blackboard, explained Matthew Saltzman, Senior Security Engineer of Blackboard's Application Security Team.

In the past, the team would spend two days assessing if a specific version of an artifact, framework or library was approved to use in a Blackboard product. Like many other companies, the team tracked its inventory of open source components in a spreadsheet. The team would review notifications from the

National Vulnerability Database to see if its open source components were free of security risks. In parallel, the legal team would perform an analysis of any license risks associated with those components.

This manual process did not scale with Blackboard's growing use of open source; it was tedious and tough to maintain. When new vulnerabilities would surface in a live product, the security team would spend days identifying a fix.

Why Sonatype?

Blackboard needed to transform its open source governance practices to work at the speed of its agile development teams. The company sought an automated solution to continuously monitor, govern and report on open source components in use. After evaluating open source and commercial options, Blackboard chose Sonatype's Nexus Lifecycle (formerly Component Lifecycle Management - CLM) because it was easy to integrate and easy to use. Nexus Lifecycle tracks usage, enforces policy and prevents the use of flawed components all the way through the SDLC. Nexus Lifecycle would also help the company track open source artifacts in production applications, altering the company's security team to new vulnerability disclosures that might impact customers or operations.

At Blackboard, Sonatype's Nexus Lifecycle is integrated directly into the continuous integration platform Jenkins—a key priority for the company. Integrated tightly inside their development tools, developers now get real-time updates about component attributes (security, licenses, and quality) so they can make the right choices.

The solution not only identifies potential issues, it also offers recommendations on safer versions of troublesome components. Nexus Lifecycle provides a complete software "Bill of Materials" that covers all open source components used and then continuously monitors that inventory for changes and vulnerabilities associated with used components. This detail, presented in a Nexus Lifecycle dashboard, keeps development, application and legal teams informed of Blackboard's overall open source inventory, including artifact and application vulnerability profiles.

> “Outsourcing all of this oversight and analysis saves an incredible amount of time. With the Sonatype product embedded across our development, we can get ahead of any major vulnerabilities before an application is released.”

Results

Blackboard's application security team has transitioned from spending time researching open source vulnerabilities to relying on Nexus Lifecycle to continuously automate the oversight and policy guardrails. The Nexus Lifecycle integration helps to both enforce the set of open source licenses vetted by the legal team and to identify potential license risks. Not only do both teams save an incredible amount of time, Blackboard now has a proactive way to use open source components safely, avoiding security, license and quality-related issues.

"In less than a day, we were up-and-running with the solution integrated into development," Saltzman said. "And to top it off, our developers needed only a 30-minute course to learn the product. We were able to recognize value right away."

> "Nexus Lifecycle provides a complete software "Bill of Materials" that covers all open source components used and then continuously monitors that inventory for changes and vulnerabilities associated with used components."

www.sonatype.com