SYNOPSYS®

NGINX Open Source

Helping developers ensure code quality and security with Coverity Scan

NGINX®

One of the world's most widely used web servers—powering sites such as Netflix, Hulu, Pinterest, and GitHub—NGINX Open Source (pronounced "engine x") is known for its high performance, stability, rich feature set, simple configuration, and low resource consumption. Other members of the NGINX Open Source family include NGINX JavaScript (njs), a module adding JavaScript support to NGINX; and NGINX Unit, a dynamic application server supporting applications written in Perl, Python, Ruby, Node.js, Go, Java, and PHP.njs.

Developers for all three NGINX Open Source projects use Coverity Scan® to find and fix defects in their code. A free online service provided by Synopsys and powered by the same engine used by Synopsys' commercial Coverity cofounded NGINX in 2011 to provide formal support for NGINX Open Source and to offer a commercial version, NGINX Plus, which adds enterprise-grade features to NGINX Open Source.

NGINX was acquired by F5 Networks, an application security and delivery company, in 2019. Today, the NGINX family of open source projects include njs, a module adding JavaScript support to NGINX and NGINX Unit, a dynamic application server.

The problem: Ensuring open source code quality and security

"We integrated Coverity Scan into our CI/CD pipeline soon after establishing NGINX," said Maxim Konovalov, one of the company's cofounders and now VP of engineering. "We've been submitting NGINX build artifacts daily since 2012."

"In many cases, NGINX acts 444 ne--f90 feforr.4 (aSontngid NGINntVa)c(aSinutedK)-11.9 (ono)6.

NGINX takes its role as a foundational technology to millions of apps and websites very seriously. Code quality and security are part of its ethos, and the tools that help support that mission are integral to its development practices.