

Spirent Realizes the Value of Code Audits During M&A Due Diligence



Company Overview

Spirent designs cutting-edge products and services that accelerate the development of new products and networks and keep the world's networks up and running, measure and optimize their performance, and ensure they are safe and secure. Spirent products enable its customers to accelerate their time to get their products to market while ensuring the quality and performance of their product protects their brand.

“Black Duck audits have become a standard part of our due diligence when we buy a software company.”

—Steve Clark,
Vice President, Mergers and Acquisitions,
Spirent

Overview

[Spirent Communications](#) has built its \$500 million performance analysis and network management solutions business on software engineering breakthroughs. The company's lab and field testing products and services, used to evaluate the performance of next-generation communications technologies such as broadband networking and satellite navigation, leverage both internally and externally developed software innovations.

The successful execution of strategic acquisitions is essential to Spirent's long-term growth plans. The company averages two to three acquisitions each year, mostly targeting software companies. “We have an active M&A program,” says Steve Clark, vice president of mergers and acquisitions at Spirent, in Eatontown, New Jersey. “We're always looking to acquire companies in complementary or adjacent areas.”

Clark credits Spirent's M&A activities with helping it deliver a sophisticated array of new services and product functionality to address the evolving needs of high-profile customers such as Cisco, AT&T, Verizon, Samsung, and China Mobile.

“We used to be a box builder—we built instruments in a rack, and it became a system,” he notes. “The hardware did the bulk of the analysis. There was code, but it was on the chips. Once you created the system, people didn't want to buy more boxes, because it was expensive. But they wanted the boxes to do more. The quickest, cheapest way to add features and functionality is through software.”

This shift in customer preferences, combined with emerging trends in virtualization and automation, drove Spirent to step up its M&A activity—which put the spotlight squarely on software code quality.

Intellectual property is the top priority in M&A

“When you buy a software company, the intellectual property is the crown jewel,” Clark says. Finding efficient, reliable ways to evaluate the quality and provenance of intellectual property, including software code, during acquisitions had always been a priority for Spirent. But the importance of this due diligence recently became even more apparent. “If the architecture isn't done correctly, we can't integrate the code from the target company into Spirent code,” Clark says. “It becomes more difficult and expensive for us.”

During one potential acquisition, it became clear relatively late in the process that the target company's software code had serious problems. “We walked away from the deal, and this was the primary reason why,” he explains. “The code was a train wreck. Our engineers said it would have taken 10 engineers two years to fix the code. That's what first spurred our internal conversation about code quality audits.”

Since this failed acquisition attempt, Spirent has retained Synopsys for its [Black Duck Open Source and Third-Party](#) and [Code Quality Audits](#). “Black Duck audits have become

a standard part of our due diligence when we buy a software company,” Clark says. “We do it every time.” At one time, Spirent didn’t assume its target acquisitions would have open source included in their codebase, but that time has passed. Open source is now an issue in every potential software company acquisition.

“There’s so much open source code out there, but people aren’t necessarily using it correctly,” he adds. “I’ve now learned there will never be an acquisition where we won’t find some type of problem with open source code. Every time we’ve run a Black Duck code scan, we’ve found some type of violation.”

And according to recent research from Gartner, companies will need to become even more vigilant regarding open source code problems as these projects become more widely used throughout large corporate enterprises. Gartner analyst Mark Driver notes that “by 2020, quality and security defects publicly attributed to open source projects will increase significantly, driven by a growing presence within high-profile, mission-critical and mainstream IT workloads.”¹

Synopsys’ well-known Black Duck Open Source and Third-Party Audit identifies open source components in a codebase and any associated risks. The Code Quality Audit is focused on identifying risk in the code or its construction techniques that can lead to quality issues. The audit determines whether code is built using industry best practices, structured to enable efficient ongoing development, and sufficiently well documented. Code is examined for functionality, reliability, usability, efficiency, and maintainability. The result of this examination is a comprehensive analysis, including comparative benchmarks and metrics, which can be used to form a plan to address code problems.

The value of code audits: Informed decisions, clear pathways to remediation

Why is this so important to Spirent’s bottom line? Clark asserts that Black Duck audits have been an invaluable tool in speeding up the due diligence process during mergers and acquisitions.

“We know right away what types of violations exist in the codebase, so we can quickly evaluate whether they will have a material impact on the value of the software as an IP asset,” Clark says. With this knowledge, the company can develop remediation plans, if applicable.

This has proven true regardless of the profile of the acquisition target, he adds. “We’ve bought startups and we’ve bought more mature businesses, and in every case, we’ve seen the clear value of code quality audits,” Clark says.

Having Synopsys as a trusted partner also provides assurance to target companies, which can be resistant to handing over source code to potential buyers. “The target signs an NDA with Synopsys, so we never see the code directly,” Clark says. “We standardized on Black Duck audits because people are familiar with them. Most investment bankers are familiar with Black Duck audits, so this helps smooth the process.”

Given the scope and technological impact of Spirent’s business, Clark says—its products and solutions help enable the growth of global communications solutions for wireline, wireless, and satellite communications—its M&A strategy has had to evolve along with the company’s technological achievements.

“Time to market is extremely important in our business,” he asserts. “Technology changes so quickly, and there is tremendous pressure on the engineers to get things done as fast as possible. The more knowledge we have about our acquisition targets and their intellectual property, the faster we can move as a company to advance solutions for our customers.”

¹ Mark Driver, [Road Map for Open-Source Success: Understanding Quality and Security](#), Gartner, March 2014.

The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior.

For more information about the Synopsys Software Integrity Group, visit us online at www.synopsys.com/software.

Synopsys, Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com