IDC LINK
Real-time IDC Research® opinion on industry news, trends and events

Veracode Bolsters Risk Management Capabilities with Acquisition of Longbow Security

April 16, 2024

By: Katie Norton

IDC's Quick Take

In acquiring Longbow Security, Veracode has expanded its capabilities to address the market need for tooling that provides a unified and holistic view of application risk. As a result of this move, Veracode will be able to identify, prioritize, and remediate vulnerabilities and security issues at scale, reinforcing its commitment to managing and reducing the risk associated with building and running applications across multiple clouds.

M&A Announcement Highlights

On April 1, 2024, Veracode announced the acquisition of Longbow Security, a provider of a security risk management solution for cloud-native environments and applications. Longbow Security was cofounded in 2019 by Dayne Myers and Derek Maki, formerly part of McKinsey & Company's Cyber Solutions group. The Austin, Texas-based company came out of stealth about a year ago, in March 2023, and had raised $10.5 million.

Longbow Security's solution discovers cloud and application assets and their associated vulnerabilities via integrations into over 50 security tools, including the major cloud providers, source code repositories, infrastructure as code (IaC) tools and security scanners, identity providers, application security testing (AST) tools, cloud-native application protection platforms (CNAPP), and more.

Findings from across tools, which include vulnerabilities, misconfigurations, overpermissioned accounts, data sensitivity issues, and indicators of compromise, are normalized, pre-investigated, and prioritized based on business, asset, and environment context. The solution identifies the owners and root cause of security issues, providing users with the "Best Next Action" — which remediation actions will reduce the most risk with the least effort. Veracode indicated that the integrated solution will enable remediation by leveraging Veracode Fix to provide AI-generated fixes.

The acquisition's financial terms were not disclosed. This acquisition is Veracode's third since 2012 and second since TA Associates made a significant investment in March 2022. Veracode's last acquisition was Crashtest Security, a developer-friendly dynamic analysis security testing (DAST) solution, in December 2022. Newly appointed CEO Brian Roche stated this acquisition ushers in a new phase for Veracode, underscoring the company's "commitment to managing and reducing risk related to building and running applications across multicloud environments."

Veracode indicated the Longbow Security capabilities are available to customers immediately.

IDC's Point of View

A clear, enterprisewide view of application security risk requires a deep understanding of the applications, from software development to their running state. For many security teams, application

development is a black box. Increased adoption of cloud infrastructure and distributed architectures, the growing use of open source software, rapid development cycles via DevOps, and developers taking on more responsibility for application security have all introduced additional complexity. Security teams often have limited visibility or understanding of the inner workings of the applications they are tasked with protecting.

Owing to this increased complexity, a growing number of tools and technologies are dedicated to application security. Recent IDC survey research found that 86% of organizations surveyed are actively or planning to consolidate their security tools, with the average organization having almost 50 security tools (see *How Many Security Tools Do Organizations Have, and What Are Their Consolidation Plans*, IDC #US51973524, March 2024). The IDC *DevSecOps Adoption, Techniques, and Tools Survey* (IDC #US50137623, May 2023) revealed that the average organization uses between 10 and 14 tools that support DevSecOps practices alone. Moreover, the same survey found that 24% of organizations indicated too many different security scanning tools and results was a DevSecOps tooling challenge.

Since these tools do not communicate with each other, security data becomes siloed. The sheer volume of vulnerabilities flagged across multiple siloed tools can overwhelm security teams. Because of this, large enterprises can have a backlog of thousands or tens of thousands of vulnerabilities that require mitigating but lack sufficient detail to determine the actual risk posed. The 2024 edition of Veracode's annual *State of Software Security* report found that security debt, defined as flaws that remain unfixed for longer than a year, exists in 42% of applications and 71% of organizations.

With the combined lack of visibility, growing tool sprawl, and increasing vulnerability backlog, security teams often forward findings to developers without the necessary context and knowledge to triage and fix them. The developers who try to act on these issues end up with duplicates, false positives, or little understanding of what needs to be fixed first, wasting already constrained time and resources. These remediation workflow issues drive a further wedge between security and development teams.

Given this situation, prioritizing and remediating security findings is a significant challenge for organizations. Efficiently and effectively prioritizing vulnerabilities requires context, as the actual risk to an application might differ depending on the technical stack, location (i.e., externally exposed), underlying data, criticality to the business, and more. Organizations need a tool that can act as a single source of truth regarding the overall risk to the business created by its applications — and this is precisely what the acquisition of Longbow Security brings to Veracode.

AST platform vendors, including Veracode, often provide dashboards displaying aggregated findings across static application security testing (SAST), dynamic application security testing (DAST), software composition analysis (SCA), container scanning, and others. However, these tests fail to capture the runtime, infrastructure, and cloud context to accurately assess and manage the risk associated with an application because they provide critical insights into how an application operates in a real-world environment and interacts with its underlying systems.

The additional context from Longbow Security will provide Veracode customers with a more holistic understanding of their application risk, pinpointing the issues posing the greatest threat and prioritizing remediation efforts. IDC has observed several recent acquisitions by security vendors seeking the same types of expanded capabilities, including Snyk's acquisition of Enso (June 2023) and Helios (January 2024) and Crowdstrike's acquisition of Bionic (September 2023).

A key feature of Longbow Security's solution is the company's "Best Next Action," which leverages automated root cause analysis to remediate the most urgent and impactful application and cloud security issues. Veracode and Longbow Security become a better together story when these Best Next Actions can be automatically remediated using Veracode Fix, as Veracode alluded to as a road map capability.

Veracode Fix generates secure code patches that developers can review and implement to remediate security flaws without manually coding a fix. Veracode Fix currently supports SAST findings for C#, Java, JavaScript, TypeScript, PHP, Scala, and Python, and it will be critical for Veracode to continue expanding the tool's coverage rapidly. The findings from Longbow needing remediation will potentially come from external tools, which will be a use case Veracode will need to explore, as it is currently limited to the Veracode platform.

While Veracode noted that the Longbow Security capabilities are available immediately to customers, they have not provided detailed plans for whether the technology will remain a standalone solution or be folded into the Veracode platform. Given the earlier point of security tool sprawl and preference for consolidation, it would behoove Veracode to explore folding Longbow Security into its platform.

Subscriptions Covered:
DevSecOps and Application Security