FROST & SULLIVAN

SONATYPE

2022 TECHNOLOGY INNOVATION LEADER

GLOBAL DEVELOPMENT AND OPERATIONS (DEVOPS) SECURITY INDUSTRY

Best Practices Criteria for World-Class Performance

Frost & Sullivan applies a rigorous analytical process to evaluate multiple nominees for each award category before determining the final award recipient. The process involves a detailed evaluation of best practices criteria across two dimensions for each nominated company. Sonatype excels in many of the criteria in the DevOps security space.

DevOps Security Market Challenges

DevOps frameworks are witnessing increasing adoption in the software development life cycle (SDLC) to meet organizations' need for automated software delivery and deployment and faster innovation of software products. However, with faster digitization and continuous innovation accompanying this shift towards DevOps, legacy software security approaches are no longer sufficient. DevOps security vendors are now tasked with providing software developers with shift-left technologies, that is, tools to detect, analyze, and remediate vulnerabilities, ensuring security is embedded throughout the SDLC.

Moreover, with software developers increasingly deploying open-source codes into the software supply chains to meet the demand for fast innovation, the attack surface of their software supply chains is expanding, largely due to the high volume of security risks in the open-source ecosystem. To maintain the security posture of customers' infrastructure while they pursue innovation, DevOps security vendors need to deliver DevOps security that supports different types of open-source codes. The challenge for DevOps security vendors is ensuring adaptability in their vulnerability detection and remediation technology to cope with the evolving supply chain attacks.

Due to the rising usage of infrastructure-as-a-code (IaC), systems or infrastructures are being saved and managed as codes, which inevitably exposes companies' SDLC to more potential threats. DevOps security vendors will need to include IaC security in their DevOps security portfolio to meet customer demands. The volume of code in an SDLC continues to rise as developers strive to meet innovation expectations.

This gives rise to more potential exploitable vulnerabilities in the code of the SDLC. While DevOps teams are focused on meeting business demands and innovation goals, security teams are concerned about the unresolved vulnerabilities in the software applications. Customers continue to face challenges like conflicting priorities between DevOps and security teams to release and deploy secure software applications or products within a tight timeline. Customers can no longer spend the majority of their time on patching (which slows down the development and operational processes) and can thus no longer afford to have a separate, siloed security process towards the end of the SDLC. DevOps security vendors must meet the challenge of delivering DevOps security that seamlessly integrates multiple-point solutions into one platform.

Commitment to Innovation and Commitment to Creativity

Headquartered in the United States, Sonatype is a software supply chain management company that offers customers software supply chain management and automation tools to manage their cloud-native development lifecycles. Since its incorporation in 2008, Sonatype has continually enhanced its DevOps security offering. In 2021, Sonatype expanded its Nexus platform to provide full-spectrum supply chain management and security support to all types of modern application building blocks, which include containerized code, IaC, and first-party proprietary source code on top of third-party open-source code. The next-generation Nexus platform integrates a range of DevOps security technologies, such as its repository manager, Nexus Repository, its world-class software composition analysis tool, Nexus Lifecycle, the Nexus Firewall, and its container security, Nexus Container, into a single platform. This platform can also be integrated with existing developer tools and DevOps pipelines. As customers increasingly look for a unified DevOps security platform that provides visibility and integrations of different point security solutions in ensuring the security of its SDLC, Sonatype's enhanced next-generation Nexus platform has addressed the key unmet technology voids in the DevOps security market.

In response to the staggering increase of open-source cyberattacks due to the injection of malicious code into open-source repositories, the platform's Nexus Firewall offers next-generation behavioral analysis and automated policy enforcement to help customers continually detect and remediate vulnerabilities from the early stage of the SDLC. Besides open-source codes, the incorporation of supply chain management for various software codes, including IaC, into Sonatype's newly enhanced Nexus platform has also boosted the cyber resilience of customers who increasingly depend on cloud-native technologies. This, in turn, has broadened Sonatype's DevOps security portfolio.

Automation is another important feature provided by the Nexus platform. With the high interdependencies between applications' components and third-party components, Sonatype offers automated security, which allows developers to efficiently identify and remediate security risks in the embedded dependencies.

Sonatype's Nexus platform offers end-to-end visibility through its unified control panel, a comprehensive security approach across different stages of the SDLC, as well as an automated security feature. Its DevOps security technologies reduce false positives, improve code quality, and automatically remediate vulnerabilities found, which help developers save time and address tight timeline issues. Sonatype's shift-left approach, coupled with its Sonatype Core Values program, which continually recognizes and promotes creativity among Sonatype's employees, exemplifies the company's commitment to innovation and

> *"Sonatype's shift-left approach, coupled with its Sonatype Core Values program, which continually recognizes and promotes creativity among Sonatype's employees, exemplifies the company's commitment to innovation and creativity. The company's technology innovation initiatives reflect its awareness of customer pain points and enable it to be one of the top enterprise choices for customers in the DevOps security market."*
>
> ***- Ying Ting Neoh, Research Analyst***

creativity. The company's technology innovation initiatives reflect its awareness of customer pain points and enable it to be one of the top enterprise choices for customers in the DevOps security market.

Stage Gate Efficiency

Sonatype has aggressively developed its product roadmap and created new or enhanced technologies through strategic partnerships and open beta programs to collect customer feedback. In 2021, the company announced the acquisition of MuseDev as it diversified its DevOps security offering through the release of its next-generation Nexus platform. MuseDev offers an innovative code analysis platform that automatically provides analysis and accurate feedback whenever software developers send a pull request.

Adopting a channel-first approach, Sonatype further expanded its channel partner ecosystem through its channel partner program. This propelled the company's success in 2021, allowing it to showcase some of the best practices it implements. Its efforts to expand its channel partner ecosystem include the release of a new program that provides comprehensive channel community resources that help expand the customer base, offer go-to-market support, enable self-serve data intelligence, and, most importantly, implement new and integrated training technologies. As a strategic partner, Sonatype continues to provide actionable education to its resellers and the market.

The company has helped set the framework of the software industry's first CycloneDX standard for the automated software bill of materials (SBOM) data exchange. In May 2021, in adherence to the industry's best practices, Sonatype developed APIs based on the CycloneDX standard for third parties to integrate SBOMs between products and systems more holistically. Besides actively engaging software developers with its global Developer Relations program, Sonatype has continually provided support to the open-source community through its active partnership with government and industry groups such as the Open Source Security Foundation, the OpenChain Project, and the Python Software Foundation in an effort to educate the market while making open source ecosystem more secure. These partnerships allow Sonatype to fully understand software developers' challenges and pain points on the ground and inform the development of the industry's standards and best practices. This has helped Sonatype foster stronger relationships with its channel partners and customers. Frost & Sullivan commends Sonatype's committed support to the market in sharing industry best practices and its strategic collaborations to extend its out-of-the-box integrations that benefit customers and channel partners.

Commercialization Success and Customer Acquisition

Sonatype's customer packages offer three basic products—the Nexus Lifecycle, the Nexus Container, and the Nexus Firewall—with optional add-on packages such as the Advanced Development Pack for

> *"Sonatype recorded steady growth across verticals, especially in the banking, financial, services, and insurance (BFSI), service provider, and manufacturing sectors. Frost & Sullivan recognizes Sonatype's focus and steadfast commitment to meeting customers' ever-evolving needs and addressing the pain points in the DevOps security market, enabling the company to continually stay ahead of the curve."*
>
> ***- Ying Ting Neoh, Research Analyst***

additional remediation support, the Advanced Legal Pack for license compliance automation, and the IaC Pack.

Backed by more than 500 employees, Sonatype is well-known for its policy engine (which enables customers to create and assign policies), its automation of open-source compliances, its vulnerability remediation and suggestions, and its praiseworthy customer service. Sonatype has solved Log4j vulnerabilities by identifying all the open-source components and the embedded dependencies of the customer in 24 hours due to its deep understanding of the SDLC and its security technologies. With an emphasis on customer engagement, the company's Customer Success group focuses on understanding customers' challenges and desired goals. This is part of the company's efforts to meet customer needs, be it a self-service, real-time automated vulnerability scanning technology or meeting new regulatory software supply chain requirements. As a result, Sonatype has achieved a high customer retention rate of approximately 90% in 2021.

Financial Performance

Sonatype was one of the first vendors to recognize the growing importance of DevOps security and develop the ability to "shift left" without neglecting "shield right" security. Over the years, the company has successfully established a strong customer base of more than 2,000 customers and 15 million software developers. Around 70% of the Fortune 100 companies are being supported by the company's DevOps security front.

According to Frost & Sullivan's estimates, Sonatype's DevOps security has successfully achieved an estimated year-on-year growth of slightly under 20% as of 2021. In the same year, Sonatype recorded steady growth across verticals, especially in the banking, financial, services, and insurance (BFSI), service provider, and manufacturing sectors. Frost & Sullivan recognizes Sonatype's focus and steadfast commitment to meeting customers' ever-evolving needs and addressing the pain points in the DevOps security market, enabling the company to continually stay ahead of the curve.

Conclusion

Sonatype has established a steadily growing position in the DevOps Security market since its establishment. The company's success is the result of its aggressive roadmap for innovation and strong customer engagement. Sonatype's innovation engines, its vision of a full-spectrum supply chain management platform, and the accuracy of its analyses bode well for its continued growth.

With its strong performance, Sonatype earns Frost & Sullivan's 2022 Global Technology Innovation Leadership Award in the development and operations (DevOps) security industry.

What You Need to Know about the Technology Innovation Leadership Recognition

Frost & Sullivan's Technology Innovation Leadership Award recognizes the company that has introduced the best underlying technology for achieving remarkable product and customer success while driving future business value.

Best Practices Award Analysis

For the Technology Innovation Leadership Award, Frost & Sullivan analysts independently evaluated the criteria listed below.

Technology Leverage

Commitment to Innovation: Continuous emerging technology adoption and creation enables new product development and enhances product performance

Commitment to Creativity: Company leverages technology advancements to push the limits of form and function in the pursuit of white space innovation

Stage Gate Efficiency: Technology adoption enhances the stage gate process for launching new products and solutions

Commercialization Success: Company displays a proven track record of taking new technologies to market with a high success rate

Application Diversity: Company develops and/or integrates technology that serves multiple applications and multiple environments

Business Impact

Financial Performance: Strong overall financial performance is achieved in terms of revenues, revenue growth, operating margin, and other key financial metrics

Customer Acquisition: Customer-facing processes support efficient and consistent new customer acquisition while enhancing customer retention

Operational Efficiency: Company staff performs assigned tasks productively, quickly, and to a high-quality standard

Growth Potential: Growth is fostered by a strong customer focus that strengthens the brand and reinforces customer loyalty

Human Capital: Commitment to quality and to customers characterize the company culture, which in turn enhances employee morale and retention

About Frost & Sullivan

Frost & Sullivan is the Growth Pipeline Company™. We power our clients to a future shaped by growth. Our Growth Pipeline as a Service™ provides the CEO and the CEO's growth team with a continuous and rigorous platform of growth opportunities, ensuring long-term success. To achieve positive outcomes, our team leverages over 60 years of experience, coaching organizations of all types and sizes across 6 continents with our proven best practices. To power your Growth Pipeline future, visit Frost & Sullivan at http://www.frost.com.

The Growth Pipeline Engine™

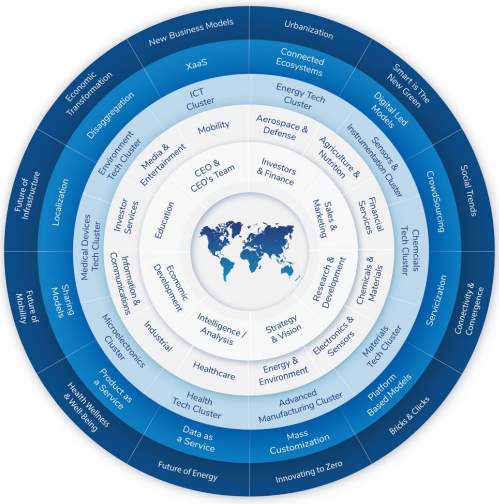
Frost & Sullivan's proprietary model to systematically create ongoing growth opportunities and strategies for our clients is fuelled by the Innovation Generator™.
Learn more.

Key Impacts:

- **Growth Pipeline:** *Continuous Flow of Growth Opportunities*
- **Growth Strategies:** *Proven Best Practices*
- **Innovation Culture:** *Optimized Customer Experience*
- **ROI & Margin:** *Implementation Excellence*
- **Transformational Growth:** *Industry Leadership*

The Innovation Generator™

Our 6 analytical perspectives are crucial in capturing the broadest range of innovative growth opportunities, most of which occur at the points of these perspectives.



Analytical Perspectives:

- Mega Trend (MT)
- Business Model (BM)
- Technology (TE)
- Industries (IN)
- Customer (CU)
- Geographies (GE)