IDC MarketScape

IDC MarketScape: Worldwide Application Security Testing, Code Analytics, and Software Composition Analysis 2022 Vendor Assessment — Coordinating Security and Quality for Resilience and DevSecOps

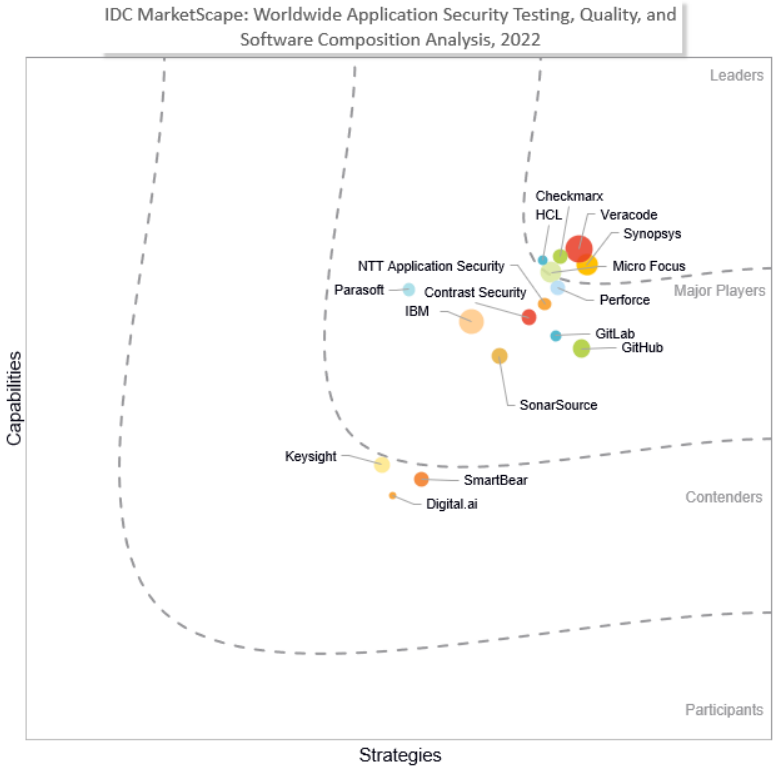
Melinda-Carol Ballou

THIS IDC MARKETSCAPE EXCERPT FEATURES GITHUB

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Application Security Testing, Code Analytics, and Software Composition Analysis Vendor Assessment



Source: IDC, 2022

Please see the Appendix for detailed methodology, market definition, and scoring criteria.

March 2022, IDC #US47097521e

IN THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Worldwide Application Security Testing, Code Analytics, and Software Composition Analysis 2022 Vendor Assessment — Coordinating Security and Quality for Resilience and DevSecOps (Doc # US47097521). All or parts of the following sections are included in this excerpt: IDC Opinion, IDC MarketScape Vendor Inclusion Criteria, Essential Guidance, Vendor Summary Profile, Appendix and Learn More. Also included is Figure 1.

IDC OPINION

Software drives competitive advantage and innovation. Quality and security are pressing business-critical issues as deployment speeds increase, development time frames compress, and application attack surface is a key risk area (made more vulnerable by the ability to easily find susceptible code). IDC's recent survey data indicated that nearly all (90.5%) responding organizations released features with a lead time of a month or less in 2021 (which increased by 26 percentage points from 2020) and those delivering features in 1–2 weeks doubled from 2020 to 2021 (see *U.S. Accelerated Application Delivery Survey,* IDC #US47924622, January 2022). At the same time, at least 55% of IDC surveyed participants experienced security breaches and at least 38% were attacked multiple times, with increasing code scan frequency cited as a proven method for reducing security risks in the near term and architecture and design improvements adding opportunities for strategic, longer-term risk mitigation (see *DevSecOps Adoption, Techniques, and Tools Survey,* IDC #US47597321, April 2021).

In an increasingly complex technology, geopolitical, and economic climate, organizations must understand and analyze software beyond the confines of traditional approaches to automated software quality (ASQ) and respond to the imperative to weave security into quality and the software development life cycle (SDLC) as part of DevOps and DevSecOps — shifting security "left" to incorporate policies, design, and programmatic code-based approaches to help ensure software security and quality. That context informs this assessment. Augmenting our IDC MarketScape ASQ analysis series, this document focuses on application security testing (AST), code quality and analytics, and software composition analysis (SCA) to help support users in their strategy and purchase decisions (following up on our prior software quality analysis and measurement [SQAM] assessment). Cloud-native applications and the push to microservices and containerization as well as the leverage of open source software (OSS) create challenges along with benefits. This includes increasingly problematic assaults on areas such as OSS utilities (like Log4J) that are relatively easy for low-skilled attackers to exploit. API vulnerabilities are an increasing attack vector as another example (with exposed, broken, or hacked APIs leading to major data breaches). As organizations bank on mobile platforms and deploy in the cloud, and as products in the manufacturing sector depend increasingly on embedded software for differentiation, IDC sees security demands extending software quality via deep code analysis, architectural assessment, and metrics. Companies are being driven to understand the impact of their design choices across application portfolios and need visibility "under the covers" via effective policies and a range of automated tools capabilities. These include static application security testing (SAST), dynamic application security testing (DAST), interactive application security testing (IAST), SCA, mobile application security testing (MAST), fuzz testing, penetration testing, metrics, and analysis to understand the consequences to the core application portfolio that runs businesses and their transactions as part of DevOps and DevSecOps continuous pipelines. IDC analyzes this market with these initial findings and for the following reasons:

- Leaders in the AST, SCA, and code quality and analytics market are providers with targeted, excellent functionality and strong strategies in the core areas for AST, SCA, and code analytics, as well as with targeted, visible business focus on code quality, strong references, and execution for secure coding and AST. DevOps combined with security and quality for DevSecOps is explicit for leaders' strategy, along with breadth of AST, SCA, and related capabilities.
- User demand and growth in this arena results from the need for code quality analytics and insight into impact on quality and security across application portfolios in increasingly complex development and deployment environments. When organizations empower developers with appropriate automated tools, process/policies, and contextualized training, the results are more secure applications, faster remediation, and developers taking ownership of security.
- With the adoption of multiple scanning and other DevSecOps automation tools (most organizations have many), both orchestration and security policy management strategies are a core execution gap and opportunity.
- User engagement and the need for visibility into architecture and code quality and security, along with effective metrics to assess performance of internal and external resources, are driving adoption in this area of the automated software quality and DevSecOps adoption.
- In a volatile economy, as companies reinvest, financial constraints, global competition, and innovation drive demand for rapid access to both AST, SCA, and quality solutions and metrics to evaluate code and project success. This complements emerging quality needs for mobile and digital quality, security, cloud, Internet of Things (IoT), agile DevOps, and other areas.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

IDC evaluated 16 vendors for inclusion in the IDC MarketScape for application security testing, software composition analysis, and code analytics, as an overlay for providers evaluated for the IDC MarketScape for our ASQ series. Vendors needed to have sufficient ASQ capabilities available and/or partner integration in key areas of concern for IDC clients, including static application security testing, dynamic application security testing, interactive application security testing, SCA, mobile application security testing, fuzz testing, penetration testing, assessment of architectural design impact on quality and security, and code analytics and reporting and across application portfolios) or integration with providers as part of their strategy. (The primary focus here is secure coding and application security testing, defined in *IDC Market Glance: DevSecOps, 1Q22,* IDC #US48599722, February 2022.) Vendors needed to appear in IDC discussions with end-user clients as part of RFP and other inquiry for AST and/or SCA or related code quality areas during 2021–2022 and needed minimum overall revenue of $10 million for CY20, with at least $5 million of that revenue from security analytics, intelligence, response, and orchestration (SAIRO), DevSecOps, and/or ASQ. Smaller targeted vendors with engaging functionality and focus were also included in this study to provide context for emerging areas of importance and partner strategies to enter the market. Although relevant for code analytics for this market, we did not include some providers at this point in our research because of the lack of broader ASQ and/or SAIRO capabilities currently but will be likely to include additional vendors in future updates to this research and can discuss as needed for inquiry. Also, we did not include standalone SCA vendors (such as Snyk, Sonotype, or Revenera) but looked to incorporate providers that offered broader security and/or ASQ capabilities along with SCA. The vendors evaluated are Checkmarx, Contrast Security, Digital.ai, GitHub, GitLab, HCL, IBM, Keysight (formerly Eggplant), Micro Focus, NTT Application Security (formerly White Hat Security), Parasoft, Perforce, SmartBear, SonarSource, Synopsys, and Veracode.

IDC structured its approach to inclusion for vendors in the quality and application security testing category based on the strength of the vendor products' associated capabilities and strategies, revenue share in part (as indicators of adoption and staying power), and differentiated position and capabilities in emerging markets of concern. The focus for IDC customers on secure coding, application security leveraging AST, SCA, code analytics, assessment of architectural design, and overall application health for security in DevSecOps environments and contextualized developer engagement for "security as code" were key factors for leadership. Product breadth and depth, scalability, coordination with continuous integration/continuous delivery (CI/CD) and DevOps for DevSecOps strategies (and end-to-end life-cycle management) and strong data analytics, and emerging machine learning (ML)/artificial intelligence (AI) capabilities as well as process support for systemic adoption and engagement for AST/SCA combining quality with security were additional leadership drivers.

VENDOR SUMMARY PROFILES

This section explains IDC's key observations resulting in a vendor's position in the IDC MarketScape. While every vendor is evaluated against each of the criteria outlined in the Appendix, the description here provides a summary of each vendor's strengths and challenges.

GitHub

GitHub is positioned in the Major Players category in the 2022 IDC MarketScape for worldwide AST, code analytics, and software composition analysis.

Microsoft acquired GitHub in 2018, and the combined product sets from each company are considered in the IDC MarketScape series for automated software quality (ASQ). From GitHub, this includes GitHub Enterprise (GHE) 3.2, GitHub Advanced Security, GitHub Actions, GitHub Codespaces, and GitHub Copilot. Microsoft's products include Azure Test Plans within Azure DevOps, Azure DevTest Labs, App Center Test, Visual Studio App Center, Test Explorer, Power Apps Test Studio, and Playwright 1.16.

GitHub, founded out of San Francisco in 2008, began as a Git repository hosting service but has broadened toward an end-to-end DevOps platform over the past decade. GitHub is the repository for most open source software projects, hosting more than 200 million private and public repositories with over 73 million registered users (as of 4Q21). GitHub also cites 90% of the Fortune 100 as customers. GitHub's ubiquity, seminal position for open source and developer communities, and popularity contributed to the company's acquisition by Microsoft in 2018. Since the acquisition, GitHub has continued to operate autonomously. Together, the companies offer a range of DevOps and ASQ tools, including two DevOps platforms (Azure DevOps and GitHub Enterprise), with their integrated testing capabilities, as well as several other testing tools under the broader Azure umbrella.

Company Strategy

GitHub is committed first to its open cloud-based platform to further development and coordination with GitHub Enterprise while leveraging its open source tradition and sustaining the community and marketplace. GitHub continues to extend the company's position as a destination platform for developers organically through product growth primarily, such as launching the cloud-based development environment GitHub Codespaces, GitHub Actions, and an enhanced GitHub Issues (available in beta), as well as through acquisition, including code analysis vendor Semmle in 3Q19 and JavaScript packaging vendor npm in 2Q20.

GitHub's testing capabilities are predominately security focused via the company's GitHub Advanced Security offering, which is an add-on SKU, available for GitHub Enterprise , with core supply chain capabilities (SCA) included as part of GitHub Enterprise. Foremost, GitHub Advanced Security leverages its semantic code analysis engine, CodeQL, to offer automated SAST for code changes in the repository. Differentiated in its code-as-data approach, code is scanned via queries, and results are displayed within the developer's workflow. In addition, GitHub offers SCA via Dependency Review, which informs users of what dependencies are leveraged across their projects via the Dependency Graph and the associated vulnerability data. Dependabot helps keep repositories secure by staying up to date with the latest releases of packages and applications and using the Dependency Graph to understand which repositories are affected. Finally, GitHub Advanced Security scans code at commit for secrets, including API keys and authentication tokens, to alert repository administrators while assisting in mitigation. Other ASQ capabilities leverage GitHub Actions, the platform's CI/CD automation tool, tightly integrating external test tools and providing each test's results in the developer's pull request. The GitHub Marketplace currently offers over 13,000 actions, with almost 1,000 in the testing category.

GitHub's platform and SAST and SCA capabilities are primary areas of focus for this IDC MarketScape, on the one hand. On the other, quality and DevOps capabilities available in coordination with Microsoft further augment and differentiate GitHub's positioning from IDC's perspective; code analytics, quality, DevOps, and DevSecOps are synergistic and reliant on one another. In that context, Microsoft's developer strategy has evolved over decades, with Team Foundation Server becoming Visual Studio Team Services, which is now Azure DevOps, Microsoft's DevOps offering. Microsoft currently offers a range of ASQ capabilities, mainly under the Azure umbrella. Microsoft's Azure Test Plans, a browser-based test management solution, offers manual and exploratory testing capabilities as part of Azure DevOps. Azure DevTest Labs provides pre-provisioned environments for developing and testing applications via a service. Announced in 4Q21, Azure Chaos Studio is a managed service for improving application resilience via fault injection. Microsoft also announced a general preview for Azure Load testing in 4Q21, a managed Azure service for developers and testers to generate high-scale load with custom Apache JMeter scripts to help find and fix performance bottlenecks and optimize Azure infrastructure. Microsoft describes this as a fully managed load-testing service optimized for Azure that helps developers and testers quickly and easily generate high-scale load, identify bottlenecks with actionable insights and recommendations, and build load testing into DevOps workflows. Finally, Azure Defender for container registries scans container images for vulnerabilities and is triggered on push, recent pulls, and imports, providing findings and recommendations in Azure Security Center.

Other testing capabilities across the broader Microsoft portfolio include:

- App Center Test is a test automation service for native and hybrid mobile applications.
- Test Explorer within Visual Studio provides unit testing and debugging, as well as code coverage analysis.
- Power Apps Test Studio is a low-code automated testing solution for business applications built in Microsoft Power Apps.
- In 2020, Microsoft also initiated Playwright, an open source, cross-browser web testing framework, which is in private preview now and will be in public preview in 2023. The project automates testing across Chromium, Firefox, and WebKit browsers; executes the tests in parallel; and provides test isolation and flexible test environment configuration. Live Unit

Testing runs impacted tests in the background as you type. You'll never forget to do a test run before check-in ever again!

- IntelliTest smartly generates fuzz test suites that aim to provide complete coverage of your code down to individual logic branches.
- Fakes is a mocking framework that generates stubs and shims to help unit test legacy code without needing to re-architect.

GitHub's and Microsoft's approach with their AST and ASQ strategy is differentiated by the ubiquity of both organizations' foundational position across their vast communities of developers and enterprise businesses. Similarly, both bake testing into their products. With GitHub, code scanning is built into the developer experience, and test results are provided directly within pull requests rather than in a disparate report or dashboard. Similarly, much of Microsoft's testing capabilities reside within a product, such as Azure DevOps or Visual Studio App Center (and Test Studio with the Power platform). With end-to-end platforms flanking testing capabilities, both Microsoft and GitHub have the chance to offer a holistic view of quality and security testing.

References with whom IDC spoke cited coordinating (or piggybacking) GitHub platform adoption with AST tools as a key point of engagement for their teams, enabling developers to better find and surface security issues. As part of its evaluation, one customer took vulnerabilities that had occurred historically and both created its own rules and used GitHub default rules to find issues (while seeking to limit the occurrence of false positives). The teams chose GitHub due to its data flow, strong Java support, and the ability to evolve basic rules to more nuanced ones (to help contain false positives and improve decision making during development, such as identifying poor practices when making pull requests and finding existing issues even if new comparable issues with appropriate severity levels were being prevented). They are now using GitHub Advanced Security on a 6,000-person GitHub Enterprise instance, and every developer must scan code when making a commit (using looks good to me [LGTM] to host the documentation so that developers have context when an issue is found). Some customers are also using GitHub capabilities for non-security use cases as a more general search engine to help determine what they need to target when refactoring code. Microsoft customers discussed the benefits of close test coordination within the developer experience for Azure DevOps and opportunities to leverage across areas.

Users who are leveraging Microsoft's testing capabilities benefited from its close coordination with Azure DevOps and leverage of IntelliTest to generate fuzz tests and improve test coverage.

Strengths

Strengths for GitHub's AST solution include developer support via close integration with the company's pervasive GitHub platform (and related capabilities such as GitHub Actions, Copilot, and Codespaces), ease of workflow engagement with processes such as pull requests and code commits, and foundational capabilities for SAST and SCA and integration with additional security testing partners and providers. Microsoft's testing capabilities are similarly incorporated into Azure DevOps primarily, with additional capabilities in Visual Studio and for low-code testing solution available as part of the Power platform. Both Microsoft and GitHub are pervasive and far-reaching in their domains and their combined presence is formidable with significant potential for cross-leverage. Poor software quality and ineffective testing are bottlenecks to rapid deployment. Incorporating testing into Microsoft's and GitHub's respective portfolios can put testing tools into the hands of developers to run tests in their individual environment, as well as automatically in the CI/CD pipeline. Both deliver collaborative and responsive customer support, and emerging AI and ML initiatives underlie automation capabilities and

are expanding to help make data actionable and pragmatic for users (with GitHub's Copilot, for instance).

Challenges

A challenge GitHub and Microsoft face is one of synergism. How do they execute effectively in separate spheres yet leverage opportunities to coordinate? GitHub Enterprise and Azure DevOps have some overlap in functionality and are aligning more closely. In that context, the future trajectory of the products and their relationship is not clearly delineated, which can create hesitancy for adoption (due to concerns about longevity). Further, the overall testing and quality strategy both is unclear and offers Microsoft and GitHub key opportunities to coordinate and execute. (Continuous testing is vital to DevOps velocity to producing quality software quickly.) Though offering some automation of testing via GitHub Actions, GitHub lacks native quality testing capabilities, and the breadth of its security testing capabilities are not as rich as mature DevSecOps standalone products. Similarly, discerning the range of testing capabilities that Microsoft provides is challenging; testing functionality is tightly integrated within products, but messaging strategy and cross-platform/cross-product integrations are not as clear. On the positive side, GitHub has been executing well with the AST capabilities it offers and with third-party integrations to testing products, reflecting GitHub's strategy to invest in securing the software supply chain, scanning, and providing organizational security overviews to customers. In that vein, GitHub is also a CVE authority and is invested in application security as it evolves its product and its leadership position for the open source community.)

On the Microsoft side, Azure DevOps teams launched relevant, targeted testing initiatives in 2021 that include Azure Chaos Studio, Playwright open source project, and a public preview release for Azure Load test as Microsoft moves in the direction of validating and renewing a test portfolio. (However, Microsoft deprecated its cloud-based load testing as part of Visual Studio in May 2020.) Microsoft needs to leverage opportunities to coordinate these testing capabilities with the Power platform (Test studio), App Studio, and App Center Test, as well as with the GitHub portfolio. In that context, the testing integration and G2M coordination between GitHub and Microsoft that would naturally enhance capabilities and deployment can be hindered by GitHub's independent positioning that it relies on to maintain its community and delineated position in the open source world. Overall, GitHub and Microsoft have significant, vital, and salient opportunities to evolve capabilities for ASQ and AST moving into 2023 and beyond to benefit the core developer and enterprise businesses and communities that rely on them, with integrated, continuous quality with effective execution.

APPENDIX

Reading an IDC MarketScape Graph

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here and now. Under this category, IDC analysts will look at how well a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis, or strategies axis, indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level

decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represents the market share of each individual vendor within the specific market segment being assessed.

Key trends driving user adoption include the urgent need to "shift left" with continuous testing by applying agile approaches to quality practices to avert the expense and reputational damage of finding code problems in production. We also increasingly see coordination between quality and security testing — the opportunity to design and architect up front for resilience and the ability to leverage emerging AI and ML capabilities to evolve better quality hygiene, processes, and workflows to improve code quality at a time of urgent demand for fast deployments. The emergence of multimodal platforms beyond mobile, including mixed reality and IoT, will continue to drive opportunities for creativity on the part of test automation vendors and broader engagement. Along with the democratization of development with no-code/low-code approaches, there is a commensurate demand to incorporate testing into these environments so that nonprofessional developers can create better quality code. Leverage of machine learning and artificial intelligence in that context becomes increasingly important. The rise of APIs as the enabling technology for services development in these environments and of RPA brings additional opportunities to automation of mundane repetitive tasks and to help ensure the quality of these enabling technologies. For these reasons, in part, we are bullish about the ASQ adoption and coordination with key organizational and process change for DevOps and DevSecOps moving forward.

IDC MarketScape Methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the vendors, publicly available information, and end-user experiences in an effort to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

Market Definition

Software Quality Analysis and Measurement

The software quality analysis and measurement (SQAM) market is a competitive market covering the following functional markets: automated software quality (ASQ), revenue from security, analytics, intelligence, response, and orchestration (SAIRO) and software change, configuration, and process management (SCCPM) to encompass revenue for code quality analytics, AST and related areas, and SCA. This market is informed by IDC's DevSecOps research, definitions, and context (see *Worldwide DevSecOps Software Tools Market Shares, 2020: Strong Growth as DevOps Teams Prioritize Security,* IDC #US48051321, July 2021).

LEARN MORE

Related Research

- *IDC Market Glance: DevSecOps, 1Q22* (IDC #US48599722, February 2022)
- *Worldwide DevSecOps Software Tools Market Shares, 2020: Strong Growth as DevOps Teams Prioritize Security* (IDC #US48051321, July 2021)
- *DevSecOps Adoption, Techniques, and Tools Survey* (IDC #US47597321, April 2021)

Synopsis

This IDC study uses the IDC MarketScape model to provide an assessment for application security testing, code analytics, and software composition analysis, evaluating automated tools capabilities to unite quality with security approaches as one of four ASQ IDC MarketScape assessments to provide a comprehensive view and overlay across key areas of the market – enterprise ASQ/DevOps, cloud testing/ASQ SaaS, and mobile testing/digital quality. Organizations seeking processes, services, and product automation capabilities for ASQ come to their decision making with varying levels of maturity, differing pain points, and challenges. This is even more the case in a volatile global economy as companies continue to struggle with both constrained and complex sourcing, limited QA resources, and varying levels of flexibility to meet business and competitive pressures. The intent with IDC's quality/security ASQ criteria and the four-document series is to demonstrate weighting approaches for the areas of greatest importance that come up for users making high-end ASQ selections currently with transformative demands for mobile, cloud, IoT, and other areas. Too frequently, users and vendors see "one" sample market assessment diagram and assume that a single model for the market will directly address all their needs (with little context for user-specific challenges or variegated maturity levels). We believe that in-context weighting and analysis as an overlay across our ASQ vendor analysis is optimal (and less simplistic) to enable pragmatic insight for users making decisions in a dynamic and increasingly chaotic, complex global competitive environment. Additional weighting and visibility are available individually – yet publishing multiple ASQ IDC MarketScape documents can enable decision makers to "see" varying approaches based on their peers' experiences, as they make use of IDC's assessments.

"Software drives competitive advantage and innovation, and quality and security are pressing business-critical issues as deployment speeds increase, development time frames compress, and application attack surface is a key risk area (made more vulnerable by the ability to easily find susceptible code)," said Melinda Ballou, research director for IDC's Application Life-Cycle Management, Quality, and Portfolio Strategies service. "At the same time, at least 55% of IDC surveyed participants experienced security breaches and at least 38% were attacked multiple times, with increasing code scan frequency cited as a proven method for reducing security risks in the near term, and architecture and design improvements adding opportunities for strategic, longer-term risk mitigation. Creating strategies that coordinate quality and security teams by leveraging effective code analytics automation and processes for DevSecOps exemplifies broader portfolio coordination. Automated solutions in this context can provide a basis for quality collaboration for security and quality teams to enable continuous quality as part of end-to-end DevOps. While this IDC MarketScape focuses on AST, code analytics, and SCA, IDC has chosen the context of three additional sample weighting strategies that have currency in 2022 moving into 2023 and are frequently requested by users speaking with us – cloud testing/ASQ SaaS, enterprise ASQ, and mobile testing/digital quality. Global organizations seeking to coordinate continuous DevOps and other areas demand high levels of functionality, scalability, and maturity overall to execute well (for an "enterprise" ASQ view)."

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com