DevSecOps and Application Security

AN IDC CONTINUOUS INTELLIGENCE SERVICE

IDC's *DevSecOps and Application Security* researches the products, technologies, and automated security processes that are used to shift security to the left-hand side of the SDLC and that inject security into applications as part of the DevOps pipeline. This includes static, dynamic, and interactive analysis, software composition analysis, secrets management, runtime application self-protection, API security, container and Kubernetes security, and web application firewalls. It also includes the role of development tool vendors that offer code security services such as commercially supported and compliance-verified open source solutions.

Markets and Subjects Analyzed

- DevSecOps adoption drivers
- Identification of DevSecOps innovators and best practices
- Establishing and tracking critical DevSecOps tools enabling automation
- Blending security and governance into DevOps processes
- IT operations runtime security practices
- Securing cloud-native application architectures
- Building a DevSecOps culture
- Impacts of modern composite applications on application security

Core Research

- DevSecOps Market Share
- DevSecOps Market Forecast
- Market Analysis Perspective: DevSecOps
- DevSecOps Survey

In addition to the insight provided in this service, IDC may conduct research on specific topics or emerging market segments via research offerings that require additional IDC funding and client investment. To learn more about the analysts and published research, please visit: DevSecOps and Application Security.

Key Questions Answered

1. What are the approaches toward DevSecOps adoption?
2. What are enterprise best practices for efficient and effective DevSecOps automation and implementations?
3. How does DevSecOps affect the roles and responsibilities of information security professionals, developers, testers, and IT operations?
4. What are the best ways to manage application development security associated with the software supply chain and the sprawling collection of artifacts?
5. What modern technologies are emerging that could impact how DevSecOps is accomplished in the future?
6. What is the size of the market for DevSecOps tools, and where is it forecast to be in the future?

Companies Analyzed

This service reviews the strategies, market positioning, and future direction of several providers in the DevSecOps market, including:

Aqua Security, Checkmarx, Cisco, Contrast Security, F5, GitHub, GitLab, IBM, Imperva, JFrog, Micro Focus, NTT Application Security, Snyk, Sonatype, Synopsys, Sysdig, Veracode, and White Source (Mend).