DevSecOps, Vulnerability Management, and Software Supply Chain Security

IDC's *DevSecOps, Vulnerability Management, and Software Supply Chain Security* researches the products, technologies, and automated security processes that are used to integrate security into applications as part of the software development life cycle (SDLC). Technologies include static, dynamic, and interactive analysis; software composition analysis; infrastructure-as-code security scanning; secrets scanning and management; runtime application self-protection; mobile application security testing and hardening; threat modeling; API security; container and Kubernetes security; LLM/AI model and application security, and web application firewalls. It also includes the tools used to manage application vulnerabilities, such as application security posture management (ASPM) and application security risk management solutions. Also covered is the security of the components that go into developing and deploying an application, such as people, processes, dependencies, and tools, including securing developer identity and access, provenance and attestation, CI/CD and pipeline security, software bill of materials (SBOM), and safe open source software curation and management.

MARKETS AND SUBJECTS ANALYZED

- DevSecOps adoption drivers and best practices
- Blending security and governance into DevOps processes
- Securing AI apps and AI-generated code
- IT operations runtime security practices
- Securing cloud-native application architectures
- Building a DevSecOps culture
- Impacts of modern composite applications on application security
- Application vulnerability prioritization and remediation
- Generating, managing, and operationalizing SBOMs
- Implications of software security standards and regulations

CORE RESEARCH

- DevSecOps Market Share
- DevSecOps Market Forecast
- Application Vulnerability Management Market Share
- Application Vulnerability Management Forecast
- Market Analysis Perspective: DevSecOps, Vulnerability Management, and Software Supply Chain Security
- DevSecOps Survey
- DevSecOps Mergers and Acquisitions

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, Vulnerability Management, and Software Supply Chain Security.

KEY QUESTIONS ANSWERED

1. Who are the major players in the market?
2. What is the size and market opportunity for solutions in the market?
3. What are the approaches toward DevSecOps adoption?
4. How does DevSecOps affect the roles and responsibilities of information security professionals, developers, testers, and IT operations?
5. What are the components of the software supply chain that organizations must secure, and what tools are available?
6. What modern technologies are emerging that could impact how DevSecOps is accomplished in the future?
7. How are these tools using generative AI today, and what is coming in the future?

COMPANIES ANALYZED

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

Amazon Web Services, Aqua Security, Broadcom, Checkmarx, Cisco, Contrast Security, CyberArk, Datadog, Dynatrace, Fortinet, GitHub, GitLab, Google, HCLSoftware, IBM, Imperva, JFrog, Mend, Microsoft, OpenText, Palo Alto Networks, ReversingLabs, Snyk, Sonatype, Synopsys, Sysdig, and Veracode.