# JFrog-Sponsored IDC Study Shows Growing Developer Focus on Software Security, Impacting Companies' Competitive Advantage

*Titled the "Hidden Costs of DevSecOps," the IDC InfoBrief Reveals Companies Spend an Average of $28K Per Developer Annually on Identifying, Evaluating, and Addressing Software Security Concerns*

**Sunnyvale, Calif., October 9, 2024** — JFrog Ltd. ("JFrog") (Nasdaq: FROG), the Liquid Software company and creators of the JFrog Software Supply Chain Platform, released the findings of an IDC survey indicating developers are spending significantly more time and companies are spending $28K per developer yearly on security-related tasks such as manual application scan reviews, context switching, and secrets detection, among other items. The IDC InfoBrief, *"The Hidden Cost of DevSecOps: A Developer's Time Assessment,"* sponsored by JFrog, showed 50% of senior developers, team leaders, product owners and development managers experienced a significant increase in the number of hours spent weekly on software security-related tasks, detracting from their ability to innovate, build, and deliver new business applications,

"Securing the software supply chain already poses significant challenges for organizations, but it becomes more complex when multiple tools are used, forcing developers to toggle between multiple environments, leading to inefficiencies, wasted time, and increased risk," said Asaf Karas, CTO of JFrog Security. "IDC's survey creates a compelling case for companies to invest in streamlined security processes, tooling and training, to empower their developers to be more efficient and effective in protecting the software supply chain."

Half of survey respondents said they spend an estimated 19% of their weekly hours on security-related tasks, oftentimes outside normal working hours, which could lead to a reactive approach to security rather than a proactive one. Other key findings from the IDC survey include:

- **Chasing Ghosts: Eliminating False Positives:** Developers spend 3.5 hours on average manually reviewing security scanning findings because of false positives and duplicates.
- **Context Matters:** 69% of developers agree or strongly agree that their security-related responsibilities require them to frequently switch contexts between various tools, slowing efficiency. Multitool context switching can also increase token usage for bypassing reauthentication per platform. Tokens can be helpful in application

development but can also be quickly forgotten and leave backdoors in companies' systems for attacks.

- **Secrets are No Fun:** Developers devote 50% of their time to understanding and interpreting secrets scanning results, making changes to code to remediate findings, and updating secrets management measures.
- **Infrastructure Investigation:** Infrastructure-as-Code (IaC) – used to automate the provisioning and management of IT infrastructure, such as servers, networking, operating systems, and storage – must be scanned every time code changes, with more than 54% of developers saying they run IaC scans weekly or monthly.
- **SAST Isn't a Blast:** Despite static application security testing (SAST) tools being integrated to local development environments to provide findings as developers code, only 23% of developers are running SAST scans before deploying code into production, leaving a huge gap for malicious code to slip through.

"DevSecOps is not just a business imperative; it is the cornerstone of building the secure applications of the future. However, a significant challenge lies in overcoming inefficient, poorly implemented tools that squander developers' time and inflate costs," said Katie Norton, Research Manager, DevSecOps and Software Supply Chain Security at IDC. "To be successful, IT and software development team leaders must automate repetitive and time-consuming tasks, ensure DevSecOps tools deliver accuracy with minimal false positives, and provide ongoing access for developers to application security education and resources so they can keep pace with a rapidly increasing threat landscape."

The IDC InfoBrief surveyed senior developers, team leaders, product owners and development managers from companies in 20+ industries with 1K+ employees across the U.S., UK, France and Germany. For more insights from the IDC InfoBrief, "The Hidden Cost of DevSecOps: A Developer's Time Assessment," (IDC #US52537524, September 2024) download the report.

###

**Like this story? Tweet this:** New @IDC survey finds developers severely underestimate the time they spend performing #DevSecOps tasks, leading to hidden costs for their organizations. Read the report: https://bit.ly/4feUtjl #DevOps #security #MLOps #softwaresupplychain

About JFrog

JFrog Ltd. (Nasdaq: FROG), is on a mission to create a world of software delivered without friction from developer to device. Driven by a "Liquid Software" vision, the JFrog Software Supply Chain Platform is a single system of record that powers organizations to build, manage, and distribute

software quickly and securely, ensuring it is available, traceable, and tamper-proof. The integrated security features also help identify, protect, and remediate against threats and vulnerabilities. JFrog's hybrid, universal, multi-cloud platform is available as both self-hosted and SaaS services across major cloud service providers. Millions of users and 7K+ customers worldwide, including a majority of the Fortune 100, depend on JFrog solutions to securely embrace digital transformation. Learn more at www.jfrog.com or follow us on X @JFrog.

**Media Contact:**
Siobhan Lyons, Sr. Manager, Global Communications, JFrog, siobhanL@jfrog.com

**Investor Contact:**
Jeff Schreiner, VP of Investor Relations, JFrog, jeffS@jfrog.com