ARCTIQ + JFrog

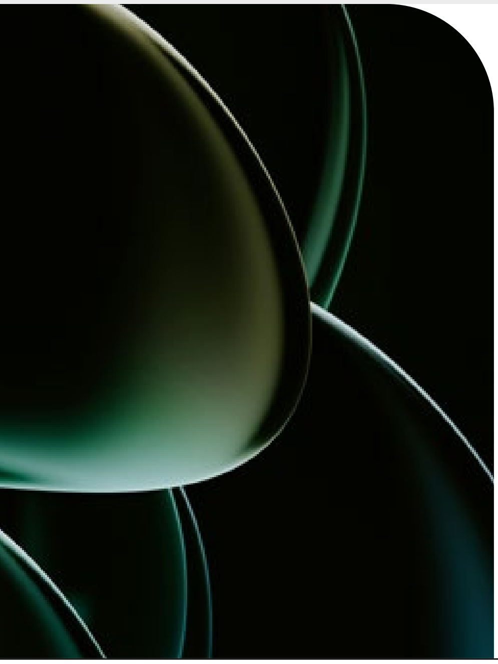
Secure the Software Supply Chain with Arctiq & JFrog

Why Shai-Hulud 2.0 Is a Stark Warning For Application Teams

Do your teams use Zapier? Postman? Do you know?

A decade ago, the most recognizable risk from a supply-chain attack was using a sketchy package. But the threat landscape has changed. Today's supply chain attacks are both carefully crafted and have enormous blast radii. Threat actors focus on compromising maintainer accounts of popular, widely-used (and quite legitimate) packages and then injecting trojanized versions of these legitimate packages into the supply chain. Within minutes, automated build pipelines pull the malicious version, which immediately begins exfiltrating CI/CD secrets and attempting to move laterally into the cloud environment – exfiltrating cloud credentials and secrets and establishing persistence.

When attackers are going after maintainers, it's no longer enough to make sure you're downloading a "legitimate" package from a trusted source. You have to make sure that the packages themselves are secure.



How JFrog + Arctiq Can Stop It From Happening To You

In the summer of 2025, JFrog's Security Research Team studied a series of supply-chain hijacking attacks. They discovered that most attacks are discovered within 48 hours, as the infected packages roll out through the community, and security teams begin to respond. Even the most sophisticated attacks are discovered generally within the first fourteen days.

Curate Your Supply Chain with JFrog Curation

JFrog Curation acts as a “package firewall” at the first gate of your software supply chain, preventing open-source security threats from ever entering your organization. It automatically vets and blocks packages with vulnerabilities, malicious code, or license compliance issues before developers download them, while seamlessly directing them toward pre-approved, trusted alternatives. This provides centralized visibility, auditable tracking, and frictionless package consumption that enhances rather than hinders developer productivity.

Secure Your Software Delivery Lifecycle with Arctiq

Arctiq’s Cloud and Application Security team can help you craft a curation policy that works for your teams and seamlessly integrate it into your existing DevSecOps process. We help you assess risk, model DevSecOps maturity, and determine a governance framework that works for your organization and then implement the engineering capabilities in your CI/CD pipelines that secure your software supply chain.

If you’ve been affected by Shai-Hulud – and especially if you can’t explicitly confirm you haven’t – now’s the time to evaluate your software supply chain security. Let Arctiq walk you through the threats, the risk, and visualize the gaps in your current application security model. We’ll help you identify a controls framework, compensating controls, and governance framework that helps you build continuous visibility, defense in depth, and a strategy for intelligent resolution.

Book a consultation