

Secure Every Transaction:

The Retail Software Supply Chain in 2026

The Retail Software Attack Surface

The Open Source Reality

90%

of modern retail applications now rely on open-source components. For DevSecOps personas, this highlights the need for the automation and blocking of malicious and immature packages

The "Retail Target"

58%

jump in ransomware attacks in 2025, with software supply chain vulnerabilities being the #1 entry point

The Forecast

By 2025

45%

of global organizations will have experienced attacks on their software supply chains—a three-fold increase from 2021



The High Cost of "Business as Unusual"



The Downtime Tax

Large-scale retailers now lose an average of **\$1.1M per hour** during peak seasonal outages (Black Friday/Cyber Monday). Even "normal" downtime averages **\$300,000+ per hour**.



The Brand Scar

44% of consumers report they will permanently stop shopping with a brand after a single public system failure or security breach.



The Technical Debt Load

Developers in retail spend an average of **30% of their time** fixing vulnerabilities rather than building new features. (DevSecOps goal: Shift security left to reclaim this time).



Open-Source
usage



The Edge Computing Frontier

Top-tier retailers now manage an average of 500 to 5,000+ remote locations (stores/warehouses). Each location is now a "mini-data center" requiring secure, zero-latency software updates.

The "Tool Sprawl" Crisis

15+

The average retail DevSecOps team manages **15+** different security and DevOps tools, leading to "Alert Fatigue."



The Distribution Gap

62%

62% of retail IT leaders cite "deployment to the edge" as their biggest bottleneck for 2025.



The Solution

50-70% reduction

Organizations using a unified binary repository (like Artifactory) see a 50-70% reduction in deployment wait times across distributed store environments.



The Consolidation Value



of the **Fortune 100** are moving toward Platform Consolidation to eliminate data silos between security and development teams.

Don't let a compromised dependency shut down your storefront.

Build a resilient software supply chain.

