5 AppSec Risks That Threaten Your Business

A single weak point in a line of code can create an open door for attackers.

The cost of an average breach is $3,920,000.[1]

Nearly 80% of apps contain at least one critical or high vulnerability.[2]

Are you protected from these common risks?

Risk 1 Dependence on open source

Open source code can have serious vulnerabilities, yet it often goes untested.

When it comes to open source components within apps, 87% of open source applications inherit a critical severity vulnerability from referenced components.[2]

The use of open source code is on the rise.

Right: percentage of projects utilizing open source components (data from past reports).

Risk 2 Long exposures

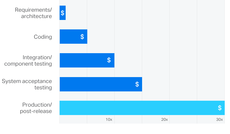
The time to patch a vulnerability has gone down over the years. However, even a prompt patch management program can leave you exposed for months, often leaving significant gaps between the identification of a vulnerability and patch availability.

The average time to identify and contain a breach is 279 days.[1]

Risk 3 Costly remediation

Removing security flaws gets more time-consuming and expensive the longer they live in code. Removing vulnerabilities—and preventing new ones from being introduced in development—keeps developers focused on delivering innovation.

Relative cost to fix vulnerabilities (based on time of detection)[3]



30x

Vulnerabilities discovered in the production/post-release phase are 30 times more costly to fix than when found earlier in the lifecycle.

2020 technical debt cost

$6.1 trillion

Technical debt is a forward-looking metric that represents the effort required to fix problems that remain in the code when an application is released.

Risk 4 Repeated security flaws

Many development teams keep making the same software security mistakes.

OWASP Top 10[4]

2013 (Previous)	2017 (New)
A1—Injection	A1—Injection
A2—Broken Authentication and Session Management	A2—Broken Authentication and Session Management
A3—Cross-Site Scripting (XSS)	A3—Cross-Site Scripting (XSS)
A4—Insecure Direct Object References *Merged with A7*	A4—Broken Access Control (Original category in 2003/2004)
A5—Security Misconfiguration	A5—Security Misconfiguration
A6—Sensitive Data Exposure	A6—Sensitive Data Exposure
A7—Missing Function Level Access Control *Merged with A4*	A7—Insufficient Attack Protection (NEW)
A8—Cross-Site Request Forgery (CSRF)	A8—Cross-Site Request Forgery (CSRF)
A9—Using Components with Known Vulnerabilities	A9—Using Components with Known Vulnerabilities
A10—Unvalidated Redirects and Forwards (Dropped)	A10—Underprotected APIs (NEW)

Risk 5 AppSec not integrated with DevOps

As more companies integrate and deploy automated security solutions, the cost of data breaches diminishes and the number and speed of remediated issues greatly improves.

90%

Organizations that had not deployed security automation experienced breach costs that were 90% higher than breaches at organizations with fully-deployed automation.

70%

Automation of AppSec processes can drive down mean time to remediation (MTTR) by as much as 70%.[5]

Don't bet your business on risky software. Take control today.

Software security checklist

1. Take ownership for the security of your software—no matter who wrote it.
2. Arm developers with the tools they need to find and fix vulnerabilities early.
3. Use AppSec testing to find and fix vulnerabilities proactively.
4. Test, monitor, and protect software throughout its lifecycle—from development and QA to production.

Learn More

Scan all your code—on demand or on premises—with Micro Focus Fortify.

Learn about Fortify ›

SOURCES

1. IBM Security: 2019 Cost of a Data Breach Report
2. 2019 Application Security Risk Report by the Micro Focus Software Security Research team
3. Technology Insight for Software Composition Analysis Report by Gartner (2018)
4. Forrester: The State of Application Security 2019
5. OWASP graph information from ActiveReach.net

microfocus.com