CYCOGNITO

QUICK TAKE

Closing the Production App Risk Gap – A Business Imperative

Managing Business Risk Across the Software Lifecycle

Business risk doesn't stop at deployment. Every live and exposed application is a digital storefront, a supply chain gateway, or a customer experience channel. And yet, many security programs still treat "done" as "secure" the moment code is merged.

60% of real-world exploited vulnerabilities are discovered after deployment

Verizon Data Breach Intelligence Report 2024

60%

This is a business risk blind spot, not just a security oversight. Leadership accountability demands visibility into real-world, post-deployment risk, not just code quality.

Mapping Risk to the Right Controls at the Right Time

Different threats emerge at different stages of the software lifecycle. Leadership must prioritize risk validation at each juncture to avoid blind spots. SAST and SCA catch flaws early in the development process but only within static code. They cannot account for how applications behave once deployed. DAST and IAST provide dynamic insight into system behavior, uncovering issues that surface during real-world execution..

While testing during development is foundational, it cannot replace visibility into how live systems interact with users, data, and third-party services. Risks introduced through misconfigurations, deployment drift, or exposed APIs can only be validated during runtime. Without this visibility, leadership is forced to make assumptions rather than informed decisions about their most critical digital assets. Effective application risk management requires applying the right level of scrutiny at each stage, ensuring there are no gaps between control and consequence.

Managing Application Risk Across the DevSecOps Lifecycle

Business risk arises at every stage of the software lifecycle. Effective risk management requires aligning the right controls to the right risks at the right time:

Stage	Risks Introduced	Controls Needed
Code & Build	Insecure logic, vulnerable libraries	• **SAST** (code analysis) • **SCA** (open-source risk)
Pre-Production	Misconfigurations, logic flaws in context	• **DAST** in staging • **IAST** for runtime visibility
Production	Live attack surface, runtime exposures	• **DAST** in production • **Runtime protection / observability** • **Attack surface monitoring**

To manage business risk effectively, leadership must ensure that security continues into production — with controls that provide continuous, attacker-aware visibility into live systems.

Once deployed, risks emerge from misconfigurations, exposed APIs, and changes in runtime environments. Static Application Security Testing (SAST) and Software Composition Analysis (SCA) are essential early in development, but they don't address the differences for when applications are run in production.

Leadership Takeaway

Security leaders are accountable not just for code quality, but for real-world outcomes. That means understanding how risk evolves as applications move from development to production.

- Risk doesn't end with secure code. It continues (and often grows) in production.
- A complete security strategy aligns controls across the lifecycle, ensuring continuous visibility and faster decision-making.
- Production environments should not be assumed identical to dev environments. This is where business value lives, and where real threats occur.

Managing business risk demands seeing it clearly, from first commit to live production.

How Can CyCognito Help Your Organization?

The CyCognito platform helps close your production risk gap by extending AppSec coverage beyond the SDLC. It continuously discovers exposed assets and uncovers critical vulnerabilities that surface after deployment.

Take a self-guided, interactive product tour to explore the platform, or request a customized demo to see how CyCognito can strengthen your external application security posture.