Application Risk Management

Prioritize and fix AppSec findings at every stage of the software development lifecycle

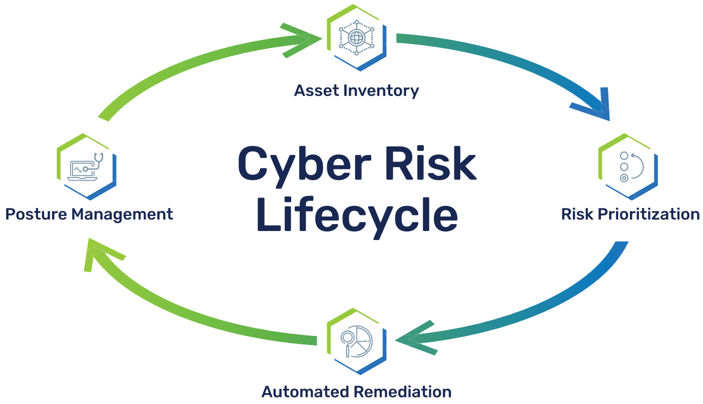
Applications are the lifeblood of modern organizations, which makes securing them vital to the business. The challenge comes when organizations must balance the speed of app development with security processes.

Each part of the software development lifecycle (SDLC) has its security tools and programs — static application security testing (SAST), dynamic application security testing (DAST), interactive application security testing (IAST), software composition analysis (SCA), and pen testing — to name just a few. Each tool produces its findings with no centralized way for app security leaders to manage application risk holistically. Developers and application owners are in the same boat. They must go into each tool, one by one, just to see the vulnerabilities they own. The more tools there are, the more time is spent logging in and reviewing the application's security findings to try and decide what to fix without understanding what matters most.

Meanwhile, the CISO struggles to map siloed, tool-level findings to a given application, its supporting infrastructure, business criticality, and the likelihood of exploit. The inability to map those findings to the overall business priorities makes it nearly impossible for other executives to grasp the importance of risk.

ADOPT A UNIFIED CYBER RISK LIFECYCLE ACROSS THE APPLICATION ATTACK SURFACE

Orchestrating the entire cyber risk lifecycle for your application security program — inventorying all apps and aggregating findings from all AppSec tools, prioritizing and automating remediation of the findings that matter, and communicating risk for each application — can deliver amazing results, such as a 75% decline in critical vulnerabilities.



CENTRALIZE APPSEC FINDINGS AND APPLICATION INVENTORIES

Brinqa enables you to gain a comprehensive understanding of your software assets, their dependencies and their vulnerabilities. Achieving this level of insight starts with inventorying your business applications, internally developed software, open-source components, and APIs. Once you have that information, it's time to model your application attack surface by incorporating AppSec findings and context to establish ownership, identify gaps in security controls, and understand the impact of a potential exploit on your business — for all software assets.

This living model of your attack surface is the single source of truth for app owners to understand the risk associated with their applications. It also provides developers with a single location where they can see all of the security findings related to their software. Taking these critical steps provides your organization with the foundation for applying business context and threat intelligence to all your AppSec tool findings to prioritize and fix the risks that pose the greatest threat to your business.

PRIORITIZE APPSEC TOOL FINDINGS WITH AN ACTIONABLE RISK SCORE YOU CAN TRUST

Too many AppSec tools producing too many findings without context? How does context-based prioritization tailored to reflect the business needs of your organization sound? Brinqa enables you to incorporate unique risk factors with security testing results from your CI/CD pipeline so you can:

- Prioritize the application risks that matter with a configurable scoring model that reflects your business through comprehensive context — relationships and dependencies between apps, supporting infrastructure, priorities, and the likelihood of exploitation.
- Further refine risk scores by adjusting out-of-the-box Brinqa risk factors or creating new business-specific risk factors.
- Foster trust among security, business and development teams by enabling them to use their time wisely by focusing on fixing what matters.

SHIP SECURE CODE EFFICIENTLY

With Brinqa, you can accelerate and improve remediation of software vulnerabilities via orchestrated workflows that enhance ticketing, automate ownership assignment, and enforce SLAs. You'll automatically assign tickets to developers in their tools, group vulnerabilities for efficiency, and validate fixes. You'll build a dynamic AppSec program that empowers key players throughout your organization to incorporate risk factors and security testing results at every stage of the SDLC — from planning to development, testing, release and beyond.

Brinqa Integrates with all existing ticketing and issue-tracking systems to enable development and application teams to work in their comfort zone. Your organization also will realize the benefits of closed-loop tracking — including escalation handling — which provides one location to manage all remediation and SLA tracking.

MONITOR AND COMMUNICATE YOUR APPLICATION SECURITY POSTURE TO ALL STAKEHOLDERS

Shift AppSec program reporting from being tool-centric to application-centric via comprehensive cyber-hygiene dashboards and reports. Elevate the risk management conversation with application security scorecards — with the bonus of gamification and competition among developers and app owners. Finally, you'll be able to communicate application risk in a language that all stakeholders and business leaders can understand while providing a holistic view of application security across the entire organization.

SOLUTION HIGHLIGHTS

- Dynamically model your application attack surface by centralizing app inventories and AppSec tool findings.
- Prioritize AppSec findings with context — relationships between apps, supporting infrastructure, business priorities. and the likelihood of exploitation — to build trust among teams.
- Evaluate cyber risk throughout the CI/CD pipeline to ship secure code efficiently by automating the creation, grouping and assigning of tickets in the developer's ITSM tool.
- Communicate an application-centric view of risk versus a tool-centric view to motivate and streamline action from application owners and developers.

ABOUT BRINQA

Brinqa is the only company that orchestrates the entire cyber risk lifecycle — understanding the attack surface, prioritizing vulnerabilities, automating remediation, and continuously monitoring cyber hygiene — across all security programs. Brinqa Attack Surface Intelligence Platform is the source of truth for cyber risk. It empowers organizations to elevate the security conversation, hold risk owners accountable, identify security control coverage gaps, and manage and track all vulnerabilities in a single platform. Based in Austin, Texas, Brinqa is backed by Insight Partners. Learn more at **www.brinqa.com.**