Collective Cyber Risk Management

Make risk reduction across the attack surface a priority for everybody — not just the security team.

According to Gartner, attack surface expansion is the top cybersecurity concern driven by the ever-changing digital footprint of the modern enterprise. The adoption of new technologies designed to fuel business growth results in an attack surface that dynamically shifts and grows. In response, security teams purchase more tools that discover and track an increasingly diverse set of assets and security findings in silos within infrastructure, application, and cloud security programs.

While this increase in tooling provides visibility, many organizations have reached the tipping point where buying additional tools leaves them with an avalanche of vulnerabilities and no clear path to identify and fix what truly reduces cyber risk. Clearly, a new approach is required.

ESTABLISH ONE SECURITY STRATEGY ALIGNED WITH BUSINESS PRIORITIES

Holistically managing cyber risk in a manner that reflects business priorities is the only way to create a shared understanding of the attack surface and drive the entire organization to improve its security posture. This collective approach to cyber risk management transforms siloed and tool-centric vulnerability overload into a unified security front — across teams, tools and programs. Truly understanding cyber risk is critical to fixing what matters to the business, converting security teams into trusted advisors, and helping prioritize future security investments.

SINGLE SOURCE OF TRUTH FOR CYBER RISK

The average enterprise has invested in 75+ security tools — and the teams to manage them — that are great for finding issues within their application and supporting infrastructure environments. However, dealing with the resulting disconnected overload of vulnerabilities makes identifying real threats to the business challenging. While buying more security tools to find more issues will always be necessary, organizations must prioritize and fix what they know about already.

Modeling your attack surface with a complete inventory of assets and security tool findings and incorporating business priorities and the likelihood of exploit creates a cyber risk source of truth. The result is a clear understanding of the attack surface that enables fixing, tracking and communicating cyber risk by applying each stakeholder's perspective — executives, business unit leaders, application owners, operations and developers.

REDUCE RISK AND YOUR ATTACK SURFACE

With a complete model and up-to-date inventory of your attack surface, an organization can access comprehensive intelligence on assets, security control coverage, threats and vulnerabilities. This intelligence powers the automation of risk reduction through context-driven prioritization of security findings and an orchestrated remediation process that quickly addresses the biggest threats to the business.

Targeted responses to these threats deliver efficiency gains with fewer security findings deemed high risk or lacking clear owners, a reduced number of tickets required to fix findings, and closed-loop tracking with SLA enforcement.

MOTIVATE AND ENABLE RISK OWNERS

Adopting a strategy that spans all security programs and incorporates business priorities establishes a common language for cyber risk that everyone agrees upon, understands and trusts. This alignment within the security team and across the business means new initiatives include more comprehensive security plans, and owners engage the security team as trusted advisors. In addition, security scorecards that track and communicate risk by application or business service create healthy competition and foster best-practice learning across teams.

ELEVATE THE SECURITY CONVERSATION

Monitoring, tracking and reporting on the overall state of an organization's cybersecurity posture becomes easier with a single source of truth, a common language, and business service roll-ups of related risk. Scorecards, dashboards and metrics communicate at the business unit, business application, asset and vulnerability levels so every stakeholder can understand cyber risk from their perspective.

ONE SECURITY PROGRAM

Aligned with business priorities

RISK SCORE CARDS

Hold risk owners accountable

REDUCED RISK

Automate the cyber risk lifecycle

REPORT SECURITY POSTURE

Elevate tool-centric conversations

BRINQA ATTACK SURFACE INTELLIGENCE PLATFORM

Brinqa empowers organizations to reduce their attack surface with a single source of truth for cyber risk that connects all security tools, teams and programs. By combining asset inventories, security findings, business context, and the likelihood of exploitation, Brinqa delivers intelligence that helps organizations prioritize, take precise action, and automate the reduction of cyber risks that pose the greatest threats to their business.

GET A NEW PERSPECTIVE

To see Brinqa Attack Surface Intelligence Platform in action or to learn more, visit **brinqa.com**

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.**