SOLUTION BRIEF

Vulnerability Risk Management

Reduce critical security findings across your attack surface

Vulnerability risk management remains an urgent priority for organizations. Stopping threats by quickly prioritizing and fixing the high-risk vulnerabilities across your company's attack surface is one of the best ways to prevent breaches. However, the rapid adoption of new technologies has made this work overwhelmingly complex.

Infrastructure has become increasingly dynamic and diverse through cloud transformation, leaving organizations without a clear understanding of their attack surface, and exposed to cyber threats. Add to this complexity all the new types of assets that also need to be secured — devices, apps, IoT and OT.

Disjointed teams are buying many siloed tools to find and fix issues across their expanding attack surface, but they can't fix everything they find. And this fragmented approach makes it impossible to prioritize the vulnerabilities that put the business at risk.

Your vulnerability management team needs a cyber risk source of truth for tracking all assets and their vulnerabilities, prioritizing those that matter most, and clearly communicating — with confidence — to the teams responsible for fixing them. And they must provide the CISO with the answers demanded by other executives about the organization's security posture and the performance of the overall cybersecurity program.

Unfortunately, many organizations still rely on vulnerability scanning instead of vulnerability risk management. They throw a huge spreadsheet of discovered vulnerabilities over the wall, with little business context, understanding of ownership, or likelihood of exploit, and expect the operations or development team to fix them all. Instead, time is wasted fixing the wrong vulnerabilities while critical vulnerabilities remain unaddressed, which causes the organization to lose trust in the security team.

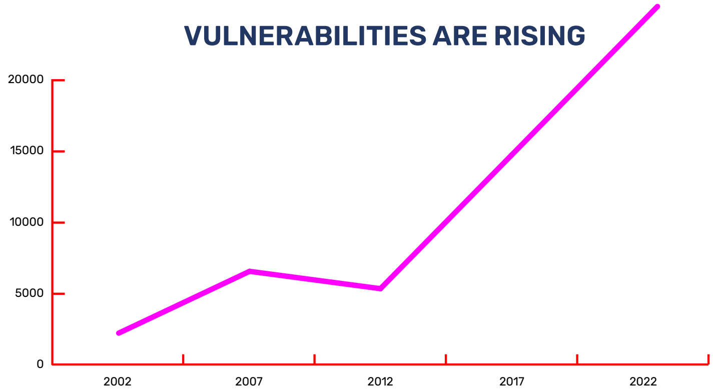
Brinqa helps organizations build a risk-based vulnerability management program that aligns with business priorities, fixes the right vulnerabilities from across the entire attack surface, understands the complexity of modern technology ownership, and can communicate risk in terms the business understands and trusts.

It all starts with the cyber risk lifecycle.

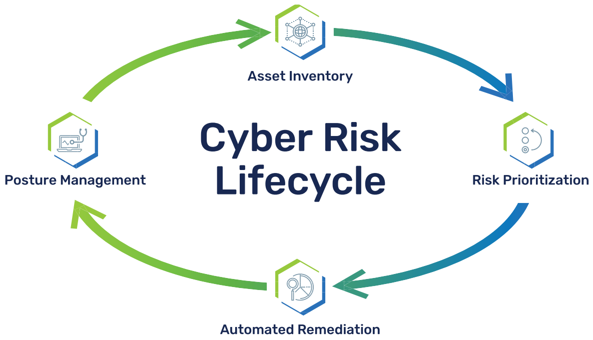
ADOPTING A CYBER RISK LIFECYCLE APPROACH TO VULNERABILITY MANAGEMENT

Vulnerability risk management with Brinqa empowers your organization to orchestrate the entire cyber risk lifecycle. You can understand and track your assets, vulnerabilities and security control gaps, prioritize and remediate the risks that pose the greatest threat to the business, and monitor and report on overall risk reduction and security posture — across all security tools, teams and programs.

VULNERABILITIES ARE RISING



Source: National Vulnerability Database



MODEL YOUR ATTACK SURFACE

You already have the tools to inventory assets and discover vulnerabilities. Now you need to unify them into a single source of truth for cyber risk. Brinqa integrates with 200+ business and security tools for complete visualization and understanding of your attack surface — across all asset types.

This living model of your attack surface delivers cyber risk intelligence through a unified and enriched profile for each asset that incorporates business context, vulnerabilities, threat intelligence, and compensating controls. Updates happen automatically, and relationships enable the dynamic creation of threat perspectives for all stakeholders across the organization.

PRIORITIZE VULNERABILITIES WITH RISK SCORING AND BUSINESS CONTEXT

Risk-based vulnerability management improves your organization's ability to assess the impact and the likelihood of exploitation so you can focus on fixing what matters.

Brinqa combines best practices for modeling risk and normalized scores from existing security tools to prioritize the threats to your business. It turns simplistic vulnerability-based scores into risk scores that reflect relationships between apps, supporting infrastructure, business priorities, and the likelihood of exploitation.

Context-based risk scoring empowers organizations to establish a common language for cyber risk, build trust between teams to fix what matters most, and communicate cyber risk at every level — e.g., business unit, application, or individual vulnerability. Scores can easily be tailored to reflect your company's unique risk tolerance.

ACCELERATE AND IMPROVE THE REMEDIATION PROCESS

Not only does Brinqa give you the intelligence to precisely target high-risk vulnerabilities, we also automate remediation processes, notifications, exception management, and SLA enforcement. Grouping vulnerabilities into fewer tickets significantly reduces ticket volume. Tickets are assigned to the right owners in their tools, and fixes are tracked and validated.

Providing the people who will fix the issues with tickets in their preferred workflow tool enables them to work more efficiently and confidently. Unlike other solutions, Brinqa doesn't force people to work with unfamiliar tools to get the job done.

REPORT RISK IN TERMS THE REST OF THE BUSINESS CAN UNDERSTAND — AND TRUST

Failing to report risk trends and security performance in a way the business understands hinders your security team from becoming a trusted advisor to the organization. In addition to helping you aggregate, prioritize and remediate vulnerabilities across your attack surface and security programs, Brinqa also helps you continuously produce security posture dashboards, reports, and KRIs/KPIs that are up-leveled with business context so all stakeholders can understand where performance is today and what is needed to improve it.

SOLUTION HIGHLIGHTS

- Dynamically model your entire attack surface to navigate systems sprawl and contextualize vulnerabilities.
- Prioritize the vulnerabilities that matter with a risk model that reflects your business priorities and the likelihood of an exploit.
- Automate remediation with dynamic SLA enforcement and verify fixes by creating tickets that are intelligently grouped and assigned to owners in their preferred tool.
- Motivate action from operations, developers, and business owners with risk scorecards they trust and in business terms they understand.

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.**