SOLUTION BRIEF

Attack Surface Management

INTEGRATED
Connect Everything

INTELLIGENT
Prioritize What Matters

AUTOMATED
Do More with Less

SCALABLE
Full Attack Surface Coverage

Productivity will always be the backbone of business growth. However, maintaining it in today's world of remote workers and cloud transformation has created an explosion of security findings that increase an organization's attack surface.

ATTACK SURFACE MANAGEMENT

Effectively managing your attack surface in this sea of millions of vulnerabilities combined with the ever-changing nature of cyber threats and siloed teams leveraging disconnected security tools requires three critical capabilities: unified asset management, risk-based security management, and comprehensive cyber hygiene.

With Brinqa, organizations gain visibility into cyber assets across their entire attack surface. Building and visualizing their baseline Cyber Risk Graph empowers true risk-based vulnerability management programs and effective security posture management.

Unified Asset Inventory

Building your Cyber Risk Graph establishes visualization and understanding of your attack surface, connecting all asset types, business context, and security controls into a single graph-based view. Brinqa consolidates asset definitions of network infrastructure, devices, apps, cloud, IoT, and OT from CMDBs and security tools into a unified profile per asset. Each asset profile combines data from every source for an enriched profile that establishes definitive ownership of the asset. Security tools (e.g., vulnerability scanners) that didn't know about the asset are reconciled through the Cyber Risk Graph, improving the effectiveness of your security controls.

Leveraging this unified asset inventory and associating security controls enforced on assets with business context enables the identification of gaps in your security posture and is crucial to reducing attackers' ability to identify and exploit vulnerabilities. Brinqa Cyber Risk Graph underpins your unified asset inventory, empowers organizations to understand their complete attack surface, and is foundational to risk prioritization and security posture management.

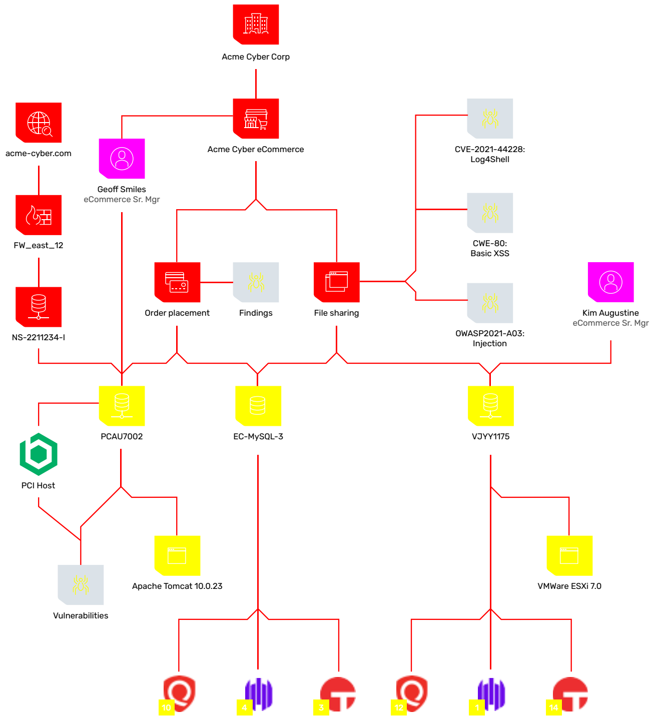


FIGURE 1

Cyber Risk Graph: Laying the groundwork for Attack Surface Management.

Risk Prioritization

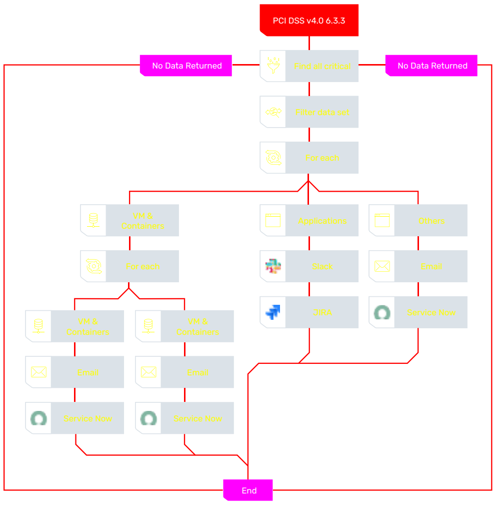
Making your cybersecurity programs and tools risk-based improves the organization’s ability to assess the impact, likelihood and cost of vulnerability exploitation so you can focus on fixing what matters.

Brinqa activates the Cyber Risk Graph of your attack surface by combining risk factors related to business context, security findings, and threat intelligence into a company-wide view of cyber risk.

Prioritize what matters

- Best practice-based risk modeling and a scalable compute engine turn highly interrelated and configurable risk factors into scores that measure risk. The resulting risk scores are normalized across your entire attack surface and are entirely unique to your business.
- Orchestrated flows increase the effectiveness of remediation processes through intelligent ticketing, automated creation of tickets, and dynamic enforcement of SLAs.

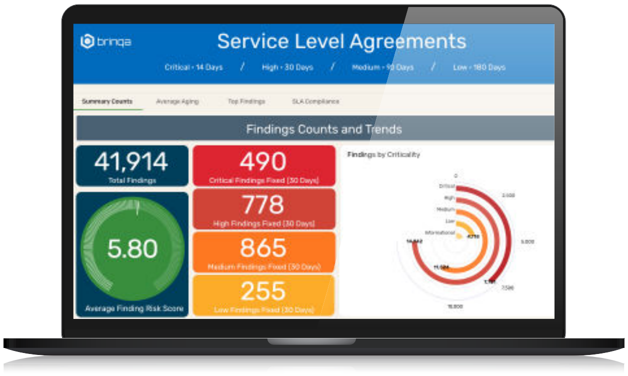
Prioritizing security findings and vulnerabilities based on risk across your organization while automating remediation reduces your attack surface.



Cyber Hygiene

A strong security posture is achieved and maintained by evaluating cyber hygiene across your entire attack surface. Continuously monitoring security control coverage and effectiveness, while consistently reporting on security initiatives’ return on investment (ROI) improves cyber hygiene. With Brinqa, organizations quickly identify gaps in applying critical security policies and controls across their Cyber Risk Graph. They validate and track the effectiveness of risk remediation processes and prove the reduction of their attack surface, risk, and the number of vulnerabilities in an environment.

The powerful Brinqa Query Language enables easy access to the answers to the most complicated security questions — am I implementing the proper security controls? Are they being applied across my entire attack surface? Are they working?


brinqa
Service Level Agreements
Critical - 14 Days / High - 30 Days / Medium - 90 Days / Low - 180 Days
Summary Counts
Average Aging
Top Findings
SLA Compliance
Findings Counts and Trends
41,914
Total Findings
490
Critical Findings Fixed (30 Days)
778
High Findings Fixed (30 Days)
865
Medium Findings Fixed (30 Days)
255
Low Findings Fixed (30 Days)
5.80
Average Finding Risk Score
Findings by Criticality
Critical
High
Medium
Low
Informational

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.**