brinqa

CASE STUDY

Elevating the Vulnerability Risk Management Conversation

Fortune 500 Financial Services Firm

SOLUTION HIGHLIGHTS

- Business Service View of Risk
- Consolidated Asset Inventory
- Context-aware Prioritization
- Orchestrated Remediation
- Bi-directional ITSM Integration
- Cross-business Risk Reporting

BACKGROUND

The customer is a Fortune 500 financial services firm that provides investment management services across the Americas, Europe and Asia. As a leader in high-value business transactions, it was crucial that the firm's infrastructure and applications enabling critical business processes were secure and protected.

While mature in its security posture, the customer recognized it lacked an understanding of cyber risk, the underlying assets, and potential impacts to the business. The combination of a traditional data center with emerging cloud and IoT assets resulted in findings from assessment and monitoring tools that overwhelmed the operations and IT teams. The lack of an understanding of assets and the deluge of problems to be fixed demanded a new approach.

USE CASE

The customer's primary goal was to understand and improve the security of the firm's crown jewels — the applications and technology assets supporting the firm's most critical business functions. To do this, the customer needed a dynamic model of their attack surface. They had multiple asset management systems — ServiceNow and homegrown — with complementary, redundant and conflicting asset information that still lacked the context required to prioritize risk.

After asset sensitivity was understood, vulnerabilities from across all security tools had to be analyzed within this context, alongside real-time threat intel to identify imminent and dangerous vulnerabilities. And they needed a balanced remediation strategy — one that reduced their attack surface in the shortest amount of time.

CHALLENGES

- Multiple security tools finding too many vulnerabilities to fix.
- Lacked business context to prioritize risk.
- Retained asset information in different systems across the organization.
- CMDB updated inconsistently.
- Customer was moving from McAfee to Nexpose for network scanning.
- Remediation ownership and SLAs were not defined or enforced consistently.

CUSTOMER ENVIRONMENT

- 100,000+ network assets
- 1,000+ applications
- Rapid7 Nexpose
- McAfee Vulnerability Manager
- IBM AppScan
- Legacy asset inventory
- ServiceNow CMDB, ITSM
- Threat intelligence feed
- QRadar
- Infoblox

> With Brinqa, our goal was to prioritize vulnerabilities. We were able to quickly evaluate the business criticality and impact of our technology assets. Using that insight, we developed and implemented a prioritized remediation strategy — starting with our crown jewels — and established a context-aware security baseline across the enterprise.

THE BRINQA SOLUTION

Brinqa enabled the customer to improve visibility into its technology infrastructure, aggregate and prioritize high-risk vulnerabilities from across the attack surface and security tools, and fix critical cyber-risk issues. Using Brinqa, the firm put in place a consistent process for managing asset information. Data was consolidated into a single context-rich profile per asset from legacy asset management, ServiceNow CMDB, scanners, and other sources of business context. Assets were organized and presented along real-world business and administration dimensions — locations, business services, network segment — providing a never-before-seen view of the attack surface.

Once application and scanner integrations were enabled, Brinqa automatically evaluated risk models. Asset sensitivity was established based on app tier, compliance requirements, data classification, dependent assets, and device type. Vulnerability criticality was evaluated using scanner-defined severity, exploit availability, age and popularity, network type, and offense magnitude. The firm used the resulting scores as the basis for their new remediation strategy. Ticket creation rules were established to prioritize vulnerabilities, assign ownership, and enforce SLAs. Integration with ServiceNow ITSM was enabled to automatically push tickets created into ServiceNow. The customer used Brinqa to create targeted metrics and reports for every program stakeholder.

80%
Reduction of high-risk vulnerabilities

30%
Vulnerability reduction across infrastructure

40%
Fewer tickets from customers

RESULTS

The customer addressed many top priorities within a month of deploying Brinqa. During this time, they implemented a consistent asset information management process by consolidating asset data from multiple sources and automatically pushing all new information into ServiceNow CMDB — making it the authoritative source.

After establishing accurate asset profiles, the customer could easily identify the applications and assets with the most significant impact on the business. They prioritized improving the security posture of their crown jewels and, over the next six months, reduced high-risk vulnerabilities on critical assets by more than 80%. They also reduced total vulnerability volume by 30%. The customer did all this while creating 40% fewer tickets, reducing the overhead associated with managing tickets and improving remediation efficiency.

Using a standardized model for representing, analyzing and prioritizing vulnerabilities, the firm engaged business, infosec and IT stakeholders with targeted metrics and reports.

BENEFITS

- Unified asset inventory that establishes asset sensitivity, criticality, and impact ratings
- Risk-based vulnerability prioritization that reduces the volume of findings to be fixed
- Efficient remediation processes with ownership and SLA enforcement
- Continuous stakeholder engagement and accountability for risk owners

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 tools and 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**.