brinqa

CASE STUDY

# Application Attack Surface Management

## Fortune 500 Healthcare Firm

**SOLUTION HIGHLIGHTS**

- Authoritative Application Inventory
- Business Rules
- Risk Prioritization
- Ticket Creation Rules
- Vulnerability Consolidation
- ITSM Integration
- Policy Enforcement
- HIPAA Compliance Reporting

## BACKGROUND

The customer is a Fortune 500 firm providing medical services and health insurance throughout the U.S. and in major international markets. Due to significant M&A activity, the customer accumulated a broad range of software assets and application security testing (AST) tools. A redesign of the firm's application security program aimed to reduce the variance in ASTs and risk remediation processes.

As a healthcare provider, the customer must be HIPAA compliant. They worked with external consultants and auditors to develop policies that govern ownership and SLAs for assets. These policies aimed to maintain and prove compliance, but without automated enforcement there were inconsistencies in implementation. The customer struggled to ensure that developers and security professionals were trained to make the policies an integral part of the software infrastructure.

## USE CASE

The customer's goal was to improve the security posture of its critical applications and implement a consistent risk analysis and remediation strategy across the software infrastructure. In addition to using multiple ASTs, they had two sets of processes and tools to manage externally sourced applications vs. those developed internally.

The firm's development organization managed Internally developed applications — using Jira as the repository for asset information and task management. The customer's IT team managed externally sourced software — using ServiceNow for business application inventory and remediation.

The customer was required to prove HIPAA compliance regularly. While they had policies for this, they struggled with manual processes for tagging HIPAA assets and enforcing ownership and SLAs.

### CUSTOMER ENVIRONMENT

- 2000+ applications
- Checkmarx
- Qualys WAS
- External pen test
- Data protection program
- ServiceNow
- Jira
- FireEye threat intelligence
- LDAP

### CHALLENGES

- Disconnected internal and external applications
- Incompatible SAST, DAST and pen-test results from vendors
- HIPAA assets inaccurately tracked
- Remediation ownership and SLAs were undefined or inconsistently enforced

## THE BRINQA SOLUTION

Brinqa enabled the customer to improve visibility into their software infrastructure and address critical application findings. A single, complete software inventory combined externally sourced business applications maintained in ServiceNow with internally developed applications in Jira. Business rules identified missing information and created corrective tasks for responsible parties.

Issues from Checkmarx and Qualys Web Application Scanning were collected using dedicated connectors. At the same time, findings from a pen-testing agency were added to the risk model using a generic XML connector. After eliminating false positives, application importance and threat intelligence aided in identifying the findings that posed significant threats to the business. Remediation rules enforced ownership, and SLA policies were leveraged automatically in the tickets created and assigned.

**50%**
Reduction of high-risk vulnerabilities

**20%**
Vulnerability reduction across infrastructure

**40%**
Fewer tickets from customers

## RESULTS

The firm addressed top priorities within a few months of deploying Brinqa. They identified gaps in their application inventory and took action to remedy them. They also aggregated application data from multiple sources into ServiceNow CMDB for management.

With all metadata consolidated, the customer quickly identified the applications most critical to the business. They prioritized improving the security posture of these crown jewels and, over a 3-month period, reduced high-risk vulnerabilities on these vital assets by more than 50%.

The customer also reduced the overall vulnerability volume across the infrastructure by 20%. They achieved these milestones while creating fewer tickets, reducing the overhead associated with ticket management, and improving remediation efficiency.

Using a standardized model for representing, analyzing and prioritizing vulnerabilities, the firm implemented a consistent risk prioritization and remediation strategy for data coming from Checkmarx, Qualys WAS, and external penetration testing.

### BENEFITS

- Complete application inventory with sensitivity, criticality and impact ratings
- Improved security posture for apps through risk-centric prioritization and remediation
- Efficient remediation processes with ownership and SLA enforcement
- Continuous stakeholder engagement with an application view of risk

> “With Brinqa, we connected our disparate application security testing initiatives into a cohesive application risk management strategy. By identifying and focusing on our most critical applications, we drastically improved our overall security posture through targeted remediation of the most dangerous and impactful vulnerabilities.”

### 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.**