CASE STUDY

PhonePe Protects its Critical Applications from Vulnerability Risk Exposure with Custom Risk Scoring and Prioritization

INTRODUCTION

PhonePe Private Limited is an Indian financial services company that stands out for its innovative range of products and services, from UPI transactions and payments to investments and personal finance management. The company is central to India's financial ecosystem, servicing millions of consumers and businesses, and processing billions of daily transactions. Because the financial sector attracts significant attention from cybercriminals, security must be a top priority.

REGISTERED USERS
600 million

INDUSTRY
Financial Services

DAILY TRANSACTIONS
270 million

THE CHALLENGE

PhonePe manages multiple customer-facing applications, including mobile and web platforms that are integral to the company's core business operations. The company needed to strengthen the security of these critical applications and services against continual cyberattacks, so the cybersecurity team needed to understand the impact of security vulnerabilities on its technology stack and identify the most urgent areas for remediation. Eliminating security risks and vulnerabilities was critical to reducing regulatory exposure and safeguarding PhonePe's business, customers, and partners.

PhonePe relied on a legacy, homegrown asset management system and Jira CMDB (Configuration Management Database). However, this system could not provide a clear context for security vulnerabilities, leaving many critical issues unattended. There was no cohesive way to prioritize vulnerabilities based on their potential business impact, and security engineers and developers often assessed security risks in isolation without considering the business function they impacted.

THE BRINQA SOLUTION

Given the high stakes involved, PhonePe recognized the need to implement a robust application security and risk management framework to address emerging threats and ensure compliance across its critical business systems. This included a scalable, business-driven application risk-scoring model to efficiently manage security vulnerabilities. PhonePe introduced the concept of the POD Security Score (PSS), a comprehensive risk-scoring model designed to assess the security posture of individual applications and assign risk based on the business services they support.

PhonePe implemented Brinqa to create a unified risk analytics platform to track, analyze, and score vulnerabilities across its ecosystem. The **Brinqa Exposure Assessment Platform** provided the framework for collecting, analyzing, and storing data from a wide variety of sources, such as penetration testing results (manual and automated), static code analysis, custom (open-source) scan results, and vulnerability management systems. Most importantly, the Brinqa platform enabled the team to factor in business context—such as the criticality of the application and the associated business services—when evaluating risk.

Copyright ©2025 Brinqa

HOW PHONEPE IMPLEMENTED BRINQA'S RISK ANALYTICS

PhonePe's Application Security Team collaborated with Brinqa to leverage its advanced risk analytics and prioritization features, successfully implementing a tailored risk management system. Here's how the process unfolded:

1. Categorization and Enrichment of Vulnerabilities

The first step involved categorizing vulnerabilities and adding relevant attributes to the existing CMDB (Configuration Management Database). This enabled a more nuanced understanding of each vulnerability, including:

Severity: How critical the vulnerability is based on the CVSS (Common Vulnerability Scoring System) score.

Business Impact: The potential impact of a vulnerability on business operations, customer trust, and financial transactions.

Likelihood: The probability of exploitation of a vulnerability.

Remediation Steps: Clear actions and timelines for addressing vulnerabilities.

Service-Level Agreement Status: SLA timelines and statuses for each security vulnerability, resulting in an overall SLA status for a business service.

By tagging vulnerabilities with business-relevant attributes, PhonePe provided developers and security teams with a more comprehensive understanding of the risks they faced. Vulnerabilities could now be assessed not only based on technical severity but also in terms of their potential business impact.

2. Integrating Multiple Data Sources

PhonePe also integrated data from a variety of security testing tools and sources, including:

Static Code Analysis: Scanning code repositories for security flaws before deployment.

Penetration Testing: Simulating real-world attacks to identify exploitable weaknesses in applications.

Open-Source & Custom Security Scanners: Customized scans (static and dynamic) of applications and their APIs.

Governance, Risk, and Compliance (GRC) Frameworks: Tracking security controls, policies, and exceptions to cater to regulatory audits.

This integration enabled PhonePe to gather comprehensive security data from disparate systems and bring it into a single platform, providing a holistic view of the organization's security posture.

3. Risk Scoring with Business Context

One of the most innovative aspects of the project was PhonePe's introduction of business context into the risk-scoring process. Each application was scored based on its:

Criticality to Business: How vital the application is to PhonePe's daily operations and customer transactions.

Inherent Risk: The baseline level of risk associated with an application based on its design, architecture, and data sensitivity.

These business-driven attributes were combined with technical risk assessments to generate the POD Security Score (PSS). The PSS reflects the severity of vulnerabilities and indicates the level of business impact, helping security teams and business owners understand which issues require the most urgent attention.

Copyright ©2025 Brinqa

4. Tailored Risk Analytics

PhonePe employed Brinqa's correlation engine to provide advanced risk analysis, aggregating data from different sources to comprehensively view the organization's overall risk. This was supported by quantitative risk scoring that considered various factors, such as risk weights, thresholds, and data normalization.

5. Interactive Dashboards and Reporting

PhonePe's vulnerability management team created interactive dashboards using Brinqa, which enabled business owners and security teams to:

Track and compare risk scores for different applications and business services.

Visualize risk metrics in real-time, enabling quick decision-making and prioritization of resources.

Foster competition and accountability by enabling different teams to compare their security risk scores, promoting healthy competition to improve security outcomes.

The dashboards provided easy-to-understand insights shared with key stakeholders, including executives, business owners, and developers. Regular reporting ensured that vulnerabilities were constantly monitored, tracked, and addressed.

RESULTS AND OUTCOMES

By implementing the Brinqa Exposure Assessment Platform, PhonePe achieved several key outcomes:

Holistic View of Application Risk

Integrating business context with technical vulnerability data provided a comprehensive view of risk across the organization. This helped the team prioritize vulnerabilities based on their technical severity and impact on the business.

Improved Risk Prioritization

The custom risk models and scoring systems enabled PhonePe to prioritize vulnerabilities aligned with the organization's business priorities, ensuring that the most critical risks were addressed first.

Enhanced Collaboration

By creating custom dashboards and reporting mechanisms, PhonePe facilitated better collaboration between security teams, developers, and business owners, ensuring that everyone had access to the information they needed to take action.

Data-Driven Decision Making

With detailed risk metrics and "what-if" analysis, PhonePe could make data-driven decisions about resource allocation, remediation strategies, and risk mitigation planning.

Increased Security Posture

Overall, the initiative helped PhonePe significantly improve its security posture, reducing the likelihood of breaches and ensuring its applications and business services remained secure, compliant, and resilient.

CONCLUSION

PhonePe's implementation of the Brinqa Exposure Assessment Platform enabled the company to move from a reactive, siloed approach to managing vulnerabilities to a proactive, business-contextualized model for managing application risk. The PhonePe POD Security Score (PSS) success and integration into the broader business strategy demonstrates the power of combining technical security measures with business-driven decision-making, ensuring that PhonePe's digital ecosystem remains secure despite constantly evolving threats.

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.**

Copyright ©2025 Brinqa