SOLUTION BRIEF

# Brinqa Vulnerability Risk Management

The integrated solution combines correlation of vulnerabilities, threat intelligence and business context with risk analysis and scoring to prioritize remediation efforts and measure program effectiveness.

## HIGHLIGHTS

- **Complete asset view via integration with CMDB, HR systems and in-house data sources**
- **Integrated threat intelligence feeds for vulnerability risk analysis and prioritization**
- **Quantitative risk ranking of vulnerabilities and assets**
- **Intelligent risk-based remediation  recommendations**
- **Out-of-the-box IT service management integrations**
- **Self-service reports and dashboards**

## The Fundamental Cyber Security Control

Vulnerability management is on the list of top priorities for forward thinking security organizations. The Council of Cyber Security emphasizes Vulnerability Assessment and Remediation as one of the top 5 controls that help organizations establish the foundation of security and have the most immediate impact on preventing attacks.

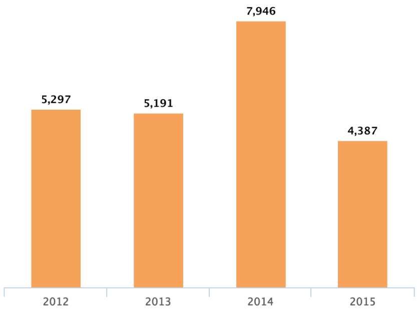
According to the 2015 Verizon Data Breach Investigation Report, 99.9 % of the vulnerabilities analyzed had been compromised more than a year after being published. Research indicates that for identified vulnerabilities, it typically takes organizations hundreds of days to remediate problems. These numbers indicate that despite a steady increase in the effectiveness of vulnerability assessment tools and in investments in this technology, the benefits have been difficult to realize.

For most organizations, vulnerability assessments result in findings that far exceed the security team's bandwidth for addressing them. The data overload problem is severely compounded by the host of manual processes commonly employed during detection, validation, and remediation.

To combat data overload most organizations employ some form of vulnerability prioritization, often based on static criteria like CVSS base score. Zero-day vulnerabilities expose how ill fitting these methods are to the ever-changing threat landscape.

With attackers frequently changing strategies and methods, security teams are hard-pressed to keep up. Failing to deliver tangible security benefits, vulnerability management programs often revert to a 'check-box' approach that meets compliance requirements but in turn exposes the organization to greater risk.

**The volume of vulnerabilities is overwhelming**



Note: Data is up to date as of Sept 8th, 2015.
Source: CVE Details (http://www.cvedetails.com)

## A Shifting Paradigm

To effectively protect against existing and emerging threats, security teams must understand and acknowledge the new and expanded scope of modern vulnerability management. Brinqa Vulnerability Risk Management focuses on critical risk functions to deliver true cybersecurity to organizations. The solution uses a risk-based approach to model  program scope and context by mapping relevant assets, their dependencies and ownership. It identifies and communicates critical assets in the organization and their impact to business and consolidates vulnerability, threat and asset data from all relevant sources, resolving conflicts or redundancies, and representing data on a normalized scale.

Brinqa Vulnerability Risk Management derives risk scores for vulnerabilities and assets by correlating with business context, threat intelligence and temporal factors. It prioritizes vulnerabilities for remediation based on impact to business, severity and relevance of compromise to deliver the highest risk-reduction and provides an easy and automated path to remediation.

The solution delivers KPIs, KRIs and metrics that communicate key controls, applications, business assets, program status, and remediation statistics to all stakeholders and continuously identifies, integrates and represents changes - in classification, exploitability, impact and status - for closed loop remediation and monitoring.

## Asset Inventory & Relationships

Complete inventory of authorized and unauthorized devices is crucial to reducing the ability of attackers to identify and exploit vulnerabilities. Brinqa Vulnerability Risk Management provides easy integration with CMDB, HR, configuration management and active monitoring systems to ensure a complete and up-to-date representation of the organization's assets and hierarchy.

## Simplified Data Collection

The Brinqa connector framework delivers comprehensive out-of-the-box integration with a wide range of external systems to consolidate asset, vulnerability and other security data. The connectors support one-click and scheduled synchronization of data while providing administrators with a host of utility functions for reconciling redundancies, duplicates and conflicts. Brinqa connectors provide a common interface for configuring, managing and monitoring the transfer of data between independent systems.

## Integrated Threat Intelligence

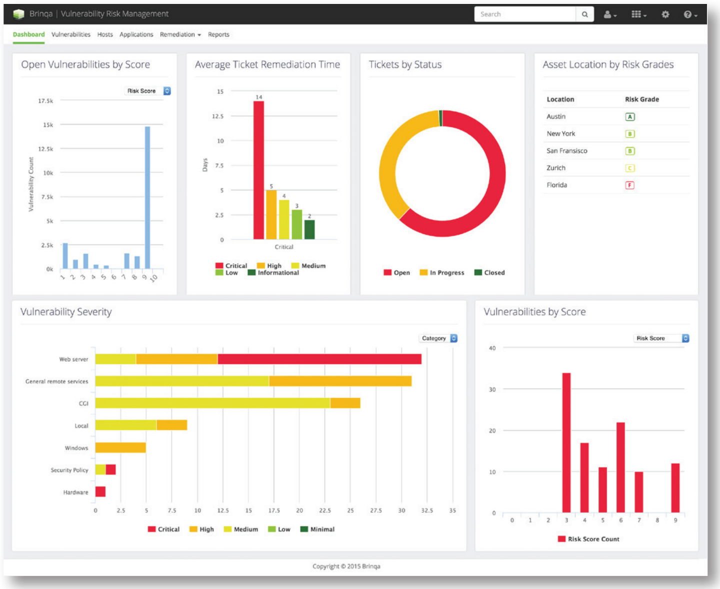
Brinqa Vulnerability Risk Management solution integrates threat intelligence feeds from a variety of public and private researchers - Verisign iDefense, iSight Partners, Alien Vault (OTX) and more - that provide comprehensive visibility into known threat actors, exploit mechanisms and toolkits, malwares, and current incidences in the wild. This information is crucial to assessing the true impact, likelihood and cost of a vulnerability.

## Quantified Risk Ranking & Prioritization

Vulnerabilities are automatically evaluated for risk to business based on external factors such as availability of public exploits, social media mentions, malware, exploit kits and targeted attacks; as well as internal factors like the business criticality and context of affected assets.

## Effective Remediation

Ticket creation rules provide administrators with flexibility in grouping vulnerabilities based on inherent classification, affected asset properties, remediation options and ownership. Tickets are created automatically, greatly reducing the lag time between vulnerability discovery and remediation. Brinqa ticketing is a complete end-to-end solution for managing and tracking remediation activities and workflow across multiple actors and roles.



| Location | Risk Grade |
|---|---|
| Austin | A |
| New York | B |
| San Fransisco | B |
| Zurich | C |
| Florida | F |

Brinqa Vulnerability Risk Management also provides ready integrations with most common enterprise ticket and task management systems like Remedy, ServiceNow and JIRA for organizations that have existing task management processes.

## Risk Intelligence & Analytics

Brinqa Vulnerability Risk Management tracks key KRIs, KPIs and program metrics to monitor risk-reduction, remediation time and window of opportunity. The self-service reports portal allows stakeholders to utilize report templates and create their own custom reports.

The solution comes with a wide variety of technology and business hierarchy based reports targeted for a diverse audience ranging from C-level executives to technical staff.

## Conclusion

Vulnerability Risk Management is a crucial aspect of every cybersecurity program and has a significant impact on the security posture of an organization. Brinqa Vulnerability Risk Management promotes an understanding of the organization's asset relationships and their business relevance, providing a cohesive remediation strategy, utilizing threat intelligence and advanced risk rating models and encouraging constant prioritization to overcome information overload.

## About Brinqa

Brinqa is a leading provider of unified risk management – enabling stakeholders, governance organizations, and infrastructure and security teams to effectively manage technology risk at the speed of business. Brinqa software and cloud services leverage an organization's existing investment in systems, security, and governance programs to identify, measure, manage and monitor risk. With Brinqa, organizations are reducing response time to emerging threats, impact to business, and technology risk and compliance costs by over 50% through real-time risk analytics, automated risk assessments, prioritized remediation, actionable insights and improved communication.