Brinqa and Digital Defense, Inc. work together to deliver accurate, complete Vulnerability Risk Management

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

HIGHLIGHTS

- **Complete asset visibility via integration with Digital Defense, CMDB, HR systems and in-house data sources**

- **Integrated threat intelligence feeds for vulnerability risk analysis and prioritization**

- **Automated ticket creation and vulnerability consolidation rules**

- **Out-of-the-box ServiceNow, Cherwell RemedyForce and JIRA integrations**

- **Self-service reports and dashboards**

Digital Defense Frontline VM

Built entirely as a SaaS platform, a fully functional GUI can be accessed whenever or wherever you happen to be. Access the platform seamlessly with browsers, on tablets and mobile devices. Streamline your workflow with granular filtering and categorizing capabilities to quickly identify areas of high risk and focus efforts on defending your enterprise, driving risk out.

Brinqa Risk Platform

Brinqa Risk Platform delivers a complete set of capabilities and features to represent, integrate, and correlate unlimited sources of security data for secure and rapid analysis. The platform provides management and automation support throughout the cyber risk identification, mitigation, validation, and communication processes.

Brinqa Threat and Vulnerability Management application combines real-time, real-world vulnerability intelligence with the business impact of technology assets, and analyzes data from all your network monitoring and assessment systems in that context.
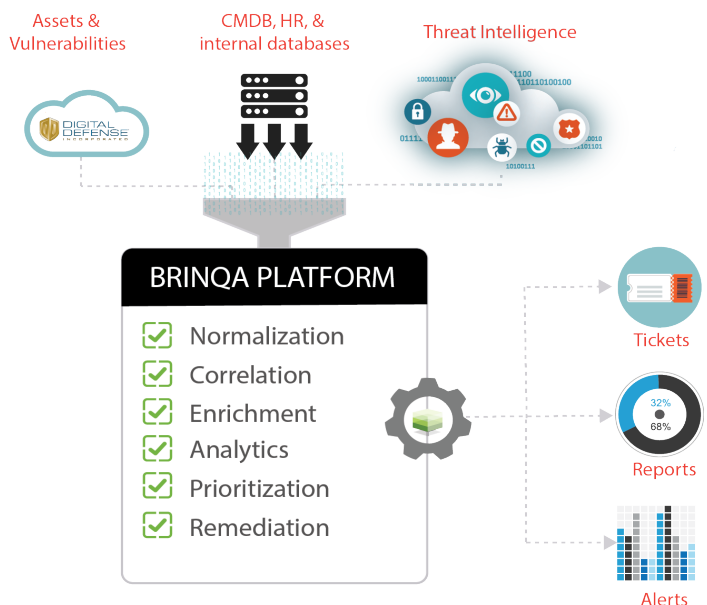
By combining advanced prioritization with automated remediation and validation management, the solution delivers an immediate improvement in the number of vulnerabilities in your environment, as well as the security posture of your critical assets and infrastructure.

Solution Overview

Digital Defense's Frontline SaaS Platform is the only vulnerability management solution that digitally audits hosts, reconciles assets (helping to minimize duplicates or unknown), prioritizes vulnerabilities, and automates workflow across the hybrid network to make better risk management decisions, faster.

Together, Digital Defense's Frontline VM and Brinqa Threat and Vulnerability Management streamline vulnerability prioritization and remediation efforts, offering a way to automate common vulnerability management processes - identifying hosts, scanning for known vulnerabilities, identifying high risk assets and hosts, managing the remediation process, and engaging and informing all relevant stakeholders.

As a member of the Brinqa partner program, Digital Defense works seamlessly with Brinqa Risk Platform to enable real-time assessment, host analysis and policy-based mitigation of endpoint security risks.

Assets & Vulnerabilities — CMDB, HR, & internal databases — Threat Intelligence

BRINQA PLATFORM

- ☑ Normalization
- ☑ Correlation
- ☑ Enrichment
- ☑ Analytics
- ☑ Prioritization
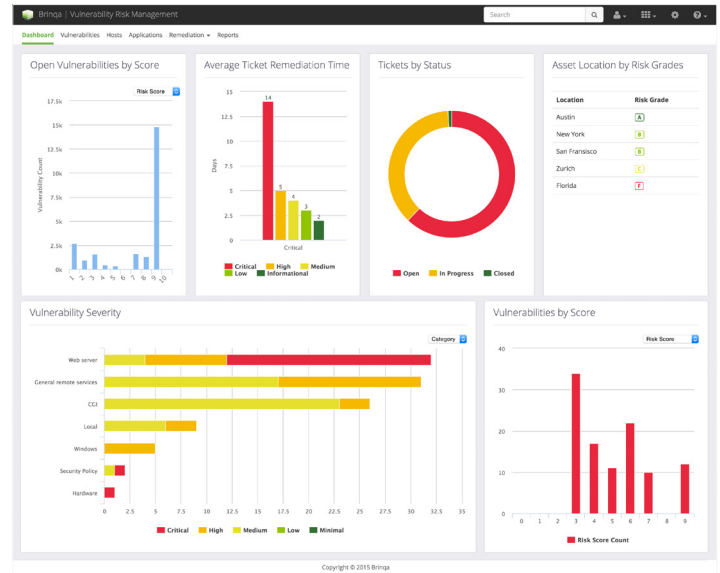- ☑ Remediation

Tickets

32% / 68% — Reports

Alerts

Complete & Accurate Analysis of Network Devices

Digital Node Attribution (DNA) is the core technology within Frontline VM that eliminates network drift. As a point in time network vulnerability scanner that feeds data into Frontline Vulnerability Manager™, DNA is able to match host identification artifacts associated with a specific endpoint over time – including dynamic identifiers like IP address, DNS hostname and NetBIOS hostname – and reconcile them back to a common entity. Regardless of how identification artifacts may change over time, – otherwise known as network drift, DNA can accurately and consistently pin vulnerability scans to each discrete endpoint over time. The reconciliation helps to automate the process to correct inaccuracies of your CMBD or asset tracking platform.

Through integration with Brinqa, the vulnerability and asset data is seamlessly enhanced with data from a variety of systems – CMDB, Network Management, Threat Intel, etc – automatically resulting in a much more comprehensive view of the risk associated with these entities. The integrated solution empowers users to correlate, analyze and prioritize vulnerabilities within a constantly changing environment and to be proactive against new threats that are introduced every day. Assets and vulnerabilities are analyzed and presented in real-world context, providing visibility into the value and impact of this technical to the business. The integrated solution automatically operationalizes this information to evaluate and improve the security posture of the organization on a continuous basis.

Effective Path to Remediation

The integrated solution increases your remediation coverage while reducing the overhead associated with managing tickets. By combining Digital Defense's remediation plans with Brinqa Rules Engine, the solution delivers a painless way to create, track and validate the most effective tickets, with minimal manual effort.

The solution ensures accurate ownership assignment and SLA enforcement and delivers improved efficiency and consistency of remediation efforts.

Communicate, Collaborate and Transform

Visual graphs provide a unique perspective for understanding the security data and deriving insights through advanced analytical processes like graph-clustering and node-classification. The integrated solution provides a comprehensive reports catalog targeted for a wide audience range from system administrators to security teams and C-level executives to ensure that stakeholders at every layer of the organization are effectively informed and actively engaged in the decision-making process.

About Digital Defense

Founded in 1999, Digital Defense, Inc. is an industry recognized provider of security assessment solutions, helping organizations defend data and protect brands. The company's Frontline™ Vulnerability Management cloud-based suite of solutions is underpinned by innovative, patented technology, complemented with unparalleled service and support, while its security awareness training promotes security-minded behavior. The company has been designated Best Scan Engine by Frost & Sullivan and ranks #16 in Cybersecurity Ventures' World's 500 Hottest Cybersecurity Companies.

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.

Founded in 2008 by industry leaders in risk management with a proven track record in delivering cutting edge, innovative and cost-effective solutions. Brinqa's award winning software and cloud services are trusted by fortune 500 companies across risk disciplines such as information technology risk, vendor risk, and regulatory compliance risk. Brinqa is headquartered in Austin, Texas and has a global presence.