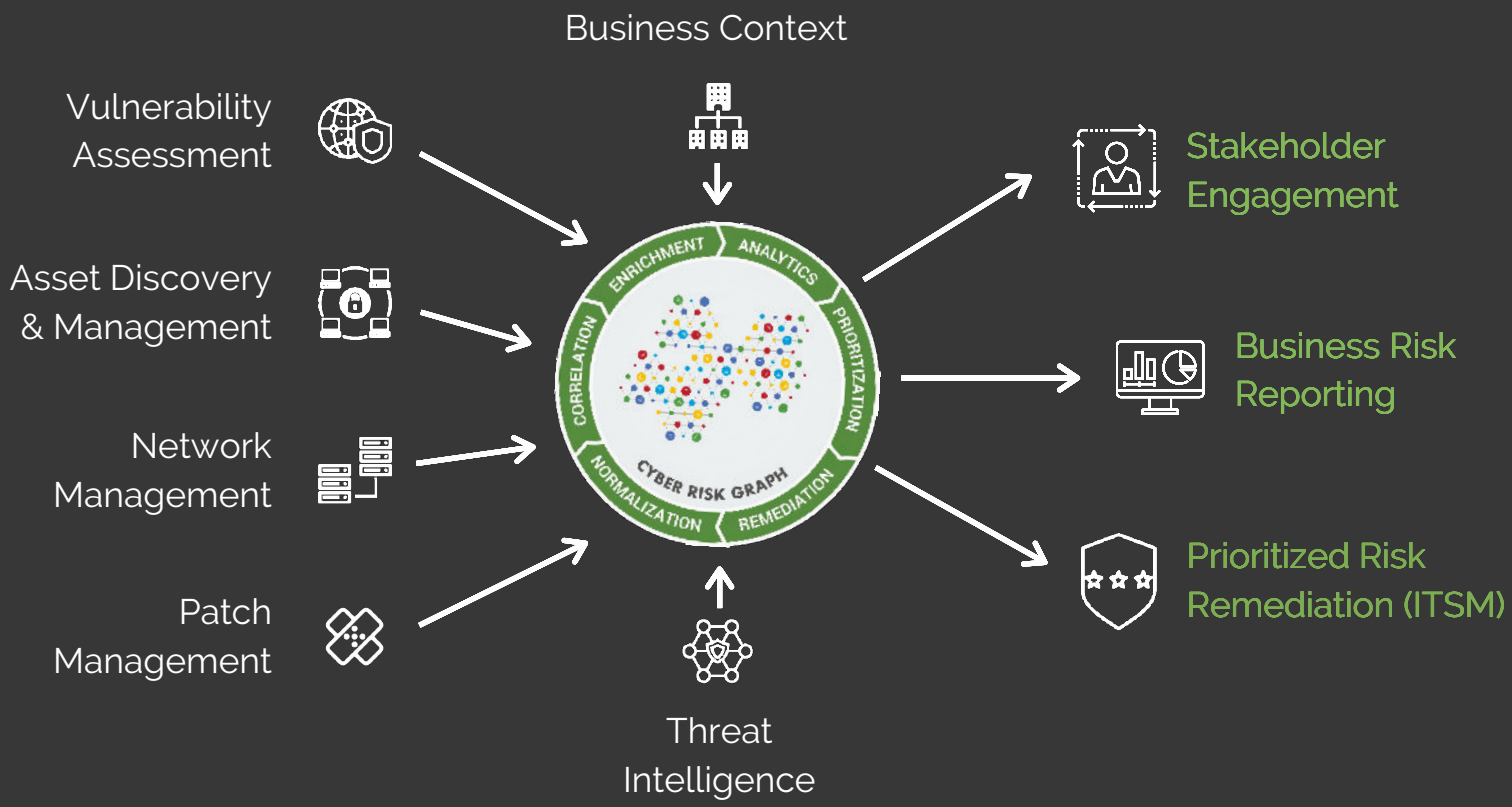
Vulnerability Risk Management

INTEGRATIONS CHECKLIST

Risk-based Vulnerability Management requires precise coordination of data and workflows across several classes of security products. Effective VM programs automate the collection, correlation, and analysis of data — from all relevant sources of vulnerability, asset, and business context — to identify and prioritize risk. This insight is then used to plan and implement human and machine actions designed to avoid, mitigate, or remediate risks. A seamlessly integrated ecosystem helps VM programs achieve these goals in an efficient, effective, and consistent manner. This document highlights important integrations to consider when designing your VM program and lists available Brinqa connectors.



Vulnerability Assessment

Vulnerability scanners are the primary source of vulnerability enumeration, and often device discovery. Brinqa implements vulnerability enumeration by utilizing our vast collection of integrations to the leading vulnerability scanning and assessment products. We take a vendor-agnostic approach that allows our customers to leverage the tools that best suit their environment and scanning requirements. However, effective vulnerability enumeration is about more than just collecting vulnerabilities. To handle real world scenarios (scanner replacement, separate scanners for internal vs. external assets, M&A activity, passive scanning, deduplication, false positives, etc.) organizations need advanced data management capabilities. The Brinqa solution allows organizations to normalize vulnerability data from disparate assessment tools into a common, standardized ontology.

Asset Discovery & Management

An organization's ability to correctly assign asset criticality directly impacts the accuracy and soundness of risk-based vulnerability prioritization. Asset management systems serve as a source of invaluable business context such as operational state, access classification, compliance requirements, data classification, ownership, escalation chain, etc. that are crucial for risk prioritization and remediation. Effective asset management is accurate (results in an exhaustive inventory of all the assets in scope of the program), comprehensive (covers every relevant factor of asset identity and usage), and functional (includes criticality, ownership, escalation chains, and all other operational aspects). In addition to the connectors listed below, Brinqa customers often employ generic connectors (flat file, direct-to-database) to pull asset context from non-IT or proprietary tools and programs.

Threat Intelligence

The ability to accurately and expeditiously determine and incorporate threat intelligence into vulnerability risk prioritization can mean the difference between a breach and a secured environment. VM programs should ensure that factors of exploitability and indicators of compromise are evaluated continuously and there are measures in place to trigger the appropriate workflows if any changes are detected. The Brinqa solution gives administrators complete control over how various threat intelligence criteria come together to determine vulnerability severity. Intelligent correlation easily sifts through large volumes of threat intel to identify and incorporate those factors that have an impact on the organization's unique technology environment.

Network Management

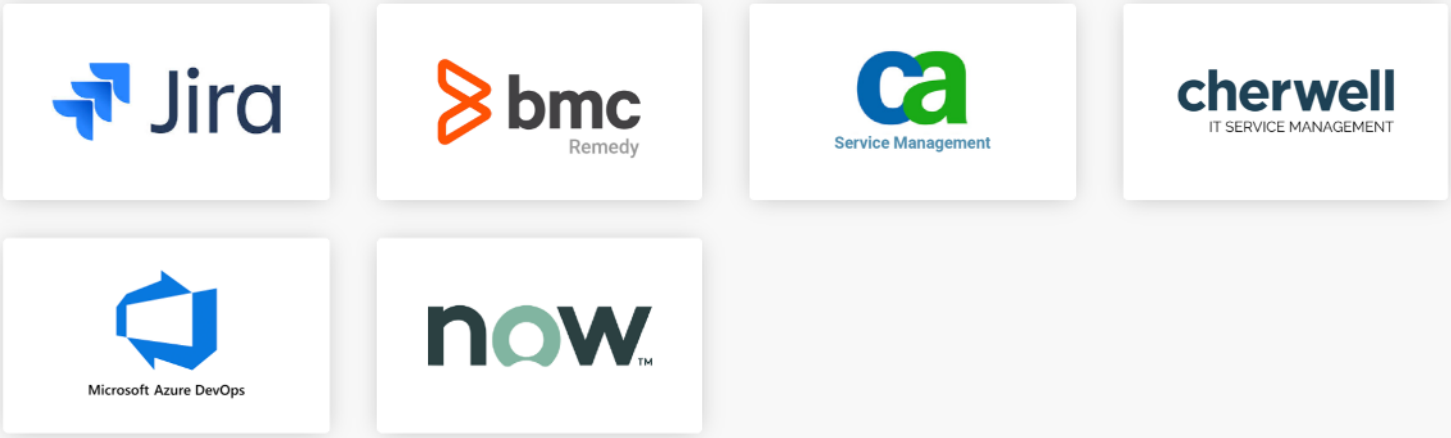
Accurately determining network exposure can help organizations understand the true structure of their network infrastructure and establish relationships and dependencies between assets that can then be leveraged for attack path analysis. Building this information into the risk model gives organizations a true picture of the risk associated with a vulnerability or asset. The solution includes an OOB network segmentation model and assets can be dynamically associated with segments based on IP ranges and other factors. Organizing assets along network segments also gives business and IT stakeholders a perspective of vulnerability risk that aligns with their day-to-day operations.

Patch Management

Patch Management tools can help organizations monitor and deploy fixes for vulnerabilities across various sections of their infrastructure. Integrating patch management with your VM program can drastically improve remediation efficiency and help achieve true closed-loop remediation.

IT Service Management (ITSM)

Brinqa implements a rule-based ticketing mechanism for automated remediation management. Brinqa customers are encouraged to formulate policies that govern how tickets should be created and managed. These rules are run automatically when new vulnerabilities are discovered. The rules allow vulnerabilities to be grouped together based on common criteria, thereby significantly reducing the volume of tickets being created (and the overhead associated with managing them). Rule configuration also allows ownership and SLAs to be set and enforced dynamically, ensuring consistency of remediation efforts. Brinqa solution includes native ticket lifecycle management but it is more common for customers to utilize an external ITSM tool for managing ticket lifecycles. This is achieved through bi-directional integrations with the leading ITSM tools. Similar to ticket creation rules, ticket closure rules can be set up to validate risk remediation effectiveness and close tickets automatically.



ABOUT BRINQA

Brinqa empowers customers to own their cyber risk with a unique, knowledge-driven approach to cybersecurity challenges. Brinqa Cyber Risk Graph - the knowledge graph for cybersecurity - connects all relevant security and business data, establishes a common risk language, a nd powers cybersecurity insights and outcomes. Brinqa Cyber Risk Services apply this knowledge to uniquely inform risk management strategies, standardize security data management and analysis, improve communication between teams, deliver actionable insights an d automate risk remediation. With Brinqa, cybersecurity programs and processes will evolve with changing risk priorities, threat landscape a nd technology trends. Learn more at www.brinqa.com and follow us on Twitter and LinkedIn.