Security teams need to identify, prioritize, and act to counter the most dangerous and trending exploits within minutes – not days. RiskSense® offers **Full Spectrum Risk-Based Vulnerability Management** and optional services to control cyber risk exposure.

- Understand Your Aggregated Vulnerability Exposure
- Take Action Based on Active Threats, Including Ransomware
- Manage Workflow and Track Vulnerability Status and History
- Reduce Costs and Maximize Security Results

User	Current Pain Points	Solutions and Positioning Tips
 **CSO, CISO, or CIO** • Needs visibility into current cyber risk and a solid understanding as to its business impact potential	• Business changes to accommodate work from home • Increased threat of ransomware • Looking at cost and coverage efficiency of current threat and vulnerability management programs	**Ransomware Assessment** Quickly understand what assets are susceptible and what prioritized remediation actions will prevent business disruption and damage. **Full Spectrum Risk-Based Vulnerability Management & Vulnerability Scanning Services** Consistent cost-effective coverage and oversight of vulnerability scanning with immediate risk prioritization. Remediation recommendations and security risk metrics with dashboard views that allow organizations to use their high-value security resources to their max potential.
 **VP or Director of Security/IT** • Must quantify vulnerabilities and collective risk across infrastructure, applications, and code • Security and IT must collaborate with cross-functional groups (network, endpoint, datacenter, DevOps, etc.) for assessment, reporting, and remediation	• A changing attack surface and rapid organizational and/or application development changes • Vulnerability findings need consistent workflow and complex remediation coordination following various change management processes that most scanning tools cannot accommodate, leading to more IT and Security overhead	**Risk-Based Vulnerability Management** Obtain a single view of vulnerability and exposure across multiple vulnerability scanning tools and the current remediation status across different groups. Workflows, automation, and detailed tracking of false-positives and risk acceptance make complex vulnerability management simple. Security and IT coordination results are faster and more effective.

User	Current Pain Points	Solutions and Positioning Tips
Security Analyst • Must analyze vulnerability scan data from numerous sources, understand active threats, and judge what to prioritize for remediation and/or compensating controls	• Difficulty and time required to map known active exploits to vulnerability scan findings • Diverse threat sources, siloed scanning tools, duplicate data, and a lack of context create a data management problem	**Risk-Based Vulnerability Management** Built-in threat contextualization allows analysts to quickly find vulnerabilities used by active exploits in-the-wild, including those used by ransomware families. Reduce the administrative tasks of managing scan data and experience a solution that allows for quick filtering across prioritized risks so you can focus on the most immediate actions that will protect the organization.

Competitors

Risk-Based Vulnerability Management (RBVM):

brinqa KENNA Security NOPSEC

RiskSense Differentiators:

- Threat attribution / filtering by name to know the context of what is being dealt with. Asset susceptibility, Vulnerability Risk Rating (VRR) and RiskSense Security Scores (RS³) make security analysts more efficient
- Application Security with dashboard views of collective weaknesses (SAST/DAST/OSS/Container)
- Automation of playbooks to support multi-group and multi-asset workflow assignments and actions
- Enterprise-grade tracking that includes changes of vulnerability status, weaponization, false-positive and risk acceptance owners, and more for historical review and audits
- Ransomware dashboard

Threat & Vulnerability Management/Scanning:

Qualys. RAPID7 tenable

RiskSense Differentiators:

- RiskSense ingests data from all leading scanners, customers are not locked into a single vendor
- Application, container, and cloud weaknesses are quantified and prioritized within one solution without having to purchase additional modules
- Configurable dashboards give personalized focus on what matters most to your organization and track changes in status and risk improvements