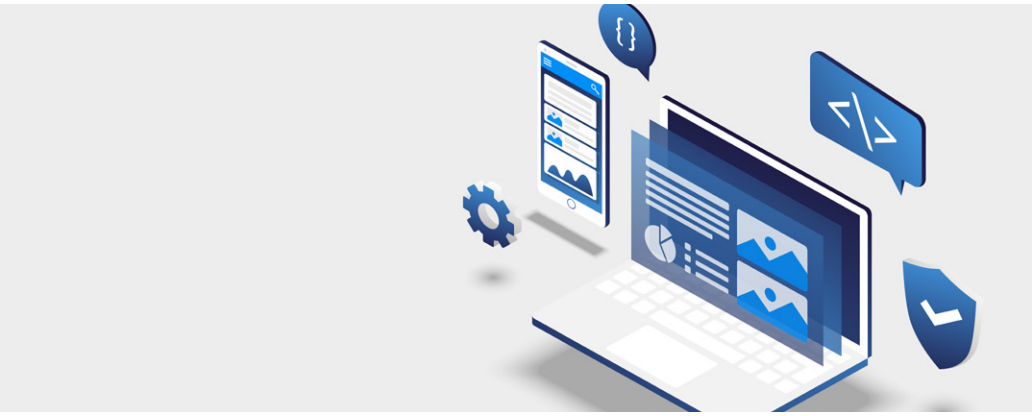
TECHNOLOGY BRIEF
RiskSense Application Security Risk Management

Risk-Based Vulnerability Management with Integrated Application Risk Exposure

KEY BENEFITS

- Normalized view of risk across CVE and CWE
- Understand your specific exposure to CWE Top 25 Software Errors and OWASP Top 10 Application Security risks
- Vulnerability Risk Ratings continuously update based on active trending threats in the wild
- Application Security Dashboard features easy drill-down to actionable data and remediation recommendations
- Filter to find the data you immediately need (i.e., by application, scanner type, use tags to identify development groups, and more)



THE CHALLENGE

Business innovation is being fueled by a software and application development revolution. Application frameworks and open source software projects allow for rapid and agile development but also introduce security risk and vulnerability exposure. Knowing your next move to cost-effectively address this exposure requires bridging the silos of infrastructure and application vulnerability management.

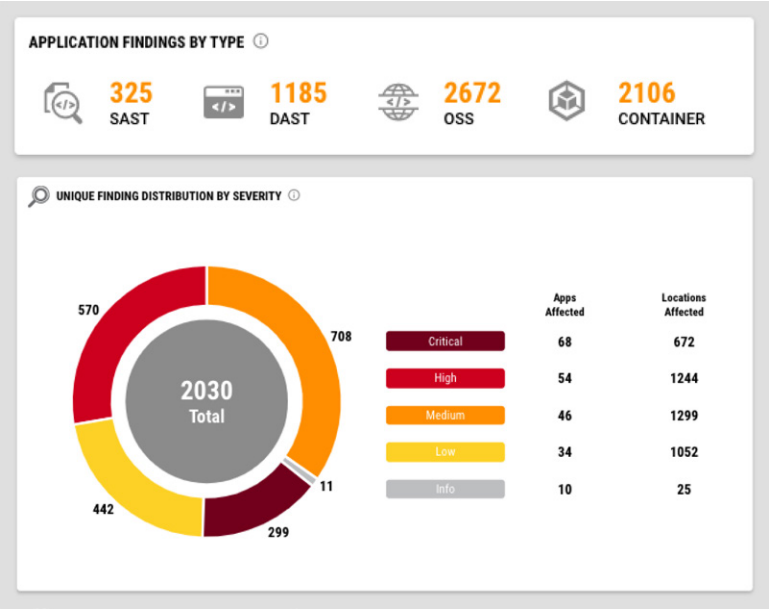
Bringing together the volumes of data from the wide arc of application scanning solutions into one view is not enough. Duplicate vulnerability findings surface across diverse development teams, within applications due to code reuse and the DevOps tools used for orchestration, containerization, and workload management. Context for vulnerability prioritization has to account for the business criticality of the application initiative, the development stage, and the supporting operational systems.

Application vulnerability prioritization and remediation tracking is a costly resource strain; researching active-threat risks, and tracking current business priorities and development phases. Centralized risk oversight is a goal not yet realized for most security programs. Enabling developers to act on what clearly matters the most before it becomes a costly endeavor to remediate is also a win for governance and audit. This only occurs when comprehensive visibility to risk can be achieved and the details of vulnerability status and changes are available to view end-to-end.

USE CASES

Full-stack Vulnerability Prioritization

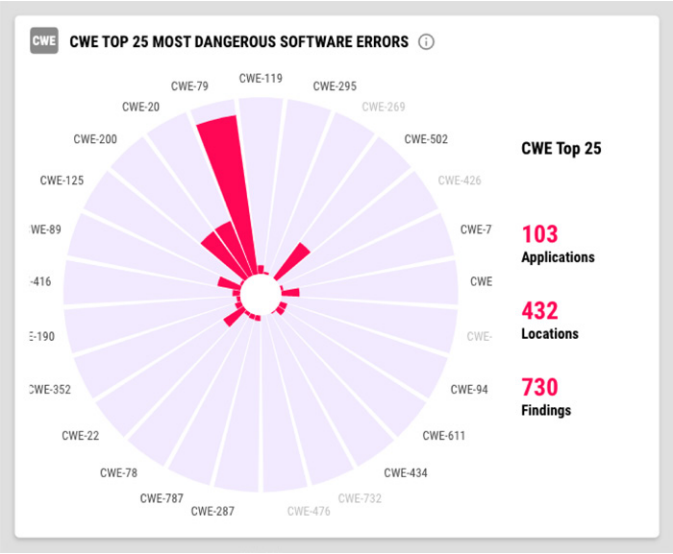
RiskSense provides application risk exposure integrated to create a full-spectrum risk-based vulnerability management program. With the Application Security Dashboard, you can focus on the key SAST, DAST, OSS, and Container scan data in one location. Enumerated count and ability to drill-down to see the full listing with the Vulnerability Risk Rating (VRR) and details for each of the individual findings. If your diverse teams use different SAST scanners, these will be consolidated in the listing and with on-page filtering, you can easily view by each scanning method or specific affected application.



RiskSense normalizes the application scanning results across multiple scanners and types with our Vulnerability Risk Rating (VRR).

Reduce Development Costs Addressing Risk Exposure Early

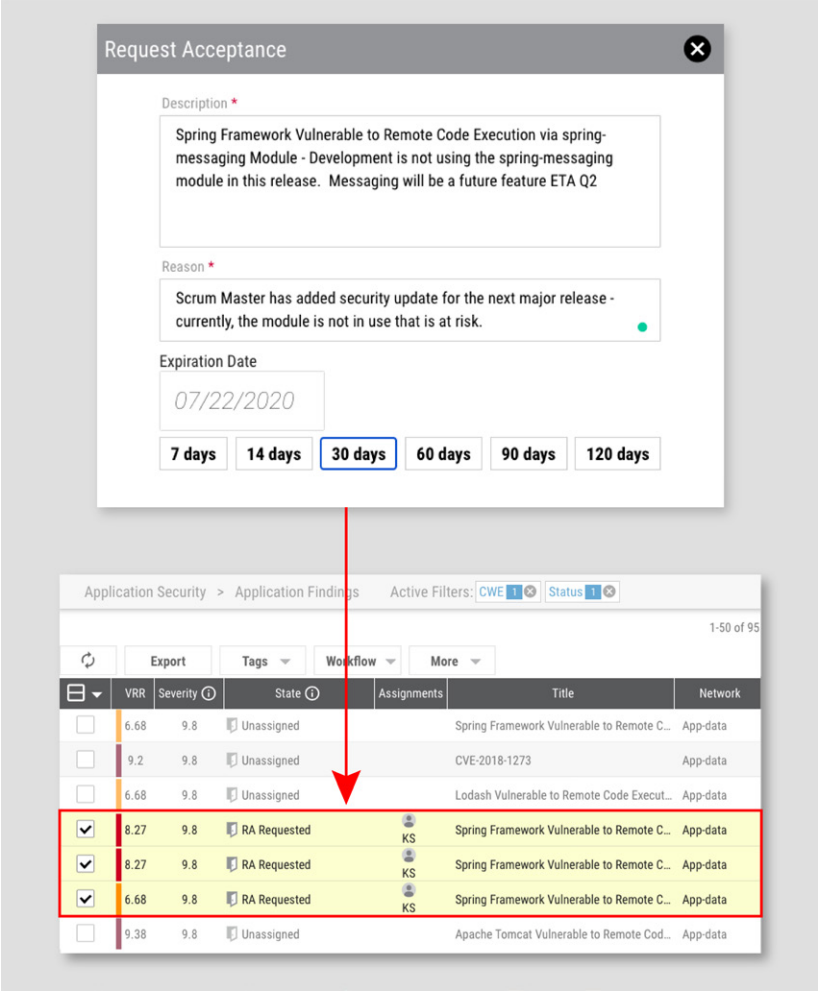
Vulnerabilities are mapped to the CWE Top 25 Most Dangerous Software Errors and OWASP Top 10 Web Application Security Risks and shown as explorable widgets. More importantly, you can now know exactly what applications are affected and where these errors are located. Clicking on any one of the categories delivers immediate details to make informed decisions on where to redirect development to fix these exposure points.



Trends from these typical errors are a great way to educate developers and grow their security awareness. Avoiding these code errors in the first place saves time on continuous 'fixing' of these common weaknesses.

Manage Application Risk Acceptance Conditions

For any vulnerability finding, RiskSense allows users to request Risk Acceptance for a specific period of time, incorporating remediation plan comments and any supporting files. Vulnerability risk oversight is now achieved from a single location with the details needed for managers to quickly accept or deny. This helps security keep pace with application development and allows for team collaboration on the exposure and business ramifications for vulnerability findings.



Users can select multiple vulnerabilities and with a single action assign and request Risk Acceptance (RA), tracking the details and expiration date for them all.

Track the Progress in Developing Secure Applications

Application development is measured by new releases of features and by addressing defined technical debt in bug fixes and maintenance. What has been missing is the ability to view the progress of application development in addressing security debt; the vulnerabilities, CWE, and OWASP findings that expose organizations. The RiskSense Application Security Dashboard provides a comprehensive VRR view of the findings. It also shows the balance of new scan findings and the rate in which they are remediated.

RiskSense integrates with all of the major IT ticketing systems with bi-directional communication providing real-time vulnerability status.

RiskSense full spectrum risk-based vulnerability management enables organizations to achieve centralized oversight for risk exposure. The solution extends the continuous prioritization based on threat context to application security and the flexibility to deliver a new cost-effective approach that also results in improving an organization's security posture.

ABOUT RISKSENSE

RiskSense®, Inc. provides vulnerability prioritization and management to measure and control cybersecurity risk. The cloud-based RiskSense platform uses a foundation of risk-based scoring, analytics, and technology-accelerated pen testing to identify critical security weaknesses with corresponding remediation action plans, dramatically improving security and IT team efficiency and effectiveness. For more information, visit www.risksense.com or follow us on Twitter at @RiskSense.

Contact us today to learn more about RiskSense
RiskSense, Inc. | +1 844.234.RISK | +1 505.217.9422 | www.risksense.com

CONTACT US | SCHEDULE A DEMO | READ OUR BLOG