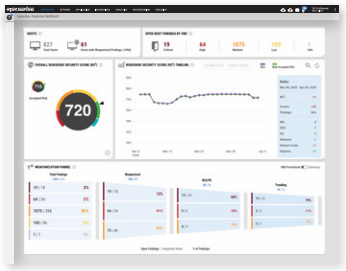
RISKSENSE

# The RiskSense Advantage

An industry first, RiskSense Full Spectrum Risk-Based Vulnerability Management offers compelling capabilities and advantages.

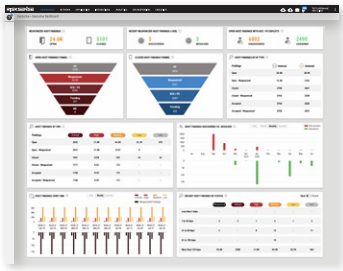
## Instant Risk Insight

RiskSense offers superior visual query and risk discovery across assets and infrastructure (network, cloud, applications, container, pen test findings, etc.) with drill-down capabilities in every view. Dashboards are fully customizable, and views can also be configured by groups and responsibilities, for example only showing a development lead the vulnerabilities that affect the application(s) they are responsible for. Built-in dashboards deliver immediate value across a range of users:



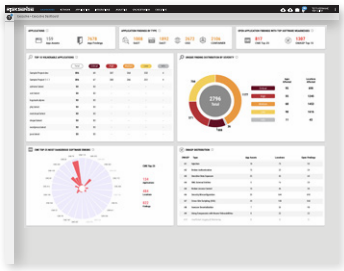
### Executive Dashboard

Provides an excellent vulnerability overview including a telling risk-based funnel showing vulnerabilities and impacted assets, those with threats, RCE/PE, and those that are trending



### Prioritization Dashboard

Presents security practitioners risk-based funnels along with views of the vulnerability risk ratings mapped to threat, asset externality, etc.



### Application Security Dashboard

Delivers an all-encompassing view across application security for senior leadership, while still giving DevOps the ability to see a more specific comparison of their apps and servers

## Multi-Client Support

Only RiskSense has the scalability to support enterprises of all shapes and sizes, including global multi-nationals with multitudes of business units, state and local governments, and MSSPs. We make it easy to cleanly separate business units/customers into "clients", facilitating easy tracking and management.

## Automation

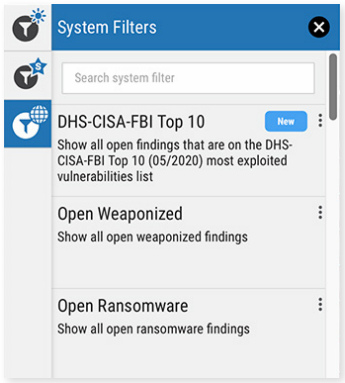
Automating common, repetitive tasks to flexibly work the way your company, business unit, or role requires is a snap in RiskSense. Once configured, automation Playbooks consistently and efficiently perform task sequences and are carried out in the background, allowing you to focus time and effort on remediation actions rather than administration. Historical tracking provides accountability and details that

reduce time spent with auditors. Adding assets containing a certain type of finding to a designated group, applying a tag to assets with specific critical-severity findings, or adding hosts with vulnerabilities tied to trending exploits to a particular group for expedited remediation are common examples.

## Threat-Focused Filtering

RiskSense shows you threats and how they are being used, allowing security professionals to better respond. Important for security analysts and threat hunters alike, correlated vulnerability and threat information ensures teams know the context of what they are dealing with. Most competing systems simplistically report static categories like "top priority" or "popular". RiskSense filters quickly show how specific threats like BlueKeep, WannaCry, or even the DHS/FBI Top 10 Exploited Vulnerabilities manifest themselves in your organization's environment, while still providing the flexibility to create your own custom filters. No other vendor offers this.




## Ransomware Dashboard

The Ransomware Dashboard quickly articulates your exposure The Ransomware Dashboard quickly articulates your exposure to the vulnerabilities that can be exploited to launch ransomware attacks. Open Findings associated with CVEs used by ransomware threats, the specific Assets Impacted, and the fixes (patches) available to address them are clearly presented, making it easy to form a risk-based action plan.

Our unique Ransomware Funnel shows the progression of risk and exposure to ransomware-related CVEs in your organization, starting with your vulnerability scanner findings, CVEs that support ransomware, then CVEs having an RCE or PE exploit threat, and finally any trending ransomware-capable CVEs. Throughout, the number of Assets Impacted are shown, with a single click revealing those affected assets. No other vendor offers this critical capability.

## Built-in and Integrated IT Workflows and Tracking

RiskSense offers native assignment and tracking, as well as integration with multiple concurrent IT workflow systems (e.g., ServiceNow, Remedy, or Jira), enables Security, IT, and DevOps to easily work together and focus on the actions that will have the most impact on the organization's cybersecurity posture.

Ticketing system integrations are bi-directional (most vendor's are one-way), ensuring data consistency. When a ticket is closed in either the RiskSense platform or the ticketing system, the state is accurately reflected in both.

RiskSense handles False Positives and Risk Acceptance with enforced approvals, sign-off, and tracking rather than relying on a simple checkbox, button, or tag. Of course, RiskSense maintains a log of a vulnerability's history for compliance and audit purposes to show what's been accepted, acted upon, and verified closed.

## Scoring

Rather than rely solely on potentially inaccurate CVSS severity values, RiskSense starts with a foundation of an accurate Vulnerability Risk Rating (VRR) for every vulnerability that incorporates threat context, allowing us to calculate a RiskSense Security Score (RS³) for each asset (think IP, host, application, etc.). To learn more about CVSS and the NVD, there are a number of great resources, including the article, "Thinking Outside the National Vulnerability Database Box" (and corresponding white paper), as well as an excellent blog, "The Art and Science of Predicting Weaponization". To learn more about the ground-breaking RiskSense Security Score, check out the white paper, "RS³ – RiskSense Security Score".

## RiskSense SRS (Security Rating Service)

RiskSense scanning and reconnaissance discovers an organization's external assets, often finding 20-25% more assets than the organization knew about. This information feeds scores across six key security categories – Network Security, DNS Security, Application Security, Email Security, Patch Cadence, and Domain Reputation – then leverages RiskSense platform threat intelligence analytics to calculate risk and prioritize remediation. No other vendor offers this "outside-in" hacker's view in concert with the "inside-out" risk-based vulnerability management view.