August 2020

"RiskSense Unifies Application and Infrastructure Security Risks Management"

Vulnerability exposure and risk continues to be a hot topic for organizations. RiskSense is looking at more ways to help in bringing operational efficiencies to businesses of all sizes.

For large enterprises, many of them continue to look at web application development as a leading means to continue to transform and create competitive advantages. 43% of breaches investigated by Verizon this past year were due to web application vulnerabilities. RiskSense announced an industry-leading capability that normalizes application and infrastructure vulnerabilities, eliminating any ambiguity about risk priorities.

We have also seen others sign-up for RiskSense comprehensive Vulnerability Management as a Service. This is the bundling of security services and the RiskSense Risk-Based Vulnerability Management (RBVM) platform. It provides a turn-key service that eliminates the need for scan licenses and allows security staff to focus where the business needs them. From scanning to remediation prioritization, customers can take action with detailed patch recommendation.

The RiskSense platform also delivers new system filters to quickly identify new threats, workflow and risk acceptance audit trails, configurable dashboards and much more. Let your prospects see how they can reduce their costs instead of trying to build-out an internal risk-based vulnerability management program.

Please continue to stay safe,

The RiskSense Team

RiskSense in the News

New Capabilities Eliminate Data Silos to Provide Contextually Aware Risk Ratings Across CVEs and CWEs from Development to Production

Learn more about the details and functionality

that now gives Security leaders visibility to their attack surface vulnerability exposure from applications to infrastructure.

Read the Details

RiskSense Updates

Measuring Adversarial Risk

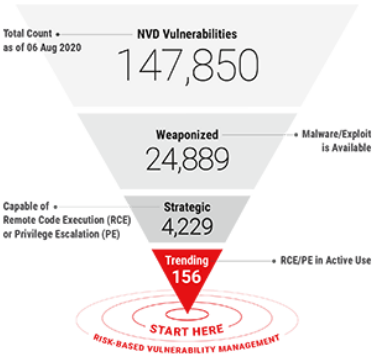
RiskSense Vulnerability Risk Rating (VRR) is the foundation that provides the capability to prioritize across CVE and CWE risk. Read this technical brief to understand the deep analysis that goes into any VRR calculation.

Read More

Threat Exposure by Name

'BootHole' is a vulnerability that affects most Linux systems, and any Window system using Secure Boot. This vulnerability has the potential to take over billions of Linux and Windows devices. If you were a RiskSense customer, and your boss asked how many systems were affected in your organization, one click on the newly released system filter for 'BootHole' – CVE-2020-10713 would tell you. Learn about the other system filters that allow organizations to find threat exposures by name (think ransomware), giving executives the details they need about their exposure with a quick way to track remediation progress.

Read About System Filters



In a Universe of Vulnerabilities Where Do You Start?

Share this quick video with prospects on how a risk-based approach to vulnerability management delivers prioritized remediation actions. This is the beginning of several quick videos RiskSense will be providing - helping organizations know where to start is just the initial step of a mature vulnerability management program.

Share the Video

RiskSense Partner Deal Registration web page.
Find more information and resources at www.risksense.com.