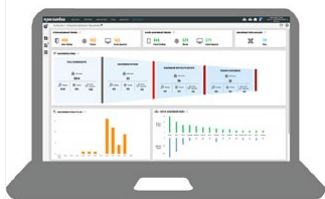




February, 2020



This month we have a lot of exciting things to share focused on enabling organizations to [#FightRansomware](#).

A new feature is now available, RiskSense Ransomware Dashboard. Within our RiskSense [Risk-Based Vulnerability Management solution](#), it's easy to track and act quickly to reduce risk against the most dangerous and actively trending ransomware families.

"RiskSense Tells Organizations if and Where They Are Vulnerable to Attacks From Specific Ransomware Strains"

- Press Coverage

Recognizing that not every organization has the immediate resources and expertise to move into action, we now offer a [Ransomware Assessment Service](#). It is a unique offering in the market that combines managed authenticated vulnerability scanning and the Ransomware Dashboard with our platform to fulfill a critical element in a risk-based vulnerability management program.

With all of this news, of course, we are rolling out Partner enablement programs. The details that will help your organization get up to speed and quickly and grow your commercial leads are on the way. Make sure you schedule with me today to find out all that we can do for you, from sales coaching, presentation materials, and specialty SLED marketing support for the hardest hit by ransomware.

- Lauren Trujillo (lauren.trujillo@risksense.com)

RiskSense In the News



We had a great response from the press and news publications from our Announcement. Read the details from the coverage on our 'Media Coverage' page.

[Go to Media Coverage](#)



RiskSense Updates



Ransomware Dashboard

RiskSense Ransomware Dashboard gives immediate insight into organizational exposure. Know which assets are affected and the priorities for remediation to proactively reduce risk.

[Learn More](#)



SOLUTION BRIEF FOR RISKSENSE RANSOMWARE ASSESSMENT

Ransomware Exposure Evaluation

Cyber Priorities to Fight Ransomware

Having a ransomware incident is not just a matter of if, but when, how, and how much. A ransomware program is powerful, it delivers the impact, and it continues to evolve. It's not just a matter of if, but when, how, and how much.

Ransomware attacks cost private and public sector enterprises more than \$2 billion per year. When Microsoft attacked in May 2017, it caught 100,000 victims in over 150 countries in one weekend. The only way to get ahead of ransomware is to take a proactive and stop an attack before it gets started. The top priority is to prevent ransomware attacks in the first place. The off-hand priority is to prevent ransomware. Have backup, shut down unnecessary ports, limit privileges, and keep up to date on patching. It's generally good advice, but can be difficult for a smaller organization to keep up with. And the difficulty is that even if an attack occurs, and you are able to restore from a backup, you may still be at risk. The fact is that good backup can lead to a major component of the vulnerability that enabled the original ransomware attack gets restored in the restored assets. The organization continues to be at risk.

The RiskSense Ransomware Assessment program is an evaluation of ransomware susceptibility. Experts perform authenticated scanning as well as automated and manual security pen-testing. Customers log in and see immediate results via the RiskSense enhanced risk-based vulnerability management (RBVM) solution. We assess and show organizations the prioritized and prescriptive actions to block ransomware. Access continues cyber risk management insights through RiskSense RBVM. Attack surface assessment from scanning and security testing yield detailed asset findings. And, only RiskSense RBVM features a ransomware dashboard, allowing organizations, from executives to IT staff, to track ransomware risk, view current remediation activities, and immediately view of any new exposure points within seconds.

The RiskSense Ransomware Assessment Program includes:

- Reassessment of the organization's attack surface, internal and external facing assets
- Authenticated vulnerability discovery using our library of scanners and custom-built tools
- The identification of misconfigurations and vulnerabilities on an organization's network
- Detailed analysis of the assessment results, including the scanning and obtained configuration data
- Threat modeling to assess the likely vector and impact of an attack focusing on account types in use and the file shares across your desktops and infrastructure
- Remediation recommendations
- Delivery of findings through the RiskSense platform delivering the details and capability to automate immediate workflows and prioritize activities.

Methodology

The RiskSense Ransomware Assessment program follows the process:

- 1. Scanning
- 2. Assessment
- 3. Analysis
- 4. Reporting
- 5. Remediation
- 6. Monitoring

Ransomware Assessment Program

The RiskSense Ransomware Assessment Program is an evaluation of ransomware susceptibility. Experts perform authenticated scanning as well as automated and manual security pen-testing. Customers log in and see immediate results via the RiskSense enhanced risk-based vulnerability management (RBVM) solution.

[Download the Solution Brief](#)



RiskSense Today Podcast

Curious about ransomware? Listen to this podcast featuring RiskSense CEO Srinivas Mukkamala as he talks about this epidemic. This podcast is a follow-up to the RiskSense Spotlight Report: Enterprise Ransomware through the Lens of Threat and Vulnerability Management. ([Share or download this report here](#)).

[Listen Now](#)



Fighting Back - Ransomware

Want to understand your current exposure to the vulnerabilities that enable ransomware attacks? Watch our webinar to learn more and see RiskSense Ransomware Dashboard in action.

[Listen Now](#)

RiskSense [Partner Deal Registration](#) web page.
Find more information and resources at www.risksense.com.

RiskSense, Inc., 1230 Midas Way, Suite 220, Sunnyvale, CA 94085, USA

[Unsubscribe](#) [Manage preferences](#)