RiskSense Ransomware Assessment

Ransomware Exposure Evaluation

Cyber Priorities to Fight Ransomware

"Having ransomware risk exposure identified, enumerated, and a dashboard that lets me track remediation progress is powerful. It delivers the insight needed to communicate to executives and my IT staff on the progress and steps we are taking to avoid this problem."

Ransomware attacks cost private and public sector enterprises more than $1 billion per year.[1] When WannaCry attacked in May 2017 it caught 300,000 victims in over 150 countries in one weekend.[2] The only way to get ahead of ransomware is to close exposure points and stop an attack before it gets started. The high-profile ransomware attacks in the news represent only a fraction of this epidemic problem. The oft-heard guidance on preventing ransomware – have backups, shut down unnecessary ports, limit privileges, and keep up to date on patching – is generally good advice, but can be difficult for a complex organization to keep up with. And the downside is that even if an attack occurs, and you are able to restore from a backup, you may still be at risk. The last known good backup can lead to a repeat compromise because the vulnerability that enabled the original ransomware attack gets restored in the re-instated assets. The organization continues to be at risk.

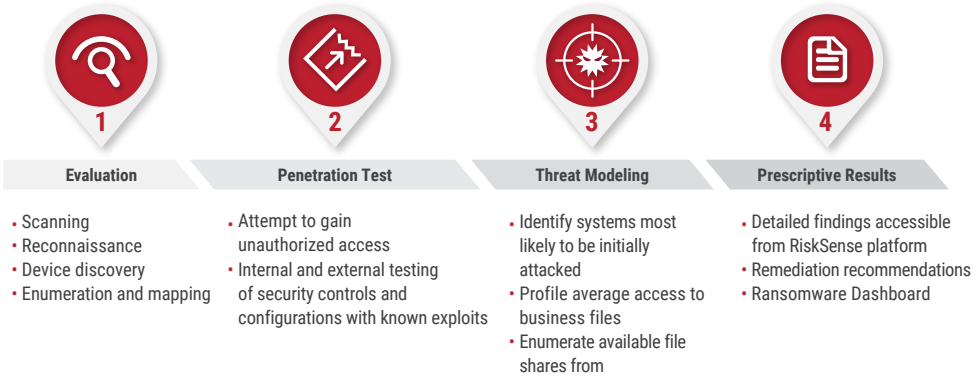
The RiskSense Ransomware Assessment program is an evaluation of ransomware susceptibility. Experts perform authenticated scanning as well as automated and manual security pen-testing. Customers log in and see immediate results via the RiskSense enhanced risk-based vulnerability management (RBVM) solution. We assess and show organizations the prioritized and preemptive actions to block ransomware. Access continuous 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 know of any new exposure points within seconds.

The RiskSense Ransomware Assessment program includes:

- Reconnaissance 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 workflows and prioritize activities

Methodology

The RiskSense Ransomware Assessment program follows this process:

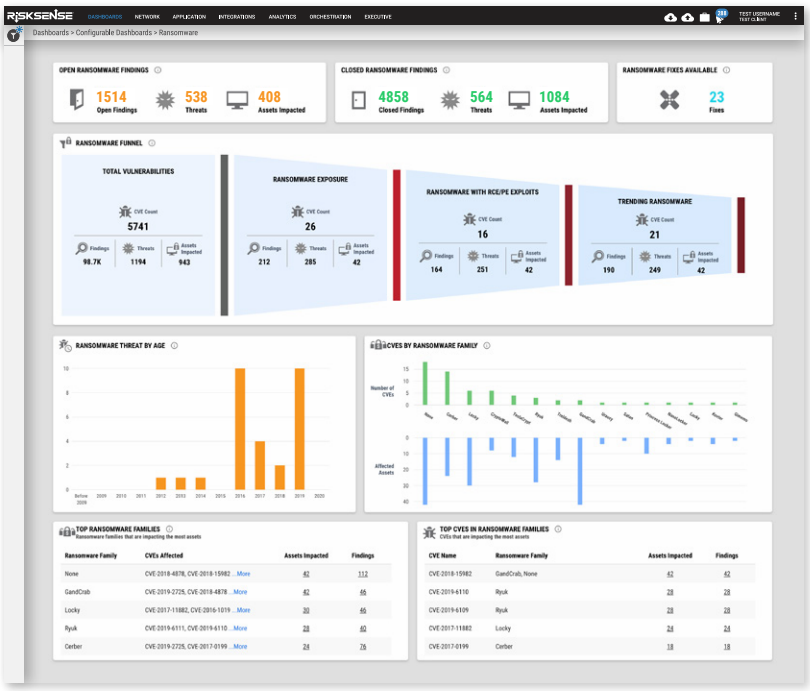


[1] https://www.zdnet.com/article/the-cost-of-ransomware-attacks-1-billion-this-year/

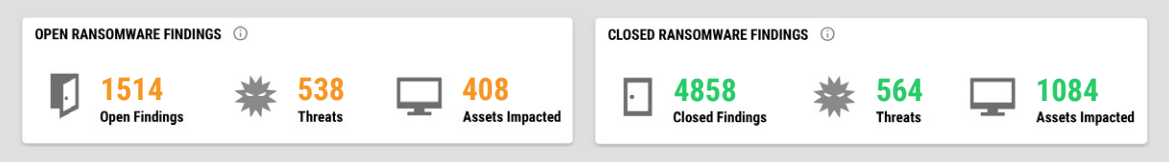
[2] https://www.zdnet.com/article/ransomware-an-executive-guide-to-one-of-the-biggest-menaces-on-the-web/

Ransomware Dashboard

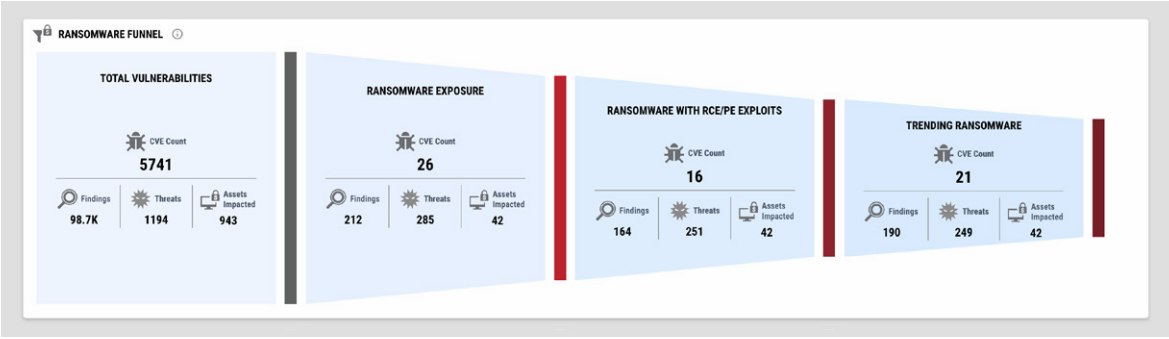
The RiskSense Ransomware Assessment program includes access to RiskSense RBVM which provides visibility on ransomware susceptibility through on-going threat correlation coupled with monthly or quarterly authenticated vulnerability scans. The results of these scans are presented in the Ransomware Dashboard. All data can be drilled into for actionable remediation recommendations and tracking.



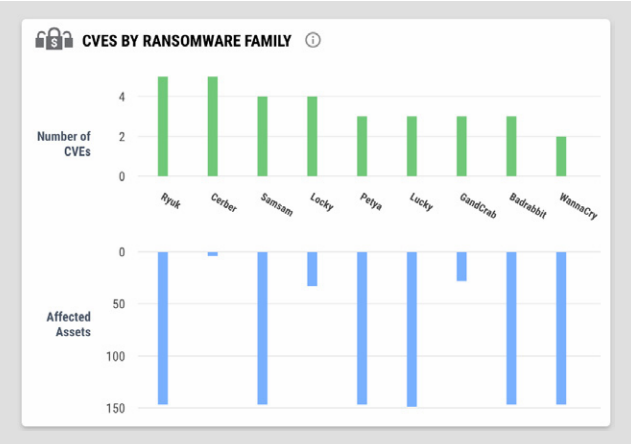
- The Ransomware Dashboard displays open and closed findings associated with ransomware CVEs and threats.



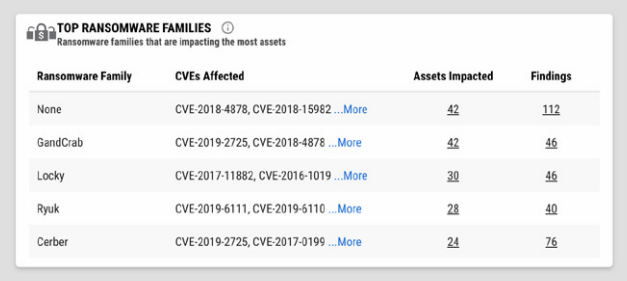
- The risk-based ransomware funnel displays your exposure to ransomware-related CVEs. The funnel view shows the number of assets impacted by these CVEs, and a single click takes you to an asset view showing which specific assets are most affected.



- The Ransomware Dashboard also shows the most common ransomware families and the number of vulnerabilities and affected assets for each. Ransomware threats are often referred to in the news and security articles by their family name, like WannaCry and SamSam, so this is a great place to see at a glance if you have exposure to a particular ransomware family and move to address it.



- The Ransomware Dashboard also shows top ransomware families and the top CVEs based on their footprint, i.e., assets impacted within your network.



TOP RANSOMWARE FAMILIES
Ransomware families that are impacting the most assets

Ransomware Family	CVEs Affected	Assets Impacted	Findings
None	CVE-2018-4878, CVE-2018-15982 ...More	42	112
GandCrab	CVE-2019-2725, CVE-2018-4878 ...More	42	46
Locky	CVE-2017-11882, CVE-2016-1019 ...More	30	46
Ryuk	CVE-2019-6111, CVE-2019-6110 ...More	28	40
Cerber	CVE-2019-2725, CVE-2017-0199 ...More	24	76

Cyber Kill Chain – Stopping Ransomware in its Tracks

The RiskSense Ransomware Assessment program assists you in determining your susceptibility at key points as outlined by the Cyber Kill Chain including before exploitation or lateral movement. Each of these steps involve patching, system configuration, and network/domain configuration identified by the assessment.

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.

The company delivers a fully-informed picture of group, department, and organizational cybersecurity risk with our credit-like RiskSense Security Score (RS³). The RiskSense platform continuously correlates customer infrastructure with comprehensive internal and external vulnerability data, threat intelligence, human pen test findings, and business asset criticality to measure risk, provide early warning of weaponization, predict attacks, and prioritize remediation activities to achieve security risk goals. For more information, visit www.risksense.com or follow us on Twitter at @RiskSense.

Contact your LRS account manager to learn more.