This article was originally published February 23,2020 on eWeek.com
https://www.eweek.com/security/how-risksense-provides-actionable-intelligence-to-fight-cyber-threats

How RiskSense Provides Actionable Intelligence to Fight Cyber Threats

By: Frank Ohlhorst | February 23, 2020

RiskSense brings vulnerability management prioritization to the masses.

Cybersecurity hygiene has become one of the most important factors of protecting enterprise networks from intrusions, data theft and other malicious activities. Yet, many enterprise security staffers have come to rely on assumptions, as opposed to measuring the actual vulnerabilities that may impact their security posture.

Simply put, assumptions are made based upon what patches have been applied, what anti-malware systems are in place and what user validation systems are being used.

Truth be told, having the latest and greatest cyber defenses may not be enough, and savvy cybersecurity managers need more than great defenses—they also need to understand the risks and vulnerabilities that evolve on an almost daily basis. Gathering that intelligence is anything but easy, unless a platform that exposes risk is deployed—and that is where RiskSense comes into the picture.

A Closer Look at the RiskSense Platform

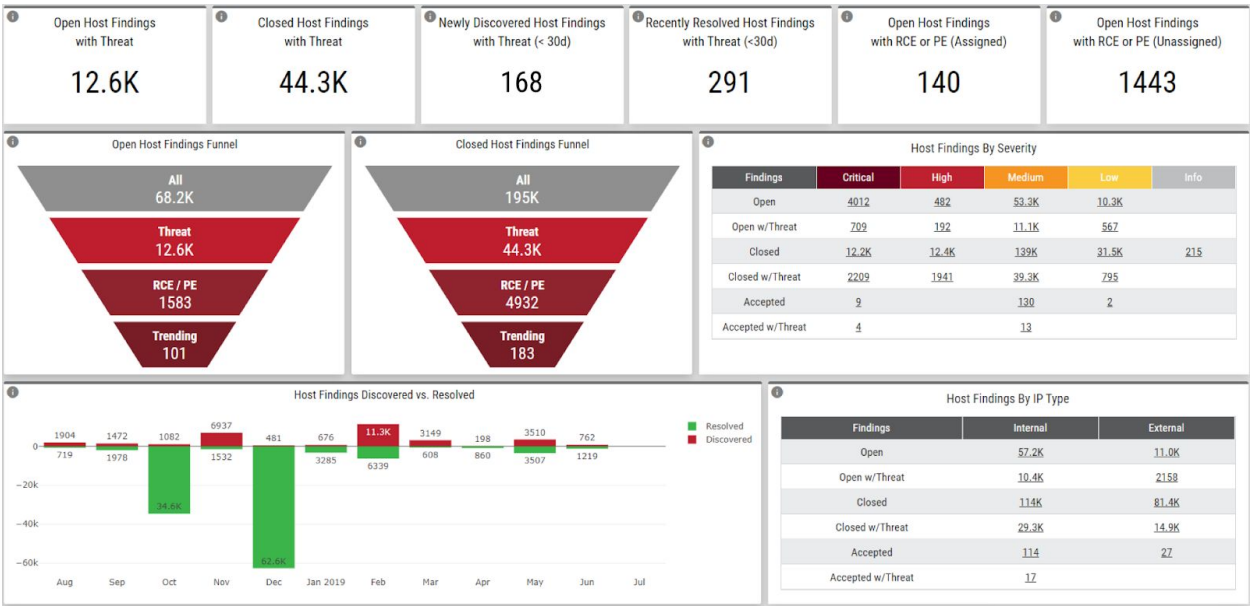
As the name implies, RiskSense is all about understanding risk. Or more aptly put, the company provides a platform that allows enterprises to assess cyber risk and then actually do something about it. The RiskSense platform offers a trifecta of capabilities: Risk-Based Vulnerability Management, Attack Surface Validation and Vulnerability Discovery. That trio of capabilities helps enterprises mitigate risk before that risk becomes an actual problem. What's more, the platform is able to "score" risk and help cyber professionals determine the level of risk and take the needed action to mitigate that risk. That said, the appropriate starting point to assess risk comes in the form of the RiskSense Risk-Based Vulnerability Management platform.

Focusing on RiskSense Risk-Based Vulnerability Management

Risk and vulnerabilities have a symbiotic relationship that can impact any enterprise. However, judging the amount of risk a particular vulnerability has can be a tricky process. Take, for example, the tens of thousands identified vulnerabilities that have been identified to date, how much risk does any one of those vulnerabilities pose to a particular enterprise? It is not a question that is easily answered. It all comes down to what assets an enterprise has to protect, along with if exploits have been created to weaponize a vulnerability.

Risk-Based Vulnerability Management brings analysis and visualization to the forefront of the cybersecurity professionals' purview. The platform combines intelligence gathering, assessment, known threats and numerous other capabilities to present administrators with a dashboard that visualizes risk. The product is able to query the network, identify vulnerabilities and offer intelligence around the risk that a vulnerability may create. What's more, the dashboard approach also prioritizes risk so that action can be taken immediately to mitigate that risk. Much of that information drives what is known as a RiskSense Security Score, or RS3, which offers a very concise measurement of how much risk an organization is exposed to and gives an indication of the priority of the threats.

The Executive Dashboard offers a plethora of actionable data in a concise fashion that allows cybersecurity professionals to understand the risk associated with their current network setup. One notable visualization is the dashboard's capability to associate risk with trends and priorities, allowing an administrator to quickly extrapolate what must be done immediately to protect the network. The dashboard also allows administrators to quickly drill down into details to ascertain a better understanding of the factors surrounding a level of risk. In addition, the dashboard lends itself well to presentations and further explaining risk factors to those decision makers who are not technically savvy.



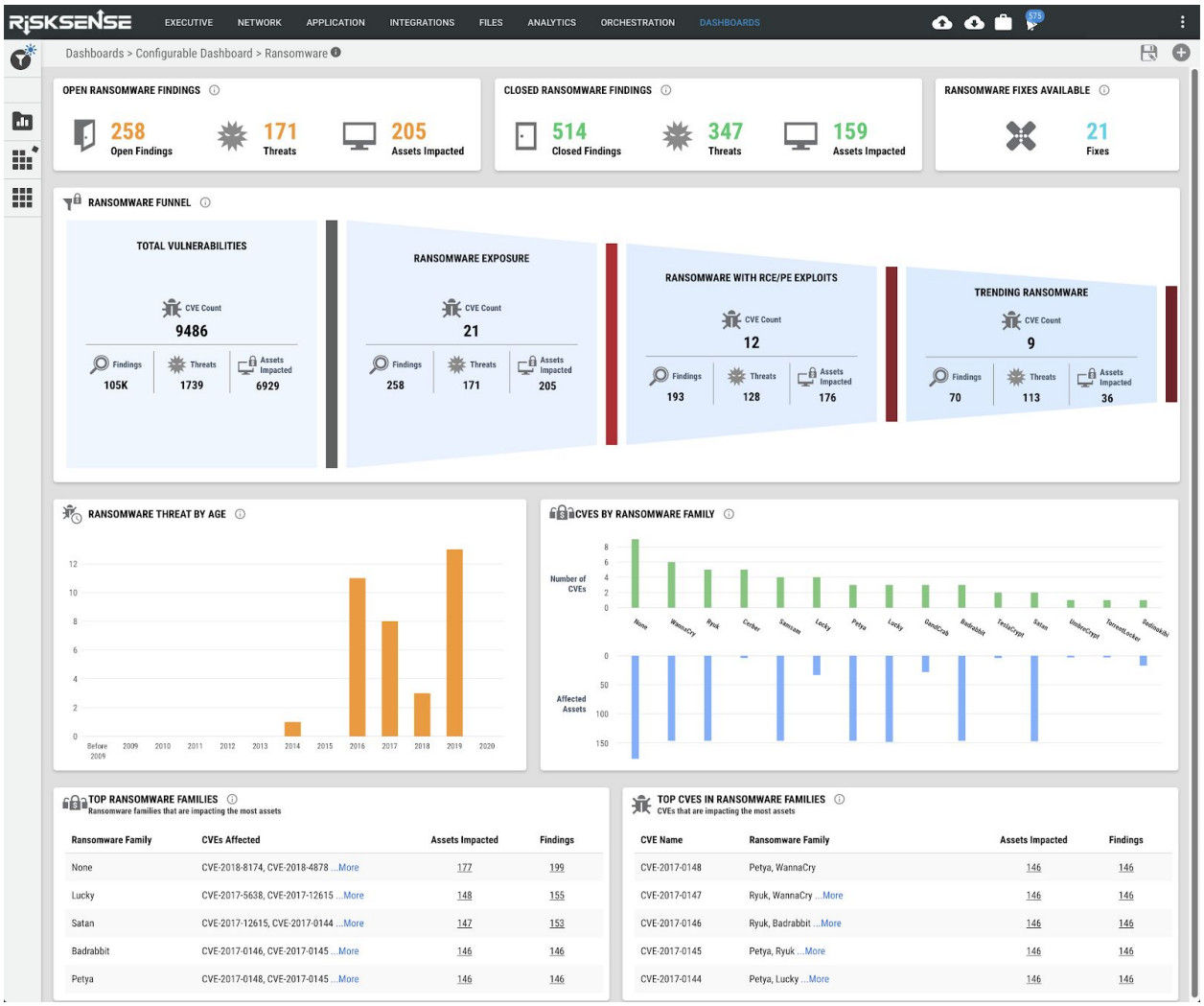
RiskSense Prioritization Dashboard

A Prioritization Dashboard further eases the burden of remediation by creating a visual correlation between threat levels and vulnerabilities, pointing administrators to the most critical threats and providing the knowledge to act quickly and follow through with needed steps to resolve the problem. It is important to note that the RiskSense platform is able to gather data from numerous sources using the company's Smart Connector Framework. That framework supports automated ingestion of data from different sources, including third-party network scanners, web application scanners, asset management systems, ticketing systems, compliance systems, cloud security systems and numerous others.

Administrators also can drill down into the full set of details surrounding a vulnerability and gather more intelligence about what risk is involved with the discovered vulnerability and pursue additional actions. Ultimately, RiskSense is able to connect the dots between vulnerabilities and the likelihood those vulnerabilities contribute to risk. What's more, the analytics provide actionable intelligence that helps administrators mitigate threats before they impact the enterprise.

What About Ransomware?

Identifying and mitigating vulnerabilities can only take a cybersecurity team so far. With that in mind, RiskSense added a new capability to the platform that allows cyber pros to take on the challenge of ransomware. Combating ransomware means that cybersecurity professionals must go on the offensive and find and remediate the vulnerabilities used by ransomware before they enable an attack on the organization. The threat of ransomware is somewhat different from that of traditional vulnerabilities, which for the most part are fixed by patches or other changes. Ransomware works more like an infection, where malicious code is deposited on the network and lies in wait.

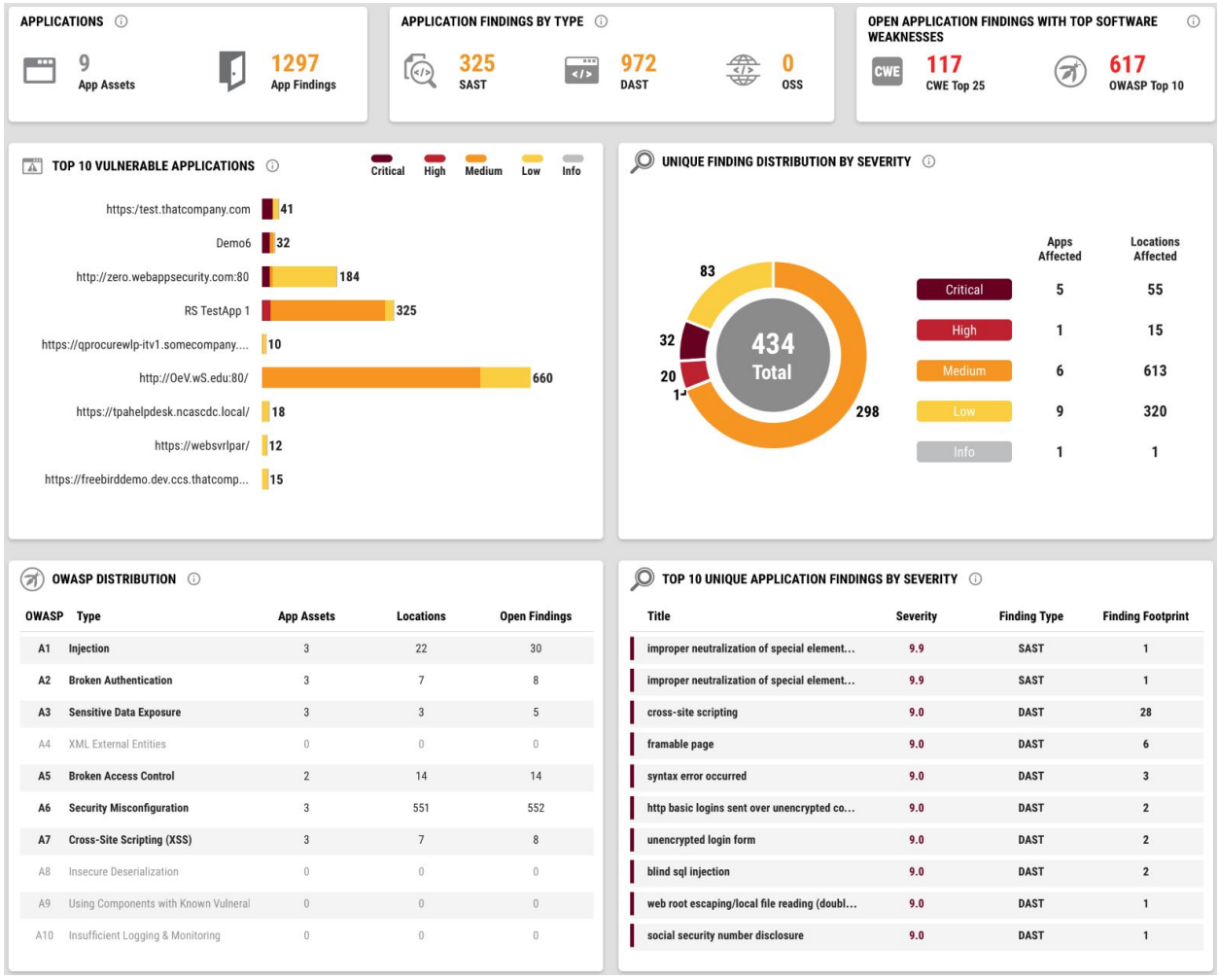


**** The RiskSense Ransomware Dashboard***

RiskSense tackles the ransomware issue with a Ransomware Dashboard, which automatically reveals an organization's susceptibility to ransomware. The dashboard reveals all assets affected by vulnerabilities that enable ransomware and visualizes the risk presented to those

assets. That risk is visualized using what the company calls a “Ransomware Funnel,” which gives cold, hard statistics on the total number of vulnerabilities present, provides focus on the exposure to ransomware and then ties that together with threats and trends. The dashboard helps administrators quickly find ransomware exposures and take action.

RiskSense provides plenty of additional information when it comes to the scourge of ransomware. At a glance, administrators can see what ransomware families to which they are exposed to, if vulnerabilities with Remote Code Execution (RCE) are present on any systems, and if any vulnerabilities that contain privilege escalation (PE) capabilities exist in the network. All of the gathered data and analysis helps cyber pros take the action necessary to remediate ransomware risks before disaster strikes.



**** The RiskSense Application Security Dashboard***

Conclusions

Ultimately, protecting IT assets all comes down to defining acceptable risk. However, the amount of risk that is acceptable varies based upon the assets that need to be protected. Some enterprises may assign a lower level of importance to risk for consumer-facing systems, such as kiosks or digital display systems, while others may focus more on their internal platforms.

Dealing with risk means knowing what the actual risk is. RiskSense does an excellent job of quantifying risk and informing enterprises on the vulnerabilities that increase risk. Since the complete elimination of risk is a mathematical impossibility, RiskSense brings critical information, such as assets, attack surfaces, known threats, threat trends and ways to mitigate threats, to the forefront, allowing administrators to prioritize vulnerability mitigation.

RiskSense is one of those rare solutions that demonstrates value right at the outset. By quickly identifying vulnerabilities and the trends behind malicious code, administrators can estimate what needs to be done and present management with the knowledge that they are on top of the complexities that define today's threat vectors. Simply put, RiskSense is a tool that most any cyber professional would want to have. RiskSense is a cloud-based SaaS solution. Annual subscription pricing starts at $12 per asset, with enterprise volume and subscription term discounts available.

Frank Ohlhorst is a veteran IT product reviewer and analyst who has been an eWEEK regular for many years.