CSO
BUSINESS RISK LEADERSHIP
June 26, 2017 www.csoonline.com

REVIEW

RedSeal offers powerful, passive network protection

The RedSeal appliance doesn't actually fix anything on its own, but it does act as a force multiplier for every other security device within a network.

By John Breeden II

Credit: Thinkstock

When CSO's sister site Network World conducted its firewall manager review, the original plan was to invite RedSeal to participate. The problem was that while RedSeal originally did manage firewalls, their product has now evolved into something else. RedSeal shares some similarities to firewall managers, but is now in a separate, unique product group. We tested the RedSeal appliance to see where it fits into cybersecurity defenses.

RedSeal today is a digital resilience platform designed to discover all network vulnerabilities, including those that go around firewalls, and map attack vectors so they can be fixed. It also tracks network health and provides an overall vulnerability score that can be monitored by either executives or IT staff.

Deployed as a physical or virtual appliance, it's unique in cybersecurity in that it is designed to work completely offline, with technicians either feeding it information physically at regular intervals, or by allowing it to collect data from other security appliances at regular intervals, and remain offline and disconnected at all other times. This is done as much as a security precaution as anything else, though you do get the advantage of not having RedSeal take up network bandwidth and resources.

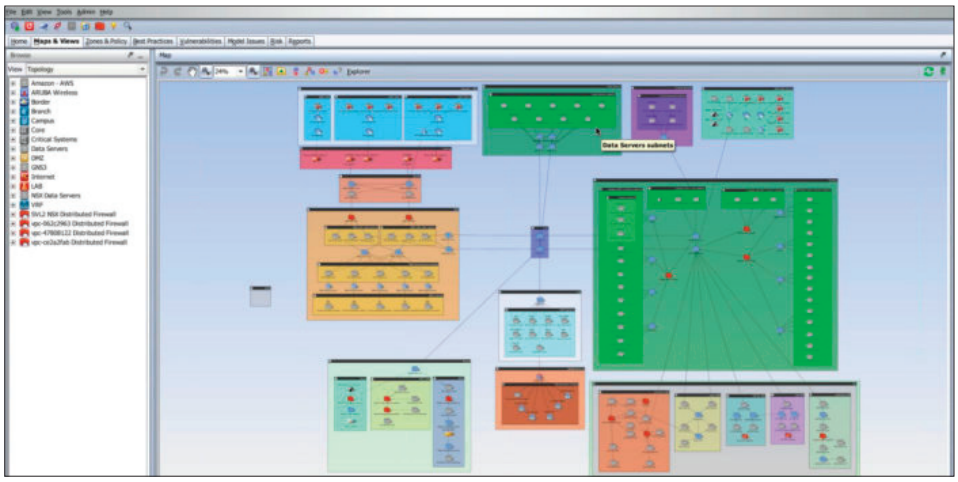
In terms of security, users are basically giving RedSeal the keys to their kingdom, allowing an internal device to accurately plot all possible attack vectors through a network from the inside. If an attacker could compromise a RedSeal box, they would have a perfect roadmap not only telling them how to attack, but where to go to get the exact data they want. So, it's best to keep the appliance out of line with regular traffic, or air gapped and not connected at all.

Network mapping

RedSeal can accept configurations and reports from firewalls – including their rule sets, routers and switches, software-defined networking rules and cloud configurations, information from network load balancers, mobile device controllers and any vulnerability data collected by other appliances such as scanners and the SOC.

Once collected, RedSeal maps out the entire network architecture including every path and possible path between devices. This map can be extremely extensive. On our test network, it mapped about 100 systems, but the company provided maps it has made of global networks with thousands of devices.

The map is extremely helpful when trying to determine an overall security picture. For example, if a firewall rule blocks traffic from the internet to a core system, then no path will be displayed on the map. But if there is a flaw in that configuration, it will be revealed as a system path. We found one previously unknown pathway between systems in our test network that was the result of a firewall rule



John Breeden

problem, and one hidden path that was put in place on purpose to route around firewalls.

Some firewall managers also have this level of functionality, but the RedSeal map is one of the best we've seen. Users will need to configure the map to reflect their system architecture and how they think of their network. For example, you can place servers and assets in groups based on their geography or physical location, or they can be grouped by function, or anything else you choose to use.

Assets can be individually selected for the map, or entire IP ranges can be specified to make up groups. Once partitioned, users are free to color code each group or individual asset however they like. You might want to make your core services a bright color like yellow to draw attention, or color your public-facing assets red to reflect the highest chance of danger. Plotting out a chart like that will take longer with larger networks, but the mapping process is straightforward, with a good user interface.

Assessing threats

In addition to the network map, RedSeal also runs asset information through its threat reference library and examines configurations to compare with a threat correlation engine. The threat correlation engine is extremely powerful, and in our testing, could highlight a truly dangerous threat as it related specifically to the test network compared to one that was not as bad because of mitigating factors.

The risk engine was extremely precise. Pulling back the curtain a little bit on how it operates, we found that it compiles the scores of connected hosts together to accentuate specific dangers. For example, we had one system in our test network that had a critical vulnerability. Almost every other security appliance would have flagged that device as a high-priority, fix-immediately situation. However, RedSeal looked at the connections associated with that system and found that users there were blocked from going almost anywhere critical within the network by security appliances. As such, it got a risk score of 104, which is minor in comparison to others.

Another system had a moderate problem that needed to be patched or otherwise mitigated. However, it connected directly to a second host with the same vulnerability, which in turn connected to a third. Eventually those minor flaws in security configurations would have allowed an attacker to horizontally move within the network and reach a core asset via an unprotected path. The combination of vulnerable downstream hosts and an unprotected critical asset ratcheted up the score of the original host with its medium-level vulnerability to 15,310.

Looking at both problems without context, most security appliances would probably have assigned the first vulnerability as a high priority and the second as a medium or low one. But because RedSeal had access to the network map, including all the vulnerabilities in the path an attacker could take, it could highlight the real danger, prioritizing the host with a 15,310 score verses the one with 104. On a large network, proper prioritizing like this could be a huge help to busy security and SOC teams.

John Breeden

Offline advantages

There are additional advantages to having an offline security appliance collect and correlate data from other sources. For example, because it can accept data from network vulnerability scanners, it can take that into account in the context of the network topography, but without having to perform any scans of its own. And, it can also act as a check for those scanners, ensuring that everything is really being scanned. On our test network, there was a configuration error that was blocking the scanner from getting to one large subnet, but the scanner didn't know this. When the scanner data was imported into RedSeal, it was compared with the total network map. The discrepancy was identified, and RedSeal told us the exact firewall and even the line of code that was blocking the scanner.

Because RedSeal has access to vulnerability data and network mapping for the entire enterprise, it can also be used to simulate attacks in a form of reverse threat hunting. Users simply select an asset and ask what would happen if it were compromised. From there, actual vulnerabilities within the asset and those connected to it can be explored and mitigated. Doing this would allow paths to be hardened, or even eliminated, to keep important data and assets safe from attackers.

Resilience scoring

The final thing that RedSeal does is provide an overall resilience score of network health as it relates to security and vulnerabilities. Read like a credit score, it shows how safe a network is on a scale where 850 is the highest attainable value. The score is available within the RedSeal interface and as an app for Android or iOS devices. The idea is to make this data available at a glance for executives so they know how healthy their networks are, letting them confirm that their IT teams are doing their jobs. It also can act as a quick starting point for IT teams, who can see at a glance whenever anything happens to lower their resilience score.

RedSeal is helpful in explaining how the resiliency score is obtained, and what needs to be done to raise it closer to 850. For example, on our test network, we lost nine points due to vulnerabilities, 25 because of configuration clashes and 22 because we had an incomplete network model. Using the app or the main interface, we could drill down and find specific problems that needed to be addressed. Fixing them changed the overall score the next time that relevant data was given to the RedSeal appliance.

The RedSeal appliance does not actually fix anything on its own, though it can direct IT teams to the exact spot that needs attention. It also does not work in real-time, and in fact should be kept offline for security reasons. What it does, however, is act as a force multiplier for every other security device within a network, finding vulnerabilities and mapping out the dangers in relation to the specific network being protected. As such, it fills a unique need in cybersecurity, providing over watch for other security devices, and helping to harden defenses across the entire network, especially in pathways it identifies as the most critically in need of protection.

John Breeden II is an award-winning journalist and reviewer with over 20 years of experience covering technology. He is the CEO of the Tech Writers Bureau, a group that creates technological thought leadership content for organizations of all sizes.

REDSEAL