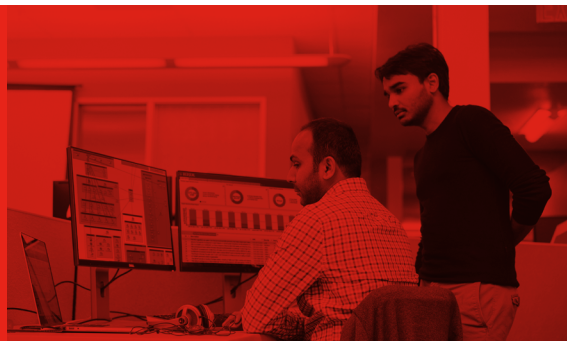
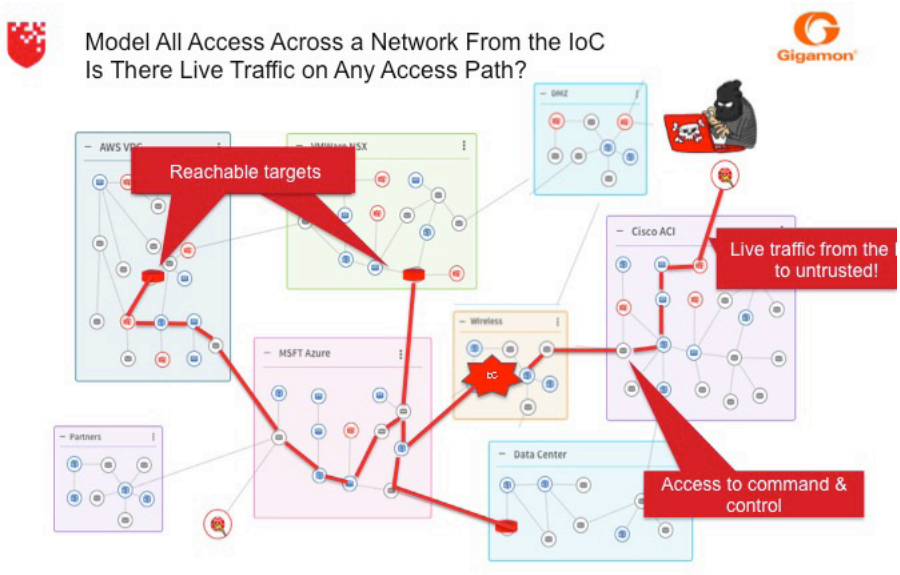
DETECT LIVE NETWORK TRAFFIC IN YOUR REDSEAL MODEL



THE CHALLENGE

Although detecting threats is critical to security, the key to minimizing a security incident's impact is a swift incident investigation phase—uncovering the affected device's location, what it is, what type of access it has, and whether it can reach other critical assets on the network. The next logical question is whether there is live traffic going from the device to critical assets or even out to an exfiltration point.

Trying to find all possible paths to all critical assets in your network and then answering the live traffic question is extremely difficult, tedious, and time-consuming. Furthermore, deciding how to contain the incident without full network context comes with the high risk that the attacker will maintain a presence in your network. While your team focuses on analysis and containment, today's threat actors can spread quickly and establish deep footholds across your network, giving them opportunities to cause more damage.



BENEFITS

- Detect live traffic from any detailed path query
- Quickly locate and investigate a breach
- Determine if a command and control server can be reached
- Mitigate risk based on asset value and potential for attack
- Block pathways an adversary can use to exploit vulnerable assets

940 Stewart Drive, Sunnyvale, CA 94085
+1 408 641 2200 | 888 845 8169 | redseal.net

December 2017

REDSEAL AND GIGAMON

SOLUTION

RedSeal's model calculates all access—intended, unintended, active and potential—between any two points on your network. With RedSeal's network visualization, you can see all the individual devices between one point and another, and pinpoint the exact rules you need to change to affect access on each device.

Our Gigamon/RedSeal integration lets you quickly know if there is live traffic across any of these access paths and more effectively prioritize your containment options. Imagine you have identified an indicator of compromise (IoC) or policy violation. RedSeal can tell you if the IoC has access to a critical asset. Gigamon's live traffic data will show you the access paths you should prioritize.

- RedSeal provides a list of the downstream assets the compromised device can access, prioritized based on asset value and the severity of known, exploitable vulnerabilities.
- RedSeal shows you detailed host information for each reachable asset. You'll be able to see detailed pathways to these downstream assets, including the firewall rule (or ACL) that is allows access to them.
- RedSeal provides each device's OS, applications (services), MAC address, subnet (e.g., finance, sales, engineering), and policy group.
- RedSeal gives you the switch and port number the device connects to.
- RedSeal highlights compromised hosts that can be accessed from an untrusted network. They might be connecting to a command and control server, which could be exfiltrating confidential information.
- RedSeal arms you with the information you need for a well thought out and thorough containment plan.

WHAT YOU NEED

- Gigamon GigaVUE-FM 5.00 or later
- RedSeal 8.5 or later

REDSEAL

940 Stewart Drive, Sunnyvale, CA 94085

+1 408 641 2200 | 888 845 8169 | redseal.net

December 2017