NETWORK ACCESS MODELING IMPROVES SECURITY, PERFORMANCE AND UPTIME FOR FEMA

When disaster strikes, the Federal Emergency Management Agency (FEMA) enterprise network is expanded to include "temporary" mobile data centers that can last from months to years. In this kind of situation, change control, network maps and configurations can get wildly out of control. The security engineers in FEMA's Security Operation Center (SOC) wanted network visibility. What's more, they needed continuous monitoring to be able to measure risk and make decisions about how to deploy their scarce time and resources.

After learning more about RedSeal's security analytics platform, FEMA's cybersecurity lead realized that it could fill a major void in the agency's solution set. RedSeal could help him understand the network, measure resilience, verify compliance, and accelerate response to security incidents and network vulnerabilities.

The FEMA SOC team deployed RedSeal to help manage their change control process — by modeling the data centers as they popped up in near real time. As data centers come online, they use RedSeal to ensure the right access is available. In the coming months, the team is expanding use of RedSeal to support their incident response program.

FEMA's network team also uses RedSeal, to visualize access from disaster sites. Initially, they were shocked by the level of network access sprawl. They had no idea how much gear was on the network at a disaster site or how many security consequences resulted from simple configuration changes.

Now, with RedSeal's continuously-updated network model, the network team is able to identify everything on the network and rapidly address any configuration changes that cause security, performance, and network uptime issues.