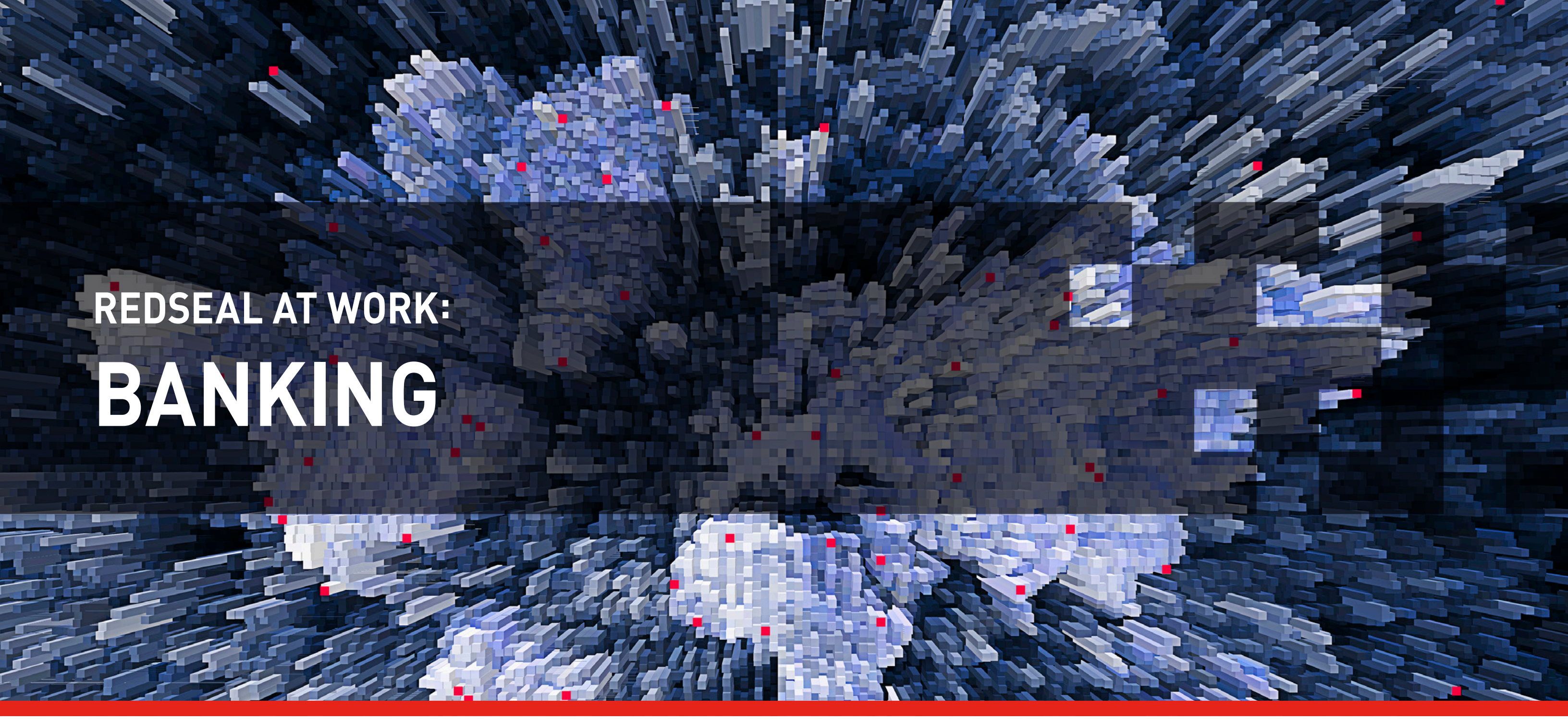

REDSEAL AT WORK:

BANKING

SITUATION

A large credit union wanted to verify its network segmentation policies across cash dispensers, ATMs, and voice networks at each branch office. To do this, they needed to first gain an understanding of their network device inventory and existing access paths. But this was a time-intensive, manual process. They didn't have an automated way to discover what was on their networks, identify unwanted access paths, or verify and monitor network segmentation—continuously.

REDSEAL SOLUTION:

The credit union first used RedSeal to discover the network infrastructure on both the corporate and branch office networks. RedSeal identified previously unknown network devices, as well as high risk issues caused by non-secure configurations. Next, they used RedSeal to create a model of access paths across and within each branch office and discovered many that were unintended.

RESULTS:

RedSeal helped discover nearly 100 network devices in the credit union's networks so the team could bring them under management. RedSeal also checked these devices for secure configurations, using industry best practices as a benchmark. The configurations on several of these devices represented high risks to the networks. Remediating and verifying these configurations greatly enhanced the security of the credit union's network infrastructure.

RedSeal's model of network access paths revealed unused (and unknown) paths that created even greater risk, leading the team to decommission several Cellular LTE tunnels. It also revealed unintended access to critical ATM machines, created to be temporary but never removed.

After identifying their network assets and understanding how they are all connected, the credit union now uses RedSeal to continuously validate segmentation policies to protect these critical assets.

REDSEAL

1600 Technology Drive, San Jose, CA 95110
+1 408 641 2200 | 888 845 8169 | redseal.net

AUGUST 2020