The Device

The SecureLink adapter operates the scanner and provides network connectivity in a puck-sized box

Workstations

Networking allows Security First to run its teller stations on barebones computers no taller than a water bottle.

Case Study: Security First Bank
The Networked Branch of Tomorrow, Today

Much has been written about networking's role in the "connected" bank branch of the future. Forward-looking ideas abound with banks rolling out "teller pods" and ATM-like self-service stations inside the branch, all driven by various touchscreens, tablets, and wireless devices. Such flashy and exciting concepts represent the future of the industry, according to many.

At the same time, though, other banks are taking advantage of what networking can do for the branch of today. Security First Bank of Rapid City, SD, is one of them.

Security First operates its branch network across 100,000 square miles of Nebraska and South Dakota, which encompasses some of the most isolated communities in the continental United States. Maintaining real-time connections across such a vast territory might seem like a daunting task – and it is (see sidebar). However, once the logistical challenges were overcome, migrating the branch environment into a thin-client networked platform made a great deal of sense in reducing costs and improving performance and security.

Utilizing Horizon™ Teller from FIS Global, as well as XenApp and Xen Desktop from Citrix, Security First has been able to reduce its technology footprint at each branch location by using thin-client workstations at the teller counter. Instead of operating a traditional desktop PC, each window utilizes an inexpensive, barebones workstation that communicates in real time with a central server, which does the heavy-duty transaction processing. Each workstation is so small, it is easy to mistake one for a small cable modem or a router.

Nonetheless, using a thin-client setup at a teller workstation presents another challenge: How to drive peripherals, such as scanners, printers, and card readers. By design, networked branches are not set up to have software installed on individual workstations. Unless a scanner can run itself, the workstation, at minimum, needs the drivers to be able to communicate with it.

In a thin-client environment, the practice of installing drivers on individual workstations is also notorious for causing conflicts. Security First reported that its workstations were unable to have both a check scanner and another scanner or ID card reader

active at the same time – one had to be turned off in order to operate the other. As a further annoyance, some peripherals would fail to register on the network if they were turned on while the teller program was already running. This resulted in employees needing to exit the teller program, restart the connected devices, and then open the teller program again.

While driving a scanner from a central server technically is possible, it would mean pushing the captured TIFF images back and forth across the network for processing, thereby using valuable bandwidth and leading to slower speeds. These have historically been the major challenges of running a check scanner in a networked environment.

Customer Profile

Security First Bank

Founded: 1898

Headquarters: Rapid City, South Dakota

Assets: ~$1 billion

Branches: 29

Employees: 270

Core system: FIS Horizon

Scanners: TellerScan® TS500 with SecureLink by Digital Check®

SecureLink by Digital Check® combined with the TellerScan® TS500 check scanner provided the solution to Security First's challenge of capturing checks at a teller window on a thin-client workstation. SecureLink is a small (3" x 4") device that adds wireless or hardwired Ethernet network capability to the TS500, while simultaneously running all the drivers and API software so nothing has to be installed on the workstation.

The unit acts as a mini-computer that not only runs the scanner, but also processes and compresses the images before sending them across the network. File sizes are reduced by up to 97%, significantly reducing bandwidth requirements. In some areas where Security First operates, the only Internet connectivity option is a slower DSL connection, so eliminating that bottleneck is critical.

For Security First, switching to SecureLink solved two problems at once: Driving the scanner directly eliminated software conflicts on the workstation; and the onboard processing and file compression took the strain off network resources, while improving the scan speed of the device itself. (SecureLink can operate Digital Check scanners at up to their full rated speeds, but poor network conditions or low bandwidth can be a limiting factor.)

Before SecureLink, scanning at the teller window had been such a slow process that the bank just did not do it at all. When a customer brought in a batch of checks, the teller simply accepted them and immediately provided provisional credit to the account, later scanning the checks at the back counter and making corrections if necessary. While this meant transactions were "faster" in terms of time spent at the teller window, the process was less than ideal. SecureLink has finally made capturing checks fast and reliable enough to do at the front counter while the customer is still present.

More recently, Security First began implementing the Teller Transaction Printer (TTP), a stackable receipt printer that sits underneath the TS500 scanner – saving even more counter space. The bank is performing a gradual rollout, installing a TTP at a teller window whenever an old printer is replaced.

Security First has turned a challenging situation into an opportunity. Betting on the newest technology has paid off with a modern system delivering big-bank customer service while running smoothly on the IT side. Digital Check's TellerScan TS500 scanner and SecureLink network device help make it possible for Security First to be a pioneer in network-enabled banking.

require regular updates and security fixes, rather than having those performed centrally on the Terminal and Application servers. While that hybrid approach was manageable, it did have unintended consequences:

"It actually worked out pretty well for us, except that everyone would save all their daily proof work until the very end of the day," Monheim recalled. "So they would all slam the servers at 4 p.m. [uploading check images], and we'd have to restart services for every-body. From an IT point of view, we like it a lot better when we see that traffic flow throughout the day."

Network uptime might sound like a serious problem in Security First's primarily rural territory; however, that has not been as much of an issue as one might think, according to Monheim. A decade ago, that may have been a concern; but in 2017, the infrastructure, even in remote areas of the contiguous United States, tends to be sufficiently reliable (when both primary and backup connections are employed) for near 100% availability.

For redundancy, the bank employs a main data center as well as a separate "disaster recovery" data center, and both of these as well as the main branches run on a multi-protocol label switching (MPLS) network. To put it simply, the ISP reroutes interrupted connections via the next-shortest path to the target destination. In some of the more remote locations where only a single connection path exists, the local branch handles transactions offline until the network comes back online, sometimes trans-porting the physical deposits to a differ-ent branch for processing. Mon-heim said that has only happened a handful of times during his tenure.

"This is a huge issue when it happens, though, and we are looking at deploying DSL backhauls or even Verizon Wireless as a backup connection," he explained. "If someone cuts a line out there, for example, we're at the mercy of the ISP's repair schedule. But that's why having secondary ISP connections as a backup helps mitigate these risks. Although this type of thing only happens maybe once a

Covering a Vast Expanse
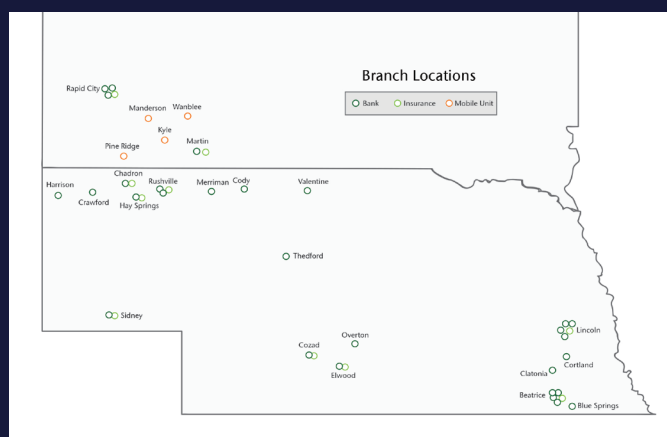
Security First Bank's branch network spans more than 100,000 square miles in South Dakota and Nebraska. A networked branch solution may have posed challenges in the past, but infrastructure is now reliable enough to operate even in very remote areas.

year or every couple of years, in maybe one of the 28 branches we have."

Security First also operates a unique form of "mobile banking" where a branch on wheels travels to a handful of extremely isolated towns within the expansive Pine Ridge Reservation. The branch is essen-tially an RV with two teller stations – which operate over the network like all of the bank's branch-es! The bank has arrangements with the local ISPs to plug in directly to a hookup on the utility pole, and the teller stations work just like any others. The bank recently bought a new, upgraded mobile branch after putting more than 200,000 miles on the

THE BADLANDS EXPRESS is a mobile "branch on wheels" that brings in-person banking service to extremely isolated areas in South Dakota - in particular, the Pine Ridge Reservation. Even this branch is part of Security First's network platform, connecting to the internet directly through hookups at designated utility poles.

previous one. It has also entered discussions with cellular carriers to explore options for running banking operations through 4G mobile hotspots. This new "mobile banking" experiment, combined with its inno-vative core branch setup, has proven that Security First is capable of projecting its network almost anywhere.