Although this type of thing only happens maybe once a connections as a backup helps mitigate these risks. But that's why having secondary ISP there, for example, we're at the mercy of the ISP's DSL backhauls or even Verizon Wireless as a backup looking at deploying during his tenure.

For redundancy, the bank employs a main data center and both of these as well as the main branches run on connections are employed) for near 100% availability. For remote areas of the contiguous United States, tends to have not been as much of an issue as one might think, Security First's primarily rural territory; however, that does pose some challenges. As a further annoyance, some peripherals would fail to register on the network like all of extremely isolated towns within the expansive Pine of South Dakota, which encompasses some of the most isolated communities in the country. 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 can sit underneath the TS500 Printer (TTP), a stackable receipt printer that sits underneath the TS500 workstation. SecureLink is a small unit that acts as a mini-computer installed on the workstation. The SecureLink adapter operates the scanner and provides network connectivity in a puck-sized box. The Device

Workstations

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

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 touchscreen, 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 can sit underneath the TS500 Printer (TTP), a stackable receipt printer that sits underneath the TS500 workstation. SecureLink is a small unit that acts as a mini-computer installed on the workstation. The SecureLink adapter operates the scanner and provides network connectivity in a puck-sized box.

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.
connections as a backup helps mitigate these risks. But that's why having secondary ISP connection, "he explained. "If someone cuts a line out though, and we are handful of times processing. Min-ent branch for transactions offline branch handles exists, the local connection path via the next-shortest path to the target destination. In put it simply, the ISP reroutes interrupted connections and both of these as well as the main branches run on For redundancy, the bank employs a main data center Security First's primarily rural territory; however, that body. From an IT point of view, we like it a lot better require regular updates and security fixes, rather than drivers to be able to communicate with it. (continued on next page)
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 everybody. 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 transporting the physical deposits to a different branch for processing. Monheim 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 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 essentially an RV with two teller stations – which operate over the network like all of the bank’s branches! 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 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 innovative core branch setup, has proven that Security First is capable of projecting its network almost anywhere.