

Allowing Secure Remote Access to Sensitive Data

Consolidated Bank of Kenya Ltd.

The Consolidated Bank of Kenya Ltd. offers the most comprehensive banking services and products currently available in Kenya. It continually develops innovative and flexible financial solutions giving its customers the resources they need to achieve personal and financial success. The bank was incorporated in 1989 as part of an effort to stabilize Kenya's financial sector by restructuring nine insolvent institutions into one functional organization.

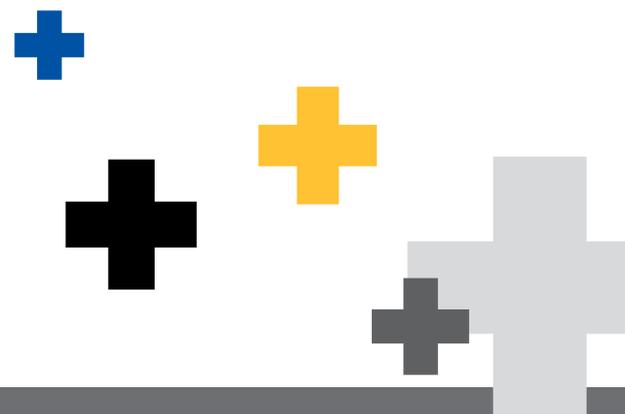
The challenge: Achieving Unified and Secure Access Control

As in most businesses, Consolidated Bank was caught off guard by the coronavirus pandemic. To ensure the safety of its customers and employees, the bank immediately instituted a work-from-home policy. While maintaining data security is essential for many businesses, for banks, it is a top priority. As a result of the sudden pandemic, Consolidated Bank was struck with the problem of ensuring that its users (mainly employees) were safe from the pandemic at home and had secure access to sensitive financial data.

The challenges they needed to solve included:

- + Unifying access control for all types of users
- + Providing clientless access to users
- + Ensuring authentication of users prior to being granted access
- + Keeping users off the network

The bank VPN that been used at the time was neither secure nor flexible enough to meet users' needs while ensuring the standard of data safety they aspire to have. Furthermore, due to its remote location, Consolidated Bank's VPN options were limited. The bank needed to find a secure and flexible option that would allow all of its internal users access to the information they needed to remain productive without putting users or customer data at risk. Preferably, this solution would allow users access through a portal rather than a VPN, requiring minimal installation on the end user's part.



The Solution: Creating Secure Access with Safe-T's ZoneZero SDP Architecture

Consolidated Bank contacted Safe-T through DataGroupIT & iSolution and requested a solution that would allow corporate users to securely access their data while requiring minimum installation on the user's end. Safe-T's Zero Trust Network (ZTNA) solution, ZoneZero Software Define Perimeter, was built to allow organizations to grant secure access to their services for all entities. It perfectly met Consolidated Bank's needs by granting a level of security appropriate for the sensitivity of the financial information users needed to access, without requiring a complex and drawn-out installation process.

Safe-T began implementing an SDP (Software Defined

Perimeter) solution in an enterprise environment (LAN/DMZ). This limits the area attackers can access and increases the security of the data.

In addition to increasing the system's security by limiting the area cyber-attackers can access, Safe-T's solution allows users to access sensitive organizational resources securely using a terminal service (RDP). To ensure security is maintained while users access data, the solution integrates an enterprise database for user identification, forcing users to authenticate their identity before receiving access to the information and ensuring that information is only accessed by those authorized to do

Benefits to Customer

- + Clientless end-users receive easy, convenient, and fast access
- + Each user receives permission for modular access to the organization's resources
- + Real-time security reports
- + Easier access to organizational resources due to reverse access technology.

Safe-T allows Consolidated Bank to continue operations without risking its employees' health or clients' data security.