vyntra

CASE STUDY

Sidian Bank

Kenya

SidianBank
Own Tomorrow

Sidian Bank wanted greater visibility over its back-office core banking platform T24, to bring more rigor to its controls and processes, and produce easy-to-understand reports.

Implementation was pretty much plug-and-play. The only preparation we had to do was work out which reports we wanted and then make sure that the relevant fields within T24 were activated to produce them. We were helped and guided in this by Vyntra' local support office. Throughout the project we had no surprises.

Peter Karichu
Head of internal audit
Sidian Bank

The Requirement

Sidian Bank, headquartered in Nairobi, Kenya, has 44 branches across the country, as well as a strong online service primarily serving urban, low-income groups alongside small to medium-sized businesses. Its core banking platform is Temenos's T24.

Early 2019, the bank suffered what it describes as a "cyber incident" on a subsidiary server. While no funds or data were lost, the subsequent IT review highlighted areas where security and processes needed improvement to reduce the risk of further such events. This included gaining better visibility of IT staff's backend activities.

The bank was also keen for all its staff to follow its security processes strictly. This included the protocol that staff must not share passwords, for example. Karichu believed he could achieve this by showing staff that the bank was monitoring everything – from the number of times an individual logged in and the IP address they used, to the task they performed and the length of time they spent doing it.

> The main challenge was that the controls we had were only ever as good as the people who used them. If they shared passwords, the control was no longer valid.

> We realized that super-users [internal experts with special system-access privileges] could do things without us having any visibility and this loophole could easily be exploited.
>
> We needed comprehensive logs of user activity right along a transaction from start to finish, and we wanted to be able to easily turn these logs into understandable reports.
>
> **Peter Karichu, Head of internal audit, Sidian Bank.**

The Solution

A member of the senior management team had worked with Vyntra at NIC Bank in the past and Karichu had previously looked into using the fintech's fraud-mitigation software. Both men had a good understanding of how it worked and what it could achieve.

Vyntra' algorithms and intelligent machine learning would allow them to develop detailed profiles of their system users and customers against which they could com pare every transaction. Whenever any given parameter deviated from the established profile, the system would raise an alert. This way the bank gets complete visibility across all transactions, including actions by super-users with special access privileges.

The bank signed a contract with Vyntra in April 2019, less than two months after the cyber incident.

Preparation for implementation was minimal. Karichu and his team had to install one new server to run the software, decide on the areas for detailed reporting, and make sure the relevant data fields within T24 were turned on. Implementation was then very fast. Work began at the beginning of October and by early November, the software was producing the majority of the reports Karichu had originally specified.

Speed of implementation is down to the plug-and-play nature of Vyntra' software. It is pre-configured to work with the major digital core banking platform providers, including T24 used by Sidian Bank.

> The data fields we needed for the reports already existed within T24; they just needed to be turned on, he says.
>
> We were helped and guided in this by Vyntra' local support office

Vyntra also helped the bank identify areas where it could extend digital monitoring, such as in-branch authorization, to reduce risk further.

> Authorization has to be in real time. If a transaction is over a set amount, the teller must make certain checks before handing over the cash. But these exceptional authorizations were piling up, with tellers dispensing cash before the checks were complete. I was pleased to find a way to stop this, he says.

The final handover was in early December 2019.

The Benefits

Even before the implementation was complete, the new software spotted and stopped a fraud at Sidian and another bank.

Sidian Bank had suspected that fraudsters were using its ATMs to collect cash from mobile wallets via SIM swaps [when a criminal persuades the mobile service provider to change the account to a new phone number that he/she controls and then empties the mobile wallet linked to the original phone]. It had asked the Vyntra software to monitor how often a customer used an ATM to withdraw cash.

One weekend in mid-December 2019, the software raised an alert about an ATM from which multiple withdrawals had been made in quick succession. The alert was passed to the mobile wallet operator Safaricom and when the fraudsters tried again at a different bank, they were stopped and arrested.

Since then the software has spotted and stopped more fraud. According to Karichu, fraud incidents in 2020 are significantly lower than for the same time last year.

> In the past, unexplained operational losses from the tellers, for example, averaged say KES 2m a year. This year, January to September, 100 percent of the teller shortages can be explained, and operational losses are down to low five figures, he says.

The amount of time the bank spends on investigating suspicious activity is also down by at least 20 percent.

> The reports the system produces are easy to read and we can drill down for the information we need quickly. Their reports speak more to our needs and have cut [an average] 10-day investigation by two days. Maybe even more for simpler cases, he says.

Looking ahead, he hopes that the Vyntra software can be integrated with the bank's SWIFT operations and Visa transactions to give a better view of its international position. But for now, Karichu is impressed with how big an impact Vyntra has already had on the bank.

> We can now explain a transaction from start to finish. This has had a huge impact not only on stopping fraud, but also on our staff, who now know we can see everything.
>
> Password sharing has stopped. It's made a huge difference, he says.

About us

Vyntra is a global leader in transaction intelligence, formed from the union of NetGuardians and Intix.

Combining deep expertise in financial crime prevention, Vyntra equips over 130 financial institutions in 60+ countries with intelligent tools to detect fraud, ensure AML compliance, and gain real-time visibility into every transaction.

For more information, please contact us:
communications@vyntra.com