observe it

CUSTOMER SUCCESS STORY

BankservAfrica Uses ObserveIT to Combat Insider Threats

ObserveIT Enables BankservAfrica's Complete "Defense in Depth" Strategy & PCI-DSS Compliance

About the Company

BankservAfrica processes billions of transactions valued at trillions of South African rand annually.

Customers include banks, corporations, government and the retail sector.

By volume of low-value transactions alone, the company is Africa's largest automated payments clearing house.

Their Challenges

BankservAfrica is a natural target for fraud due to the high volume of electronic transactions they process. They are targeted for malicious data processing with the goal of financial gain.

This fraud can include:

- Tampering with data
- Malicious code edits
- Interfering with audit mechanisms
- Unauthorized access to sensitive data

Threat actors for a business like BankservAfrica include employees (privileged users and developers), third-party support staff, organized crime syndicates, and disenfranchised employees.

To combat these threat actors, as well as to meet key compliance mandates such as PCI-DSS, BankservAfrica takes a "defense in-depth" stance. Their aim is to minimize the probability of a successful compromise and mitigate the impact of any incidents that do take place.

To accomplish this, they need deep and granular visibility into user activity across their infrastructure and across the billions of transactions they process each year.

> "ObserveIT gives us assurance that our environment is being monitored 24/7, with real-time alerts. It is our security guard, and it never sleeps."
>
> *~ Hamman Ferreira, Chief Technology Officer, BankservAfrica*

CASE STUDY SUMMARY

As an international financial transaction infrastructure processor, BankservAfrica needed to monitor for insider threats and develop a comprehensive security strategy to protect against threats, as well as meet key compliance mandates including PCI-DSS.

Their belief in "defense in-depth" led them to invest in ObserveIT, which provides visibility into user activity 24/7 across all systems.

Since adopting ObserveIT in 2011, BankservAfrica has benefited from:

- Zero insider-caused fraud incidents
- Money saved through fraud avoidance
- Time saved for the IT security team
- Increased visibility into user activity
- Powerful search capabilities across systems

How ObserveIT Helps

BankservAfrica adopted ObserveIT in 2011 to gain visibility into user activity in depth, both to protect transactions against fraud and to meet PCI-DSS compliance.

ObserveIT allows BankservAfrica to monitor 24/7 and report comprehensively on specific high-risk activities, especially those related to insider threats.

With ObserveIT, BankservAfrica can apply their "defense in depth" strategy and greatly decreased their insider threat risk, while ensuring that, if an incident does take place, they will have full visibility into what happened. As a result, they have been able to close security gaps and protect their valuable assets against fraud.

The Results

ObserveIT has empowered BankservAfrica to gain visibility into user activity across all of their infrastructure—from production servers to card data environments to backend servers.

With ObserveIT in place, the IT security team at BankservAfrica receives real-time alerts whenever suspicious user activity takes place, enabling them to quickly investigate and respond appropriately.

Since implementing ObserveIT is 2011, BankservAfrica has not experienced any insider threat incidents. With ObserveIT as a key part of their overall "defense in-depth" strategy, the company is able to monitor for file activity and other user behaviours that could indicate an insider threat in progress. The IT security team can rely on ObserveIT to offer visibility into user activity 24/7; they do not have to waste time reviewing logs when something goes awry. They are alerted only when there is an actual issue that requires further investigation, and when this takes place, they have the context they need readily at their fingertips.

In a few instances, BankservAfrica has received reports from others within their community that a fraudulent transaction has been attempted. With ObserveIT, BankservAfrica was able to identify the culprit of the attempted fraud and prove they were not at fault. This protects the business and ensures confidence in transaction data.

Detect Investigate Prevent

ObserveIT Enables

Visibility and reporting on **high-risk user activities**, such as:

- ✓ Connecting USB storage devices
- ✓ File copying and transfers
- ✓ Installation and uninstallation of applications

PCI DSS compliance requirements, such as:

- ✓ Monitoring of user activity
- ✓ Monitoring of privileged users
- ✓ Monitoring of third-party remote access