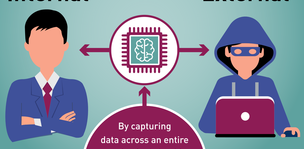
NetGuardians

Using dynamic profiling in the smart battle against fraud

There are two categories of threats:

Internal **External**



By capturing data across an entire organization's banking system and using machine learning, NetGuardians can constantly update its profiles.

Internal

By incorporating 360° profiling and using a holistic approach, the NetGuardians platform can monitor the bank's operations, looking for user behavior signals:

Unusual front-office / back-office user behavior

Unusual privileged IT admin activities

EXAMPLE When a user exits the building using their security card NetGuardians will pick up if his or her computer login or a printer ID is used in their absence and an alert will be raised.

When an alert is raised, the staff responsible will be notified and can investigate further.

External

External threats start in one of two ways:

Customer's device/ computer becomes infected with a virus or worms

Example: A bad actor can gain access to account details and passwords when a customer opens an illicit email and unwittingly infects the system.

A bad actor uses social engineering or mail / phone phishing on a customer to gain access to their account

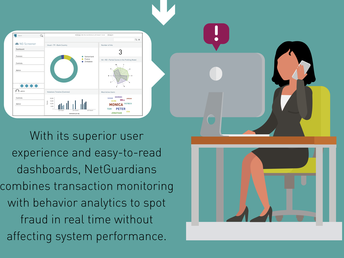
Example: A bad actor can use a customer's social media profile and find enough data to guess at passwords and impersonate the customer.

How it works

The NetGuardians platform uses real-time data capture to calculate a transaction risk score

Transaction score

If the transaction score is irregular a red flag is issued to the relationship manager to contact the customer to verify the transaction.



With its superior user experience and easy-to-read dashboards, NetGuardians combines transaction monitoring with behavior analytics to spot fraud in real time without affecting system performance.

Fraudsters are smart Banks need to be smarter

netguardians.ch
info@netguardians.ch

NetGuardians