WORLDLINE

Digital Security Suite

Secure your devices against frauds thanks to an AI-powered solution.

What are the market needs?

The rise of cyberattacks

Malwares

Any type of software designed to harm a computer system, disrupt its operation, steal information, gain control or cause other damage to data, devices or users.

Mobile Sim Swap

Fraud technique that involves transferring a victim's phone number from their original SIM card to a new SIM card controlled by an attacked.

Bad faith

A payer who refuse to admit that they have actually validated the transaction. The bank has 10 days to prove negligence or bad faith.

Authorized Push Payment

A payer is miled into authorizing a transfer of funds to a scammer or fraudster.

Phishing

A payer who refuse to admit that they have actually validated the transaction. The bank has 10 days to prove negligence or bad faith.

Social engineering (app scams, impersonation, etc)

Tactic of manipulating, influencing, or deceiving a victim in order to steal personal and financial information.

Account takeover

An anauthorized access and control of a user's account by an unanthorized individual or entry. This occurs when a malicious actor gains access to a personal's login credentials.

42%
of banks have seen an increase in deepfakes,

36%
for synthetic identity fraud,

34%
for account opening fraud.
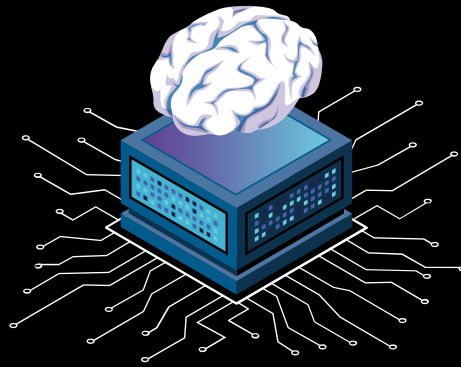
Source: Global fraud report

The use of Artificial Intelligence

Artificial Intelligence (AI)

> *Anything which enables the computers to behave like humans.*

Broader concept of machines being able to carry out tasks in a smarter way.

Machine Learning (ML)

Subset of AI

> *Deals with the extraction of patterns from a historical datasets.*

Includes unsupervised, semi or supervised learning; more effective with the rise of large good quality dataset.

22%

of european fraud prevention professionals believe GenAI used to create convincing synthetic identities is their biggest concern.

Almost a third of respondents plan to invest in newer AI fraud detection solutions like machine learning and predictive analytics.
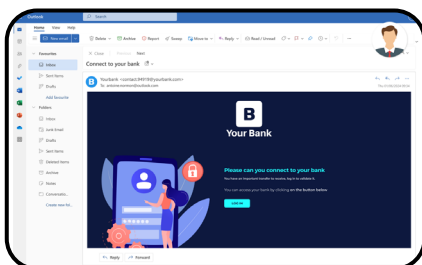
Source:
Global fraud report

How will our solution respond to concrete fraud use cases?

Phishing use case.
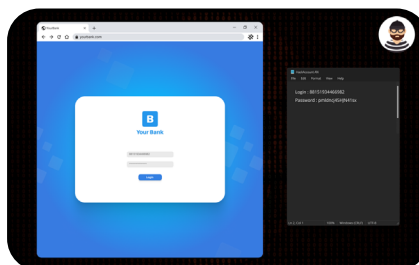
#1

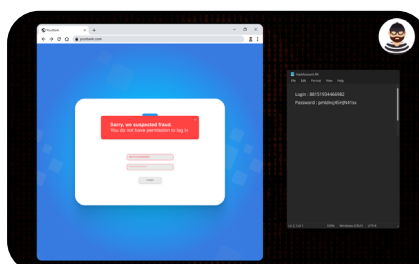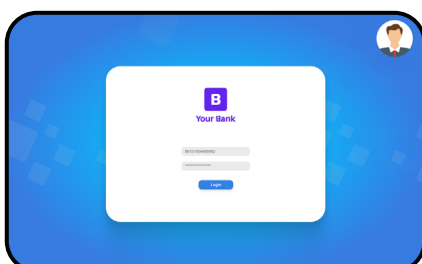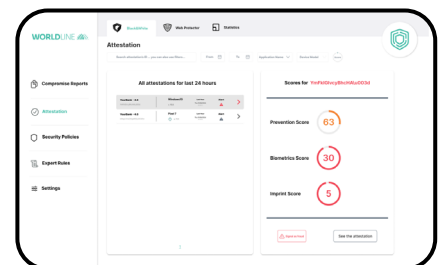The user receives a fake e-mail pretending to be his bank, he provides his credentials information.

#2

The fraudster uses the user's credentials to connect to bank. He will be blocked in his attempt to connect.

#3

Why was he blocked? Because the Digital Security Suite scores indicated a high risk in biometrics and fingerprint, prompting an appropriate response.

Using Worldline Digital Security Suite to prevent fraud use cases

Scoring engine to detect cyberattacks

AI in action

Prevention Score

Behavioral Score

Worldline Digital Security Suite

Imprint Score

Guaranteed fraud detection

Prevention Score

As a first line of defence, an initial check that prevent potentiel threats from progressing further.
This score detects whether the device is subject to potentiel alteration or malware.

Imprint Score

Functioning like a digital detective, observes and records the unique characteristics of the device used and browsing habits. It determines whether we recognise the device of the user.

Behavioral Score

It monitors how the user interacts with the device (orientation, movement, keystrokes...).
It determines whether we recognize the behaviour of the user.

Worldline Digital Security Suite

The digital threat landscape is constantly evolving with fraudsters employing ever more sophisticated forms of fraud to target businesses and their users. To effectively combat these threats and provide robust protection for your activities, Worldline Digital Suite harnesses the power of artificial intelligence, offering a defense against digital security threats.

Local Protection (Security SDK)

Our solution provides more than 100 probes & detectors for Android, iOS and browser in order to be able to detect locally attacks and attest eligibility of the device (anti-tempering, anti-hooking, anti-debugging, jailbreak / root detection, etc.). Furthermore, with the local policy, you can define the right level of security for each detectors, and to block the usage of the application in case of attacks.

+30%

improved fraud detection using AI scores

Collect device information

Data managed in the smartphone needs to be secured in different use case: the storage of data with our safe, the entry of the data with our DVK in order to protect against keyloggers, and the data displayed.

Our solution collects data from device (IDS reports), it collects user behavioral data and collect data from external sources (SIM swapping, etc.) to secure devices.

+100

number of detectors on our devices

Intelligence & Scoring (Security Platform)

Our scoring engine will calculate 3 different scores (imprint, prevention & biometrics) to assess the risk of each operations on device. Furthemore, thanks to our remote policy, customers will have the autonomy to customize the security policy remotely and in real time. It will improve the reactivity for a change, espacially in case of security breach which requires reactivity.

PAYTECH AWARDS
2024
Digital Security Suite
AI Tech of the Future
WINNER

Benefits of our solution

Improved fraud detection

Digital Security Suite allows a seamless integration across multiple devices and operations systems. Furthermore, it provides an adaptable and flexible response to fraud thanks to our AI machine learning and our 3 scores that assess risks of each operation on your devices. It improves by 30% the fraud detection.

Secure different use cases

Our solution is based on device intelligence and not dependent of card or specific use cases. Thanks to our solution, we are capable to detect different types of fraud for several use cases such as payment, enrolment, digitalization, and so on.

Innovation within security solution

By combining AI and machine learning with a security solution, we offer a comprehensive solution capable of addressing new challenges in cyberattacks. Our solution won the AI Tech of the Future in 2024 thanks to our scoring fraud prevention feature.

Who can benefit from Digital Security Suite?

Banks | **Public Sector** | **Healthcare** | **Transport** | **Merchants**

Mobile Payment

Mobile payment (HCE, HPE, ...) certifications require an attestation of the device in order to check the eligibility or sanity of the device.

Digitalisation of sensitive use cases

The digitalisation of sensitive use cases (such as identity card, transportation subscription, health cards,...) require security control to check that the device is not altered nor dupiblicated.

Banking fraud prevention

In-app protection / PIN protection thanks to Digital Security Suite.

- Authentication: PSD2 require to have malware detection and possession factor to control no possible detections.
- 3DS/CIAAM: risk of the transction includes the evaluation of the risk of the device.
- Identity Fraud Prevention.

We are able to provide a package
to meet your needs with...

Access Control Server

3DS Issuer

Our solution is a PCI-DSS & PCI-3DS solution that enables Issuing banks to manage 3-D Secure process and to authenticate their cardholder during online payments.

Trusted Authentication

SCA/Authentication

A Strong Customer Authentication solution available on all devices to provide a seamless and secure authentication for your users.

Fraud Management

Security

By using deep learning AI, Worldline Fraud Management provides complete prevention against fraud attempts in account payments, instant payments, card payments and token-based payments - a true holistic service offreing.

About Worldline

Worldline [Euronext: WLN] helps businesses of all shapes and sizes to accelerate their growth journey – quickly, simply, and securely. With advanced payments technology, local expertise and solutions customised for hundreds of markets and industries, Worldline powers the growth of over one million businesses around the world. Worldline generated a 4.6 billion euros revenue in 2023. **worldline.com**

More information