C-Prot Fraud Prevention

Prevent fraud and provide a seamless digital experience for your customers.

Top Features

Anti-Fraud and Security
It can detect and prevent fraud attempts using fingerprint data from users' devices.

Remote Connection Detection
It is determined whether the device is used by remote desktop applications or by the user himself.

Behaviour Analysis
It uses a system behaviour analysis that analyses user behaviour and analyses it to identify abnormal or potentially fraudulent activities.

Root/JailBreak Detection
It provides an additional layer of defence against fraudsters by detecting operating system changes made to the user's device.

Sectors Used

Finance:
Enhances financial security during online banking, detectsphishing attempts and prevents malware.

E-Commerce:
Blocks fraudulent websites, secures customer payments, and protects against phishing attempts.

Insurance:
Prevents fraud, detects fraudulent claims and protects customer data.

Healthcare:
Secures health records, detects phishing attempts and protects against prescription fraud.

Transportation:
Protects travel bookings, secures customer card informationand prevents phishing attempts.

Telecommunications:
Detects phishing attempts, prevents account fraud, and secures subscriber information.

FRAUD PREVENTION

C-Prot Fraud Prevention is a comprehensive solution that helps organisations detect and prevent fraud attempts such as financial fraud, phishing and money laundering through mobile and web channels. Depending on the needs, various integration methods such as cloud or on-prem are also offered.

Highlights

★ ★ ★ ★ ★

Behavioural Biometrics

It offers a technology that analyses customers' interaction with their devices such as mouse movements, clicks, taps, scrolling speed and more to determine whether a device is being used by a legitimate user. It evaluates the user's real-time interactions and creates a unique user profile.

SMIPhising

It detects if there is information on the phone for SMS fraud.

Sim Card Change Detection

It determines whether the user has a sim card in the device and whether the sim card has been changed.

Fast Travel Detection

The panel detects whether a position change has been made within the specified time.

Device ID Spoofing Detection

Application information may change on rooted devices. This information is determined whether it is changed or original.

Bot Detection

It determines whether a bot like Selenium or a real human is using the browser.

User Agent Spoofing Detection

The information of the browser used by the user may change. The information of the browser is detected whether it is original information or fake information.

VPN / Proxy Detection

It is determined that the user is connected via VPN.

Tor Browser Detection

It is determined whether the user is using Tor Browser or not.

Country, City, Time Zone Change Detection

It detects when users appear in a different location than the country, city and time zone specified in their previous entries.

Multiple Account Detection on the Device

When detecting a registered phone logging into the user's device, it also detects people using guest mode.

C-Prot will continue to keep you safe in the digital world with a wide range of high-tech cybersecurity products, from smart televisions to mobile devices, while maintaining its commitment to providing it's customers with the best endpoint protection products.

C-Prot
cprotglobal
cprotglobal
cprot
Known more at **https://www.c-prot.com**