C-Prot Device Fingerprint

Identify your web and mobile visitors with the most accurate device identification platform.

Top Features

Unique Digital Fingerprint
It generates a unique digital fingerprint identifier for users by analyzing browser and device features with special algorithms.

Easy Integration for Developers
Easily add C-Prot DFP SDK to your applications get started quickly by integrating.

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.

Fast Travel Detection
It detects whether the location change has been made within the period specified in the manage-ment panel.

Sectors Used

Finance:
Banks and financial institutions can improve account security by recognising users' devices. They can also use it to strengthen fraud detection and authentication processes.

Advertising:
Used for target audience identification and segmentation. It is used to show the right adverts to the right users. Prevents advert fraud.

Healthcare:
Provides security and access control for healthcare services. Strengthens authentication and authorisation processes. Protects the confidentiality of medical data.

Cryptocurrency:
With a state-of-the-art scanner fingerprint API with close to 100% accuracy, you can detect and block crypto fraudsters who want to steal account data and transfer money to their own wallets.

E-Commerce:
Distinctly recognise potential fraudsters visiting your trading platform by detecting them with an exceptional accuracy rate of close to 100%.

Online Gaming:
Allows you to fight against common gaming and gambling fraud techniques, including automatic credential stuffing, fraudulent strategies and various other illegal activities.

DEVICE FINGERPRINT

C-Prot Device Fingerprint is a solution developed to securely identify users and analyze web traffic on websites. This solution aims to provide high-level security and improve user experience by uniquely identifying users.

Highlights

★ ★ ★ ★ ★

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

Remote Connection Detection
C-Prot Device Fingerprint detects users who access via remote desktop connection programmes such as AnyDesk, TeamViewer.

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

Incognito Tab Usage Detection
Detects users who access websites in private browsing mode.

Central Management Console
Available as cloud-based or On-prem Manage all your endpoints with C-Prot Remote Administrator it allows you to manage from anywhere.

Automation Usage Detection
It detects the requests made by web automation tools targeting Internet addresses.

Malicious User Detection
Incompatible time zones, use of incognito mode and malicious users with features such as proxy and pinpoints it precisely.

Multiple Account Detection on Device
It detects multiple logged in users on the same browser.

VPN and Proxy Usage Detection
It analyses the user's IP address to determine whether this address belongs to a VPN or proxy server.