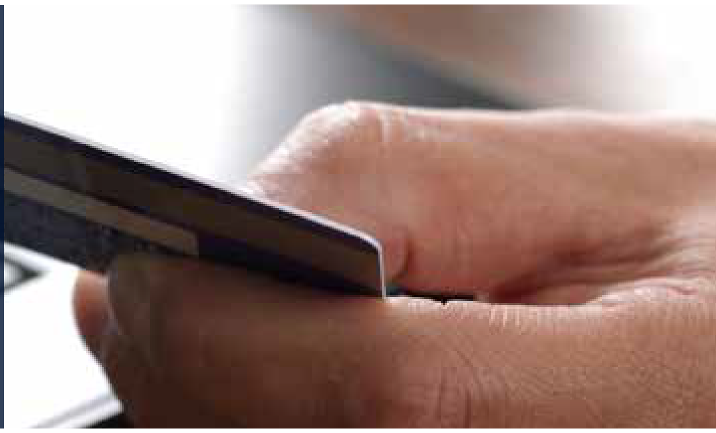
Total Fraud Protection®

Stop Mobile Fraud

Eliminate Malicious Apps & Phishing Scams Before They Pose a Threat to Mobile Devices



Sophisticated cybercriminals are increasingly targeting mobile devices in their fraud attacks. Smartphones or tablets infected with malware can create a nightmare situation for an unsuspecting user – who could be at risk of having their credit card details compromised or bank login information stolen.Cyxtera provides a full range of protection measures to defend against mobile malware, by preventing fraudulent connections to your customers' mobile devices, boosting the security of your company's native mobile app and removing phishing attacks at industry-leading speeds.

Highlights:

> Scanning of all major app stores and a vast number of third-party marketplaces for malicious apps

> Real-time threat analysis and analytics reporting

> End-user push and OTP authentication for added security

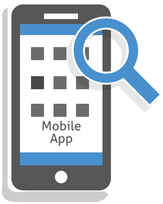
> Mobile SDK integration to secure your native mobile banking app

> An industry-leading phishing takedown time of 3.6 hours per attack

> Reduce the malicious app lifecycle and threat window

Total Fraud **Protection**®

Stop Mobile Fraud Features



Stop Rogue App Brand Impersonation

Our agents scan the Google Play Store, iTunes App Store, the Windows App store and Blackberry App World, as well as a wide range of third-party app marketplaces. When they find a potential rogue app impersonating a trusted brand name, they perform tests to confirm whether the app is legitimate, and if it isn't, our agents take all steps necessary to remove it from the internet.

Safeguard End-User Mobile Devices

The Detect Safe Browsing solution protects an end user's mobile device with regular scans, stopping the fraudulent connections made by malware so that browsing only takes place on authorized websites. It can also detect and defend against malware-infected files on Android platforms, identify jail-broken iOS phones and blacklist websites that host phishing scams.

Give Your Company's Mobile App a Security Boost

Obligating end users to download and install a separate security application can lead to low adoption, a less convenient mobile banking experience and a larger quantity of unprotected devices that are vulnerable to attacks. With the Detect Safe Browsing and DetectID Mobile SDKs, secure browsing and push authentication technology can be seamlessly integrated into any native mobile application.

Unique Device Hardware Identification

Cyxtera provides hardware-based identification to uniquely identify all smartphones and tablets accessing your banking or online purchase platform. The solution records the individual characteristics of a mobile device's physical components to prevent a fraud event. Also, the Detect ID solution prompts an end user to confirm risky transactions with a simple 'push' or One-Time Password (OTP) security feature.

Comprehensive Brand Threat Intelligence

You have spent a lot of time and energy building a reputation for reliability and security, all of which can be undone by a few attacks spread on social media. Keep track of brand mentions on thousands of social media sites, blogs, app stores and domain registrations, and turn the data into actionable intelligence that can be used to stop imminent fraud attacks.

Lower the Risk of Unsafe End-User Mobile Practices

There are hundreds of unsupervised third-party application stores where fraudulent apps are offered free of charge or sold. Detect Monitoring Service mitigates the risk of a user reducing device security settings by finding and removing malware before it can take advantage of a smartphone's or tablet's vulnerable state.