ThreatCast
GUARDSQUARE

Make informed mobile app security decisions with real-time threat intelligence

After an Android or iOS app is released, security teams and developers often lack visibility into the most common attack vectors and vulnerable parts of their code...until it's too late.

Without this visibility, malicious actors can have free reign to set up attacks that could expose sensitive customer data, steal code and other intellectual property, cause financial or reputational damage, and more.

ThreatCast, Guardsquare's real-time threat monitoring mobile app security console, solves this visibility challenge. With ThreatCast, organizations can detect and analyze threat events happening across iOS and Android apps protected by **iXGuard** and **DexGuard** as they occur. ThreatCast gives teams continuous insight into their apps' security once the app is published and downloaded—areas which have historically been black boxes for organizations.

Protect mobile apps with real-time threat monitoring

Get actionable insights

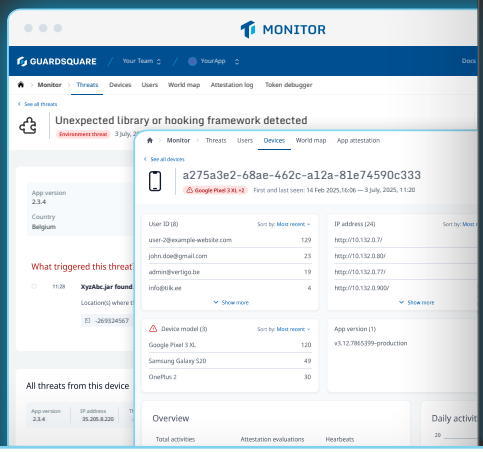
Analyze threat data to respond immediately to attacks or block suspicious users.

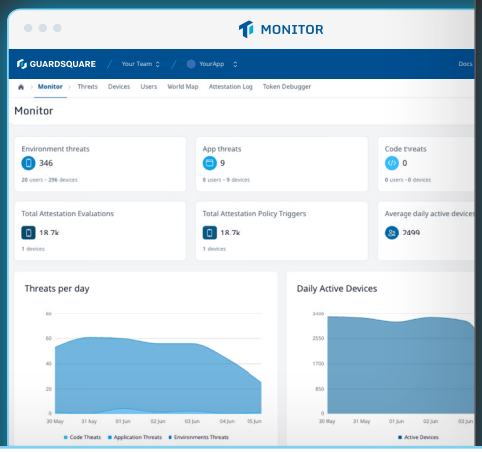
Detect threats in real time

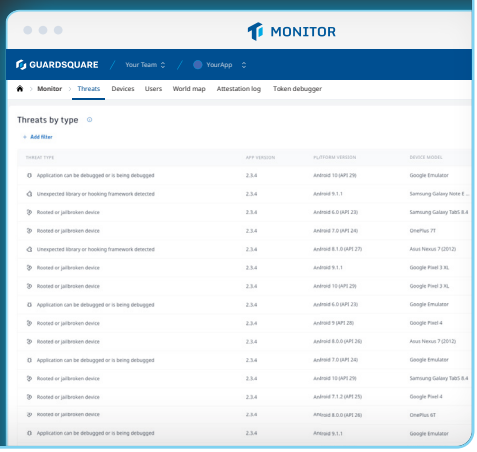
Use easy-to-navigate dashboards and custom alerts to detect threat events as they happen.

Integrate security into the development lifecycle

Prioritize mobile security within the development process, without sacrificing speed-to-market.







Analyze environment, application, and code threats with ThreatCast

Environment threats

These general security threats don't directly target mobile applications, but are often the basis for targeted attacks. For example, your DexGuard or iXGuard protected application detects that it is being run in a potentially harmful environment—such as a rooted or jailbroken device.

Code threats

These occur when someone attempts to statically or dynamically alter the internal logic of apps and modify their intended behavior. Code threats are the most explicit indicators that malicious users are targeting specific mobile apps.

Application threats

These are related to the integrity of the application, and indicate that there was an attempt to tamper with the application and possibly modify its behavior. If this happens, DexGuard and iXGuard RASP functionality is automatically triggered to respond to the detected threat.

Leverage ThreatCast data to strengthen your app security

Defend against primary attack vectors

DexGuard and iXGuard help you implement security best practices, while ThreatCast allows you to fine-tune your exact security protocols based on real threats.

Adjust release frequency to strengthen code protection

DexGuard and iXGuard's applied code protection is different in every build, so attackers must start from the beginning with each new release. ThreatCast shows you the average time it takes to compromise a new app version, so you can adjust release frequency.

Optimize response to runtime analysis & live attacks

Decide - based on objective data - whether an application should terminate, limit the available functionality, or display a notification when a particular subcategory of threats is detected.

Guardsquare offers the most complete approach to mobile application security on the market, delivering the highest level of protection, with ease. Guardsquare's software integrates seamlessly across the development cycle, from app security testing to code hardening to real-time visibility into the threat landscape. Guardsquare products provide enhanced mobile application security from early in the development process through publication.

More than 900 customers worldwide across all major industries rely on Guardsquare to help them identify security risks and protect their mobile applications and SDKs against reverse engineering and tampering in the ever-evolving threat landscape.

GUARDSQUARE
Mobile application protection

www.guardsquare.com