YOUR APP IS YOUR BUSINESS

Four reasons to embed application security

Mobile apps enhance the customer experience and differentiate your business. However, trojanized apps, compromised devices and screen overlays pose serious risks to the personally identifiable information (PII) customers entrust to your apps.

You can’t protect against the unseen
Without knowing the severity and classifications of threats your customers are faced with, it’s impossible to build a secure experience.

Brand reputation is on the line
Mobile apps threats evolve quickly and can be broadly distributed with ease. One version of a trojanized banking app can lead to millions of breached accounts.

Threats are increasing
In 2019, there were more than 7,500 samples of the banking trojan BancaMarStealer. By the end of 2020, that number grew to more than 70,000, with over 30 new samples every day.

Existing tools aren’t enough for mobile
Traditional app shielding strategies, such as relying on open-source or signature-based tools, can’t keep up with today’s advanced malware. A modern approach purpose-built for mobile will protect your customers from mobile fraud and zero-day attacks.

What should embedded security achieve?
Modern embedded security should detect all types of mobile risks without impacting app performance or customer experience. Embedding security in apps protects customers from unseen malware and network attacks while safeguarding your brand reputation.

Looking for an embedded app security solution?
Visit lookout.com to learn more.