Lookout + buguroo Partnership Brief

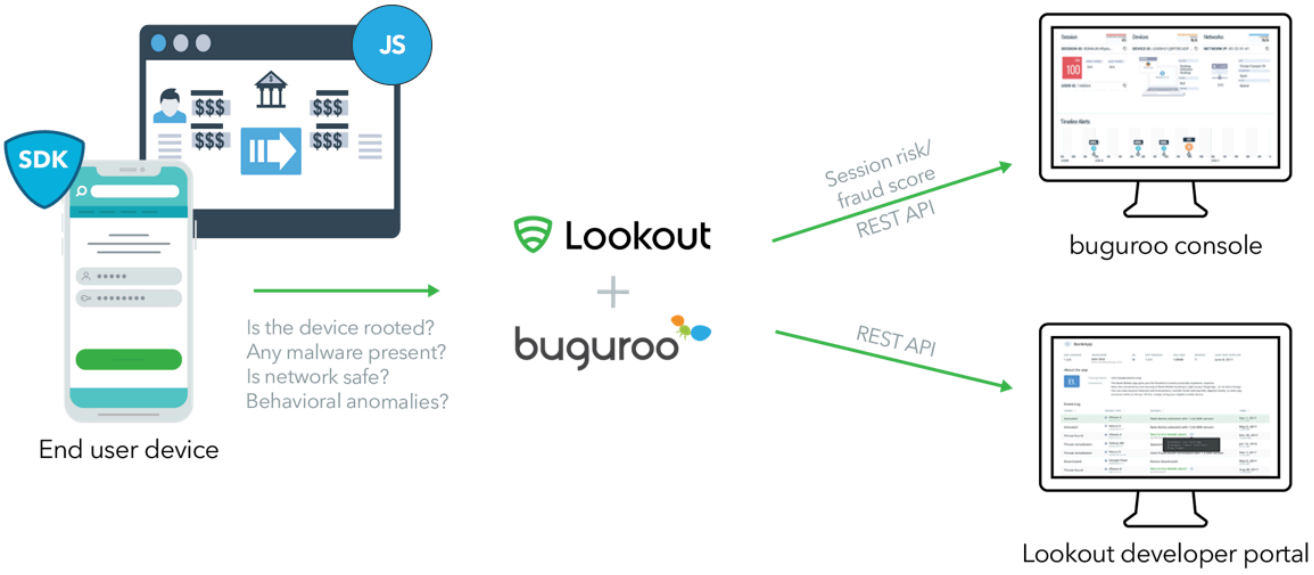
Combatting data compromise and fraud on web and mobile platforms

Web and mobile apps – the new hacker battleground

Web and mobile apps have become a key part of everyday life to manage everything from booking travel to handling finances. Service providers and financial companies increasingly rely on these mobile apps to deliver innovative consumer experiences and increase brand engagement. However, the rise in adoption of web and mobile channels is creating a corresponding rise in cyber threats in the client side, which is a shift from more traditional server-side attacks. Malicious attackers are now primarily targeting mobile users to steal login credentials and customer data for financial gain or committing fraud through both the mobile and web channels.

Most enterprises and banks have some fraud detection in place but lack a holistic solution. Lookout and buguroo work side-by-side to protect against fraud on both mobile and web platforms, which ensures full coverage by securing the consumer-facing enterprise mobile app as well as the customer website. Enterprises oftentimes overlook mobile because they assume it's more secure than web by nature, when in fact credentials and data can be compromised on mobile just as easily as other channels. Once malicious actors have that information, they can use it across both web and mobile to initiate an account takeover and other fraudulent activity.

Scalable solution built to detect threats and drive actionable insights



Lookout app defense SDK

The Lookout App Defense solution allows developers to protect mobile apps using an embeddable lightweight SDK for both Android and iOS. Once the SDK is integrated into the app, it connects to the Lookout Security Cloud, which enables threat detection fed by data from over 170 million devices and 70 million analyzed mobile apps.

Organizations and developers can access security telemetry generated by Lookout App Defense to mitigate risks their app faces based on the severity and type of threat. The SDK has existing integrations with security tools such as SIEM and risk rating models via the Lookout Event Feed API, which provides a feed of raw security event telemetry. Overall, the SDK can help you reduce the risk of fraud and data compromise, comply with standards such as GDPR and PSD2, and actively protect customers and enterprises by identifying potential threats present on the user device running the mobile app.

buguroo bugFraud

buguroo bugFraud collects dynamic data around user behavior and sensors in the environment to differentiate between legitimate user sessions and fraudulent ones. Thanks to proprietary deep learning algorithms powered by artificial intelligence neural networks, bugFraud can detect and predict cybercriminal activity – even during the online service enrollment phase. By analyzing information on the different events surrounding each user transaction made through any device or channel, bugFraud can identify the user as legitimate or fraudulent, understand whether an intruder is tampering with data being accessed by the user in their session, and predict whether the cybercriminal is trying to commit fraud during the enrollment phase.

Contact the Teams

Lookout

San Francisco · Boston · Amsterdam · London · Singapore · Sydney

www.lookout.com/products/app-defense

appdefensesales@lookout.com

buguroo

Madrid · London · Ciudad de México · Bogotá · Miami · Sao Paulo

www.buguroo.com

info@buguroo.com