Visibility and control of private messaging apps

Lookout helps financial firms securely implement BYOD

Sharing of corporate data via private messaging apps is a major risk

The broad adoption of BYOD strategies increases the risk of data leakage for financial services organizations, increasing compliance violations. Since personal mobile devices are used to manage both work and personal life, they contain apps that are not necessarily approved by the enterprise and present risk of misuse. Among these private applications, are popular messaging apps such as WhatsApp, Signal, iMessage, Facebook Messenger, WeChat, and Telegram, which employees at financial institutions have misused by sending messaging containing sensitive regulated information.

BYOD puts pressure on data security and end user privacy

Record keeping provisions of the Securities Exchange Act of 1934 require that financial firms promptly produce records upon request and detect and prevent violations. However, gaining visibility and control over an unmanaged personal mobile device while respecting user privacy is more challenging. A successful BYOD strategy strikes the balance between data protection and user privacy by deploying a mobile threat defense solution that can detect threats, enforce acceptable use policies, log end user activity, and provide visibility into installed apps. Lookout Mobile Endpoint Security enables financial firms to achieve these goals while balancing security and end user privacy.

Challenges

1. Users are sharing sensitive corporate data using personal messaging apps
2. Visibility and control over personal mobile devices are limited
3. Regulations require firms to promptly produce communication records

Lookout Critical Capability

With deep app intelligence, Lookout can set policies based on risky app configurations, capabilities, and vulnerabilities to mitigate app risk and meet compliance requirements. Lookout can also set policies for specific apps, such as messaging apps, and domains to either block or allow access while also providing a risk warning to the end user. By logging all user activity, including message deletions, Lookout enables organizations to produce mobile records in response to strict record keeping requirements. Lookout secure BYOD for financial services firms on both iOS and Android devices, protecting devices in a consistent way independent of the mobile platform.

Why Lookout

Lookout Mobile Endpoint Security with Continuous Conditional Access ensures security and compliance on every device, leveraging a large data set fed by over 200 million devices and the analysis of over 175 million mobile apps. With the Lookout Security Platform, it’s easy to deploy Lookout and apply security policies across the entire organization for both managed and unmanaged devices. Users receive alerts and remediation steps on malicious apps, network connections, and system anomalies in real time; accompanied by dynamic device health checks to provide Continuous Conditional Access to sensitive corporate applications and data.