Lookout for Financial Services in the EU

European Financial institutions secure mobile users as data moves to the cloud with Office 365

Industry-Wide Security Challenges

European financial institutions are increasingly adopting cloud services as they move sensitive corporate data into Microsoft Office 365. With Office 365 employees connect to corporate resources anytime from their personal devices. This flexibility provides cost and efficiency benefits but also introduces greater exposure to mobile threats such as phishing, malicious apps, and OS vulnerabilities. Progressive firms, however, recognize the benefits of empowering a secure, mobile workforce, and are leveraging the integration of Lookout with Microsoft Office 365 to protect sensitive corporate data from cybersecurity threats.

Industry Challenges

1. Significant adoption of mobile
2. Stringent privacy regulations
3. Prime target of cyber attacks

Real World Use Case for Financial Services

As of November 2018, all EU member states were to have incorporated standards set by the European Commission NIS Directive, which is the first EU-wide cybersecurity legislation. The goal of the legislation is to establish a common high level of network and information security. By implementing cybersecurity standards, financial firms across different EU-member states can confidently transact knowing that safeguards are in place to protect their sensitive data. As transactions increasingly occur on mobile devices, EU Financial Institutions must safeguard their data from sophisticated cyber threats whilst adhering to strict GDPR data privacy law. In particular, robust protection against mobile phishing attacks is imperative as these threats are very effective and increasingly target mobile devices.

Lookout Critical Capability

Lookout Phishing and Content Protection inspects any URL requests from email (corporate or personal), SMS texts, messaging apps, and those embedded in app browsers, dynamically blocking requests for websites identified by Lookout as malicious. For example, with this feature enabled, Lookout would prevent a phished employee from potentially entering login credentials to a malicious replica of an Office 365 login page. Additionally, to ensure user privacy, Lookout only reports the existence of an issue and the number of detections to the Mobile Endpoint Security Console. Administrators cannot view browsing history or traffic.

Why Lookout?

Lookout Mobile Endpoint Security ensures continuous security and compliance on every mobile device, leveraging a large data set fed by over 170 million devices, and the analysis of over 70 million mobile apps. With the Lookout Security Cloud, it's easy to deploy Lookout and apply security policies across the entire organization for both managed and unmanaged devices. Users receive alerts on malicious apps, network connections, and system anomalies at the OS level in real time; accompanied by simple on-device remediation capabilities. For European Financial organizations, Lookout simultaneously delivers the security and visibility necessary to ensure compliance and gain visibility into every aspect of the mobile risk landscape without sacrificing personal privacy.