How Lookout Protects Pharmaceutical Companies

Lookout provides protection against the full spectrum of mobile threats

Industry-Wide Security Challenges

In the post-perimeter world, pharmaceutical professionals rely on mobile devices and apps to access proprietary data behind new medicines. This includes lab work, trial results, and personal information about patients. As mobile phishing becomes more common, the risk spectrum goes beyond securing the devices and apps to include employees being targeted by false login portals and other tactics used to steal credentials.

At the risk of damaged brand reputation or hefty lawsuits and compliance violations, pharmaceutical organizations must implement mobile security that ensures risks are being identified and mitigated on an ongoing basis.

Industry Challenges

1. Significant adoption of mobile devices to increase efficiency
2. Protecting sensitive trial patient PII and R&D data
3. Increased mobile risk due to prevalence of targeted phishing campaigns

Real World Use Case for Pharmaceuticals

When it comes to research and development for pharmaceutical companies, time is of the essence in order to stay ahead of the competition and deliver new drugs. Shifting to the cloud and leveraging mobile devices more heavily provides a powerful collaborative environment to decrease time to market, which means security and compliance teams need to ensure that any mobile device accessing internal data complies with standards such as HIPAA and GDPR.

Protection policies should cover a broad spectrum. Phishing attacks are becoming more common and are more difficult to spot on mobile devices where red flags like suspicious URLs are hidden or shortened. A successful phishing attack on just one employee can result in the company's entire data corpus being exposed and cause massive compliance violations.

Making sure the device OS, apps on the device, and network are secure covers the other end of the mobile risk spectrum. Something as simple as ensuring that no apps on these devices can access trial patient data in the address book, as a major healthcare provider did, can protect a vulnerable source of data leakage.

Lookout Critical Capability

Lookout Mobile Endpoint Security with Phishing and Content Protection protects users and organizations from web, application, device, and network threats. Lookout Phishing & Content Protection inspects and blocks any malicious URL requests across all apps including corporate and personal email, SMS, messaging apps, and apps containing URLs attempting to download malicious plug-ins. Lookout offers customizable policies that block devices from accessing cloud data when threats are detected to protect sensitive pharmaceutical data and align with regulatory policies.

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 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 and remediation steps on malicious apps, network connections, and system anomalies in real time; accompanied by dynamic device health checks to provide conditional access to sensitive corporate applications and data.