How Lookout Protects Law Firm Client Cloud Data

Lookout ensures mobile devices are secure before accessing sensitive resources

Industry-Wide Security Challenges

Law firms are highly dependent on mobile devices, allowing attorneys to be responsive to client needs. This means a large amount of information they are required to keep private and confidential is accessed outside the four walls of a firm, and outside the reach of traditional security tools. The need to work at any time and from anywhere means devices are used for personal and work life, which often results in a conflict between security and privacy for attorneys. A mix of personal and corporate-owned devices also poses a significant challenge for law firms, particularly as more customer data is stored in cloud-based services.

Industry Challenges

1. Significant adoption of mobile devices for all firm employees
2. Protecting sensitive client PII and case documentation
3. Wider use of cloud-based case management apps being accessed from mobile devices

Real World Use Case for Law Firms

While on the road working with clients, attorneys not only have to access sensitive data in cloud platforms such as Microsoft O365 and Google G Suite, but they also collaborate on legal documents with services like TrialWorks, Clio, PracticePanther, and others to support cases and clients. Attorneys are inevitably accessing this data from mobile devices, where IT has very limited visibility into the health of the apps, devices, and networks compared to traditional laptops. With sensitive client data being accessed from a mobile device, malicious actors are targeting users with mobile malware that steals login credentials allowing hackers to pose as a legitimate user and steal sensitive legal and financial documentation. IT and security teams must be able to ensure the devices that attorneys rely on are healthy and secure before accessing valuable client data in the cloud.

Lookout Critical Capability

Leaked or exposed sensitive data is one of the top mobile-related security incidents organizations have experienced in the last year according to IDC[1]. By leveraging Lookout Continuous Conditional Access, which dynamically monitors the health of the endpoint anytime a user is connected to corporate resources, you can continuously protect your valuable corporate data from being leaked or exposed on mobile devices.

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.

[1] IDC Enterprise Mobility Decision Maker Survey 2018, Nov 2018: https://www.idc.com/getdoc.jsp?containerId=US44434018