Lookout for Government Field Agents

Securing mobility for federal, state and local government

Government Security Challenges

Federal, state, and local government field agents rely on mobile devices to access work resources such as email, case files, and other applications. Often traveling to various geographies, field agents can be exposed to app-based, network-based, and device-based threats. These threats seek to exploit mobile devices as they operate outside the traditional security perimeter, often targeting high stake users like field agents in particular. Back-end systems accessed remotely by these agents contain sensitive government data and personally identifiable information (PII), which could be used to compromise the financial well-being, privacy, and identity of US citizens.

Agency Challenges

1. Lack of visibility into health of the mobile fleet
2. Stringent privacy regulations
3. Prime target of advanced cyber attacks

Real World Use Case for Government Agencies

As of May 2017, by Executive Order, government agencies have been required to apply the Risk-Management Framework to federal information systems. Established by the Federal Information Security Act (FISMA), the Framework requires that agencies maintain secure mobility standards specified in NIST Special Publication 800-53. This publication states that 'malicious code protection mechanisms' must be in place at 'entry and exit' points and that integrity verification tools also exist to detect unauthorized changes to software and firmware. To fulfill these obligations, its imperative that government agencies not only protect their mobile fleets from phishing, malware, and other mobile threats but also continuously monitor mobile device health to persistently safeguard government data.

Lookout Critical Capability

Lookout Mobile Endpoint Security provides comprehensive and continuous assessment of risk across iOS and Android devices to secure against phishing, malicious apps, OS vulnerabilities, and man-in-the-middle attacks. By continuously monitoring the health of mobile devices and assigning risk-levels, Lookout protects government data by permitting access to only healthy, low-risk devices. Additionally, with Lookout Phishing & Content Protection, field agents have bullet-proof protection against mobile phishing attacks. With these capabilities, Lookout helps agencies meet the security obligations of FISMA.

Why Lookout?

Lookout Mobile Endpoint Security ensures continuous 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 and phishing protection 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 US government agencies, Lookout simultaneously delivers the security and visibility necessary to ensure compliance and gain visibility into every aspect of the mobile risk landscape. Read how Lookout stopped a phishing site targeting the DNC.