Lookout + AT&T FirstNet for Emergency Responders

Healthcare organizations gain mobile security supported by enhanced network speed and reliability within budget

Security Challenges for First Responders

Emergency responders rely on secure access to accurate patient medical records for critical life-saving information. By tampering with medical records and information systems, cybercriminals can have devastating effects on people in need of emergency care. Security teams must adapt their cybersecurity strategy to increase visibility into mobile devices and apps to protect sensitive data. Phishing, app, network, and device-based mobile threats are prevalent, so healthcare organizations must combat these threats while also strengthening their HIPAA compliance posture.

Real-world Use Case for Emergency Responders

In March 2017, First Responder Network Authority (FirstNet) announced a public-private partnership with AT&T to create a single, nation-wide, interoperable network for public safety. The FirstNet broadband network and ecosystem of vetted devices and apps enables reliable, and seamless communications across the spectrum of emergency responders. To enhance the value for healthcare organizations, Lookout provides promotional pricing for FirstNet customers. These promotional offers address budget constraints by combining Lookout with FirstNet rate plans at an even lower price than the standard commercial AT&T plan.[1]

Emergency Responder Challenges

1. Stringent privacy regulations and frameworks
2. Access to patient data via mobile devices during emergency
3. Cyberattacks targeting emergency situations

Lookout Critical Capability

Lookout Mobile Endpoint Security enables healthcare organizations to create over 55 types of custom app security policies to block the use of apps that request access to data such as the address book and location. With Lookout Phishing and Content Protection, emergency responders can confidently use email, SMS, messaging apps, and other applications, knowing they are protected. Lookout helps fulfill the HIPAA requirement to protect patient data accessed by mobile devices and apps from malicious software.

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 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 emergency responders, Lookout ensures secure mobile access to potentially life-saving information.

[1] Promotional pricing offers are subject to change.