Secure Mobility for Remote Public Sector Workers

Lookout helps public sector organizations scale mobile security as employees go remote

When everyone works remotely

Most public sector organizations rely on employees based in offices to conduct business operations. When the need arises to work remotely, organizations are faced with logistical, technological, and cultural challenges. Not only must public entities ensure employees have sufficient connectivity and reliable devices for work, they must provide security that extends beyond the organization's perimeter. With employees connecting from home networks and other remote locations, traditional perimeter-based security is no longer as relevant. Public sector organizations must move critical perimeter security services to the endpoint, and access to data must be based on a continuous assessment of trust, starting from an assumption of zero trust.

Real world use case

With public sector workers at home, or in remote locations, the one constant for them all is the increased use of their mobile device to continue performing their job. In times of crisis the US CDC recommends organizations explore flexible work options including telecommuting, and at the same time the CDC recommends organizations "have the information technology and infrastructure needed to support multiple employees who may be able to work from home." As organizations scramble to rollout sufficient remote working capabilities, cybercriminals seek opportunities to exploit system and operational vulnerabilities by launching advanced phishing and network attacks.

Challenges

1. Remote public sector workers rely on connecting to home Wi-Fi and cellular networks
2. Public sector organizations may have a cybersecurity vulnerability window while new remote workers come up to speed
3. Sensitive data is increasingly being accessed from mobile devices outside the reach of traditional security tools

Lookout Critical Capability

Lookout Phishing and Content Protection inspects any URL requests, across corporate and personal email, SMS, messaging apps, and apps containing URLs that download malicious plug-ins. Lookout dynamically blocks all URL requests identified by Lookout as malicious or phishing. Additionally, Lookout detects network-based attacks that attempt to steal personal or sensitive company data over Wi-Fi or cellular networks. End users are notified when a network being used is dangerous while Lookout blocks access to corporate resources.

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 180 million devices and the analysis of over 100 million mobile apps. With the Lookout Security Platform, 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 Continuous Conditional Access to sensitive corporate applications and data.