How Lookout Protects Executives

Lookout provides mobile protection for company executives and leaders

Widespread Security Concerns

Executives are constantly on the road, which means that an organization's most sensitive data, financial performance, product pricing, and corporate development plans are regularly being accessed from smartphones and tablets. More importantly, this data is frequently being accessed outside the four walls of the company and beyond the reach of traditional security tools. This means that traditional security tools for phishing and malware aren't securing your executives for a large part of their workday.

Challenges

1. Constant travel means executives are connecting to risky Wi-Fi and foreign cellular networks
2. Executives are prime targets for financially motivated whaling attacks
3. Highly sensitive data is being accessed from mobile devices outside the reach of traditional security tools.

Real World Use Case for Executives

While traveling, especially internationally, connecting to Wi-Fi access points is a common practice. However, these networks often lack security, leaving executives susceptible to network-based man-in-the-middle attacks. This could allow the malicious actor to route all traffic through a rogue router or silently drop malware on the device. Either way, this is an easy gateway into a device that has access to corporate cloud data.

Executives are prime targets for highly targeted and socially engineered phishing attacks called 'whaling attacks'. These attacks can be detrimental to the company from both a brand and financial perspective, and over 50% of organizations named whaling and CEO fraud as their top email-related threats.[1] Whaling attacks are almost always financially motivated, whether by directly trying to phish funds or by gaining access to highly valuable research data that a malicious actor could turn around and sell to a competitor.

Lookout Critical Capabilities

Lookout Phishing and Content Protection inspects any URL requests, including corporate and personal email, SMS, messaging apps, and Apps containing URLs that download malicious plug-ins. Lookout dynamically blocks URL requests for websites identified by Lookout as malicious and phishing. Additionally, Lookout detects network-based attacks that attempt to steal personal or sensitive company data over Wi-Fi or cellular networks. The end user will be notified that the network being used is dangerous and be shown instructions on how to disconnect while admins can put policies in place that block access to corporate resources in the case on an unsecured connection.

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 Continuous Conditional Access to sensitive corporate applications and data.

[1] Phishing Response Trends UK: Stop the Chaos. Cofense 2019