Lookout Enables Continuous Conditional Access

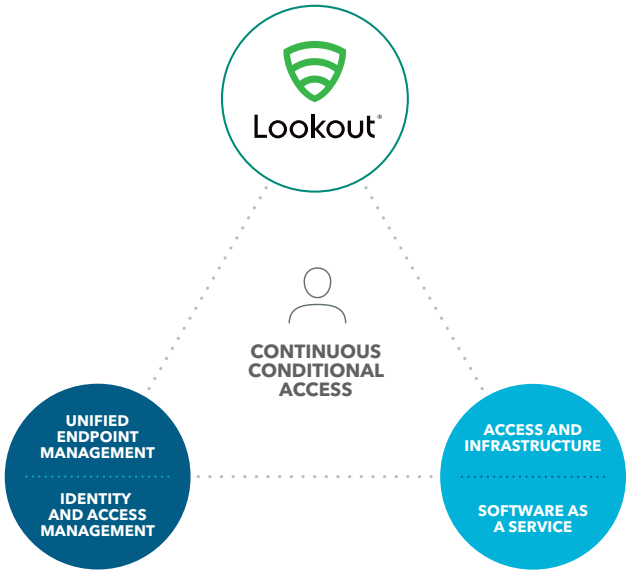
Organizations need a way to continuously guarantee device health as employees access sensitive corporate data via mobile apps and devices

Industry-Wide Security Challenges

As organizations increasingly depend on mobility to empower employee productivity, there is a need to protect organizations from the risks that come with corporate data accessed by mobile devices. Some mobile management platforms only update app details every four hours, IAM solutions only renew identity tokens every 24 hours, which makes it difficult to have continuous visibility of the devices employees use to access corporate infrastructure and data.

Real World Need for Continuous Visibility

Since attacks like mobile phishing and device vulnerability exploitation can take place in a matter of seconds without the end user realizing it, Lookout continuously assesses the health of any device accessing corporate data by dynamically monitoring the health of an endpoint while a user is connected to the enterprise. By using Continuous Conditional Access to monitor risk and trust, organizations can allow only healthy devices to connect to platforms storing sensitive data; removing the threat from device, app, or network risks.



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 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 and remediation steps on malicious apps, network connections, and system anomalies in real time; accompanied by continuous device health checks to provide continuous conditional access to sensitive corporate applications and data to ensure employee devices aren't leveraged by malicious actors to steal assets.

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