How Lookout Enables CCPA Compliance

California Consumer Privacy Act (CCPA) requires companies to adopt cybersecurity to protect user privacy

Securing User Privacy

On January 1, 2020, CCPA will come into effect. This privacy regulation, much like GDPR, will establish strict requirements for protecting privacy for California citizens. In doing so, firms will need to re-examine their data protection strategies to ensure they are meeting 'reasonable security' standards in an era of increasingly sophisticated cyberthreats. Breaches of privacy under CCPA can result in significant fines for organizations. This regulation will be the benchmark for future state and federal privacy regulations across the United States.

Real-World Use Case

In preparation for CCPA, California Attorney General recommends using the CIS Controls as a minimum starting point for implementing data privacy protections. Specifically, CIS Control #5 recommends that organizations:

*"Establish, implement, and actively manage (track, report on, correct) the security configuration of **mobile devices**, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings."*

Lookout continuously monitors mobile devices to prevent malicious actors from taking advantage of vulnerable services and configurations on Android and iOS devices.

To prepare for CCPA compliance, organizations should:

1. Evaluate current security posture against the CIS Controls and NIST framework.
2. Identify gaps in mobile security relative to the cyber threats targeting mobile devices.
3. Use Mobile Threat Defense to manage the security of mobile devices to stop exploits.

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 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 mobile 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.

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