Lookout + Okta Cloud Identity

With Continuous Conditional Access for authentication informed by mobile threat intelligence.

As the number of applications, devices, and platforms accessing corporate data continues to increase, IT administrators seek comprehensive visibility into system access. Businesses are adopting Identity Access Management (IAM) solutions for managing user authentication and for preventing unauthorized access to business applications. By incorporating Lookout Mobile Endpoint Security with the Okta Identity Cloud, mobile device health is verified even before Okta authentication begins; only healthy devices advance to the user authentication stage. Together, Lookout Continuous Conditional Access and Okta Identity Cloud create a powerful post-perimeter security solution.

Okta Identity Cloud

- Seamless access to enterprise apps with SSO
- Intelligent access policies based on login context
- Policy verification factors for app and VPN security
- Real-time reporting of all authentication events
- Automation of business life cycles that involve users
- Native mobile app for identity access management

Lookout Mobile Endpoint Security

- Continuous assessment of risk for mobile apps
- Protection against phishing attacks
- Detection of man-in-the-middle attacks
- Control of app data leakage to ensure compliance
- Visibility and detection of sideloaded applications
- Custom remediation policy across threats types

Seamless integration to provide secure mobility

Risks	Okta Identity Cloud	Lookout + Okta Identity Cloud
App distribution	Secure authentication to access all enterprise apps in one location	Secure authentication to access all enterprise apps in one location
Policy violations	If a non-compliant device is detected, automated actions are to bring the device back into compliance	Compliance decisions can now take into account presence of threats or risky applications detected by Lookout
Unprotected networks	Use location context such as new IP, specified IP zones, and network anonymizers as input to risk-based authentication.	Okta authentication protection against untrusted networks enhanced by Lookout protection against man-in-the-middle attacks on encrypted enterprise data in transit
Continuous Conditional Access	Access to corporate resources can be revoked automatically if compliance policies are violated	• Authentication to applications can be revoked following Lookout detection of app, network, or OS-based threats • Following threat remediation, access is granted
Insecure authentication	Intelligent, risk-based access controls enabling SSO across web, cloud and mobile apps	Intelligent, risk-based access controls enabling SSO across web, cloud and mobile apps
App-based risks		Provides visibility into apps that leak data as well as malware such as trojans and spyware
Jailbreaking and rooting		Analyzes hundreds of OS signals to identify attempts to bypass basic jailbreak/root detection
Phishing attacks		Prevents connections via malicious URLs in email, SMS, messaging apps and those embedded into apps

Continuous Conditional Access with Okta Identity Cloud

With Okta Identity Cloud integration, at risk devices are denied access in real-time using custom remediation policies. This includes the ability to block access to Okta Identity Cloud apps on unmanaged devices based on Lookout risk status. When Lookout detects a threat, the device will be categorized as either "high risk", "moderate risk", or "low risk" depending on your security policy settings. The threat remediation process follows these basic flows: