Global pharmaceutical leader protects critical research with Lookout mobile security

The Challenge

One of the world's leading pharmaceutical organizations wanted to prevent data leakage of intellectual property. They also wanted to meet their compliance requirements for mobile devices used to access the firm's research data. The CISO identified a gap in their ability to protect against the risk of mobile phishing attacks and app risks that could lead to data leakage across more than 20,000 mobile users.

While the CISO had a budget allocated for mobile security, it was up to the IT team to manage the deployment of any new solution. To limit any impact on current vaccine research, they had a critical requirement to minimize disruption during the deployment process across the entire mobile fleet.

Support for personal devices used for work is pervasive across industries including pharmaceuticals. This creates significant risk when personal devices access research data. The CISO realized that more than any other endpoint, the organization needed to take a Zero Trust approach in securing personal devices. Only personal devices that met key compliance and security requirements could access data. The challenge was how to apply a Zero Trust model to these endpoints and continuously enforce security requirements.

Customer Profile

Industry: Pharmaceutical

Healthcare Mobile Devices: 20,000

Mobility Policy: Bring-your-own-device (BYOD)

Enterprise mobility management Solution: Microsoft Endpoint Manager

Security Solution: Lookout Mobile Security Platform

Integrated Solution

Integrated Microsoft Endpoint Manager

Lookout Modern Endpoint Protection

Lookout Phishing and Content Protection

Results

- Prevented mobile phishing attacks across work and personal apps
- Gained real-time visibility into mobile device risks
- Enabled conditional access policies to restrict data access to until mobile threats are remediated
- Secured mobile endpoints with "single pane-of-glass" management

Once deployed, the selected mobile endpoint security solution would have to protect against:

- Mobile phishing attacks across all apps, not just email
- iOS and Android malware on employee-owned devices
- Attacks over compromised or unsecured Wi-Fi networks
- Apps that leak data and have the potential to put the organization out of compliance

The Solution

After evaluating a shortlist of mobile security solutions, the CISO concluded that the integration between Microsoft Endpoint Manager, and Lookout Modern Endpoint Protection represented the best possible choice. The integration provides an essential capability to continuously adapt the access control for a BYOD mobile device based on real-time changes in the risk-level of the device. If the risk-level became unacceptable, access could automatically be modified to protect the organization's intellectual property.

This capability is Lookout Continuous conditional access and it delivers real-time visibility into mobile risks to the endpoint manager, enabling the deployment of a Zero Trust strategy. With continuous monitoring against risks such as advanced mobile threats, app data leakage, and compromised Wi-Fi networks, Lookout enables the organization to limit access to compromised mobile devices. For example, if an employee in the research department unknowingly downloads a malicious mobile application, Lookout will identify the threat and trigger conditional access policies to restrict access to corporate data until the threat is removed from the endpoint.

Both the CISO and the CIO of this leading pharmaceutical company agreed that the combined Lookout and Microsoft solution delivers a combination of mobile security and mobile zero trust to protect their intellectual property. In addition, they realized that Enterprise Mobility Management (EMM) alone is insufficient.

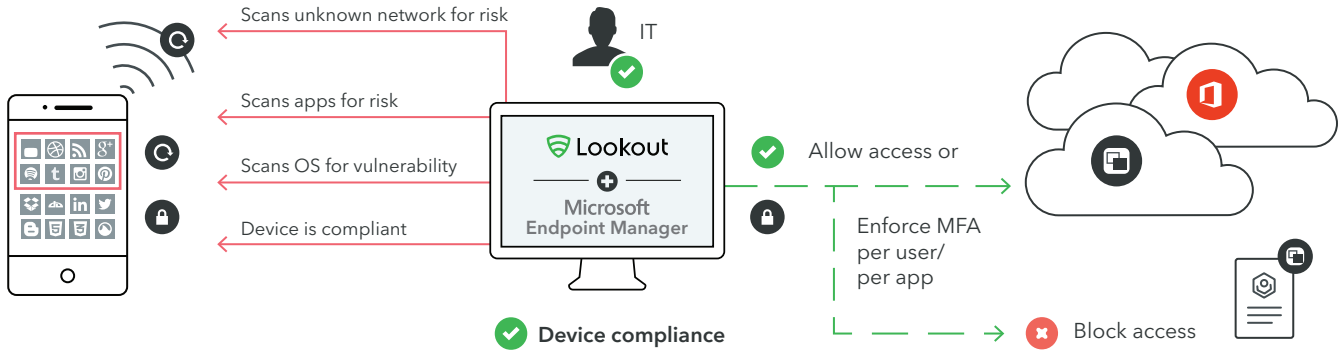
Lookout Continuous Conditional Access policies provide real-time mobile threat detection and risk assessment, whereas EMM only checks in on devices once every couple of hours. With Lookout, the CIO was able to enforce integrated policy management for users and groups. The CISO has one-click access to risk and compliance reporting for all users and apps installed on their devices.

The Results

With seamless deployment of Lookout, this pharmaceutical giant is able to establish a global security policy for employees. If a mobile device is found to be non-compliant due to a mobile risk, the user's access to corporate resources is blocked. They will only regain access once they resolve the issue by following remediation instructions from Lookout.

Since Lookout Modern Endpoint Protection with Phishing and Content Protection integrated seamlessly into the Microsoft Enterprise Mobility Management solution, the organization is able to manage everything through a "single pane of glass."

The CISO and CIO of this global leader are able to meet the CEO and Board requirements for protecting all endpoints against cybersecurity attacks and deliver a measurable reduction in mobile risks across the global workforce.



Lookout

lookout.com