Case Study

Global Pharmaceutical Leader Protects Critical Research with Lookout

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 Cloud Security Platform

Integrated Solution

Integrated Microsoft Endpoint Manager

Lookout Mobile Endpoint Security

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
- Executed their BYOD mobility policy with Lookout securing all unmanaged devices

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 Mobile Endpoint Security 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.

Lookout enables this risk-based access by delivering real-time visibility of mobile risk to the endpoint manager, which in turn enables a zero-trust strategy for users on mobile devices. 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.

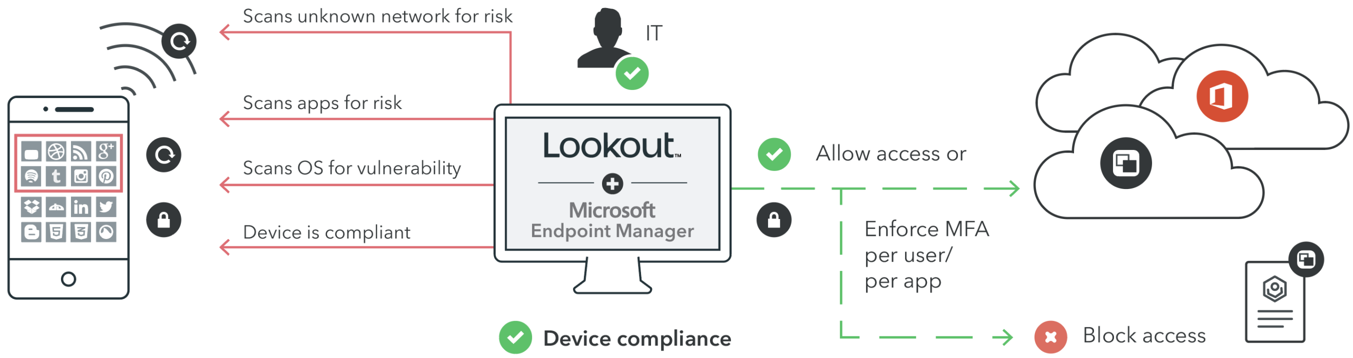
Lookout policies provide real-time mobile threat detection and risk assessment, whereas EMM only checks in on devices once every couple of hours. With Lookout, the CIO was able to enforce integrated policy management for users and groups. The CISO has one-click access to risk and compliance reporting 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 Mobile Endpoint Security with Phishing and Content Protection integrated seamlessly into the Microsoft EMM 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.



About Lookout

Lookout, Inc. is the endpoint to cloud security company purpose-built for the intersection of enterprise and personal data. We safeguard data across devices, apps, networks and clouds through our unified, cloud-native security platform — a solution that's as fluid and flexible as the modern digital world. By giving organizations and individuals greater control over their data, we enable them to unleash its value and thrive. Lookout is trusted by enterprises of all sizes, government agencies and millions of consumers to protect sensitive data, enabling them to live, work and connect — freely and safely. To learn more about the Lookout Cloud Security Platform, visit www.lookout.com and follow Lookout on our blog, LinkedIn, and Twitter.

For more information visit
lookout.com

Request a demo at
lookout.com/request-a-demo