How International Law Firm Taylor Vinters LLP Protects its Android Workforce with Lookout

Challenges

- The firm handles a great deal of sensitive information, including corporate intellectual property, client and financial data and personally identifiable information (PII). This data is accessible by Taylor Vinters' employees via their work-issued Android smartphones and laptops.
- The firm's IT team is responsible for providing employees with video conferencing, web browsing and secure access to a whole host of SaaS-delivered applications. It must also support requests for the use of non-traditional apps, to meet client preferences for modern communication tools like WhatsApp and others. The apps may seem harmless, but have the potential to put Taylor Vinters out of compliance or give bad actors an additional avenue to compromise the firm's data.
- The firm's vision is to create an agile working environment which requires a move from on-premises to the cloud. Unlike desktops, laptops and mobile devices can't be secured by perimeter-based security tied to corporate offices. Working out of the office brings new attack surfaces that could put the firm's proprietary information at risk of exposure, Taylor Vinters' IT team sought a solution that could help it protect its data and meet regulatory requirements.

Taylor Vinters

The Customer

Taylor Vinters is an international law firm supporting the businesses which drive the innovation economy, and the entrepreneurs and private wealth that underpin them.

Its practice is global, operating from innovation clusters in the U.K., Asia and the U.S. The firm's clients range from Fortune 500 technology multinationals through fast growth venture backed and owner managed businesses, to individuals driven by great ideas and a passion.

Industry: Legal

The Solution

Lookout Mobile Endpoint Security with Phishing and Content Protection and Modern Endpoint Protection

The Results

- Confidence that the firm's Android Enterprise devices around the world are secured
- Enhanced app control; users are alerted of compromise
- Full management and support
- Comprehensive modern endpoint protection

Solution

Appurity, a U.K.-based Lookout Elite channel partner, delivered the **Lookout Security Platform** with **Phishing and Content Protection** and **Modern Endpoint Protection** to optimise security across all Taylor Vinters' devices. The entire project, including reviewing alternative vendors and conducting a controlled assessment of the Lookout offering, was completed in less than one month. All work was carried out remotely while everyone was working from home during the Covid-19 pandemic.

The Lookout Security Platform is purpose-built for mobile devices and protects user privacy by not collecting personal information. By leveraging telemetry from nearly 200 million devices and over 135 million apps, Lookout understands what a mobile threat looks like – it can automatically detect and respond to app, device and network threats.

- **The Lookout Security Platform's cloud-based architecture allows customers to scale to hundreds of thousands of endpoints with cloud modules aligned to the customer's specification.**

  Whether Taylor Vinters' employees would unintentionally download malware onto their mobiles or would be the target of the latest ransomware or phishing scam, they are protected – the firm's IT team won't need to take any action. When a threat or an attack occurs, the Lookout app provides the device user with step-by-step instructions to investigate what is happening and how to fix it.

- **Lookout Phishing and Content Protection stops both known and unknown phishing threats.**

  The Lookout Phishing AI engine continuously monitors reputation lists of known phishing sites for the establishment of new websites purpose-built for phishing. With Phishing AI, Lookout provides near real-time protection against zero-hour phishing attacks. It compares every web request from a Taylor Vinters employee's mobile device with this combined dataset - this comparison is also made for every network interface on the employee's device, including Bluetooth, Wi-Fi and cellular. The user's privacy remains protected because the comparison is performed on the local endpoint device rather than in the cloud.

- **Lookout Modern Endpoint Protection protects Taylor Vinters' mobile workforce from app, device and network threats.**

  Lookout analyzes security telemetry of nearly 200 million mobile devices and over 135 million apps in the Lookout Security Graph. This enables Lookout to proactively protect against malicious apps, advanced device compromise attacks, and network threats on the mobile device. With insight into real-time changes on a device in the context of the broader mobile ecosystem, Lookout Modern Endpoint Protection can detect zero-day threats that have never been seen before. The result is comprehensive modern endpoint protection that secures the Taylor Vinters' employee mobile devices and the corporate data they access from evolving mobile threats.

> "The freedom to work anywhere comes with risk, so we need to ensure every mobile device our employees touch for work-related matters is secure. With Lookout in place, we now have a best-in-class security platform protecting our mobile workforce as we open up the functionality which modern mobile devices and cloud delivered applications can bring."

Steve Sumner, IT Director

Results

- **Anti-phishing secures sensitive data:** With more work being carried out on mobile devices, the company was more susceptible to phishing attacks, especially with smaller device screens and countless apps enabling cyber-attackers to deliver socially engineered attacks.

  Lookout Phishing and Content Protection uses AI to automatically stop known and unknown phishing threats.

- **Safeguarding devices and data from advanced malware:** All staff needed to be able to access cloud services from any device. But advanced mobile malware can exploit mobile device and app vulnerabilities to discreetly exfiltrate data from any service to which the device has access.

  By continuously monitoring device and app behaviours, Lookout Modern Endpoint Protection protects Taylor Vinters' mobile fleet against threats ranging from jailbreaking or rooting a device to advanced device compromise.

- **Ensuring personal applications don't add risks:** Even though their devices are corporate-issued, phones and tablets are treated as personal devices. With work and personal lives converging on them, Taylor Vinters needed to ensure the apps their legal staff use won't put their clients' information at risk.

  Lookout Risk and Compliance provides Taylor Vinters with data from Lookout's analysis of more than 125 million apps to enforce policies. This means the firm can automate the monitoring to know when an app is introducing risk into their company and take appropriate action.

About Lookout

Lookout is a leading cybersecurity company. Our mission is to secure and empower our digital future in a privacy-focused world where mobility and cloud are essential to all we do for work and play. We enable consumers and employees to protect their data, and to securely stay connected without violating their privacy and trust. Lookout is trusted by millions of consumers, the largest enterprises and government agencies, and partners such as AT&T, Verizon, Vodafone, Microsoft, Google, and Apple. Headquartered in San Francisco, Lookout has offices in Amsterdam, Boston, London, Sydney, Tokyo, Toronto and Washington, D.C.