Henkel extends compliance to mobile by securing Android & iOS devices across global workforce

The Challenge

In the summer of 2016, the Digital Workplace Mobility team at Henkel's headquarters in Düsseldorf, Germany, was facing the challenge of setting up a two-platform mobile device strategy for their global workforce. Market changes led the team to determine that only Android and iOS devices were qualified for their workforce. With impending GDPR regulations and the increasing risk of malware in their mobile fleet, Henkel completed an Enterprise Mobile Risk Assessment with Lookout Mobile Endpoint Security and its trusted mobility consultant EBF.

As the Head of Digital Workplace Mobility at Henkel, Marco Siedler and his team are part of an IT organisation which supports all Henkel business units. The team decided not to proceed with a container-based solution based on the following argumentation: "After testing a container approach that divided the devices into personal and work, we found the pilot group of employees had issues synchronising contacts to their car phone systems, which was a big pain point for our sales teams."

At this point Marco and his team initiated the required tool selection process for a Mobile Threat Defense solution that would deliver complete security for their devices and data.

Henkel

Customer Profile

Henkel operates globally with a well-balanced and diversified portfolio. The company holds leading positions with its three business units in both industrial and consumer businesses thanks to strong brands, innovations and technologies. Founded in 1876, Henkel looks back on more than 140 years of success. Henkel employs more than 50,000 people globally – a passionate and highly diverse team, united by a strong company culture, a common purpose to create sustainable value, and shared values. As a recognised leader in sustainability, Henkel holds top positions in many international indices and rankings. Henkel's preferred shares are listed in the German stock index DAX.

Industry: Consumer and industrial goods

Size: 286 on Forbes 2000

Mobility Policy: Corporate only

EMM solution: MobileIron

Security Challenges

- Extending compliance policies to mobile
- Guaranteeing secure mobile access to sensitive data for corporate-owned Android devices
- Achieving complete device security and avoiding containers

The Solution

After a fast and thorough proposal review process, Marco and his team chose to collaborate with Lookout Mobile Endpoint Security to secure global mobility at Henkel. This solution provides worldwide protection from malicious threats and data leakage, enabling Henkel to guarantee secure access to sensitive data and extend policies for GDPR compliance to mobile.

Lookout thoroughly fulfilled Henkel's integration criteria by offering seamless connectivity with both its MobileIron instance, hosted in Deutsche Telekom's data centre, and its IBM QRadar SIEM.

> "Lookout gives us the policy controls we need to protect sensitive corporate and regulated personal data at scale, enabling us to extend compliance policies to mobile, achieve a measurable risk reduction, and do so while ensuring employee privacy."
>
> **Marco Siedler,**
> Head of Digital Workplace Mobility, Henkel AG & Co. KGaA

Lookout met Henkel's requirements for data privacy by enabling the team to "turn off" collection and storage of end-user personal data, including data collected from devices and from third-party integrations such as their MobileIron MDM. Additionally, the Henkel team is limiting access rights to data through a role-based administration feature including three tiers of console access and a "Read Only" role. In Marco's words, "Lookout fulfils our requirements for dealing with personal data. Their approach is that all data reported to the Lookout cloud is anonymised, which directly supports our principles in terms of processing personal data only when and where it's really needed."

Since more than 80 per cent of Henkel's employees work outside of Germany, a key part of the business case for Lookout was the ability to deliver protection worldwide. Lookout provides unique global capabilities including access to a CDN with region-specific access points, the capability to configure sync intervals for low-bandwidth locations, and the Lookout Mobile Risk API with connectors to SIEM, NAC and other systems for incident response and remediation.

The Results

Henkel's decision to collaborate with Lookout contributed to increased data security, which is a requirement for GDPR compliance. Taking advantage of their visibility into possible data leaking apps (e.g. "mashup apps") and mobile threats, the Henkel team has established a conditional access rule for Android devices: Only devices with an activated Lookout for Work app are enabled to access corporate data and resources. At the time Henkel evaluated the available solutions, Marco determined that Lookout is a must, "For Android devices we see Lookout for Work as the best option to release the Android platform for enterprise usage."