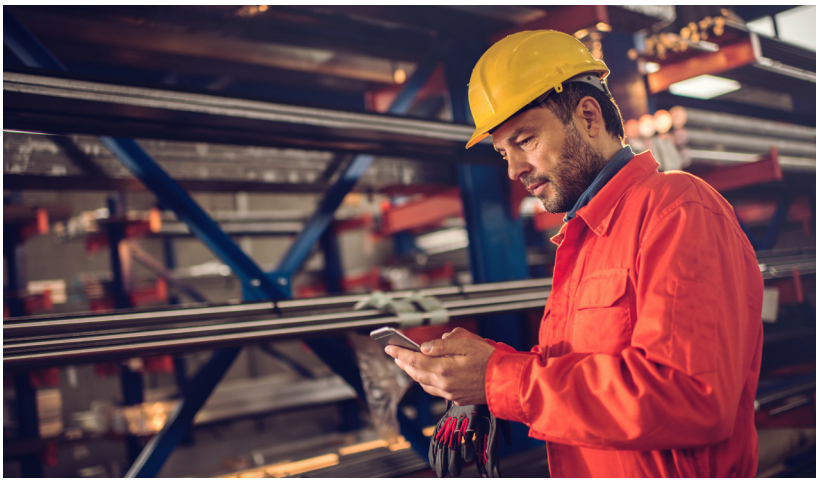
Henkel sichert Android- und iOS-Geräte seiner Mitarbeiter weltweit ab und weitet so die Compliance auf mobile Technologien aus



Die Herausforderung

Im Sommer 2016 stand das „Digital Workplace Mobility"-Team der Henkel-Zentrale in Düsseldorf vor einer Herausforderung: die Einführung einer zwei Plattformen umfassenden Mobilgerätestrategie für ihre Mitarbeiter weltweit. Änderungen am Markt hatten das Team schlussfolgern lassen, dass nur Android- und iOS-Geräte als Firmengeräte infrage kamen. Aufgrund des bevorstehenden Inkrafttretens der DSGVO und der zunehmenden Gefahr durch Malware in dem Mobilgerätepool führte Henkel gemeinsam mit seinem bewährten Mobility-Berater EBF ein Enterprise Mobile Risk Assessment von Lookout Mobile Endpoint Security durch.

Marco Siedler, Head of Digital Workplace Mobility bei Henkel, und seine Kollegen sind Teil eines IT-Teams, das für alle Henkel-Geschäftseinheiten zuständig ist. Das Team entschied sich gegen eine containerbasierte Lösung und begründete dies so: „Als wir eine containerbasierte Lösung testeten, bei der die Geräte in privat und dienstlich unterteilt wurden, zeigten sich bei der Pilotgruppe der Mitarbeiter Probleme beim Synchronisieren ihrer Kontakte mit der Telefonanlage ihres Dienstfahrzeugs – ein echtes Manko für unsere Vertriebsteams."

Dies war der Anlass für Siedler und sein Team, einen Auswahlprozess für eine umfassende „Mobile Threat Defense"-Lösung zu starten, die die Sicherheit aller Geräte und Daten gewährleisten sollte.

Henkel

Kundenprofil

Mit seinem gut abgestimmten und vielfältigen Portfolio ist Henkel global aktiv. Dank starken Marken, Innovationen und Technologien ist das Unternehmen mit allen drei Geschäftseinheiten sowohl in der Industrie als auch auf dem Verbrauchermarkt führend. Henkel wurde 1876 gegründet und blickt somit bereits auf über 140 erfolgreiche Jahre zurück. Weltweit sind über 50.000 Menschen bei Henkel beschäftigt – eine engagierte, äußerst vielfältige Belegschaft, vereint durch eine solide Firmenkultur, nachhaltige Wertschöpfung und gemeinsame Werte. Die führende Rolle von Henkel im Bereich Nachhaltigkeit wird durch viele internationale Indizes und Rankings bestätigt. Henkels Vorzugsaktien werden im DAX gehandelt.

Branche: Konsum- und Industriegüter

Größe: 286 unter den Forbes 2000

Mobilitätsrichtlinie: Nur Firma

EMM-Lösung: MobileIron

Sicherheitsspezifische Herausforderungen

- Ausweitung der Compliance-Richtlinien auf Mobilgeräte
- Gewährleistung eines sicheren mobilen Zugriffs auf sensible Daten für unternehmenseigene Android-Geräte
- Umfassende Absicherung aller Geräte und Vermeidung von Containern

Die Lösung

Nach einer schnellen, eingehenden Prüfung entschieden sich Siedler und sein Team für Lookout Mobile Endpoint Security zur Absicherung des globalen Mobilgerätepools von Henkel. Die Lösung bietet weltweiten Schutz vor Malware-Bedrohungen und Datenverlust und ermöglicht Henkel so den sicheren Zugriff auf sensible Daten. Damit werden auch die Compliance-Richtlinien des Unternehmens gemäß DSGVO-Vorgaben auf Mobilgeräte ausgeweitet.

Lookout erfüllte die Integrationskriterien von Henkel dank der nahtlosen Anbindung an seine MobileIron-Instanz, die im Rechenzentrum der Deutschen Telekom gehostet wird, sowie an IBM QRadar SIEM.

> „Lookout gibt uns die nötigen Kontrollmechanismen, um sensible Unternehmensdaten und behördlich regulierte personenbezogene Daten in großem Umfang zu schützen. So können wir die Compliance auf Mobilgeräte ausweiten und die damit verbundenen Risiken messbar senken, ohne die Privatsphäre der Mitarbeiter zu beeinträchtigen."
>
> **Marco Siedler,**
> Head of Digital Workplace Mobility, Henkel AG & Co. KGaA

Auch Henkels Anforderungen an den Datenschutz waren kein Problem für Lookout, denn es bietet dem Team die Möglichkeit, die Erfassung und Speicherung personenbezogener Daten von Endanwendern zu deaktivieren – einschließlich Daten, die von Geräten und Drittanbieterintegrationen wie der mobilen Geräteverwaltung (MDM) von MobileIron erfasst wurden. Außerdem beschränkt das Henkel-Team den Datenzugriff mithilfe einer rollenbasierten dreistufigen Verwaltungsfunktion und einer Rolle ausschließlich mit Lesezugriff. Siedlers Kommentar: „Lookout erfüllt unsere Anforderungen zum Umgang mit personenbezogenen Daten. Alle der Lookout-Cloud gemeldeten Daten werden anonymisiert, und das kommt unserem Prinzip entgegen, personenbezogene Daten nur dann zu verarbeiten, wann und wo es wirklich nötig ist."

Zudem punktete Lookout mit der Fähigkeit, weltweiten Schutz zu bieten, schließlich sind mehr als 80 Prozent der Mitarbeiter von Henkel außerhalb Deutschlands tätig. Lookout bietet einzigartige globale Funktionen wie den Zugriff auf ein Content Delivery Network (CDN) mit regionsspezifischen Zugriffspunkten, der Möglichkeit, Synchronisierungsintervalle für Standorte mit geringer Bandbreite zu konfigurieren, sowie die „Lookout Mobile Risk"-API mit Anbindung an SIEM, NAC und andere Systeme für die Reaktion auf Sicherheitsvorfälle und deren Beseitigung.

Das Ergebnis

Henkels Zusammenarbeit mit Lookout führte zu besserer Datensicherheit, einer Grundvoraussetzung für die Einhaltung der DSGVO. Dank des Einblicks in potenziell Daten ausschleusende Apps (z. B. „Mashup-Apps") und andere mobile Bedrohungen konnte das Team von Henkel eine geräteabhängige Zugriffsregel für Android-Geräte einrichten, damit nur Geräte mit aktivierter „Lookout for Work"-App auf Unternehmensdaten und -ressourcen zugreifen können. Bei der Evaluierung der infrage kommenden Lösungen stellte Siedler fest, dass Lookout unverzichtbar ist: „Für Android-Geräte ist Lookout for Work die beste Option, um die Android-Plattform für die dienstliche Nutzung freigeben zu können."