Lookout®

LOOKOUT MOBILE ENDPOINT SECURITY

SICHERHEIT FÜR DAS GERÄT, DAS SIE ÜBERALLHIN BEGLEITET

Schützen Sie das Gerät, das Sie am häufigsten verwenden

Traditionelle Cybersicherheitsstrategien zielen seit langem in erster Linie darauf ab, feste Endpunkte wie Server, Laptops und Desktops vor Cyberbedrohungen zu schützen. Ihre Sicherheitsanforderungen haben aber im Laufe der Zeit organisch zugenommen.

Leider werden gerade mobile Endgeräte sicherheitstechnisch oftmals vernachlässigt, sodass eine Lücke in der Sicherheitsarchitektur entsteht. Auch wenn mobile Betriebssysteme als robuster gelten, werden sie immer häufiger Ziel von Cyberangriffen. Immerhin stehen Mobilgeräte an der Schnittstelle zwischen Privat- und Berufsleben. Diese Geräte enthalten unzählige wertvolle Daten und werden von Angreifern oft als Ausgangspunkt für den Zugriff auf Unternehmensdaten genutzt.

Bei der Wahl der richtigen Sicherheitslösung für mobile Endgeräte müssen Sie wie so oft zwischen einer umfassenden Plattform und führenden Einzellösungen wählen. Da die Zunahme von mobilen Endgeräten mit dem Anstieg der Cloud-Nutzung einhergeht, können Sie mit einer Endpoint-to-Cloud Security Lösung für vollumfängliche Sicherheit sorgen, die Benutzerfreundlichkeit verbessern, die Benutzerflexibilität steigern und Betriebskosten im Vergleich mit einer Zusammenstellung aus eigenständigen Lösungen senken.

VORTEILE

- Cloudbasierter Schutz für mobile Endgeräte
- Schutz von iOS-, Android- und Chrome OS-Geräten
- Endpoint Detection & Response entwickelt von Threat Researchern
- Schlanke App ohne Beeinträchtigung der Akkulaufzeit und Performance
- Sicherung von Unternehmens- und Privatgeräten
- Einhaltung von Compliance-Richtlinien ohne Verletzung der Privatsphäre von Anwendern
- Einfache Bereitstellung auf allen Mitarbeitergeräten
- Skalierung für Umgebungen mit hunderttausenden Endgeräten

Mittlerweile nutzen mehr als die Hälfte der Geräte, mit denen Mitarbeiter auf Ihre Unternehmensdaten zugreifen, iOS, Android oder Chrome OS.

Mobiles Arbeiten birgt neue Chancen für Cyberkriminelle

Die Sicherung von Mobilgeräten unterscheidet sich von Grund auf von der Sicherung von Desktops und Laptops. Auch wenn Bedrohungen auf Mobilgeräten denen auf Desktops sehr ähnlich sind, müssen diese Geräte mit einem ganz anderen Ansatz geschützt werden. Daher müssen Sie neue Sicherheitsanforderungen für Ihre Mobilgeräteflotte erfüllen.

Risiken beim mobilen Arbeiten erfordern modernen Endgeräteschutz

Auch wenn mobile Betriebssysteme robuster sind, werden sie immer häufiger Ziel von Cyberangriffen. Immerhin stehen Mobilgeräte an der Schnittstelle zwischen Privat- und Berufsleben. iOS-, Android- und Chrome OS-Geräte enthalten unzählige wertvolle Daten und werden von Angreifern als Einstieg für das Eindringen in Ihr Unternehmen genutzt.

Ein häufiger Angriffsvektor besteht aus Malware für Mobilgeräte, darunter Spyware, Banking-Trojaner und Rootkits. Malware kann über Mobilfunk-, WLAN- und Bluetooth-Verbindungen an Mobilgeräte übermittelt werden. Nach Ausführung der Malware umgeht diese die Gesamtsicherheit des Mobilgeräts.

Moderner Endgeräteschutz muss Bedrohungen in Apps, Geräten und Netzwerkverbindungen erkennen. Er muss den Anwender, das Gerät und das Unternehmen schützen und die Privatsphäre des Nutzers respektieren. Er muss sowohl für private Geräte von Mitarbeitern als auch für Firmengeräte geeignet sein.

> **„Sicherheitstools für Mobilgeräte sind nicht mehr nur für stark regulierte Branchen und Behörden erforderlich, sondern mittlerweile unerlässlich für alle Unternehmen."**
>
> – **Phil Hochmuth**, Program Vice President, Enterprise Mobility bei IDC.

Ermöglichen Sie Angreifern keinen Zugang durch Phishing auf Mobilgeräten

Die Verwendung traditioneller Ansätze zum Phishing-Schutz auf Mobilgeräten kann schnell zu einem Datenschutzproblem werden, da diese E-Mail-Nachrichten untersuchen, um Angriffe abzuwehren. Alle Mobilgeräte, selbst vom Unternehmen vergebene, gelten als persönliche Geräte. Die reine Untersuchung des E-Mail-Inhalts reicht zudem nicht aus, um die anderen Methoden zu erkennen, mit denen Phishing-Links versendet werden.

Die meisten Lösungen zum Phishing-Schutz basieren auf einer Liste bekannter bösartiger Domains und Webadressen. Es kommen aber jeden Monat mehr als 1,5 Millionen neue Phishing-Sites hinzu. Die meisten von ihnen werden innerhalb weniger Stunden oder Tage aufgebaut und wieder entfernt. Daher können Phishing-Angriffe auf Mobilgeräten nicht einfach nur mit herkömmlichen Methoden erkannt werden.

> **Pro Tag wird einer von 50 Unternehmensanwendern** Opfer eines Phishing-Angriffs auf seinem Mobilgerät. Dabei finden **87 % der Phishing-Angriffe auf Mobilgeräten** außerhalb von E-Mails statt.

Sie müssen die richtigen App- und Betriebssystem-Versionen für erfolgreiches Patchen kennen

Zuvor zielte das Schwachstellen- und Patch-Management in erster Linie auf Server und nicht auf Endgeräte ab. Immerhin wurden Desktops und Laptops verwaltet und regelmäßig gepatcht und nutzten ein gemeinsames Image. Daher war der nicht gepatchte Server die größte Schwachstelle.

Aktuell können Sie mit Mobile Device Management (MDM) nur sicherstellen, dass Mobilgeräte eine Mindestversion des Betriebssystems ausführen. Mitarbeiter nutzen aber zunehmend private Smartphones und Tablets für die Arbeit, sodass MDM keinen Komplettschutz mehr bieten kann. Diese Lücke kann von traditionellem Schwachstellenmanagement nicht geschlossen werden, da Geräte hierbei mit dem Unternehmensnetzwerk anstelle von privaten WLAN- oder Mobilfunknetzen verbunden sein müssen.

> Die Financial Times hat über eine Schwachstelle in WhatsApp berichtet, über die Spyware ohne Benutzerinteraktion an iOS- und Android-Geräte übertragen werden konnte. So kann das Gerät kompromittiert werden, ohne dass Sie den Anruf entgegennehmen.[1]

1. Srivastava, Mehul, Financial Times, "WhatsApp voice calls used to inject Israeli spyware on phones", 13. Mai 2019

Nutzung von Mobilgeräten muss in Ihre Zero-Trust-Netzwerkarchitektur aufgenommen werden

Mobiltelefone und Tablets eröffnen uns viele Freiheiten, bergen aber auch Risiken. Jeder von uns stellt nun ein Remote-Netzwerk dar, das gesichert werden muss. Bei der fortwährenden Arbeit außerhalb der früheren Perimetersicherheit kann nicht garantiert werden, wem oder welchem Gerät Sie vertrauen können.

Mobile Benutzer verwenden keine VPN-Verbindungen zu den Unternehmensdaten in der Cloud. Sie müssen von überall aus darauf zugreifen können, während Sie sicherstellen, dass sensible Daten geschützt bleiben. Nur Geräten mit geringem Risiko darf der Zugriff auf die Ressourcen Ihres Unternehmens gewährt werden. Anschließend können Sie dank einer kontinuierlichen Risikobewertung den Zugriff auf Daten dynamisch anpassen.

„Die Authentifizierung von Benutzern auf persönlichen Geräten mit ZTNA (Zero Trust Network Access) kann die Sicherheit verbessern und BYOD-Programme vereinfachen, indem Verwaltungsanforderungen reduziert werden und der direkte Anwendungszugriff in höherem Maße gesichert wird." [2]

Senken Sie das Risiko dank besserer Einblicke in Apps

Die meisten Unternehmen können einsehen, wie ihre Desktop- und Laptop-Anwendungen Daten verarbeiten, verfügen aber nicht über die gleichen Einblicke für Mobilgeräte. Die Ausführungsweise von Apps unter iOS, Android und Chrome OS macht eine Untersuchung schwierig. Ohne diese Einblicke weiß Ihr Sicherheitsteam aber nicht, wie Daten von diesen Apps verarbeitet werden.

Bei verwalteten Geräten erhalten Sie Transparenz und Kontrolle über die von Mitarbeitern genutzten Apps dank Mobile Device Management (MDM) oder Mobile App Management (MAM). Diese Methoden bieten allerdings keine Einblicke in Echtzeit-App-Berechtigungen und Datenzugriffskontrollen. Bei nicht verwalteten Privatgeräten verfügen Sie noch nicht einmal über die eingeschränkte Transparenz, die mit MDM und MAM möglich ist.

„Bis 2022 sind über 75 % der im Unternehmen genutzten Smartphones Privatgeräte im BYOD-Modell. Dadurch wird eine Migration vom geräteorientierten Management zum app- und datenorientierten Management erforderlich." [3]

Verhindern Sie Sicherheitsverletzungen mit Tools für die Bedrohungserkennung und -abwehr

Viele Unternehmen überwachen Server, Desktops und Laptops zwar umfassend, erfassen aber nicht dieselben Telemetriedaten für iOS-, Android- und Chrome OS-Geräte. Je mehr Mitarbeiter ihre Mobilgeräte für die Arbeit einsetzen, desto mehr nehmen die Angriffe auf diese Geräte zu.

Um Datensicherheitsverletzungen effektiv zu unterbinden, benötigen Sicherheitsteams dieselben umfangreichen Daten für Mobilgeräte wie für Server, Desktops und Laptops. Da mobile Betriebssysteme nie den Kernelzugriff ermöglichten und für isolierte App-Ausführung sorgten, wurde fälschlicherweise davon ausgegangen, dass keine umfassende Telemetrie erfasst werden konnte.

Bis Ende 2023 haben über 50 % der Unternehmen ältere Virenschutzprodukte durch kombinierte EPP- und EDR-Lösungen ersetzt, die nicht nur Abwehr- sondern auch Erkennungs- und Reaktionsfunktionen bieten.[4]

Sicherheit für Mobilgeräte muss sich in die umfassende Sicherheitsarchitektur integrieren lassen

Einige Unternehmen verwalten die Mobilgeräte ihrer Mitarbeiter mit Tools wie Mobile Device Management (MDM) oder Unified Endpoint Management (UEM). Sie nutzen auch Security Information and Event Management (SIEM), um Bedrohungsdaten zu aggregieren. Dank vordefinierter Integrationen mit MDM/UEM und SIEM können Sie den sofortigen Nutzen einer Sicherheitslösung für Mobilgeräte maximieren.

2. Gartner "Market Guide for Zero Trust Network Access", Steve Riley, Neil MacDonald, Lawrence Orans, Juni 2020
3. Gartner "Define BYOD Ownership and Support Expectations in Contracts to Ensure Successful Implementation", DD Mishra, David Ackerman, 3. Juli 2019
4. Gartner, "Market Guide for Endpoint Detection and Response Solutions", Paul Webber, Prateek Bhajanka, Mark Harris, Brad LaPorte, Dezember 2019

„Der Markt für die Sicherung von Mobilgeräten basiert in erster Linie auf Partnerschaften, Integrationen und Ökosystemen anstatt auf führenden Einzellösungen für Bedrohungsabwehr und -beseitigung (auch wenn diese Kernfunktionen sicherlich wichtig sind). Suchen Sie nach Anbietern mit Partnern in wichtigen Kanälen, wie Mobilfunkanbieter, sowie leistungsstarken Integrationen mit EMM/SIEM-Plattformen."

– **Phil Hochmuth**, Program Vice President, Enterprise Mobility bei IDC.

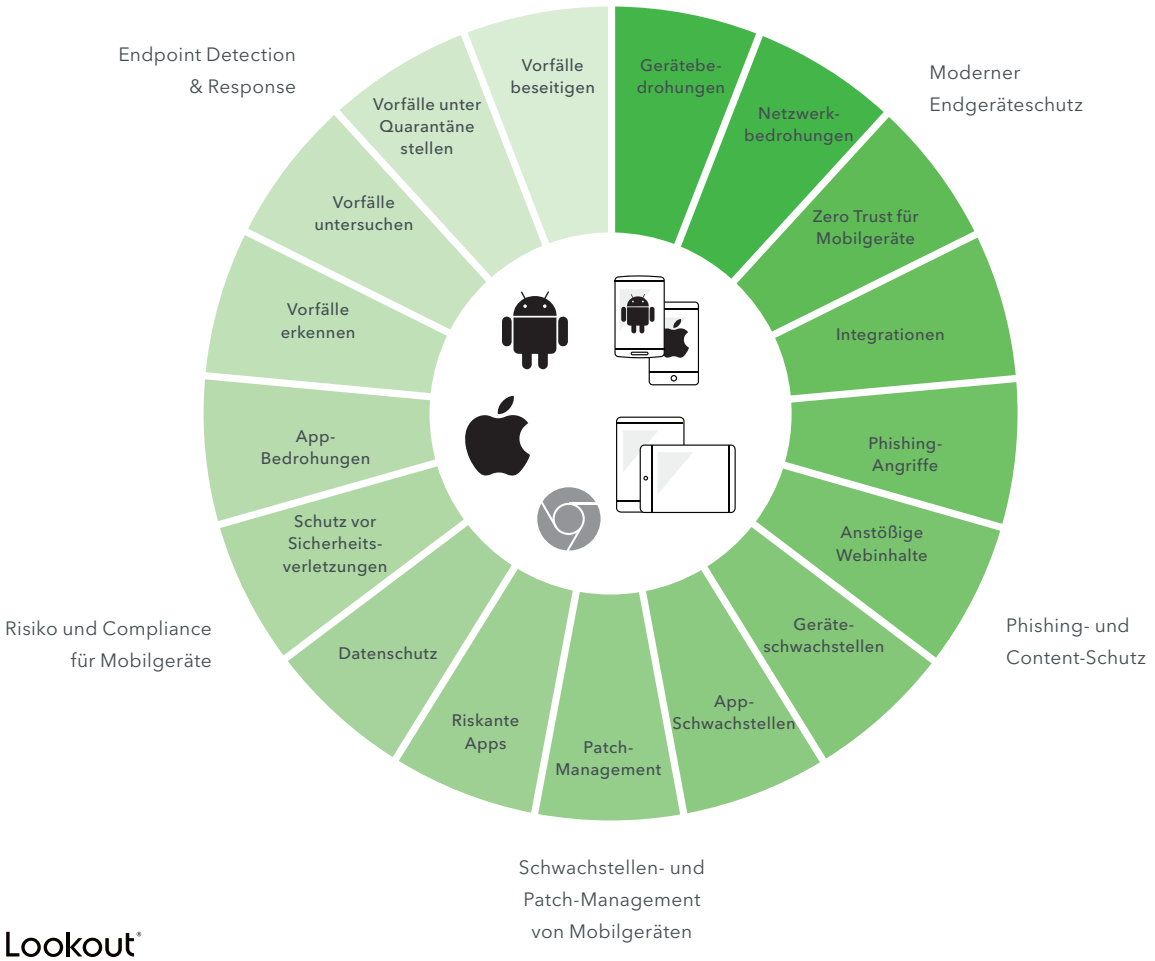
Von Grund auf für Mobilgeräte konzipierte Endgerätesicherheit

Lookout Mobile Endpoint Security (MES) erfüllt Ihre sich stets verändernden Anforderungen an die Mobilgerätesicherheit. Lookout MES basiert auf dem Lookout Security Graph und lässt sich für Hunderttausende Endgeräte skalieren. Sie können Mobile Endpoint Security dank seiner Cloud-Module an Ihre Anforderungen anpassen.

Unser Security Graph ist auf künstliche Intelligenz gestützt und schützt Sie vor bekannten und unbekannten Bedrohungen. Wir können auf einen der größten Datensätze zur mobilen Sicherheit mit über 200 Millionen analysierten Geräten und über 135 Millionen analysierten Apps zurückgreifen. Unsere Algorithmen durchsuchen täglich das Internet, um speziell für Phishing-Zwecke erstellte Websites aufzufinden, desweiteren wurden unzählige benutzerdefinierte Apps von unserer API analysiert.

Ob Sie Apps mit neuer Malware herunterladen oder Ziel des neuesten Ransomware- oder Phishing-Betrugs werden – jetzt sind Sie automatisch geschützt. Bei einer Bedrohung oder einem Angriff erhalten Sie von uns detaillierte Anweisungen zu Untersuchung und Beseitigung.

Lookout Mobile Endpoint Security



Über Lookout

Lookout ist ein Anbieter von integrierten Sicherheitslösungen von Endgerät bis hin zur Cloud. In einer Welt, in der Datenschutz höchste Priorität hat und Mobilität und Cloud bei der Arbeit und in der Freizeit unverzichtbar geworden sind, haben wir es uns zur Aufgabe gemacht, Sie sicher in die digitale Zukunft zu führen. Wir geben Verbrauchern und Mitarbeitern die Möglichkeit, ihre Daten zu schützen und sicher miteinander in Verbindung zu bleiben, ohne ihre Privatsphäre oder ihr Vertrauen zu verletzen. Lookout wird von Millionen Anwendern, den größten Unternehmen und Behörden sowie Partnern wie AT&T, Verizon, Vodafone, Microsoft, Google und Apple genutzt. Lookout hat seinen Hauptsitz in San Francisco und verfügt über Niederlassungen in Amsterdam, Boston, London, Sydney, Tokio, Toronto und Washington, DC. Weitere Informationen finden Sie unter **www.lookout.com/de**. Folgen Sie Lookout auf seinem **Blog**, **LinkedIn** und **Twitter.**

Weitere Informationen finden Sie auf
lookout.com/de

Fordern Sie eine Demo an unter
https://www.lookout.com/de/info/de-enterprise-contact-us

Integrierte Sicherheit von Endgerät zu Cloud

Weitere Informationen finden Sie unter **lookout.com/de**

© 2021 Lookout, Inc. LOOKOUT®, das Lookout Shield Design®, LOOKOUT mit Shield Design®, SCREAM® und SIGNAL FLARE® sind eingetragene Marken von Lookout, Inc. in den USA und anderen Ländern. EVERYTHING IS OK®, LOOKOUT MOBILE SECURITY®, POWERED BY LOOKOUT® PROTECTED BY LOOKOUT® sind eingetragene Marken von Lookout, Inc. in den USA und anderen Ländern. POST PERIMETER SECURITY ALLIANCE™ und DAY OF SHECURITY™ sind auch Marken von Lookout, Inc. Alle anderen Logos und Markenzeichen sind Eigentum ihrer eingetragenen Besitzer.
20210406-Lookout-DEv1.0

Lookout®