Lookout®

LOOKOUT MOBILE ENDPOINT SECURITY

PROTÉGEZ L'APPAREIL QUI VOUS SUIT PARTOUT

Ne négligez pas l'appareil que vous utilisez le plus

Depuis longtemps, les stratégies de cybersécurité traditionnelles sont axées sur la protection de vos terminaux fixes, notamment les serveurs, ordinateurs portables et ordinateurs de bureau, contre les cybermenaces. Cependant, vos besoins en sécurité ont évolué à grande vitesse au fil du temps.

Le problème, c'est que la sécurité des terminaux mobiles est souvent négligée, ce qui crée une faille dans votre architecture de sécurité. Bien que les systèmes d'exploitation mobiles soient considérés comme plus résilients, les pirates informatiques les ciblent de plus en plus car les appareils mobiles sont au croisement de votre vie privée et de votre vie professionnelle. Regorgeant de données, ces appareils sont une mine d'or pour les pirates informatiques, qui les utilisent comme une porte d'entrée dans votre organisation.

Lorsque vous évaluez les différentes solutions de sécurité mobile à ajouter à votre architecture, vous êtes confronté à un défi familier : choisir entre une plateforme complète ou une solution de pointe. Dans la mesure où l'engouement à l'égard des appareils mobiles et du Cloud a pris de l'ampleur de manière proportionnelle, une solution de sécurité du terminal au Cloud promet de réduire les contraintes, d'améliorer l'ergonomie et le confort, d'offrir une certaine liberté à l'utilisateur et de diminuer le coût opérationnel par rapport à une série de solutions autonomes.

AVANTAGES

- Sécurité mobile reposant sur le Cloud
- Protection des appareils iOS, Android et Chrome OS
- Détection et réponse au niveau des terminaux, conçues par des chercheurs sur les menaces
- Application légère optimisée pour les performances du processeur et la durée de vie de la batterie
- Sécurisation des terminaux de l'entreprise et de l'employé
- Respect des exigences de conformité et de la vie privée de l'utilisateur
- Déploiement fluide sur tous les appareils des employés
- Adaptation aux parcs mobiles de centaines de milliers de terminaux

Aujourd'hui, plus de la moitié des appareils que les employés utilisent pour accéder aux données de votre organisation exécutent iOS, Android et Chrome OS.

Le mobile a ouvert de nouveaux horizons aux pirates informatiques

La sécurisation des appareils mobiles est radicalement différente de celle des ordinateurs de bureau et des ordinateurs portables. Bien que les menaces qui touchent les appareils mobiles soient très similaires à celles qui touchent les ordinateurs portables, l'approche utilisée pour les protéger est différente. Par conséquent, vous devez tenir compte des nouvelles exigences de sécurité introduites par votre parc mobile.

Les risques mobiles impliquent une protection moderne des terminaux

Bien que les systèmes d'exploitation mobiles soient plus résilients, les pirates informatiques les ciblent de plus en plus car ils sont au croisement de votre vie privée et de votre vie professionnelle. Regorgeant de données, les appareils iOS, Android et Chrome OS sont une mine d'or pour les pirates informatiques, qui les utilisent comme une porte d'entrée dans votre entreprise.

Un vecteur d'attaque courant consiste à utiliser des logiciels malveillants mobiles pouvant inclure des logiciels espions, des chevaux de Troie bancaires et des rootkits. Les logiciels malveillants peuvent être transmis par les connexions cellulaires, Wi-Fi et Bluetooth des appareils mobiles. Dès que le logiciel malveillant est exécuté, il compromet la sécurité globale de l'appareil mobile.

Une protection moderne des terminaux doit détecter les menaces au sein des applications, de l'appareil et des connexions réseau. Elle doit protéger l'utilisateur, l'appareil et l'entreprise tout en respectant leur confidentialité. Elle doit traiter de manière égale les appareils de l'employé et ceux de l'entreprise.

> **« La sécurité mobile est passée d'un outil pour les secteurs très réglementés et les organismes gouvernementaux à une solution de sécurité essentielle pour toutes les organisations. »**
>
> - **Phil Hochmuth**, Vice-président du programme, Mobilité d'entreprise, IDC

Ne laissez pas le phishing mobile être la porte d'entrée du pirate informatique

Les approches anti-phishing traditionnelles utilisées sur les appareils mobiles soulèvent rapidement un problème de confidentialité dans la mesure où elles consistent à inspecter des e-mails pour bloquer les attaques. Tous les appareils mobiles, même ceux fournis par l'entreprise, sont considérés comme des appareils personnels. Le simple fait d'inspecter le contenu des e-mails ne permet pas de détecter les autres méthodes utilisées pour envoyer un lien de phishing à un utilisateur mobile.

La plupart des solutions anti-phishing s'appuient sur une liste de domaines et d'adresses Web malfaisants. Cependant, plus de 1,5 million de sites de phishing mobile sont créés chaque mois. La plupart des sites de phishing sont créés et supprimés en quelques heures ou quelques jours. S'appuyer seulement sur des méthodes basées sur la réputation pour détecter une attaque de phishing mobile est insuffisant.

> **1 utilisateur professionnel sur 50** est la cible de tentatives de phishing au quotidien et **87 % des attaques de phishing mobile** ne concernent pas des e-mails.

Vous devez connaître les bonnes versions d'applications et d'OS pour que vos correctifs soient efficaces

La gestion traditionnelle des correctifs et des vulnérabilités était axée sur les serveurs plutôt que sur les terminaux. En effet, les ordinateurs portables et de bureau étaient gérés, utilisaient une image commune et étaient régulièrement corrigés. Par conséquent, le principal risque de vulnérabilité était le serveur non corrigé.

Aujourd'hui, seule la gestion des appareils mobiles (MDM) permet de garantir que les appareils mobiles exécutent une version de système d'exploitation minimale. Néanmoins, comme les employés utilisent de plus en plus des tablettes et smartphones personnels non gérés pour le travail, la MDM n'est pas en mesure d'assurer une couverture complète. La gestion traditionnelle des vulnérabilités ne peut pas combler cette lacune puisqu'elle porte sur les appareils qui se connectent au réseau de l'entreprise, et non aux réseaux Wi-Fi ou cellulaires de la maison.

> Selon le Financial Times, une vulnérabilité de WhatsApp permettait de diffuser des logiciels espions sur les appareils iOS et Android sans aucune interaction de l'utilisateur. Sans même répondre à un appel, l'appareil pouvait être compromis[1].

1. Srivastava, Mehul, Financial Times, « WhatsApp voice calls used to inject Israeli spyware on phones », 13 mai 2019

Le mobile doit être inclus dans votre Zero Trust Network Architecture

La liberté que les smartphones et tablettes nous ont offerte n'est pas sans risque. Chacun de nous représente désormais un réseau d'entreprise distant qui doit être sécurisé. Tandis que nous continuons à travailler hors de la portée du périmètre de sécurité existant, nous n'avons aucune garantie quant aux utilisateurs et aux appareils dans lesquels nous pouvons avoir confiance.

Vos utilisateurs mobiles n'utilisent pas de VPN pour se connecter aux données de votre organisation dans le Cloud. Ils ont besoin d'y accéder n'importe où et vous devez vérifier qu'ils ne font pas courir un risque à vos données sensibles. Seuls des appareils présentant un risque faible doivent être autorisés à accéder aux ressources de votre organisation. Une fois l'accès octroyé, une évaluation continue des risques vous permet de modifier les accès de manière dynamique pour protéger vos données.

> « L'authentification d'utilisateurs sur des appareils personnels au moyen de l'approche ZTNA [Zero Trust Network Access] peut renforcer la sécurité et faciliter les programmes BYOD (Bring Your Own Device) en réduisant les exigences de gestion complètes et en permettant un accès applicatif direct plus sécurisé » [2].

Gagnez une meilleure visibilité sur les applications pour réduire les risques

La plupart des organisations disposent d'une visibilité sur la manière dont les applications des ordinateurs portables et de bureau traitent les données, mais cela ne s'applique pas aux appareils mobiles. En raison de la manière dont iOS, Android et Chrome OS exécutent leurs applications, il est difficile de les inspecter. Sans cette inspection, votre équipe de sécurité n'aura aucune idée de la manière dont ces applications traitent vos données.

Avec des appareils gérés, vous avez une visibilité et un contrôle sur les applications que vos employés utilisent via la gestion des appareils mobiles (MDM) ou la gestion des applications mobiles (MAM). Toutefois, cela ne vous renseigne pas sur les autorisations de l'application et les contrôles d'accès aux données en temps réel. Avec des appareils personnels non gérés, vous n'avez même pas la visibilité limitée que vous offrent les solutions de MDM et de MAM.

> « D'ici à 2022, l'approche BYOD (Bring Your Own Device) représentera plus de 75 % des smartphones apportés par les employés au sein de l'entreprise, ce qui obligera à migrer de la gestion centrée sur les appareils à la gestion centrée sur les applications et les données » [3].

Évitez les failles au moyen d'outils dédiés à la détection et à la correction d'incidents

Tandis que de nombreuses organisations assurent un suivi complet de l'activité des serveurs, des ordinateurs de bureau et des ordinateurs portables, il leur manque la même télémétrie pour les appareils iOS, Android et Chrome OS. Plus les employés utilisent leurs appareils mobiles pour le travail, plus les attaques se multiplient sur ces mêmes appareils.

Pour stopper efficacement les violations de données, les équipes de sécurité ont besoin des mêmes données complètes pour les appareils mobiles que celles qu'ils ont pour les serveurs, ordinateurs de bureau et ordinateurs portables. Étant donné que les systèmes d'exploitation mobiles n'ont jamais autorisé l'accès au noyau et qu'ils exigeaient que les applications fonctionnent de manière isolée, il a été supposé à tort qu'il était impossible de collecter une télémétrie complète.

> D'ici à la fin de l'année 2023, plus de 50 % des entreprises auront remplacé leurs anciens produits antivirus par des solutions EPP et EDR combinées qui compléteront la prévention par des capacités de détection et de réponse[4].

La sécurité mobile doit être intégrée à votre architecture de sécurité globale

Certaines organisations gèrent les appareils mobiles de leurs employés avec des outils tels que la gestion des appareils mobiles (MDM) ou la gestion unifiée des terminaux (UEM). Elles s'appuient également sur une solution Security Information and Event Management (SIEM) pour agréger les renseignements sur les menaces. Des intégrations préconçues avec des solutions MDM/UEM et SIEM vous permettront de maximiser la valeur immédiate que vous pourrez tirer d'une solution de sécurité mobile.

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

« Le marché de la sécurité mobile est davantage axé sur les partenariats, les intégrations et les écosystèmes que sur la prévention et la correction des menaces (bien que ces capacités de base soient certainement importantes). Intéressez-vous aux fournisseurs qui ont des partenariats solides avec des canaux clés, tels que des opérateurs mobiles, et des intégrations robustes avec des plateformes EMM/SIEM. »

- **Phil Hochmuth**, Vice-président du programme, Mobilité d'entreprise, IDC

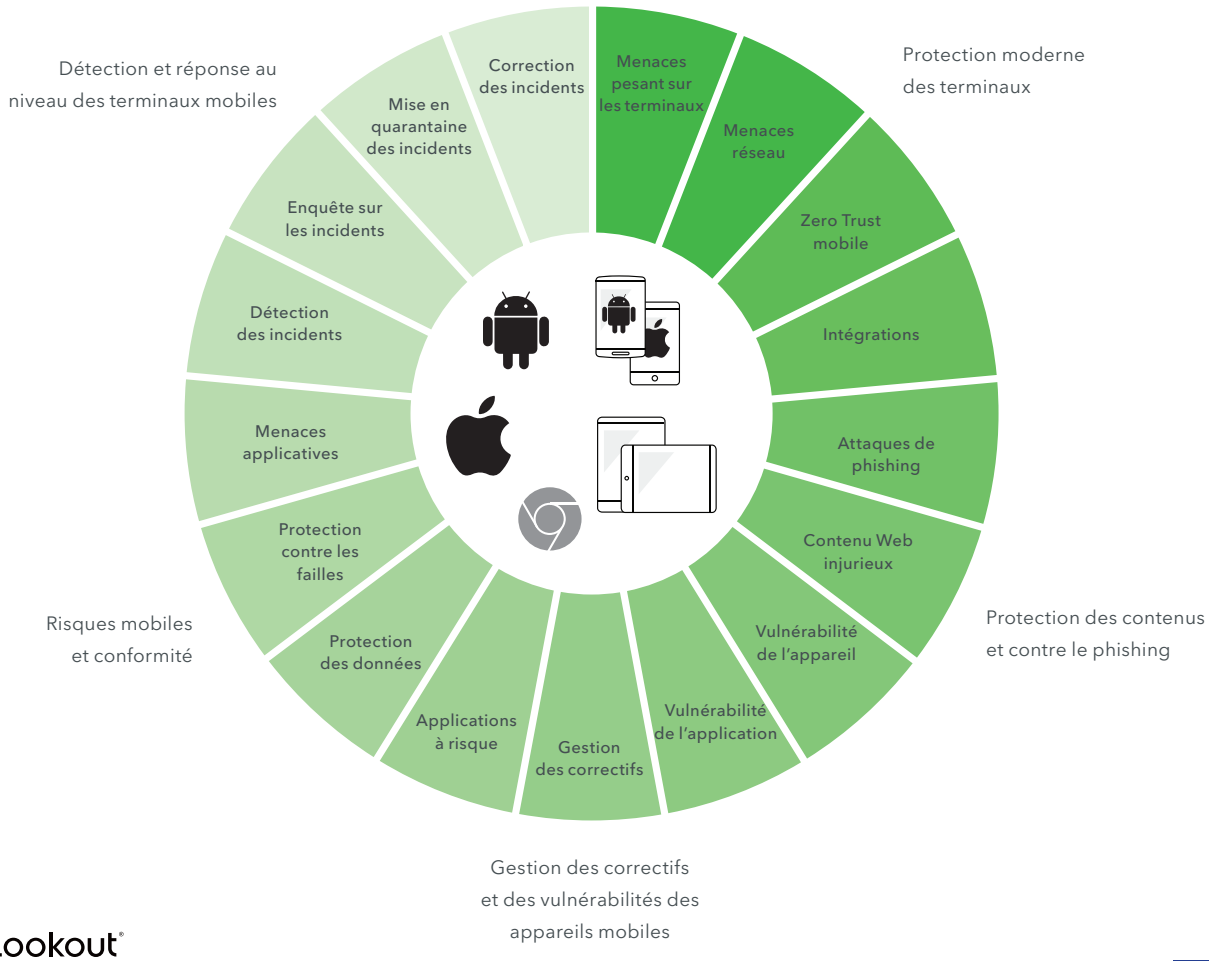
Une sécurité au niveau des terminaux initialement conçue pour le mobile

La solution Lookout Mobile Endpoint Security (MES) est conçue pour répondre à l'évolution constante de vos besoins en sécurité mobile. Lookout MES s'appuie sur Lookout Security Graph et s'adapte à des centaines de milliers de terminaux. Avec ses modules Cloud, vous pouvez personnaliser Mobile Endpoint Security en fonction de vos besoins.

Notre solution Security Graph s'appuie sur l'intelligence artificielle pour vous protéger contre les menaces connues et inconnues. Nous disposons du plus vaste ensemble de données mobile, constitué grâce à l'analyse de plus de 200 millions d'appareils mobiles et plus de 135 millions d'applications. Nos algorithmes parcourent Internet au quotidien pour trouver des sites Web spécialement conçus pour le phishing, et un nombre incalculable d'applications ont été analysées par notre API.

Que vous téléchargiez des applications comportant de nouveaux logiciels malveillants ou que vous soyez la cible du dernier ransomware ou de la dernière attaque de phishing, vous êtes protégé sans avoir à lever le petit doigt. Lorsqu'une menace vous cible ou qu'une attaque survient, nous vous fournissons des instructions étape par étape pour enquêter sur ce qui se passe et trouver une manière d'y remédier.

Lookout Mobile Endpoint Security



À propos de Lookout

Lookout est une entreprise leader dans la cyber sécurité. Notre mission est de sécuriser et de dynamiser notre futur digital dans un monde ou la mobilité et le cloud sont omniprésents dans nos activités. Nous permettons aux consommateurs et aux employés de protéger leurs données et de rester connectés en toute sécurité sans violer ni leur vie privée ni leur confiance. Lookout bénéficie de la confiance de millions d'utilisateurs particuliers, d'entreprises, d'administrations publiques et de partenaires tels qu'AT&T, Verizon, Vodafone, Microsoft, Google et Apple.Lookout a son siège social à San Francisco et possède des bureaux à Amsterdam, Boston, Londres, Sydney, Tokyo, Toronto et Washington D.C. Pour en savoir plus, rendez-vous sur Lookout a son siège social à San Francisco et possède des bureaux à Amsterdam, Boston, Londres, Sydney, Tokyo, Toronto et Washington D.C. Pour en savoir plus, rendez-vous sur **www.lookout.com/fr** et suivez Lookout sur son **blog**, sur **LinkedIn** et sur **Twitter**.

Pour en savoir plus, rendez-vous sur
lookout.com/fr

Demandez une démo sur
lookout.com/fr/info/fr-enterprise-contact-us

Une sécurité complète, du terminal jusqu'au Cloud

Plus d'informations sur **lookout.com/fr**

Lookout®