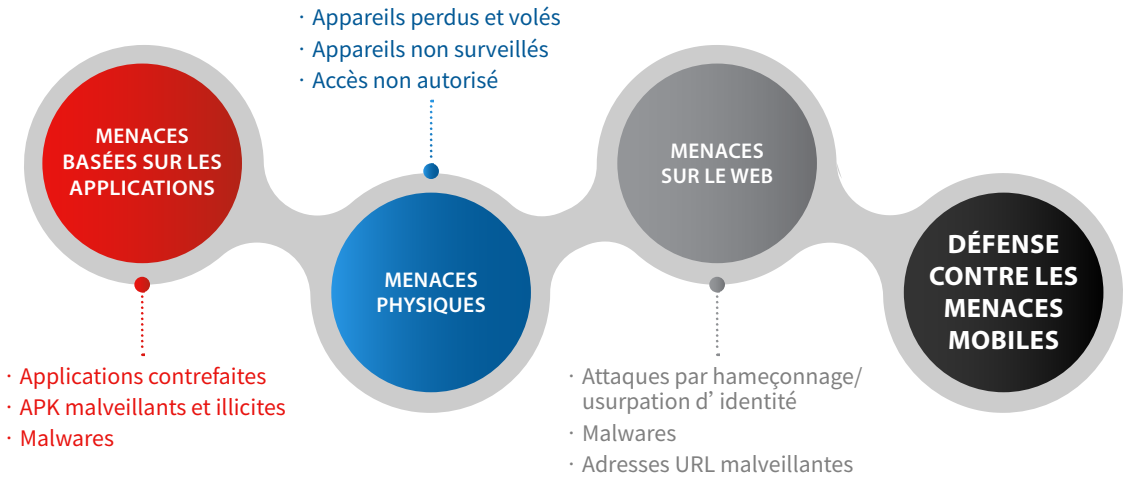
FICHE TECHNIQUE

WATCHGUARD MOBILE SECURITY

LES PETITS APPAREILS PEUVENT CAUSER DE GROS PROBLÈMES

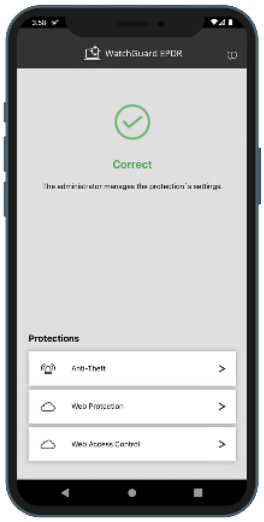
Face à l'ampleur et à la diversité des menaces sur les appareils mobiles, les entreprises ont besoin de solutions de sécurité pour les protéger. Cela est d'autant plus vrai que le nouveau lieu de travail hybride, avec des possibilités de travail à distance et à domicile, fait de ces appareils mobiles un élément plus courant et plus critique de l'infrastructure informatique d'une entreprise.

Il est plus que jamais essentiel pour les entreprises de sécuriser les postes de travail et leurs données afin d'éviter les violations de données et l'accès non autorisé aux informations sensibles.



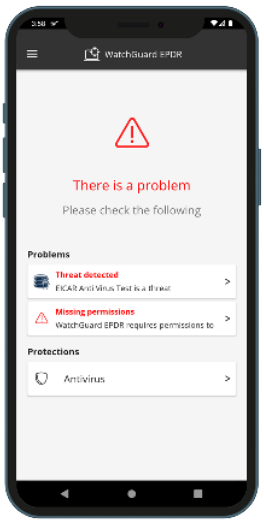
POURQUOI CHOISIR MOBILE SECURITY ?

WatchGuard Mobile Security permet aux entreprises de centraliser la gestion de la sécurité et de la confidentialité des données stockées sur leurs smartphones et tablettes Android et iOS sans nécessiter de connaissances techniques particulières ou de serveurs de sécurité dédiés on-premise. En outre, les outils que la suite fournit sont disponibles partout et à tout moment pour protéger les appareils mobiles des malwares, pertes et vols.



La productivité est désormais mobile

- Les données de l'entreprise sont de plus en plus souvent consultées sur des appareils mobiles situés en dehors de son périmètre. C'est pourquoi les employés travaillant à distance ont accéléré le processus d'adoption des appareils mobiles dans les entreprises.
- La sécurisation des appareils mobiles dans l'entreprise ne représente que la moitié du problème. L'autre moitié consiste à s'assurer que les employés sont en mesure de travailler efficacement.
- Mettez les employés en confiance quant à la sécurité de leurs appareils mobiles et fournissez un lieu de travail moderne où la sécurité et l'efficacité sont à égalité.



Cybermenaces mobiles potentielles

- Les menaces physiques qui pèsent sur les appareils mobiles concernent le plus souvent la perte ou le vol, ce qui permet aux pirates informatiques d'avoir un accès direct au matériel où sont stockées les données privées.
- Les menaces basées sur les applications : les utilisateurs téléchargent des applications qui semblent légitimes mais qui, en réalité, volent des données de leur appareil.
- Menaces sur le Web : les utilisateurs visitent des sites infectés qui semblent normaux à première vue mais qui, en réalité, téléchargent automatiquement des contenus malveillants sur les appareils. Les tentatives d'hameçonnage sur mobile ne cessent de croître chaque année.

Une application de gestion des terminaux mobiles (MDM) n'est pas suffisante

- L'outil de gestion MDM permet d'administrer les appareils mobiles, et non de les sécuriser. L'outil MDM est important mais il ne constitue qu'un seul élément.
- Les stratégies BYOD (Bring Your Own Device) constituent un véritable défi pour les professionnels de la sécurité, car un mauvais clic de la part de l'utilisateur peut avoir de graves conséquences. À mesure que les malwares se développent et évoluent, il est de plus en plus difficile de repérer une menace une fois qu'elle s'est infiltrée dans le réseau.
- WatchGuard Mobile Security peut détecter et empêcher les menaces de cybersécurité mobile de nuire à votre entreprise.

AMÉLIORER LA SÉCURITÉ DE L'ENTREPRISE AVEC MOBILE SECURITY

CATÉGORIES	FONCTIONNALITÉS	ANDROID	iOS
Analyse des malwares	Analyse des APK malveillants	✓	
	URL des malwares*		✓
	Analyses à la demande	✓	
	Analyses planifiées	✓	
	Protection antivirus en temps réel	✓	
Protection sur le Web	Filtrage des URL*		✓
	Anti-hameçonnage*		✓
Antivol	Verrouillage à distance	✓	✓
	Effacement à distance	✓	✓
	Géolocalisation	✓	✓
	Cliché et localisation du voleur	✓	
	Alarme à distance	✓	✓
Génération de rapports de sécurité unifiés	Alertes en cas de malware	✓	✓
	Alertes en cas d'appareils non protégés	✓	✓
	Rapports centralisés	✓	✓
Déploiement	Sans MDM	✓	✓
	Utilisant notre WatchGuard MDM		✓
	MDM tiers	✓	✓
	"Appareils supervisés/non supervisés"		✓
	Mises à niveau de la protection	Google Play	Apple Store

* Le mode supervisé d'iOS permet aux administrateurs d'utiliser ces fonctionnalités supplémentaires, tandis que le mode non supervisé ne permet que les fonctionnalités de base.

Solutions compatibles dans la plateforme Endpoint Security pour Android et iOS :

WatchGuard EPDR WatchGuard EPP Configuration système requise pour Android Configuration système requise pour iOS

SERVICE COMMERCIAL FRANCE +33 97 755 4336 ADRESSE EMAIL france@watchguard.com SITE INTERNET www.watchguard.com/fr WatchGuard Technologies, Inc.