PRADEO SECURITY

PROTECTION DE FLOTTE MOBILE

Protection de la flotte mobile face au spectre complet des menaces mobiles

Les smartphones, tablettes et applications multiplient les points d'accès aux SI des entreprises. Aujourd'hui, les équipes de sécurité recherchent des solutions simples à déployer, qui vont renforcer leur conformité aux réglementations et **prévenir intégralement du vol ou de la fuite de données** professionnelles sensibles.

Pradeo Security est reconnu comme **leader** par :

IDC Gartner FROST & SULLIVAN

Securité «on-device» au niveau applicatif, réseau et OS

Un mobile peut être compromis par 3 vecteurs : les applications, le réseau et l'OS. La protection de flotte mobile Pradeo Security protègent tous ces points d'entrés.

Menaces **applicatives**	Menaces **réseau**	Menaces **OS**
76%	16%	8%

Déploiement d'agent 0-touch

Agent préconfiguré pour un **déploiement simple** et une adoption générale

Synchronisation avec les UEM

Suivi de la conformité dans l'interface MDM et activation d'un **accès contionnel**

Remédiation en temps réel

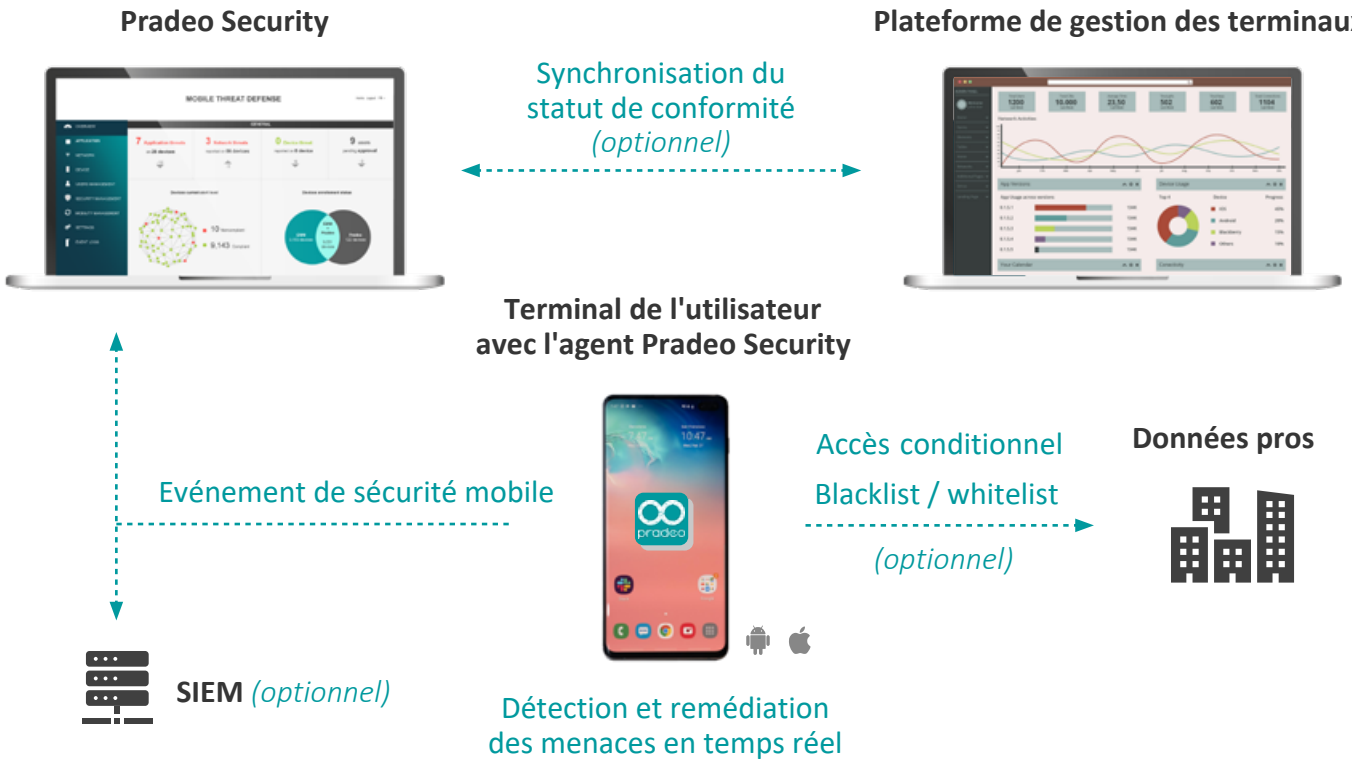
Blocage immédiat des menaces détectées en accord avec la **politique de sécurité** définie

Reporting simple

Visibilité sur **toutes les menaces mobiles** détectées sur la flotte

Intégré avec BlackBerry IBM MaaS360 Microsoft SOTI vmware SAMSUNG Knox Manage SAMSUNG SDS

Comment ça fonctionne



Couverture de détection des menaces

Détection des menaces applicatives

Détection de toutes les attaques d'exécution de code et des comportements intrusifs pour empêcher **l'exfiltration de données, le vol de données et la fraude.**

- Malwares inconnus
- Screenlogger
- Keylogger
- Data sending trojan
- SMS trojan
- Ransomware
- Overlay
- Application intrusive et qui fuite les données

Détection des menaces réseau

Détection de toutes les exploitations de réseau pour prévenir l**e vol de données et les écoutes.**

- Attaque Man-in-the-Middle
- Atatque de phishing
- Activité NFC anormale
- Activité Bluetooth anormale
- Connexion à un point d'accès pirate
- Connexion WiFi non sécurisée
- Connexion à un proxy malicieux
- Connexion VPN
- Prise de contrôle
- Pharming

Détection des menaces OS

Détection de toutes les utilisations abusives du terminal afin d'éviter **l'escalade des privilèges, la prise de contrôle et le vol de données.**

- Vulnérabilité OS
- Root / Jailbreak
- Profil malveillant
- Prise de contrôle
- Consommation de la batterie
- Certificat inconnu
- Mode debug
- Sources inconnues
- Mode accessibilité