PRADEO SECURITY

MOBILE THREAT DEFENSE

Mobile fleet protection from the full spectrum of mobile threats

Smartphones, tablets and mobile apps multiply the access points to companies' information systems. Today, security teams are looking for solutions that are **easy to deploy**, that will reinforce their **compliance** to data protection regulations and that will fully **prevent the theft and leakage** of sensitive corporate data.

Pradeo Security is recognized as **leader** by

IDC Gartner FROST & SULLIVAN

On-device security at the applicative, network and device levels

A mobile device can be breached through the exploit of 3 vectors: applications, the network and the OS. Pradeo Security Mobile Threat Defense secures all of these entry points.

Application threats	Network threats	OS threats
76%	16%	8%

Easy Deployment

Pre-configured agents for a burden-less deployment and full adoption

MDM synching

Compliance tracking in MDM interface and enablement of conditional access

Real-time remediation

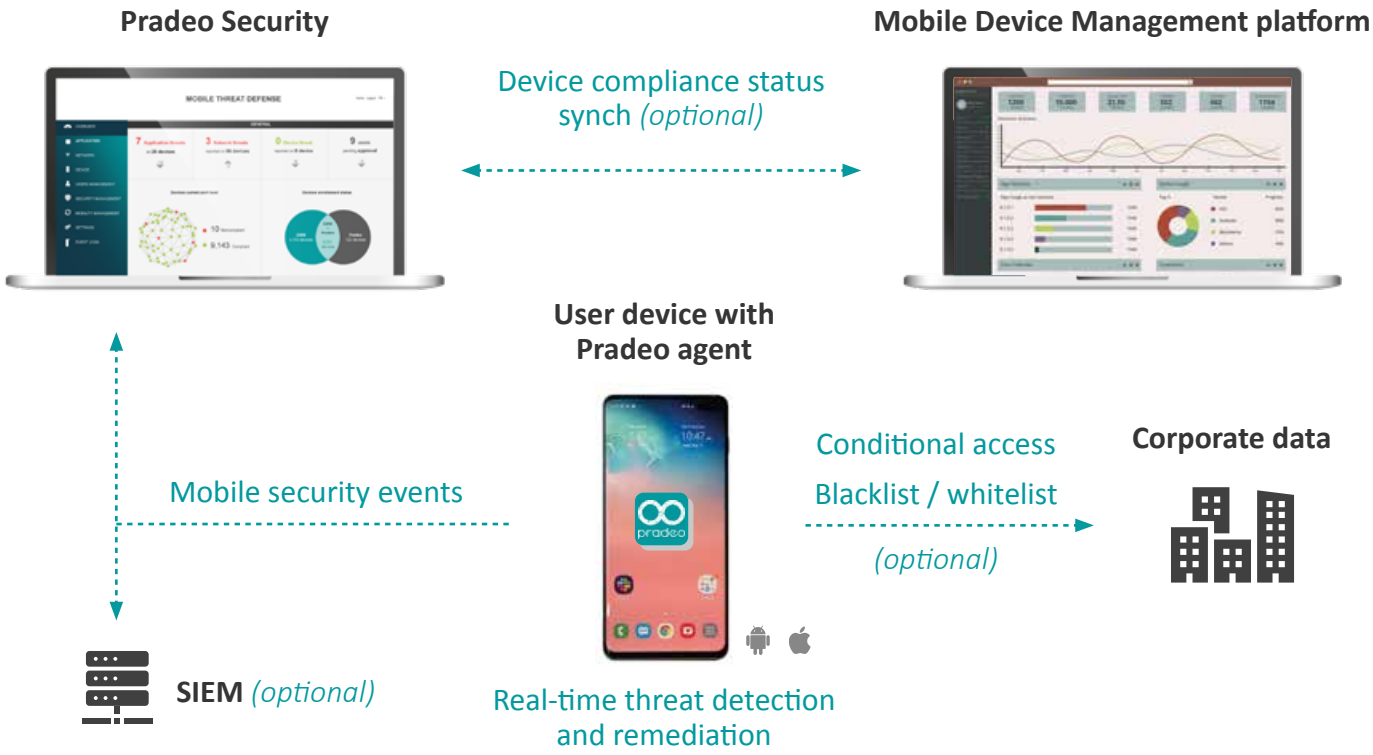
Immediate blocking of threats detected according to the chosen security policy

Comprehensive reporting

Visibility on all mobile threats detected on the fleet

Integrated with BlackBerry IBM MaaS360 ivanti Microsoft SOTI vmware SAMSUNG Knox Manage SAMSUNG SDS

How it works



Threat detection coverage

Application-borne threat detection

Detection of all code execution attacks and leaky behaviors to **prevent data exfiltration, data theft and fraud.**

- 0-day malware
- Screenlogger
- Keylogger
- Data sending trojan
- SMS trojan
- Ransomware
- Overlay
- Intrusive application
- Leaky application

Network-borne threat detection

Detection of all network exploits to prevent **data theft and eavesdropping.**

- Man-in-the-Middle attack
- Phishing attack
- NFC abnormal activity
- Bluetooth abnormal activity
- Rogue cell tower connection
- Unsecure WiFi connection
- Malicious proxy connection
- VPN connection
- Session highjacking
- Pharming

Device-borne threat detection

Detection of all device misuses to prevent **privilege escalation, takeover and data theft.**

- OS vulnerability
- Root / Jailbreak
- Hidden root / Jailbreak
- Malicious profile
- System takeover
- Abnormal battery consumption
- Non-trusted certificate
- Debug mode
- Authorized unknown source
- Accessibility mode