

► KASPERSKY SECURITY FOR MOBILE

Sicurezza multilivello, gestione e controllo per gli endpoint mobili

I dispositivi mobili diventano un bersaglio sempre più allettante per i cybercriminali. Intanto, la tecnologia BYOD (Bring Your Own Device) contribuisce a una combinazione di dispositivi sempre più complessa, creando un ambiente di gestione e controllo impegnativo per gli amministratori IT. Kaspersky Security for Mobile protegge il dispositivo, ovunque si trovi. Protezione dal malware mobile in continua evoluzione. Visibilità e controllo rapidi e semplici per gli smartphone e i tablet inclusi nell'ambiente, da un'unica posizione centrale e con interruzione delle attività ridotta al minimo.

- Potente protezione anti-malware
- Anti-phishing e anti-spam
- Protezione Web
- Controllo delle applicazioni
- Rilevamento dei tentativi di rooting e jailbreaking
- Containerization
- Protezione contro i furti
- Mobile Device Management
- Portale self-service
- Gestione centralizzata
- Console Web
- Piattaforme supportate:
 - Android™
 - iOS
 - Windows Phone

CARATTERISTICHE PRINCIPALI

ANTI-MALWARE AVANZATO PER DISPOSITIVI MOBILI E SICUREZZA DEI DATI

Solo nel 2014, Kaspersky Lab ha rilevato quasi 1,4 milioni di attacchi malware unici a dispositivi mobili. Kaspersky Security for Mobile combina l'anti-malware con livelli avanzati di tecnologie di protezione, difendendo dalle minacce sconosciute e conosciute i dati memorizzati sui dispositivi mobili.

MOBILE DEVICE MANAGEMENT (MDM)

L'integrazione con le principali piattaforme di dispositivi mobili consente la distribuzione e il controllo remoti "Over the Air" (OTA) per una maggiore facilità d'uso e gestione dei dispositivi Android, iOS e Windows Phone.

MOBILE APPLICATION MANAGEMENT (MAM)

Le capacità di containerization e cancellazione selettiva consentono la separazione dei dati aziendali da quelli personali nello stesso dispositivo, supportando le iniziative BYOD. Insieme alle funzionalità di crittografia e antimalware, queste rendono Kaspersky Security for Mobile una soluzione di protezione mobile proattiva, anziché una che si limita a tentare di isolare un dispositivo e i suoi dati.

GESTIONE CENTRALIZZATA

Gestione di più piattaforme e dispositivi dalla console, aumentando la visibilità e il controllo senza altre attività o tecnologie da gestire.

FUNZIONALITÀ DI SICUREZZA MOBILE E GESTIONE

POTENTE PROTEZIONE ANTI-MALWARE

Protezione basata su firme, proattiva e assistita da cloud (tramite Kaspersky Security Network - KSN) contro le minacce malware conosciute e sconosciute. Scansioni su richiesta e programmate, combinate con gli aggiornamenti automatici per aumentare la protezione.

ANTI-PHISHING E ANTI-SPAM

Le potenti tecnologie anti-phishing e anti-spam proteggono il dispositivo e i suoi dati dagli attacchi di phishing e aiutano a filtrare chiamate e messaggi indesiderati.

WEB CONTROL/SAFE BROWSER

Supportate da Kaspersky Security Network (KSN), queste tecnologie funzionano in tempo reale per bloccare l'accesso ai siti Web nocivi e non autorizzati. La funzione Safe Browser fornisce l'analisi dei dati di reputazione costantemente aggiornati, garantendo la navigazione mobile sicura.

CONTROLLO DELLE APPLICAZIONI

Integrata con KSN, l'Application Control limita l'utilizzo delle applicazioni al solo software approvato, vietando l'impiego di software indesiderato o sconosciuto. La funzionalità del dispositivo dipende così dall'installazione delle applicazioni richieste. Il controllo dell'inattività delle applicazioni consente agli amministratori di richiedere il nuovo accesso dell'utente a un'applicazione dopo che è trascorso un periodo di inattività specificato. Questo protegge i dati anche se un'applicazione è aperta quando il dispositivo viene smarrito o rubato.

RILEVAMENTO DEI TENTATIVI DI ROOTING E JAILBREAKING

Rilevamento e report automatici di tentativi di rooting o jailbreaking possono essere seguiti dal blocco automatico dell'accesso ai contenitori, dalla cancellazione selettiva o dalla cancellazione totale del dispositivo.

Modalità di acquisto

Kaspersky Security for Mobile è incluso in:

- Kaspersky Endpoint Security for Business – Select
- Kaspersky Endpoint Security for Business – Advanced
- Kaspersky Total Security for Business

Kaspersky Security for Mobile può inoltre essere acquistato separatamente come soluzione mirata.

Contatta il tuo rivenditore per i dettagli e i prezzi.

CONTAINERIZATION

Separazione dei dati aziendali e personali isolando le applicazioni in contenitori. Per proteggere i dati sensibili si possono applicare criteri aggiuntivi come la crittografia. Con la cancellazione selettiva si eliminano i dati inseriti nei contenitori di un dispositivo, senza conseguenze per i dati personali dell'utente.

PROTEZIONE CONTRO I FURTI

Le funzionalità anti-furto includono il rilevamento del dispositivo con cancellazione, blocco del dispositivo, localizzazione, SIM watch, foto segnaletica e allarme e si possono attivare in caso di furto e smarrimento. A seconda del caso, i comandi antifurto si possono applicare in modo molto flessibile. Ad esempio, l'integrazione con Google Cloud Messaging (GCM) consente di inviare i comandi in modo immediato, abbreviando i tempi di reazione e migliorando la sicurezza, mentre l'invio di comandi tramite Portale Self-service non richiede azioni dell'amministratore.

MOBILE DEVICE MANAGEMENT (MDM)

Supporto per Microsoft Exchange ActiveSync, Apple MDM e Samsung KNOX 2.0: consente una vasta gamma di criteri con un'interfaccia unificata, indipendentemente dalla piattaforma. Ad esempio si possono attivare crittografia e password o controllare l'uso della fotocamera, applicando criteri a singoli utenti o gruppi, gestendo impostazioni APN/VPN e così via.

PORTALE SELF-SERVICE

Delegate la gestione della sicurezza di routine ai dipendenti, abilitando l'auto-registrazione dei dispositivi approvati. Durante il processo di abilitazione del nuovo dispositivo, tutti i certificati richiesti possono essere forniti in automatico attraverso il portale, senza necessità di intervento dell'amministratore. Nel caso di perdita del dispositivo, il dipendente può eseguire tramite il portale tutte le azioni anti-furto richieste.

GESTIONE CENTRALIZZATA

Gestione centralizzata di tutti i dispositivi mobili, da un'unica console, che consente anche la gestione della sicurezza IT per gli altri endpoint. Web Console consente agli amministratori di controllare e gestire da remoto i dispositivi, da qualunque computer.