

KASPERSKY SECURITY FOR MOBILE

رؤية أكثر وضوحًا للإدارة وأمن لنقاط النهاية بالأجهزة المحمولة - دون التعقيد المتعلق بحل منفصل.

ليس بالضرورة أن يكون نشر بيئة تكنولوجيا المعلومات لأجهزة المحمول لديك وإدارتها وتأمينها معقدًا أو مكلفًا. يعمل **Mobile Device Management (MDM)** على الحيلولة دون أي مشقة في عملية تكوين أمن الأجهزة المحمولة وتبسيطها، بينما يتم تثبيت **عمل متنقل** على الجهاز لتوفير الحماية التي تحتاج إليها للتصدي لتهديدات اليوم - حتى على الأجهزة التي يملكها الموظف!

◀ مثالي لمبادرات "إحضار الأجهزة الشخصية" (BYOD)

يستخدم الكثير من الموظفين أجهزتهم الخاصة لأداء كل من المهام الشخصية والخاصة بالشركة. وفي الواقع، تُشجع بعض المؤسسات العاملين لديها على اختيار هواتفهم الذكية أو الجهاز اللوحي المفضل لديهم من أحد الموزعين، ثم يضيف قسم تكنولوجيا المعلومات إلى الجهاز المملوك للمستخدم إمكانية استخدام البريد الإلكتروني والوصول إلى الشركة.

وعلى الرغم من الفوائد المتعلقة بالتوفير والإنتاجية، فيمكن أيضًا أن تعرض BYOD المؤسسة لمخاطر مرتبطة بالأمن. فمن السهل استغلال بيانات الشركة غير المؤمنة جيدًا والتي من المحتمل أن تكون متداخلة على نحو تبادلي مع البيانات الشخصية. كما يستخدم أفراد العائلة هذه الأجهزة غالبًا دون الاكتراث بأمن التطبيق. وقد يكون بعضها أيضًا تعرض لانتهاك امتيازات المستخدم الفائق أو قيود الجهاز.

يقوم Kaspersky Security for Mobile بحل هذه المشاكل عن طريق تمكين التكوين والنشر الآمن للهواتف الذكية والأجهزة اللوحية باستخدام نفس وحدة التحكم المستخدمة في أمن الشبكة. ويستطيع مسؤولو تكنولوجيا المعلومات الوثوق في تكوين أجهزة المستخدمين باستخدام الإعدادات الصحيحة وتأمين الأجهزة في حال فقدانها أو سرقتها أو إساءة استخدامها من قبل المستخدم.

الميزات الرئيسية:

- دعم الأجهزة اللوحية والهواتف الذكية
- التوفير عبر الأثير (OTA)
- أمن أجهزة المحمول المستند إلى العميل الذي أثبت كفاءته بمرور الوقت
- التنفيذ الآمن لـ APPLE MDM و MICROSOFT EXCHANGE و ACTIVESYNC
- التكامل الأصلي مع KASPERSKY SECURITY CENTER للتكوين والتحكم وتقديم التقارير والمخزونات وإعداد السياسة

الأنظمة الرئيسية المعتمدة للأجهزة المحمولة:

- iOS
- ANDROID™
- WINDOWS® PHONE
- WINDOWS MOBILE
- BLACKBERRY®
- SYMBIAN



