

Obrana proti hrozbám na mobilních zařízeních se systémy iOS, Android a Chromebook

GravityZone Security for Mobile

Chytré telefony a tablety změnilы způsob, jakým využíváme vzdálený přístup k práci. Spolu s pohodlím se na pracovišti objevila nová rizika, protože zaměstnanci mají přístup ke komunikačním kanálům, jako je e-mail, SMS zprávy a aplikace. Mnozí z nich mají prostřednictvím svých mobilních zařízení přístup k téměř stejným datům, jako v kanceláři: citlivým informacím o zákaznících a ke kritickým podnikovým systémům. Kompromitované mobilní zařízení může představovat významné riziko pro data zákazníků, duševní vlastnictví a klíčové systémy organizace.

GravityZone Security for Mobile chrání mobilní zařízení tak, aby zaměstnanci získali bezpečný přístup k firemním datům. Detekuje známé i neznámé hrozby, včetně útoků typu zero-day, phishingu a síťových útoků. Řešení chrání zařízení před primárními vektory útoků, i když zařízení není připojeno k síti.

Mobilní zařízení potřebují ochranu

- E-maily jsou nejčastějším vektorem phishingových útoků (90 %), a 60 % e-mailů je otevřeno na mobilních zařízeních
- 18 % rozkliknutých phishingových e-mailů pochází z mobilního zařízení
- 79 % lidí přiznalo, že používá služební zařízení k soukromým činnostem, jako je kontrola osobních e-mailů, nakupování nebo streamování.

Funkce

- **Ochrana aplikací** - využívá technologie umělé inteligence, v zařízení i mimo něj, k detekci škodlivých aplikací (Android a iOS).
- **Prověřování aplikací** - detekce aplikací, které nejsou v souladu s legislativou.
- **Ochrana webu** - ochrana proti phishingu a řízení přístupu k webu.
- **Ochrana sítě** - detekuje síťové hrozby, pokusy o průnik, slabá bezpečnostní rozhraní a útoky typu man-in-the-middle.
- **Ochrana zařízení** - detekuje zranitelnosti operačního systému, zařízení, která nelze aktualizovat, chybějící šifrování, jailbreak nebo root, zásahy do systému, apod.

Zkušební verze zdarma

GravityZone Security for Mobile si můžete [zdarma vyzkoušet](#).

Přehledně

GravityZone Security for Mobile poskytuje organizacím přehled o jejich mobilních zařízeních a souvisejících rizicích, aby bylo možné předcházet útokům, chránit je před útoky odhalovat napadená zařízení a reagovat na jejich případné napadení, a také integrovat mobilní zařízení do všech bezpečnostních struktur.

Hlavní výhody

- Viditelnost a ochrana proti mobilním hrozbám.
- Pokročilá kybernetická bezpečnost
- Zabezpečení, nezávislé na zařízení a platformě, pro systémy iOS, Android a ChromeOS.
- Komplexní přehled a kontrola napříč všemi platformami.
- Snižuje riziko krádeže dat, ztráty přístupových údajů a nesouladu s legislativou.