

Ochrona przed zagrożeniami dla urządzeń mobilnych z systemami iOS, Android i Chromebooków

GravityZone Security for Mobile

Smartfony i tablety zmieniły sposób, w jaki wykonujemy pracę zdalną. Oferując pracownikom dostęp do różnego rodzaju kanałów, takich jak poczta e-mail, wiadomości SMS, aplikacje i rozbudowane komunikatory, oprócz wygody przyniosły nowe zagrożenia. Wiele osób korzysta za pośrednictwem urządzeń mobilnych z dostępu do tych samych danych co w biurze: wrażliwych informacji o klientach i najważniejszych systemach firmowych. Urządzenie mobilne, którego warstwa zabezpieczeń została złamana, może stanowić poważne zagrożenie dla danych klientów, własności intelektualnej i podstawowych systemów organizacji.

GravityZone Security for Mobile chroni urządzenia mobilne, aby za ich pośrednictwem pracownicy mogli korzystać w bezpieczny sposób z dostępu do danych korporacyjnych. Wykrywa ono zarówno znane, jak i nieznane zagrożenia, w tym ataki typu 0-day, phishing i ataki sieciowe. Program zabezpiecza urządzenia mobilne przed głównymi wektorami ataków, nawet kiedy sprzęt nie jest podłączony do sieci.

Urządzenia mobilne potrzebują ochrony

- Wiadomości e-mail to główny cel wektorów ataku w przypadku phishingu (90%), a 60% z nich otwieranych jest na urządzeniach mobilnych.
- 18% przypadków kliknięć linku, stanowiącego źródło phishingu, to wiadomości e-mail otwarte na urządzeniach mobilnych.
- 79% osób przyznaje się do korzystania ze służbowego sprzętu mobilnego w celach osobistych, takich jak sprawdzanie prywatnych wiadomości e-mail, zakupy lub streaming.

Funkcje

- Ochrona aplikacji – wykorzystuje technologie sztucznej inteligencji w urządzeniu i poza nim do wykrywania złośliwych aplikacji (Android i iOS).
- Weryfikacja aplikacji – wykrywa aplikacje niezgodne z zasadami.
- Ochrona internetowa – zapobiega próbom phishingu i umożliwia zarządzanie dostępem do sieci.
- Ochrona sieci – wykrywa zagrożenia w sieci, próby wstępnego rozpoznania terenu, niebezpieczne połączenia sieciowe i ataki MITM (Man-in-the-Middle).
- Ochrona urządzenia – wykrywa luki w zabezpieczeniach systemu operacyjnego urządzenia, których nie da się zaktualizować, brakujące szyfrowanie, rootowanie i jailbreaking, ingerencje w ustawienia systemowe itp.

W skrócie

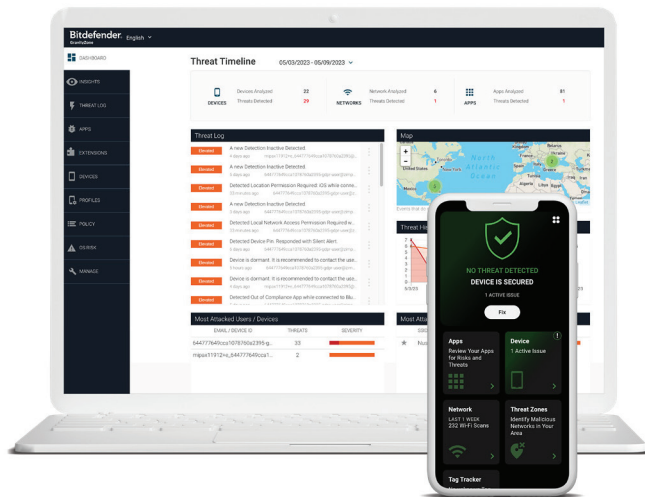
GravityZone Security for Mobile zapewnia firmom informacje na temat wpływu, jaki ich urządzenia mobilne wywierają na strukturę bezpieczeństwa, a także na kwestie związane z tymi zagrożeniami. Wszystko po to, aby zapobiegać atakom i chronić przed nimi Twoją organizację; wykrywać zagrożenia i szybko na nie reagować oraz integrować urządzenia mobilne z ogólnymi strukturami bezpieczeństwa.

Główne zalety

- Widoczność zagrożeń i ochrona przed nimi w urządzeniach mobilnych.
- Zaawansowana ochrona w obszarze cyberbezpieczeństwa w aplikacjach, ruchu sieciowym i na urządzeniach.
- Kompleksowe wykrywanie zagrożeń i kontrola zgodności z polityką firmy.
- Wszechstronna ochrona dla wszystkich urządzeń i platform na systemach iOS, Android i ChromeOS.
- Pełny wgląd i kontrola na wszystkich platformach.
- Obniża ryzyko kradzieży informacji, danych uwierzytelniających oraz braku zgodności.

GravityZone Cloud MSP Security for Mobile

GravityZone Cloud MSP Security for Mobile oferuje dostawcom usług zarządzanych narzędzia, których potrzebują do zapewnienia urządzeniom mobilnym bezpieczeństwa i ochrony przed potencjalnymi zagrożeniami. Dostawcy usług zarządzanych mogą mieć pewność, że ich dane i sieci pozostają bezpieczne, a informacje na temat klientów są chronione. To kompleksowe rozwiązanie do ochrony urządzeń mobilnych przed zagrożeniami (Mobile Threat Defence – MTD) posiada pojedynczą, łatwą w użyciu konsolę dla wielu użytkowników oraz elastyczny, miesięczny model licencjonowania.



Bezpłatna wersja próbna

Przetestuj GravityZone Security for Mobile za darmo, kliknij [tutaj](#).

Kontakt

Jeżeli chcesz uzyskać więcej informacji na temat GravityZone Security for Mobile, [skontaktuj się z nami](#).