A végpontvédelem fontosabb, mint bármikor

A digitális transzformáció és a rugalmas munkavégzés drámaian növelte a hálózatok sebezhetőségét. A gyengén védett felhasználói eszközökön és otthoni hálózatokon keresztül a malware, ransomware és más támadások erős kihívás elé állítják a vállalatokat. A támadások növekvő összetettsége és a zsarolóvírusok terjedése miatti aggodalmak – a vállalatok 85 százaléka a ransomware-t tartja a legnagyobb fenyegetésnek – rávilágítanak egy minden eddiginél erősebb végpontvédelmi igényre.

Az első generációs végpontvédelmi platformok (EPP-k), amelyek a gyártói támadás-elhárítási adatbázisokra hagyatkoztak, átengedik a teret a viselkedés alapú védekezésnek. Azonban még így sem nyújthat 100 százalékos biztonságot egy rendszer, ha hosszabb időtávon át és a támadások szofisztikáltságát figyelembe véve vizsgáljuk a hatékonyságot. Ennek megfelelően az első generációs EDR-termékek – amelyek a hagyományos végpontvédelmi rendszerek kiegészítései – sem birkóznak meg a növekvő számú és gyorsan változó támadással.

A riasztások áradatának kezelése és a valós fenyegetések kiszűrése a fals-pozitív eredmények közül időbe telik, így a security osztály egyre inkább lemarad az eseményekről, ezzel növelve a vállalat biztonsági kockázatait. Ez a hozzáállás folyamatos hibajavításokat eredményez, és már nem elegendő a mai szervezetek számára.

A modern végpontbiztonságnak egyesítenie kell ezeket a funkciókat a következő képességekkel:

– Támadások előrejelzése, megelőzése a támadási felület csökkentésével és a malware-ek kiszűrésével.

– Fenyegetések valós idejű észlelése, hatástalanítása.

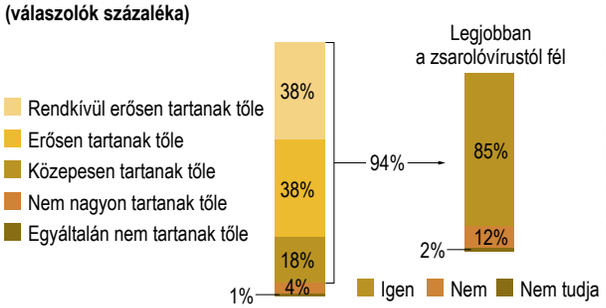
– Mélyelemzéssel támogatott összehangolt válaszlépés indítása.

A FortiEDR egységes végpontvédelmet nyújt

A kezdetektől fogva arra tervezték, hogy viselkedésalapú megközelítést alkalmazzon mind a támadások megelőzésében, az azok utáni védelem, a támadásészlelés és a válaszadás területén. Ez az egyedülálló kombináció automatikusan blokkolja, észleli és hatástalanítja a hálózati betöréseket és akadályozza meg a zsarolóvírus támadásokat.

Más EDR szállítók gyakran a kezdeti észlelésre adott kézi válaszokra támaszkodnak, amelyek behatárolása 30 perctől akár több óráig is eltarthat. A FortiEDR még a rosszindulatú beavatkozás előtt blokkolja a malware-ek külső kommunikációját, és megtagadja a fájlrendszerekhez való hozzáférést, ezzel valós időben megakadályozza a fájlok kiszivárgását és a zsarolóprogramok titkosítását. A fenyegetéseket a folyamatok megszakítása vagy a végpont karanténba helyezése nélkül is hatástalanítja. A rendszert annak működésében granuláris módon vizsgálja, így a legapróbb részletekig átláthatóvá teszi, és ezzel támogatja a blokkoló műveletek pontosságát. Ez csökkenti a fals-pozitív eredmények kockázatát, miközben számos kibertámadás végrehajtását akadályozza meg.

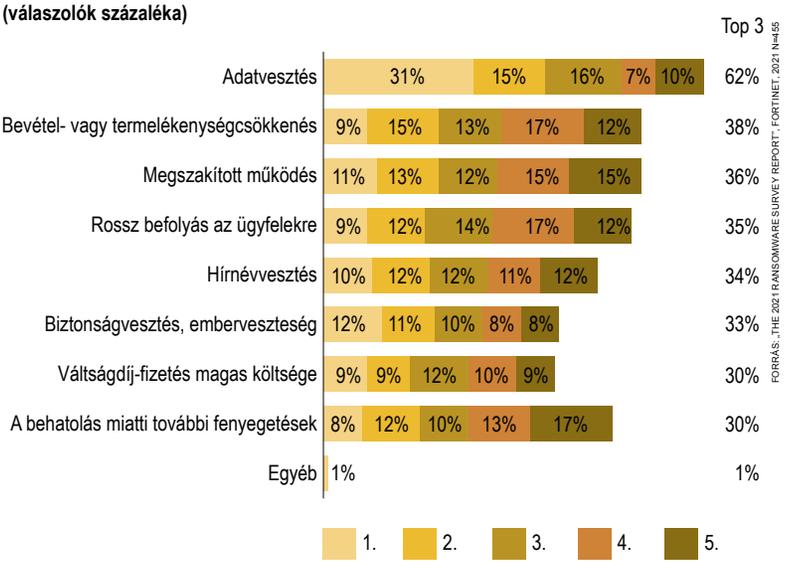
Nagyon félnek a cégek a zsarolóvírusoktól
(válaszolók százaléka)



FORRÁS: „THE 2021 RANSOMWARE SURVEY REPORT", FORTINET, 2021 N=455

Annak a 94%-nak, akik legalább közepesen tartanak a zsarolóvírusoktól a 85%-a az összes fenyegetés közül ezt tartja a legveszélyesebbnek.

A top 5 zsarolóvírus-kockázat
(válaszolók százaléka)



FORRÁS: „THE 2021 RANSOMWARE SURVEY REPORT", FORTINET, 2021 N=455

A FortiEDR automatizál

A FortiEDR a fentieken túl automatizálja a gyanús események folyamatos értékelését és osztályozását. A felhőalapú mesterséges intelligencia tovább elemzi a blokkolási küszöbérték alá eső észleléseket. Ítélet után a rendszer válaszlépést kezdeményez testre szabható playbookok alapján. Így a vállalatok előre meghatározhatják intézkedéseiket – a fenyegetések kategorizálása és jogosultságcsoportok alapján – az automatizált válasz- és helyreállítási eljárásokhoz.

A munkatársak így időt nyernek, hogy felügyeljék ezt a nagyrészt autonóm végpontbiztonsági megoldást, tanuljanak az azonosított kibertámadásokból, és folyamatosan emeljék a vállalat biztonsági szintjét.