kaspersky BRING ON THE FUTURE

Kaspersky Endpoint Detection and Response Optimum

Építsen ki igazi mélységi védelmet azonnali automatikus reagálással és egyszerű eredendőok-elemzéssel

A probléma

2019-ben az összes vállalat 91%-át érte valamilyen kibertámadás, amelyek közül **10-ből 1** célzott támadás volt[1].

Az összetett fenyegetések összeomláshoz vezethetnek

A végletekig egyszerű kártevő programok ideje rég elmúlt, és a fenyegetések mára sokkal összetettebbek, és egyre súlyosabb károkat és nagyobb üzleti veszteségeket okoznak, miközben hosszabb ideig felderítetlenek maradnak.

Önt is megtámadják

Ezek az összetett fenyegetések sokkal olcsóbbá és sokkal gyakoribbá váltak, így azoknak a vállalatoknak, amelyek azt gondolták, hogy nem kerülnek a látótérbe, most fedezniük kell a hátukat.

Nagyon fontos a hatékonyság

Az erőforráshiány – köztük a két legfontosabbé, az időé és a képzett szakembereké –, amit a vállalatok most átélnek, csak olaj a tűzre.

„A gyenge EPP-megoldások aláássák az EDR-eszközök hatékonyságát."[2]

„Így hát az ember és az idő lett az EDR-eszközök megtérülésének új mértékegysége."[2]

Így segíthetünk

A Kaspersky Endpoint Detection and Response (EDR) Optimum segít megőrizni a biztonságot az összetett és magas szintű fenyegetésekkel szemben. Ehhez fejlett észlelést, egyszerűsített vizsgálatot és automatikus reagálást használ.

Az alapszintű képességeken túl

Jó átláthatóságot, egyszerű vizsgálati eszközöket és automatikus reagálási lehetőségeket kínál annak érdekében, hogy a rendszer ne csak észlelje a fenyegetést, de feltárja annak teljes kiterjedését és eredetét is, és azonnal reagáljon is rá, megelőzve a vállalat működésének összeomlását.

Igazi mélységi védelem

Egy egyszerűen használható, magas szinten automatizált észlelő és reagáló eszközkészletet párosít a Kaspersky Endpoint Security for Business (Kaspersky vállalati végpontvédelem) páratlan végpontvédelmével és fejlett észlelési képességeivel, egyetlen egységes megoldást alkotva.

Az intelligens eszköz biztosítja a hatékonyságot

Egyszerű központi vezérlést és magas szintű automatizálást kínálva munkaidőt szabadít fel, és optimalizálja az emberi erőforrásokat és a fölös informatikai erőforrásokat. A gördülékeny munkafolyamat egyetlen helyi vagy akár számítási felhőben[3] lévő konzolról irányítható.

A legfőbb előnyök

- Megvédheti magát a leggyakoribb és legkártékonyabb magas szintű, összetett fenyegetésekkel szemben
- Időt és erőforrásokat takaríthat meg egy egyszerű, automatizált eszközzel
- Láthatja az összetett fenyegetés teljes kiterjedését az egész hálózaton
- Megismerheti a fenyegetés eredendő okát, és hogy konkrétan miként fordulhatott ez elő
- Gyors, automatikus reagálás segítségével elkerülheti a további károkat

Gyakorlati példák az EDR kritikus fontosságára

Válaszoljon néhány fontos kérdésre.

- Mi a riasztás környezete?
- Milyen intézkedések történtek már a riasztással kapcsolatban?
- Még mindig aktív az észlelt fenyegetés?
- Támadás ért más gazdagépeket is?
- Milyen útvonalon történt a támadás?
- Mi a fenyegetés tényleges eredendő oka?

Ismerje meg a fenyegetés teljes kiterjedését.

Amikor tudomására jut, hogy globális fenyegetésnek van kitéve – például abból, hogy a szabályozó hatóság kéri, hogy keressen adott sérülésjelző adatokat (IoC) –, a következőket teheti

- Megbízható forrásokból importál sérülésjelző adatokat, és rendszeres időközönként a támadás jeleit kutató vizsgálatot végez
- Alaposan megvizsgálja a riasztást, a felderített fenyegetések alapján saját sérülésjelző adatokat hoz létre, és vizsgálatot végez a teljes hálózaton, hogy kiderítse, érintett-e a támadás más gazdagépeket is

Azonnali reagálás a burjánzó fenyegetésekre

- Az összetett fenyegetéssel kapcsolatba hozható fájlok automatikus karanténba helyezése minden végponton
- A fertőzött gazdagépek automatikus leválasztása a hálózatról a gyorsan terjedő fenyegetéshez kapcsolódó sérülésjelző adatok vizsgálatának idejére
- A kártevő fájl futásának és a hálózaton való terjedésének megakadályozása a vizsgálat idejére

[1] The Kaspersky Global IT Risk Report (A Kaspersky globális informatikai veszélyekről szóló beszámolója), Kaspersky, 2019.

[2] IDC, Endpoint Security 2020: The Resurgence of EPP and the Manifest Destiny of EDR, Doc # US45794219, 2020 (IDC, Végpontbiztonság 2020: Az EPP (endpoint protection platform, végpontvédelmi platform) feltámadása és az EDR nyilvánvaló rendeltetése, US45794219 sz. dokumentum, 2020.)

[3] A számítási felhőben lévő konzolról kezelhető szolgáltatások és funkciók választékára vonatkozóan van néhány korlátozás. A részletes tudnivalókért lásd: https://kas.pr/epp-management-options.

Most a következőket teheti:

A fenyegetés teljes kiterjedésének megtekintése

Tekintse meg a végponton jelenlévő riasztásokat, és elemezze őket tovább, hogy megtudja a fenyegetés mélységi és területi kiterjedését. Ez segít biztosítani azt, hogy az események teljesen el legyenek hárítva, és a fenyegetésnek semmilyen maradványa ne maradjon a végponton.

A munkafolyamat egyszerűsítése

A gördülékeny munkafolyamat egyetlen helyi vagy akár számítási felhőben lévő konzolról irányítható, és egyszerű EDR-eljárásokkal és kezelőszervekkel van összekapcsolva, beleértve a részletes képi megjelenítést, a sérülésjelző adatok vizsgálatát és a jelentős kiberbiztonsági szakértelmet vagy időt nem igénylő reagálási lehetőségeket.

A védelem megerősítése

A Kaspersky Sandbox hozzáadásával egy teljes egyesített végponti biztonsági megoldás jön létre, amely egyszerű, hatékony és nagymértékben automatizált többrétegű védelmet nyújt a vállalat pénzügyeit befolyásoló, összetett és jól rejtőzködő fenyegetések ellen.

A részletgazdag riasztási adatok elemzése

A Kaspersky EDR Optimum szükséges részletességű adatokat csatol az eseményekhez, és a támadás terjedési útvonalának képi megjelenítésével segít megismerni a különböző események közötti kapcsolatokat.

A hálózatra kapcsolódó összes gazdagép átláthatósága az importált vagy helyben előállított sérülésjelző adatok keresése révén válik lehetővé.

Automatikus reagálás

A sérülésjelző adatok vizsgálata révén az összes végponton észlelt fenyegetésekre adott automatikus ellenintézkedések beállítása vagy azonnali reagálás az eseményekre azok észlelésekor egykattintásos lehetőségeket választva.

A reagálási lehetőségek többek között: a gazdagép leválasztása a hálózatról, fájlok karanténba helyezése, keresés indítása a gazdagépen és adott fájlok futtatásának megakadályozása.

Az EDR további felhasználási lehetőségei

A Kaspersky Endpoint Detection and Response Optimum az általunk kínált számos, egyéni ügyféligényekre szabott EDR-lehetőség egyike. Javasoljuk még az alábbiak átgondolását is:

Kaspersky Endpoint Detection and Response

Az iparági szereplők és az ügyfelek által értékelt, jól felépített informatikai biztonsági rendszerrel rendelkező informatikai vállalatok számára tökéletes szakértői EDR-megoldás, amely segít a legkifinomultabb kidolgozott és célzott támadásoknak is alaposan a végére járni. Korszerű fenyegetésfelderítést, hatékony vizsgálatot, megelőző jellegű fenyegetésfelkutatást és az eseményekre központilag történő reagálást tesz lehetővé.
https://www.kaspersky.com/enterprise-security/endpoint-detection-response-edr

Kaspersky Managed Detection and Response

A teljes mértékben felügyelt és egyedileg testreszabott szünetmentes észlelés, fontossági sorrend beállítási lehetősége, vizsgálat és reagálás – amelynek több mint 20 év folyamatosan kiemelkedő színvonalú fenyegetéskutatás áll a hátterében – lehetőséget ad arra, hogy anélkül élvezze a saját biztonsági műveleti központ birtoklásának összes főbb előnyét, hogy tényleg létre kellene hoznia egy ilyet.
https://www.kaspersky.com/enterprise-security/managed-detection-and-response

Ha szeretne többet megtudni arról, hogyan hárítja el a Kaspersky Endpoint Detection and Response Optimum a kiberfenyegetéseket, miközben erőforrásokat szabadít fel és megkönnyíti a biztonsági részleg munkáját, lásd:
http://www.kaspersky.com/enterprise-security/edr-security-software-solution

Kiberfenyegetésekkel kapcsolatos hírek: www.securelist.com
Informatikai biztonsági hírek: business.kaspersky.com
Informatikai biztonság nagyvállalatok számára: kaspersky.com/enterprise
Fenyegetésfelderítési portál: opentip.kaspersky.com

www.kaspersky.com

Már bizonyítottunk. Függetlenek vagyunk. Tevékenységünk átlátható. Elkötelezettek vagyunk egy biztonságosabb világ felépítése iránt, ahol a technológia jobbá teszi az életünket. Ezért tesszük biztonságossá, hogy mindenki mindenhol hozzáférhessen a benne rejlő végtelen lehetőségekhez. Gondoskodjon a kiberbiztonságról a biztonságosabb jövő érdekében!

Proven. Transparent. Independent.