Kaspersky Endpoint Detection and Response

kaspersky BRING ON THE FUTURE

Verkkorikolliset käyttävät entistä kehittyneempiä tekniikoita ja pystyvät ohittamaan monet nykyisistä suojauksista. Siitä seuraa riskejä, jotka voivat johtaa tärkeiden liiketoimintaprosessien keskeytymiseen, tuottavuuden heikentymiseen ja käyttökustannusten nousuun kaikilla yrityksen osa-alueilla.

Kaspersky EDR:n avulla organisaatiosi saa käyttöönsä seuraavat ominaisuudet:

- Tehokas uhkien – myös muiden kuin haittaohjelmien – **VALVONTA**
- Tehokas uhkien **TUNNISTUS** – kehittyneen teknologian avulla
- Raakadatan ja tulosten keskitetty **KOOSTAMINEN**
- Hyökkäysten nopea **KÄSITTELY**
- **Havaittujen uhkien haitallisten toimien ESTÄMINEN**

Kaikki nämä ominaisuudet ovat käytettävissä intuitiivisessa verkkoliittymässä, joka helpottaa uhkien tutkimista ja käsittelyä.

Kaspersky EDR ja IDC:n Endpoint Security 2020 -raportin tärkeimmät havainnot*

Heikko päätelaitteiden suojausratkaisu (EPP) nollaa EDR-työkalun hyödyt

Kaspersky tarjoaa kattavan ja tehokkaan päätepistesuojauksen (EPP+EDR) yhdellä agenttiohjelmalla

Henkilöstön määrästä ja käytetystä ajasta on tullut EDR-työkalujen uusi ROI-mittari

Kaspersky vapauttaa asiantuntijoiden aikaa automatisoimalla monimutkaiset toimet tehokkaasti

EDR-ratkaisun on kyettävä hyödyntämään päätepisteiden ulkopuolisia tietoja

Kaspersky parantaa EDR-suojauksen tehokkuutta kehittyneellä posti- ja verkkopohjaisella uhkien tunnistuksella ja yhden työkalun näkyvyydellä

Tehosta ensisijaisesti päätepisteiden suojausta

Verkkorikollisten ensisijaisena kohteena ovat edelleen yrityksen päätepistelaitteet, joissa tiedot, käyttäjät ja yritystiedot kohtaavat ja joilla liiketoimintaprosesseja suoritetaan. Tietoturvatiimen on kyettävää suojaamaan päätepisteet ja estämään niiden käyttäminen sisäänpääsykohtina yrityksen infrastruktuuriin, mikä edellyttää niiden suojauksen tehostamista. Jotta päätepisteet voidaan suojata, tarvitaan edistyneillä torjuntaominaisuuksilla täydennettyjä estotekniikoita, jotka hoitavat kattavasti kaiken automaattisesta uhkien estämisestä monimutkaisten häiriöiden käsittelemiseen nopeasti ja asianmukaisesti.

Kaspersky Endpoint Detection and Response (EDR) on tehokas suojausratkaisu, joka antaa kattavan näkymän kaikkiin päätepisteisiin yrityksen verkossa. Sen ylivertaiset suojausominaisuudet mahdollistavat monimutkaisten uhkien ja APT-tyyppisten hyökkäysten havaitsemiseen, priorisointiin, tutkimiseen ja neutraloimiseen liittyvien rutiinitehtävien automatisoinnin.

Keskeisimmät ominaisuudet

- Kaspersky EDR lisää testattuun ja palkittuun päätepisteiden suojausympäristöömme **Kaspersky Endpoint Security for Businessiin** tehokkaat EDR-toiminnot ja parantaa yleistä suojausta. Automaattinen suojaus tavanomaisilta uhilta ja monimutkaisten hyökkäysten edistynyt torjunta hoituva samalla agenttiohjelmalla, mikä helpottaa häiriöiden käsittelyä ja minimoi ylläpitokustannukset. Ei lisäkuormitusta päätepisteille eikä ylläpidon lisäkuluja – vain tieto siitä, että työasemasi ja palvelimesi ovat täysin suojattuja kaikkein kehittyneimpiä uhkia ja kohdistettuja hyökkäyksiä vastaan.
- Kaspersky EDR nopeuttaa alustavien tulosten keruuta, kokoaa täyden telemetria-analyysin ja maksimoi EDR-prosessien automatisoinnin, joten se auttaa nopeuttamaan häiriöiden käsittelyä IT-tietoturvaresurssien tarvetta kasvattamatta.
- Kaspersky EDR voidaan sulauttaa **Kaspersky Anti Targeted Attack Platformiin**, jolloin EDR-toiminnot ja verkkotason kehittyneiden uhkien tunnistus hoituvat samalla järjestelmällä. Tietoturva-asiantuntijoilla on kaikki tarvitsemansa työkalut moniulotteiseen uhkien havaitsemiseen sekä päätepiste- että verkkotasolla, johtavat tekniikat, tehokas tutkinta ja nopea reagointi – kaikki yhdessä ratkaisussa.

* IDC PERSPECTIVE, Endpoint Security 2020:
The Resurgence of EPP and the Manifest Destiny of EDR -tutkimus

Kaspersky EDR on ihanteellinen ratkaisu organisaatioille, jotka haluavat:

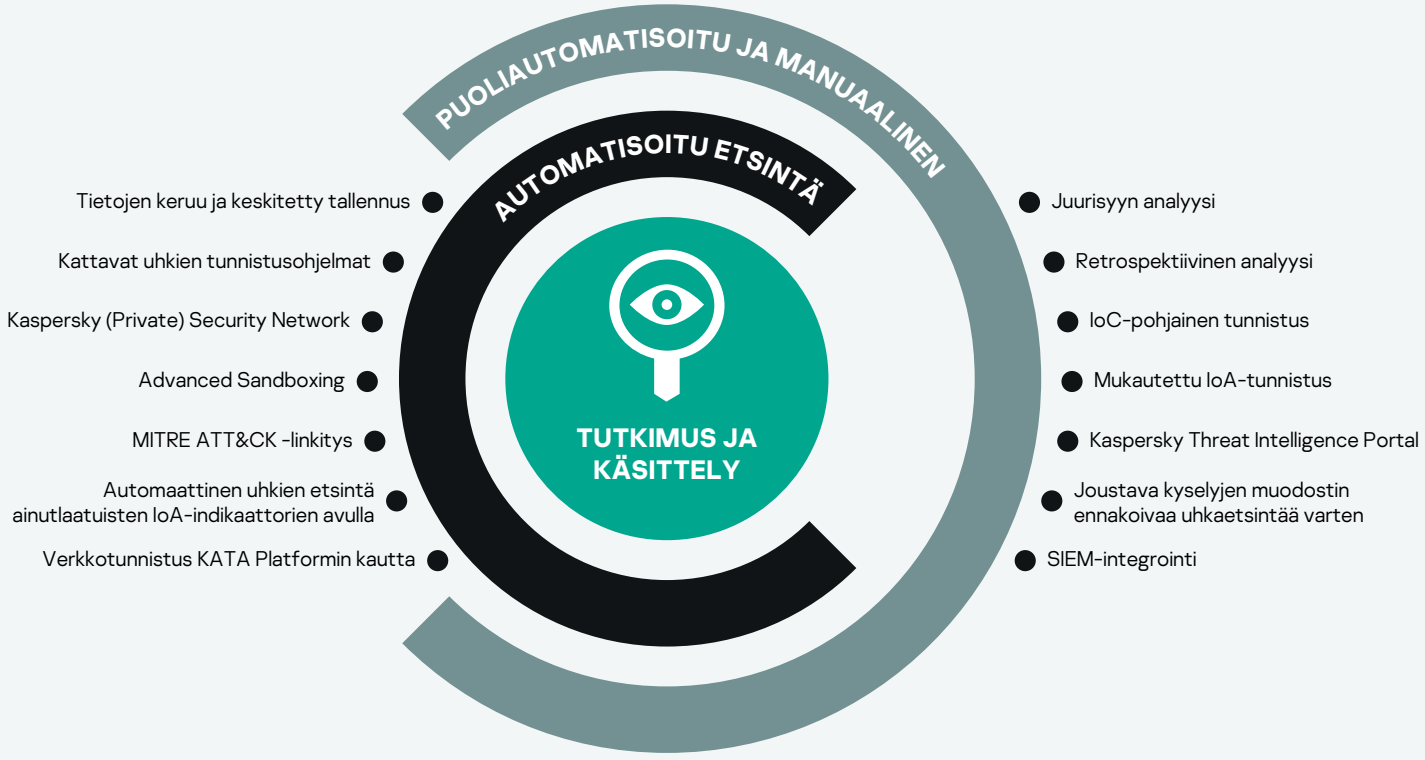
- Päivittää suojauksen ja häiriöiden käsittelyn helppokäyttöiseen yritystason ratkaisuun
- Automatisoida uhkien tunnistuksen ja käsittelyn – ilman liiketoimintakeskeytyksiä tutkimuksen aikana
- Parantaa päätepisteiden näkyvyyttä ja niiden uhkien tunnistusta edistyneillä teknologioilla
- Tehostaa suojausta ja tietoturvaresurssien kohdentamista hankkimalla tietoa hyökkääjien käyttämistä taktiikoista, tekniikoista ja periaatteista (TTP)
- Ottaa käyttöön yhtenäiset ja tehokkaat uhkien tunnistus-, häiriöiden hallinta- ja käsittelyprosessit
- Parantaa sisäisen tietoturvavalvonnan (SOC) tehoa eliminoimalla epäolennaisten päätepistelokien analysointitarpeen
- Auttaa vaatimusten-mukaisuusvaatimusten täyttämisessä päätepistelokien, hälytysarviointien ja tutkimustulosten dokumentoinnilla

Havaita ja eristää jopa kaikkein kehittyneimmät uhat tehokkaasti

Kaspersky EDR suojaa päätepisteet korkeatasoisesti ja parantaa SOC-tiimin tehokkuutta antamalla käyttöön kehittyneen uhkien tunnistusratkaisun ja varmistamalla historiatietojen käytettävyyden myös tilanteissa, joissa vaarantuneet päätepisteet eivät käytettävyssä tai hyökkäys on johtanut tietojen salaamiseen. Ainutlaatuiset IoA-hyökkäysindikaattorimme, MITRE ATT&CK--tuki ja joustava kyselyjen muodostustoiminto sekä pääsy Threat Intelligence Portal -tietokantaamme tehostavat uhkien tutkimusta. Nämä ominaisuudet helpottavat uhkien löytämistä ja nopeuttavat häiriöiden käsittelyä, mikä auttaa rajoittamaan ja ehkäisemään vahinkoja.

Käyttökohteet:

- **Tunkeutumiseen viittaavan aineiston ennakoiva etsiminen koko verkosta**
- **Nopea tunkeutumisten tunnistus ja korjaus – ennen kuin tunkeutuja ehtii aiheuttaa merkittäviä vahinkoja ja häiriöitä**
- **Tuhansien päätepisteiden häiriöiden nopea tutkiminen ja keskitetty hallinta saumattomilla työnkuluilla**
- **Hälytysten ja havaittujen mahdollisten häiriöiden varmistus muilla tietoturvaratkaisuilla**
- **Manuaalisten tehtävien minimoiminen, resurssien vapautaminen ja hälytysruuhkan riskin estäminen automatisoimalla rutiinitehtävät**



Kaspersky nimettiin huipputoimittajaksi Gartner Peer Insightsin Customers' Choice for EDR Solutions 2020 -asiakastutkimuksessa

Kaspersky on yksi kuudesta palveluntarjoajasta maailmassa, joka sai tunnustusta Gartner Peer Insightsin vuoden 2020 Customers' Choice -tutkimuksessa. Kasperskyn Endpoint Detection and Response -ratkaisu sai parhaat arvosanat kaikista toimittajista palvelu- ja tukiosioissa. Kaspersky EDR on siis todistetusti asiakkaiden mieleen.

Gartnerin vastuuvapauslauseke

Gartner Peer Insights Customers' Choice ovat yksittäisten loppukäyttäjien omiin kokemuksiin perustuvia subjektiivisia mielipiteitä, arvioita ja dokumentoituihin menetelmiin sovellettuja tietoja. Ne eivät edusta Gartnerin tai sen tytäryhtiöiden kantaa eivätkä ole osoitus antamastamme tuesta.

MITRE | ATT&CK®

MITRE ATT&CK -arvioinnin vahvistama tunnistuslaatu

Tunnustamme TTP (taktiikat, tekniikat ja periaatteet) -analysoinnin tärkeyden monimutkaisten häiriöiden tutkinnassa ja MITRE ATT&CKin roolin nykyisillä tietoturvamarkkinoilla:

- Kaspersky EDR oli mukana MITRE Evaluation Round2 (APT29) -arvioinnissa, jossa sen todettiin tunnistavan erittäin tehokkaasti Round2-arvioinnissa testatut tärkeimmät ATT&CK-hyökkäystekniikat, jotka vastaavat nykyaikaisia kohdennettuja hyökkäyksiä.
- Kaspersky EDR:n tunnistusta on tehostettu MITRE ATT&CK -tietokannan tiedoilla, joiden avulla hyökkäysten taktiikat, tekniikat ja periaatteet (TTP) voidaan syväanalysoida.

Lisätietoja: kaspersky.com/MITRE

Kaspersky EDR:n liiketoimintaedut yritykselle:

- Auttaa paikkaamaan tietoturva-aukkoja ja nopeuttaa hyökkäysten havaitsemista
- Automatisoi manuaalisia tehtäviä uhkien tunnistuksessa ja käsittelyssä
- Vapauttaa IT- ja tietoturvahenkilöstön muihin tärkeisiin tehtäviin
- Yksinkertaistaa uhkien analysointia ja häiriöiden käsittelyä
- Lyhentää uhkien tunnistamiseen ja käsittelyyn kuluvaa aikaa
- Auttaa vaatimustenmukaisuuden varmistamisessa

Jos haluat entistäkin kattavamman ratkaisun – valitse Kaspersky Managed Detection and Response

Täysin hallittujan ja yksittäin räätälöityjen jatkuvatoimisten suojaustoimintojen lisääminen Kaspersky EDR:hen auttaa säästämään IT-tietoturvaresursseja jättämällä häiriöihin liittyvät prosessointitehtävät Kasperskyn vastuulle. Annamme myös asiantuntija-apua ja uhkien etsimistukea, jos yrityksesi omassa tiimissä ei ole riittävää tietoturva-asiantuntemista yksittäisissä tapauksissa.

Lisätietoja Kaspersky EDR:stä:

kaspersky.com/enterprise-security/endpoint-detection-response-edr

Kyberuhkauutisia: securelist.com
IT-tietoturvauutisia: business.kaspersky.com
PK-yritysten tietoturva: kaspersky.com/business
Suuryritysten tietoturva: kaspersky.com/enterprise

www.kaspersky.com

Toimimme varmasti. Toimimme itsenäisesti. Toimimme läpinäkyvästi. Olemme sitoutuneet rakentamaan turvallisempaa maailmaa, jossa tekniikka parantaa elämänlaatua. Siksi haluamme suojata sen, jotta kaikilla kaikkialla olisi samat rajattomat mahdollisuudet. Kybersuojaus takaa turvallisemman tulevaisuuden.

Lisätietoja: kaspersky.com/transparency

Proven. Transparent. Independent.