Kaspersky Endpoint Detection and Response

kaspersky BRING ON THE FUTURE

Nettkriminelle har blitt stadig mer avanserte og i stand til å omgå eksisterende beskyttelse. Hvert forretningsområde kan være utsatt for risikoer som forstyrer forretningskritiske prosesser, skader produktivitet og øker driftskostnader.

Med Kaspersky EDR kan organisasjonen din:

- Effektivt **OVERVÅKE** trusler – annet enn malware
- Effektivt **OPPDAGE** trusler – ved hjelp av avanserte teknologier
- Sentralt **SAMLE INN** rådata og vurderinger
- Raskt **REAGERE** på angrep
- **FOREBYGGE** ondsinnede angrep fra oppdagede trusler

... alt via et intuitivt webgrensesnitt som gjør det enklere å utrede og reagere.

Kaspersky EDR og viktige konklusjoner i IDC-rapporten* Endpoint Security 2020

- **En svak EPP-løsning vil redusere verdien av et EDR-verktøy**

  Kaspersky tilbyr kraftige endepunktforsvar (EPP+EDR) via en enkelt agent

- **Personer og tid blir dermed den nye ROI-metrikken for EDR-verktøy**

  Kaspersky bruker høye nivåer av automatisering for komplekse problemer og frigjør dine sikkerhetseksperters verdifulle tid

- **EDR må utnytte data som ligger utenfor endepunktene**

  Kaspersky øker EDR-effektiviteten ved å legge til avansert e-post- og webbasert trusseloppdagelse og synlighet gjennom ett verktøy

Forsterk dine endepunktforsvar først

For nettkriminelle er bedriftens endepunkter, der data, brukere og bedriftssystemer møtes for å generere og implementere bedriftsprosesser, hovedmålet. For å beskytte disse bedriftsendepunktene, og hindre at de blir brukt som inngangspunkter til infrastrukturen, bør IT-sikkerhetsteamene vurdere måter å styrke det eksisterende forsvaret på. Implementering av en full syklus av endepunktbeskyttelse, fra automatisk blokkering av vanlige trusler til rask og riktig respons på komplekse hendelser, krever at man supplerer forebyggende teknologier med avanserte forsvarsfunksjoner.

Kaspersky Endpoint Detection and Response (EDR) gir omfattende oversikt over alle endepunkter i bedriftens nettverk, med et overlegent forsvar, og muliggjør automatisering av rutineoppgaver for å oppdage, prioritere, undersøke og nøytralisere komplekse trusler og APT-lignende angrep.

Hovedpunkter

- Kaspersky EDR forbedrer vårt mest testede, mest prisbelønnede flaggskip Endpoint Protection Platform (EPP) – **Kaspersky Endpoint Security for Business** – med kraftig EDR-funksjonalitet som forsterker dine totale sikkerhetsnivåer. En enkelt agent for automatisk beskyttelse mot vanlige trusler og avanserte forsvar mot komplekse angrep forenkler hendelseshåndtering og minimerer vedlikeholdskrav. Det oppstår ingen ekstra belastning på endepunkter og ingen ekstra kostnader – bare vissheten om at arbeidsstasjonene og serverne er fullt beskyttet mot de mest avanserte og målrettede angrepene.
- Kaspersky EDR reduserer tiden som går med til første bevisinnsamling, tilbyr full telemetrianalyse og optimaliserer automatisering av EDR-prosesser. Dette kutter samlet hendelsesresponstid uten å legge beslag på flere IT-sikkerhetsressurser.
- Kaspersky EDR kan absorberes til **Kaspersky Anti Targeted Attack Platform**, som kombinerer EDR-kapasitet og avansert trusseloppdagelse på nettverksnivå. IT-sikkerhetsspesialister har alle verktøyene de trenger for overlegen flerdimensjonal trusseloppdagelse på både endepunkt- og nettverksnivå. De kan bruke avansert teknologi, foreta effektive undersøkelser og iverksette rask og sentralisert respons – alt via én løsning.

* IDC PERSPECTIVE, Endpoint Security 2020: Ny fremvekst av EPP og EDRs tydelige utvikling

Kaspersky EDR er ideelt hvis organisasjonen din ønsker å:

- Oppgradere sikkerheten med en brukervennlig foretaksløsning for hendelsesrespons
- Automatisere trusselidentifisering og -respons – uten avbrudd i virksomheten under utredninger
- Forbedre endepunktsynlighet og trusseloppdagelse via avanserte teknologier
- Forstå de bestemte TTPs (Tactics, Techniques, and Procedures) som trusselaktører bruker for å oppnå sine mål, og legge til rette for mer effektivt forsvar og allokering av sikkerhetsressurser
- Etablere ensartede og effektive prosesser for trusselsøk, hendelsesadministrasjon og respons
- Øke effektiviteten til ditt interne SOC – ikke kaste bort deres tid ved å analysere irrelevante endepunktlogger
- Bidra til overholdelse ved å fremtvinge endepunktlogger, varselvurderinger og dokumentasjon av utredningsresultater

Raskt avsløre og avskjære de mest avanserte trusler

Kaspersky EDR tilbyr endepunktbeskyttelse på høyt nivå og øker SOC-effektiviteten ved å levere avansert trusseloppdagelse og gi tilgang til retrospektive data, selv i situasjoner der eksponerte endepunkter er utilgjengelige eller når data har blitt kryptert under et angrep. Forsterkede utredningsmuligheter gjennom våre unike Indicators of Attack (IoAs), MITRE ATT&CK-utvidelse og en fleksibel spørringsbygger, pluss tilgang til vår kunnskapsbase Threat Intelligence Portal – alle disse legger til rette for effektive trusselsøk og rask hendelsesrespons, som bidrar til skadebegrensning og -forebygging.

Bruksområder:

- **Proaktivt søk etter bevis på inntrengning over hele nettverket**
- **Rask oppdagelse og utbedring av en inntrengning – før angriperen kan forårsake alvorlig skade og forstyrrelse**
- **Rask utbedring og sentralisert administrasjon av hendelser på tvers av tusenvis av endepunkter med en sømløs arbeidsflyt**
- **Validering av varsler og potensielle hendelser som oppdages av andre sikkerhetsløsninger**
- **Automatisering av rutineoperasjoner – for å bidra til å redusere manuelle oppgaver, frigjøre ressurser og redusere sannsynligheten for "varseloverbelastning"**

Gartner peerinsights customers' choice 2020™

Gartner "Peer Insights" kundevalg for EDR-løsninger 2020 navngir Kaspersky som "Top Vendor"

Kaspersky er en av bare 6 leverandører verden over som har mottatt anerkjennelsen Gartner Peer Insights Customers' Choice for oppdagelse av og respons på endepunkt i 2020, med den høyeste rangeringen blant alle leverandører for vår service og support – det optimale kundekomplimentet for Kaspersky EDR.

Gartner-fraskrivelse

Gartner Peer Insights Customers' Choice utgjør subjektive meninger fra individuelle sluttbrukere i omtaler, vurderinger og data som brukes i dokumentert metodikk. De verken representerer synspunktene til eller utgjør anbefalinger fra Gartner eller dets datterselskaper.

MITRE | ATT&CK®

Oppdagelseskvalitet bekreftet av MITRE ATT&CK-evaluering

Anerkjenner viktigheten av Tactics, Techniques and Procedures-analyse (TTPer) i undersøkelsen av komplekse hendelser og rollen til MITRE ATT&CK i dagens sikkerhetsmarked:

- Kaspersky EDR har deltatt i MITRE-evalueringsrunde 2 (APT29) og fremvist et høyt ytelsesnivå ved å oppdage viktige ATT&CK-teknikker fra runde 2-omfanget som brukes i kritiske faser av dagens målrettede angrep
- Kaspersky EDRs oppdagelser er beriket med data fra MITRE ATT&CK-kunnskapsbasen for dyp analyse av din motstanders TTPer.

Finn ut mer på kaspersky.com/MITRE

Kaspersky EDR-forretningsfordeler i hele foretaket:

- Bidrar til å eliminere sikkerhetshull og redusere angrepets 'hviletid'
- Automatiserer manuelle oppgaver under trusseloppdagelse og -respons
- Frigjør IT- og IT-sikkerhetspersonell til andre viktige oppgaver
- Forenkler trusselanalyse og hendelsesrespons
- Reduserer tiden som går med til å identifisere og reagere på trusler
- Bidrar til full overholdelse

Og hvis du vil ha enda mer... Kaspersky Managed Detection and Response

Å tilføye fullt administrerte og individuelt skreddersydde 24/7-forsvar til Kaspersky EDR betyr at dine IT-sikkerhetsressurser kan bevares ved å overlate hendelsesrelaterte behandlingsoppgaver til Kaspersky, eller kontakte oss for å motta trusselsøkekspertise når ditt interne team mangler tilstrekkelig med sikkerhetsspesialister for å takle bestemte scenarier.

Hvis du vil finne ut mer om Kaspersky EDR, kan du besøke:

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

Nyheter om nettrusler: securelist.com
Nyheter om IT-sikkerhet: business.kaspersky.com
IT-sikkerhet for SMB: kaspersky.com/business
IT-sikkerhet for større bedrifter: kaspersky.com/enterprise

www.kaspersky.com

Vi er anerkjente. Vi er uavhengige. Vi er tydelige. Vi er opptatt av å bygge en tryggere verden, der teknologi gjør livene våre bedre. Derfor sikrer vi den, slik at alle overalt får de endeløse mulighetene den gir. Nettsikkerhet for en tryggere fremtid.

Finn ut mer på kaspersky.com/transparency

Proven. Transparent. Independent.