

Kaspersky Anti Targeted Attack Platform

Dagens nettkriminelle spesialiserer seg på å designe unike og nyskapende metoder for å trenge inn i systemer og skade data. Etter hvert som trusler fortsetter å utvikle seg og blir mer avanserte og ødeleggende, har både rask oppdagelse og den raskeste, mest hensiktsmessige responsen blitt mer kritisk.

Det er livsviktig at store bedrifter fortsetter å tenke nytt om sine IT-sikkerhetsforsvar.

For å holde seg ett trinn foran cybertrusler som vokser i styrke, og for å begrense eventuelle økonomiske tap som oppstår.

Uovertruffen cybersikkerhet i en forenet løsning

Profesjonelle cyberkriminelle i disse dager foretrekker en tilnærming langs flere vektorer. Kaspersky Anti Targeted Attack Platform kombinerer avansert trusseloppdagelse på nettverksnivå med EDR-funksjonalitet. Samtidig gir det spesialister på IT-sikkerhet alle våpnene de trenger for å oppnå overlegen trusseloppdagelse i flere dimensjoner, ta i bruk avanserte teknologier, foreta effektive utredninger, søke etter trusler proaktivt og levere en rask, sentralisert respons – alt gjennom en enkel løsning.

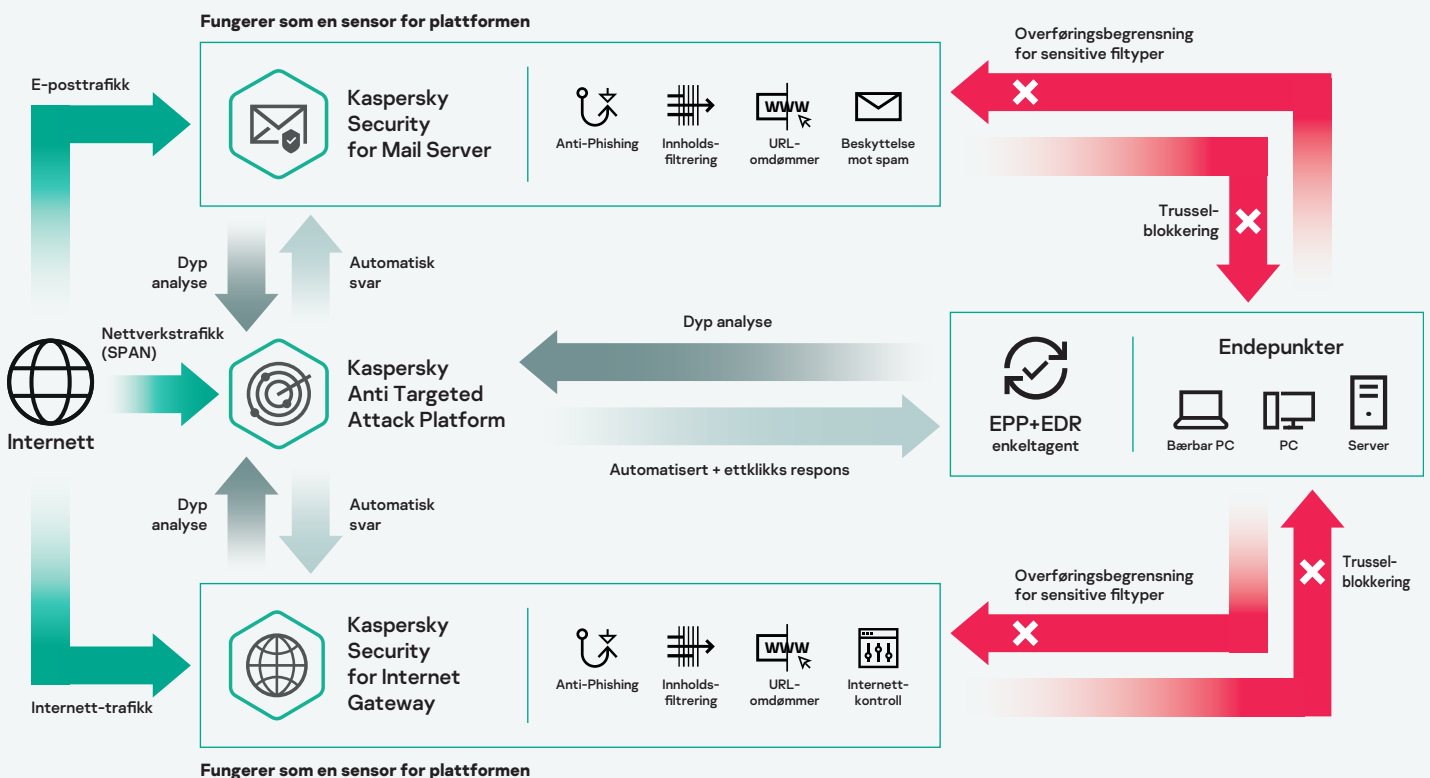
De mest avanserte angrepene under din fokus og kontroll

Kaspersky Anti Targeted Attack Platform:

- **REDUSERER** tiden som går med til å identifisere og reagere på trusler
- **FORENKLER** trusselanalyse og hendelsesrespons
- **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
- **STØTTER** full regulatorisk overholdelse

Plattformen fungerer som en løsning for utvidet oppdagelse og respons, og leverer alt-i-ett APT-beskyttelse drevet av vår trusselintelligens og tilordnet MITRE ATT&CK-rammeverket. Alle potensielle inngangspunkter for trusler – nettverk, web, e-post, stasjonære og bærbare PCer, servere og virtuelle maskiner – er under din kontroll.

Kaspersky Anti Targeted Attack Platform er fullt integrert med **Kaspersky Endpoint Security for Business**, og deler en enkelt agent med Kaspersky EDR. Den kan også integreres med både **Kaspersky Security for Mail Server** og **Kaspersky Security for Internet Gateway**, som fungerer som sensorer for plattformen og tilbyr en automatisert respons på mer komplekse trusler fra e-post og Internett.



En klart sikkerhetsløsning som leverer komplett beskyttelse mot innsyn

All objektanalyse utføres på stedet, uten noen utgående dataflyt, og Kaspersky Private Security Network leverer sanntid inngående omdømmeoppdateringer mens det samtidig bevarer full isolasjon av bedriftsdata.

En forenet løsning for å akselerere innovasjon i digital transformasjon gjennom:

- **Integrert forretningskontinuitet.**
Vi bygger inn sikkerhet og overholdelse i nye prosesser direkte fra start
- **Full synlighet** over hele IT-infrastrukturen i bedriften
- **Maksimal fleksibilitet** muliggjør implementering på tvers av både fysiske og virtuelle miljøer, hver gang synlighet og kontroll er nødvendig
- **Automatisering av trusseloppdagelse og responsoppgaver,** optimaliserer kostnadseffektiviteten i din sikkerhet, hendelsesrespons og SOC-team
- **Tett, direkte integrering** med eksisterende sikkerhetsprodukter forbedrer totale sikkerhetsnivåer beskytter tidligere sikkerhetsinvesteringer

Hovedfunksjoner:



Flerlags sikkerhetsarkitektur – total synlighet oppnå gjennom en kombinasjon av nettverk, Internett- og e-postsensorer og endepunktagerter.



Omfattende trusseloppdagelsesmotorer – for å arbeide med data fra nettverkssensorer (nettverkstrafikkanalyse) og endepunktagerter (EDR-funksjonalitet) for raske beslutninger og færre falske positive.



Advanced Sandbox – tilbyr et sikkert miljø for dyp analyse av trusselaktivitet, støtte for vilkårlig tildeling av OS-komponenter, tidsakselerering i virtuelle maskiner, antiomgåelsesteknikker, brukeraktivitetssimulering og tilordning av resultater til MITRE ATT&CK-kunnskapsbasen - alt bidrar til svært effektiv atferdsbasert oppdagelse.



Retrospektiv analyse – selv i situasjoner der komprimerte endepunkter er utilgjengelige eller når data har blitt kryptert - gjennom automatisert data-, objekt- og bedømmelseinnsamling, samt sentralisert lagring.



To modi for trusselintelligenssamspill – automatisert sammenligning med globale omdømmedata fra Kaspersky Security Network og manuelt søk etter trusler og utredningsspøringer gjennom Kaspersky Threat Intelligence Portal.



Sanntids automaisk søk etter trusler – hendelser korreleres med et unikt sett av IoAs (Indicators of Attack) generert av Kasperskys trusselsøk og tilordnet til MITRE ATT&CK-matrisen, gir klare hendelsesbeskrivelser, eksempler og responsanbefalinger.



Proaktive trusselsøk med vår kraftige og fleksible spørringsbygger – analytikere kan bygge komplekse spørringer for atypisk atferd og mistenkelige aktiviteter, og for trusler som gjelder spesielt for din infrastruktur.

Kort fortalt

Pålitelig databeskyttelse, sikkerhet for IT-infrastruktur, stabilitet for forretningsprosesser og overholdelse av regelverk er forutsetninger for bærekraftig bedriftsutvikling i dag.

Kaspersky Anti Targeted Attack Platform hjelper dere som en organisasjon med veletablerte IT-sikkerhetsløsninger med å bygge opp et pålitelig forsvar som beskytter bedriftens infrastruktur mot APT-lignende trusler og målrettede angrep og understøtter overholdelse av regelverk, uten at det kreves ytterligere IT-sikkerhetsressurser. Komplekse hendelser blir raskt identifisert, undersøkt og respondert på, noe som avlastet det interne IT-sikkerhets- eller SOC-teamet for manuelle oppgaver, slik at det kan arbeide mer effektivt, takket være en enhetlig løsning som maksimerer bruken av automatisering og kvaliteten på resultatene.

Dokumentert å være bransjens mest effektive løsning



SE Labs testet Kaspersky Anti Targeted Attack Platform mot en rekke forskjellige hackingangrep, **og ga oss en AAA-rangering.**



I den uavhengige testen 'ICSA Labs: Advanced Threat Defense (Q3 2019) leverte Kaspersky Anti Targeted Attack Platform **100 % oppdagelsesfrekvens, med null falske positive.**



THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

Radicati Group anerkjenner Kaspersky som **en topp aktør innen sin APT-beskyttelse (Advanced Persistent Threat) – Market Quadrant 2020.**



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

Som én av bare 6 leverandører globalt som ble anerkjent som en Gartner Peer Insights Customers' Choice for EDR-løsninger i 2020 - det endelige kundekomplimentet for vår utvidede EDR-løsning - Kaspersky Anti Targeted Attack Platform med Kaspersky EDR i kjernen.

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

Kjerneelementet i Kaspersky Anti Targeted Attack Platform - Kaspersky EDR - deltok i MITRE-evalueringrunde 2 (APT29), og fremviste høye ytelsesnivåer ved å oppdage viktige ATT&CK-teknikker som brukes ved viktige trinn i dagens målrettede angrep.

Finne ut mer på kaspersky.com/MITRE

Hvis du vil finne ut mer om Kaspersky Anti Targeted Attack Platform, kan du besøke:

kaspersky.com/enterprise-security/anti-targeted-attack-platform

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

2020 AO Kaspersky Lab.
Registrerte varemerker og servicemerker tilhører sine respektive eiere.



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.

Finne ut mer på kaspersky.com/transparency



**Proven.
Transparent.
Independent.**