



# Kaspersky Endpoint Detection and Response

**Cyberbrottslingar blir allt mer sofistikerade och kan kringgå befintliga skydd. Varje område i ditt företag kan utsättas för risker som stör affärskritiska processer, skadar produktiviteten och ökar driftskostnaderna.**

**Med Kaspersky EDR kan din organisation:**

- Effektivt **ÖVERVAKA** hot – bortom skadlig kod
- Effektivt **UPPTÄCKA** hot – med avancerad teknik
- Centralt **SAMLA IN** rå data och utlåtanden
- Snabbt **SVARA** på attacker
- **FÖREBYGGA** skadliga handlingar genom att upptäcka hot

... allt via ett intuitivt webbgränssnitt som gör det lättare att undersöka och reagera.

**Kaspersky EDR och viktiga slutsatser från IDCs Endpoint Security 2020-rapport\***

### ● En svag EPP-lösning underminerar värdet på ett EDR-verktyg

Kaspersky erbjuder kraftfulla kompletta försvar för klienter (EPP + EDR) via en enda agent

### ● Människor och tid blir således den nya ROI-mätetalet för EDR-verktyg

Kaspersky tillämpar höga nivåer av automatisering på komplexa problem vilket frigör dina säkerhetsexperters värdefulla tid

### ● EDR måste utnyttja data som ligger utanför klienterna

Kaspersky ökar effektiviteten hos EDR genom att lägga till avancerad e-post- och webbaserad hotupptäckt och insyn via ett enda verktyg

## Förbättra dina försvar vid klienterna först

För cyberbrottslingar är företags klienter – där data, användare och företagssystem alla samlas för att generera och implementera affärsprocesser – det huvudsakliga målet. För att skydda företagets klienter och förhindra att de används som inträden i din infrastruktur bör ditt IT-säkerhetsteam granska sätt att förbättra din befintliga säkerhet. Att implementera fullständigt klientskydd, från automatisk allmän hotblockering till att svara snabbt och ändamålsenligt på komplexa incidenter kräver förebyggande tekniker baserade på avancerade försvarsfunktioner.

**Kaspersky Endpoint Detection and Response (EDR)** levererar kraftfull säkerhet med omfattande insyn i alla klienter i företagets nätverk och tillsammans överlägsna försvar. Du kan automatisera rutinuppgifter för att upptäcka, prioritera, undersöka och neutralisera avancerade hot och APT-liknande angrepp.

## Fördelar

- Kaspersky EDR förbättrar vårt mest testade och belönade plattform för skydd av klienter (EPP) – **Kaspersky Endpoint Security for Business** – med kraftfulla EDR-funktioner som ytterligare stärker dina övergripande säkerhetsnivåer. En enda agent för automatiskt skydd mot vanliga hot och avancerat skydd mot komplexa angrepp förenklar hanteringen och minimerar underhållskraven. Det finns ingen extra börda för klienterna och inga extra kostnader – bara vetskapen om att dina arbetsstationer och servrar är helt skyddade mot de mest sofistikerade hoten och riktade angreppen.
- Kaspersky EDR reducerar den tid som krävs för att inleda bevisupptagning, tillhandahåller full telemetri-analys och maximerar automatiseringen av EDR-processer vilket reducerar den totala responstiden för händelser utan att behöva spendera ytterligare IT-säkerhetsresurser.
- Kaspersky EDR kan absorberas i **Kaspersky Anti Targeted Attack-plattformen** och kombinerar EDR-funktionaliteterna och avancerad hotupptäckt på nätverksnivå. IT-säkerhetsspecialisterna har alla verktyg de behöver för att hantera flerdimensionell hotupptäckt på både klient- och nätverksnivå med tillämpning av ledande teknik och effektiva undersökningar vilket levererar en snabb centraliserad åtgärd – med bara en enda lösning.

\* IDC PERSPECTIVE, klientsäkerhet 2020: EPP:s återupplivning och EDR:s förutbestämda öde

## Kaspersky EDR är perfekt om din organisation vill:

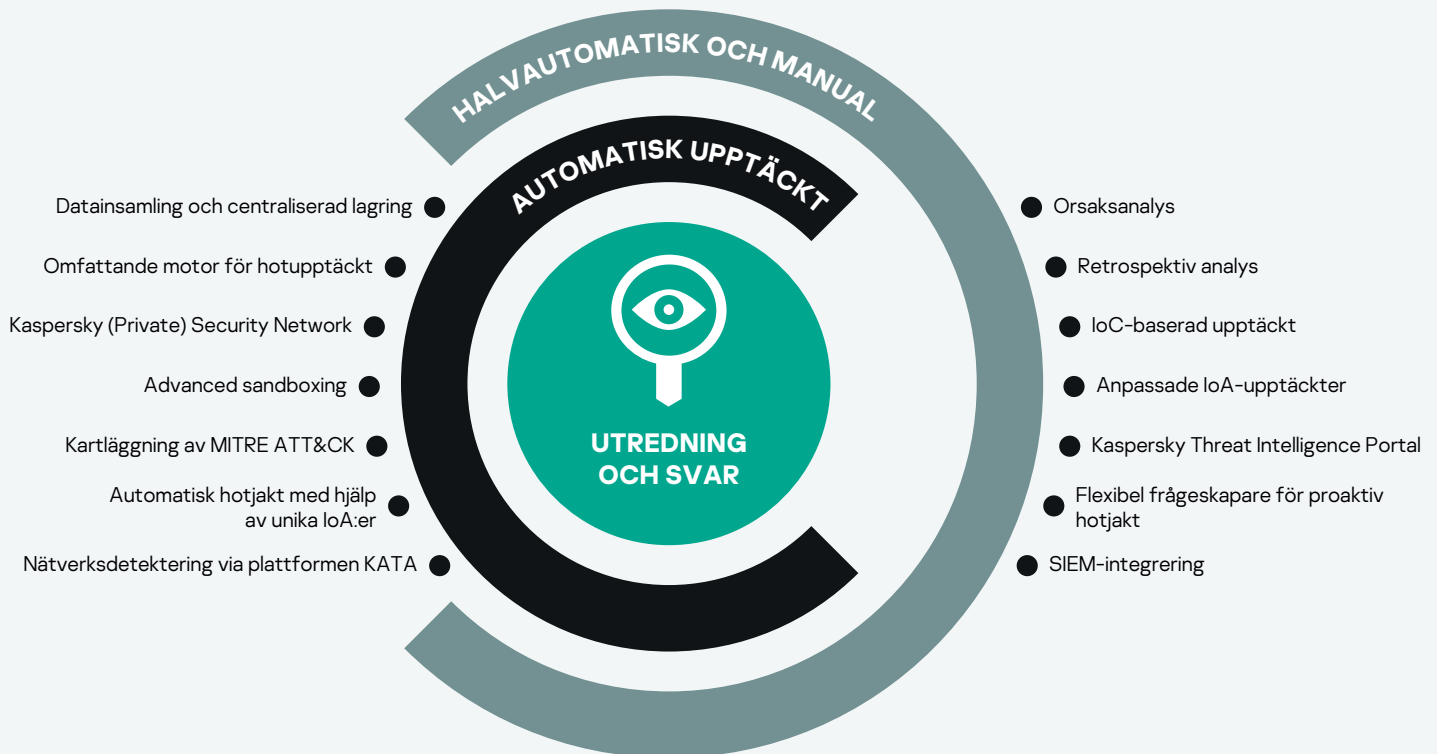
- Uppgradera sin säkerhet med en lättanvänd företagslösning för incidentrespons
- Automatisera hotidentifiering och -svar – utan verksamhetsstörningar under utredningar
- Förbättra dina klients insyn och hotdetektering via avancerad teknik
- Förstå de specifika taktikerna, tekniker och förfaranden (TTP) som används av hotaktörer för att uppnå sina mål vilket möjliggör effektivare försvar och allokering av säkerhetsresurser
- Upprätta en enhetlig och effektiv hotjakt, händelsehantering och svar på processer
- Öka effektiviteten i ditt interna SOC – slösa inte bort tiden på att analysera irrelevanta loggar från klienter
- Hjälper efterlevnaden genom att upprätthålla loggar för klienter samt granska varningar och dokumentation av undersökningsresultat

# Upptäcker snabbt och hindrar de mest sofistikerade hoten

Kaspersky EDR levererar ett skydd på hög nivå och ökar SOC-effektiviteten, levererar avancerad hotupptäckt samt tillgång till retrospektiv data även i situationer där komprometterade klienter är otillgängliga eller när data har krypterats under en attack. Förbättrade utredningsmöjligheter genom våra unika attackindikatorer (IoAs), MITER ATT&CK-anrikning och en flexibel frågeskapare samt tillgång till vår Threat Intelligence Portal-kunskapsbas – alla dessa underlättar effektiv hotjakten och snabb incidentrespons vilket leder till begränsningar av skador och förebyggande.

## Användningsfall:

- Proaktiv sökning efter bevis på intrång över hela nätverket
- Snabb upptäckt och sanering av ett intrång – innan inkräktaren kan orsaka stora skador och störningar
- Snabb utredning och centraliserad hantering av incidenter över tusentals klienter med ett sömlöst arbetsflöde
- Validering av varningar och potentiella incidenter som upptäckts av andra säkerhetslösningar
- Automatiserade rutinmässiga funktioner – för att minimera manuella uppgifter, frigöra resurser och reducera sannolikheten för "varning för överbelastning"





### Gartner Peer Insights Customers' Choice för EDR-lösningar under 2020 namngav Kaspersky som toppsäljare

Kaspersky är en av endast sex leverantörer världen över som tog emot Gartner Peer Insights Customers' Choice som erkännande för lösningar gällande upptäckt och åtgärdande av attacker mot nätverkets klienter under 2020 med högsta betyg bland alla leverantörer för vår service och support – den ultimata komplimangen från våra kunder för Kaspersky EDR.

#### Gartners friskrivning

Gartner Peer Insights Customers' Choice är subjektiva åsikter från enskilda användares recensioner, betyg och data använda med hjälp av dokumenterad metod. De motsvarar inte Gartners eller dess dotterbolags synpunkter och Gartner eller dess dotterbolag stöder inte heller dem.

## MITRE | ATT&CK®

### Detekteringskvalitet bekräftad av MITRE ATT&CK Evaluation

Erkänner hur viktigt det är med taktik, TTP-analys i komplexa incidentutredningar och vilken roll MITRE ATT&CK spelar på säkerhetsmarknaden idag:

- Kaspersky EDR har deltagit i MITERs utvärderingsrunda 2 (APT29) och visat en hög prestanda när det gäller att upptäcka ATT&CK-tekniker från omfattningen av runda 2 tillämpade i avgörande stadier i dagens riktade attacker
- Upptäckter gjorda av Kaspersky EDR är berikade med data från kunskapsbasen MITER ATT&CK för djupanalys av din motståndares TTP:er

Läs mer på [kaspersky.com/MITRE](https://kaspersky.com/MITRE)

# Affärsfördelar med Kaspersky EDR över hela företaget:

- Hjälper till att eliminera luckor i säkerheten och reducera attackens "uppehållstid"
- Automatiserar manuella uppgifter under hotdetektering och -svar
- Frigör IT-resurser och -säkerhetspersonal för andra viktiga uppgifter
- Förenklar hotanalys och incidentrespons
- Reducerar tiden det tar att identifiera och svara på hot
- Hjälper till att möjliggöra fullständig efterlevnad

## Och om du vill ha ännu mer ... Kaspersky Managed Detection and Response

Att lägga till ett helt hanterat och individuellt anpassat försvar till Kaspersky EDR som fungerar dygnet runt innebär att dina IT-säkerhetsresurser kan bevaras genom att avlasta incidentrelaterade bearbetningsuppgifter till Kaspersky eller kontakta oss för expertbedömningar och unik hotjaktkompetens när ditt IT-team saknar tillräckligt kvalificerade säkerhetsspecialister för att möta specifika scenarier.

Få mer information om Kaspersky EDR genom att besöka:

[kaspersky.com/enterprise-security/endpoint-detection-response-edr](https://kaspersky.com/enterprise-security/endpoint-detection-response-edr)

Nyheter om cyberhot: [securelist.com](https://securelist.com)  
IT-säkerhetsnyheter: [business.kaspersky.com](https://business.kaspersky.com)  
IT-säkerhet för SMB: [kaspersky.com/business](https://kaspersky.com/business)  
IT-säkerhet för stora företag: [kaspersky.com/enterprise](https://kaspersky.com/enterprise)

[www.kaspersky.com](https://www.kaspersky.com)

2020 AO Kaspersky Lab.  
Registrerade varumärken och service  
märken tillhör sina respektive ägare.



Vi är beprövade. Vi är oberoende. Vi är transparenta. Vårt mål är att skapa en säkrare värld, där tekniken förbättrar våra liv. Det är därför vi gör den säkrare, så att alla kan dra nytta av de oändliga möjligheterna. Använd cybersäkerhet för en säkrare framtid.

Läs mer på [kaspersky.com/transparency](https://kaspersky.com/transparency)



Proven.  
Transparent.  
Independent.