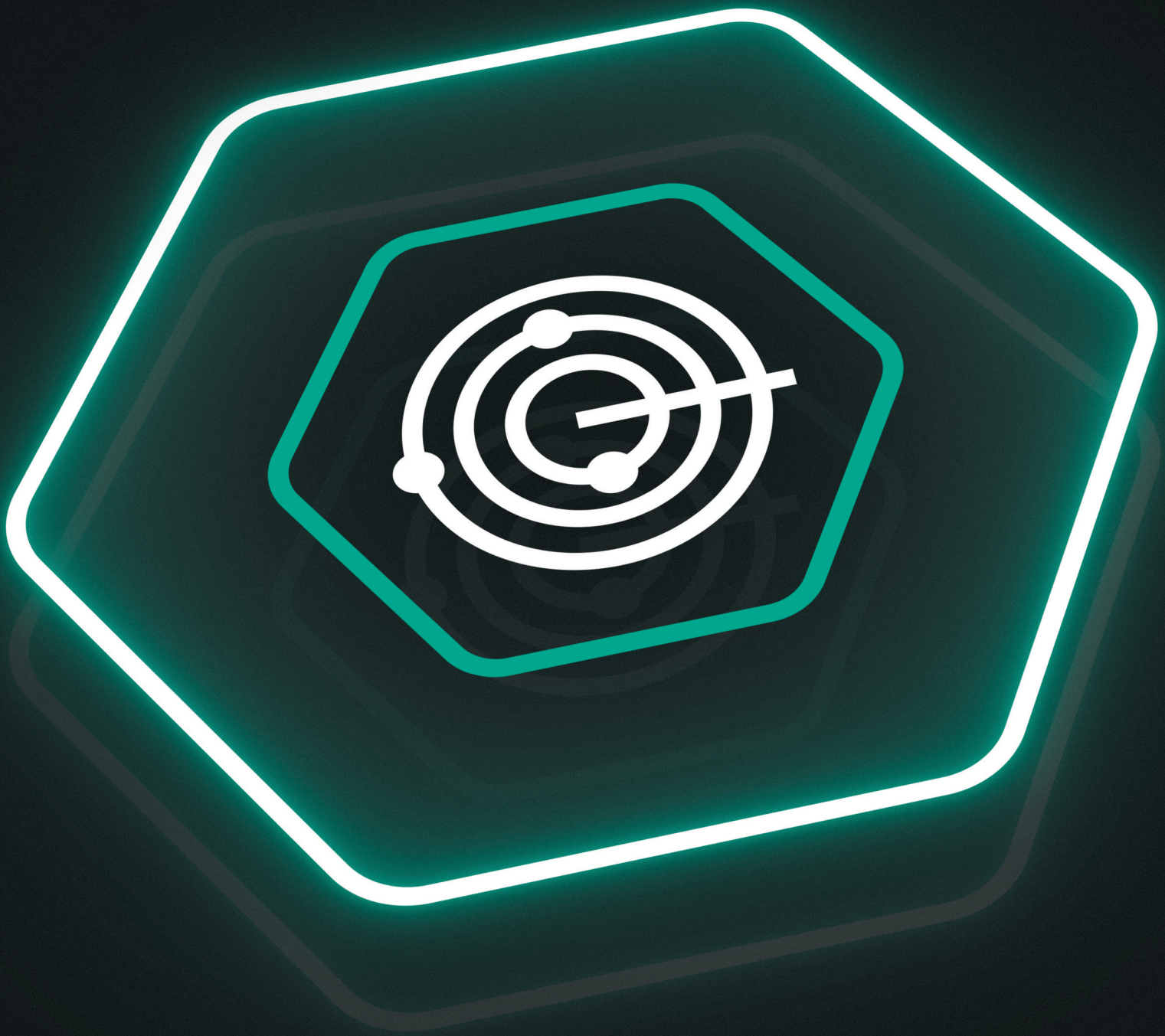


Kaspersky Anti Targeted Attack Platform

kaspersky BRING ON THE FUTURE

Dagens cyberbrottslingar är specialiserade på att designa unika och innovativa metoder för att ta sig in i och kompromettera system. Allt eftersom hot fortsätter att utvecklas och blir mer sofistikerade och förödande har både snabb upptäckt och det snabbaste och bäst lämpade svaret blivit kritiska.

Det är grundläggande att företag fortsätter att tänka igenom sina IT-säkerhetsförsvar,

för att kunna förbli ett steg före den växande andelen cyberhot och för att begränsa eventuella ekonomiska förluster.

Oöverträffad cybersäkerhet i en enhetlig lösning

Professionella cyberbrottslingar föredrar nu för tiden en strategi med flera vektorer. Kaspersky Anti Targeted Attack Platform kombinerar avancerad hotupptäckt på nätverksnivå och EDR-funktionaliteter samtidigt som IT-säkerhetsspecialister får alla verktyg de behöver för att hantera överlägsen multidimensionell hotupptäckt, tillämpa ledande tekniker, genomföra effektiva utredningar, hotjaga proaktivt samt leverera ett snabbt och centraliserat svar – allt med en enda lösning.

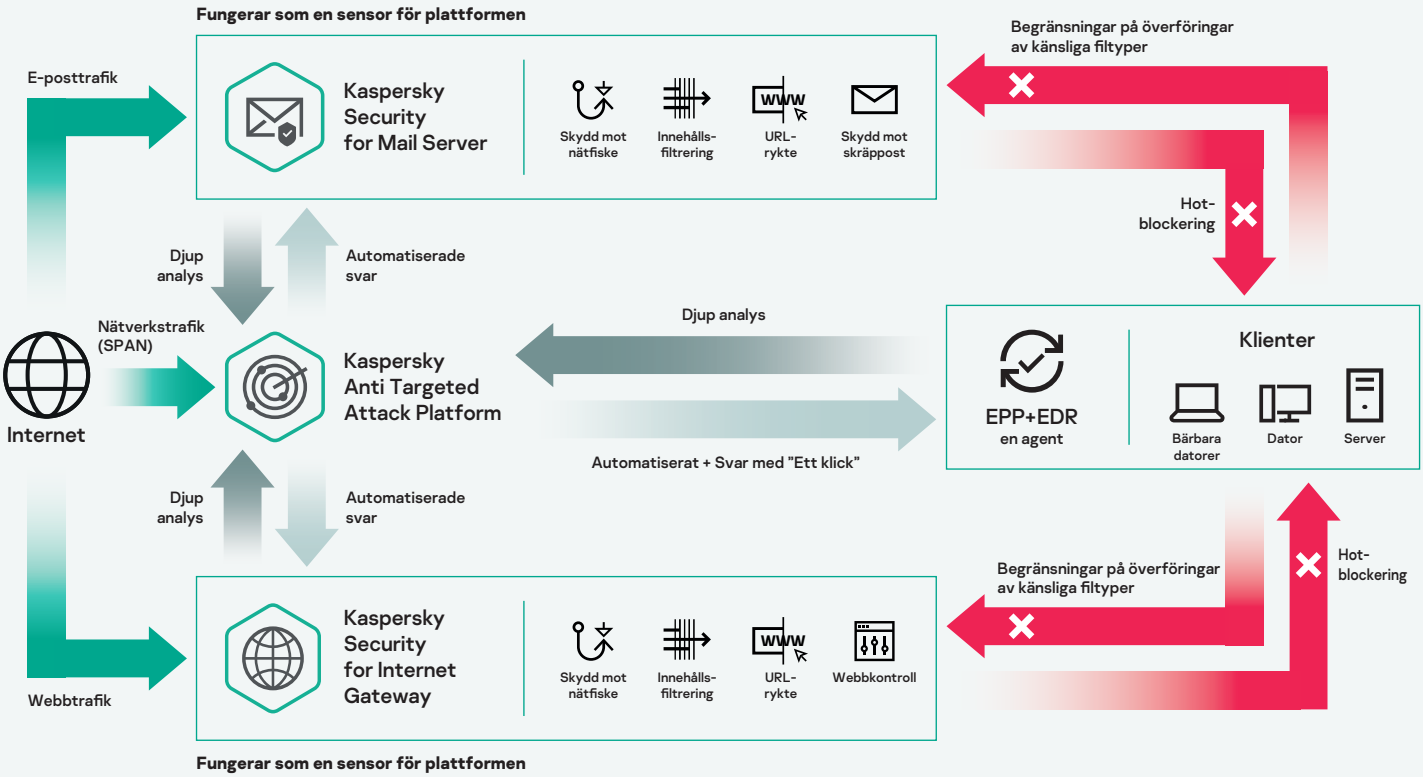
De mest sofistikerade attackerna som du kan och kontrollera

Plattformen fungerar som en utökad lösning för detektering och respons som levererar ett allt-i-ett-APT-skydd som drivs av vår Threat Intelligence och kartläggs till MITER ATT&CK-ramverket. Alla potentiella ingångspunkter för hot – nätverk, webb, e-post, datorer, bärbara datorer, servrar och virtuella maskiner – är under din kontroll.

Kaspersky Anti Targeted Attack Platform är helt integrerad med **Kaspersky Endpoint Security for Business** och delar en enda agent med Kaspersky EDR. Den integrerar även med både **Kaspersky Security for Mail Server** och **Kaspersky Security for Internet Gateway** som fungerar som sensorer till plattformen vilket levererar ett automatiskt svar på mer komplexa e-post- och webbaserade hot.

Kaspersky Anti Targeted Attack Platform:

- **REDUCERA** tiden det tar att identifiera och svara på hot
- **FÖRENKLAR** hotanalys och incidentrespons
- **HJÄLPER TILL ATT** eliminera luckor i säkerheten och reducera attackens "uppehållstid"
- **AUTOMATISERAR** manuella uppgifter under hotdetektering och -svar
- **FRIGÖR** IT-teamets säkerhetspersonal för andra viktiga uppgifter
- **HAR STÖD FÖR** fullständig regelefterlevnad



En pålitlig säkerhetslösning som levererar fullständig integritet

All objektanalys utförs på plats utan utgående dataflöde och Kaspersky Private Security Network levererar inkommande ryktesuppdateringar i realtid samtidigt som den fullständiga isoleringen av företagsdata bevaras.

En enhetlig plattform för att accelerera innovation inom digital transformation genom:

- **Integrerad affärskontinuitet.** Vi bygger säkerhet och efterlevnad i nya processer från början till slut
- **Fullständig insyn** över företagets IT-infrastruktur
- **Maximal flexibilitet** som möjliggör implementering i både fysiska och virtuella miljöer där insyn och kontroll behövs
- **Automatisering av hotupptäckt- och svar** som optimerar kostnadseffektiviteten för din säkerhet, incidentrespons och SOC-team
- **Stram och entydig integration** med befintliga säkerhetsprodukter, förbättrade övergripande säkerhetsnivåer och skydd för äldre säkerhetsinvesteringar

Huvudfunktioner:

Sensorarkitektur på flera nivåer – fullständig insyn uppnås genom en kombination av nätverks-, webb- och e-postsensorer samt agenter för klienter.

Motorer för omfattande hotupptäckt – arbetar med data från nätverkssensorer (analys av nätverkstrafik) och agenter för klienter (EDR-funktioner) för snabba bedömningar och färre falska positiva.

Advanced Sandbox – erbjuder en säker miljö för djup analys av hotaktivitet som har stöd för randomisering av OS-komponenter, tidsacceleration i virtuella maskiner, tekniker mot undvikande, simulering av användaraktiviteter och resultatkartläggning till MITER ATT&CK-kunskapsbasen – allt bidrar till en mycket effektiv beteendebaserad detektion.

Retrospektiv analys – även i situationer där komprometterade klienter är otillgängliga eller när data har krypterats – genom automatiserad data, insamling av objekt och utlåtande samt centraliserad lagring.

Två lägen för Threat Intelligence-interaktion – automatiserad jämförelse med global ryktesinformation från Kaspersky Security Network och manuell hotjakt samt utredningsfrågor via Kaspersky Threat Intelligence Portal.

Automatisk hotjakt i realtid – händelser korreleras med en unik uppsättning attackindikatorer (IoAs) genererade av Kasperskys hotjägare och kartläggs till MITER ATT&CK-matrisen som tillhandahåller tydliga händelsebeskrivningar, exempel och rekommendationer på svar.

Proaktiv hotjakt med vår kraftfulla och flexibla frågeskapare – analytiker kan skapa komplexa frågor för att söka efter atypiskt beteende och misstänkta aktiviteter och efter hot som är specifika för din infrastruktur.

Kortfattat

Tillförlitligt dataskydd, IT-infrastruktursäkerhet, stabilitet för affärsprocesser och efterlevnad är förutsättningar för en hållbar affärsutveckling idag.

Kaspersky Anti Targeted Attack Platform hjälper IT-säkerhetsteamet på ditt företag att bygga upp ett tillförlitligt försvar som skyddar företagets infrastruktur mot APT-liknande hot och riktade angrepp och ger stöd för regelefterlevnad, utan krav på ytterligare IT-säkerhetsresurser. Komplexa incidenter blir snabbt upptäckta, utredda och åtgärdade, vilket ökar effektiviteten hos dina IT-säkerhets- eller SOC-team genom att avlägsna behovet av manuell hantering, med hjälp av en enhetlig lösning som maximerar användningen av automatisering och ger bättre resultat.

Har visat sig vara branschens mest effektiva lösning

SE Labs testade Kaspersky Anti Targeted Attack Platform mot ett antal attacker från hackare **och gav oss högsta betyg**.

I det oberoende testet från ICSA Labs: Advanced Threat Defense (Q3 2019) levererade Kaspersky Anti Targeted Attack Platform **100 % detektering med noll falska positiva**.

The Radicati Group erkänner Kaspersky som **en toppspelare med sitt Advanced Persistent Threat (APT) -skydd – Market Quadrant 2020**.

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

Som en av endast sex leverantörer världen över att erkännas som en Gartner Peer Insights Customers' Choice för EDR-lösningar under 2020 – den ultimata komplimangen från våra kunder för vår utökade EDR-lösning – Kaspersky Anti Targeted Attack Platform med Kaspersky EDR i sin kärna.

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.

Detekteringskvalitet bekräftad av MITRE ATT&CK Evaluation

Det grundläggande elementet i Kaspersky Anti Targeted Attack-plattformen – Kaspersky EDR – deltog i MITER-utvärderingsrundan 2 (APT29) och demonstrerade höga prestandanivåer för att upptäcka ATT&CK-tekniker som används i viktiga stadier i dagens riktade attacker.

Läs mer på kaspersky.com/MITRE

Läs mer om Kaspersky Anti Targeted Attack Platform genom att besöka:

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

Nyheter om cyberhot: securelist.com
IT-säkerhetsnyheter: business.kaspersky.com
IT-säkerhet för SMB: kaspersky.com/business
IT-säkerhet för stora företag: kaspersky.com/enterprise

www.kaspersky.com

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

Proven. Transparent. Independent.