



Svaret til cybersikkerhed og risikobegrænsning i en æra med digital forandring

Digital forandring er nøglen til vækst i virksomhederne og institutionel effektivitet globalt. Men at sikre infrastrukturen af den digital organisation repræsenterer en betydelig udfordring. Avancerede trusler og målrettede angreb på unikke netværkselementer, skjulte og inerte indtil de trigger, tilføjer blot til risikofaktorer til den digital forandring, hvilket sætter virksomhedens vækst og udviklingsinitiativer på spil. Mens de teknikker, som cyberkriminelle bruger, konstant udvikler sig og bliver mere og mere fokuserede målrettet mod specifikke miljøer, afhænger for mange organisationer fortsat af konventionelle sikkerhedsteknologier for at beskytte sig mod nuværende og fremtidige trusler.

Digital forandring - en ny rolle for cybersikkerhed

Cybersikkerhed sammen med efterlevelse og dataforbrug er blevet primære strategiske prioriteter for digital virksomheder. Organisationer leder efter nye tilgange til sikkerhed, der faciliterer et klart fokus på virksomhedens behov.

Nye udfordringer for større virksomheder:

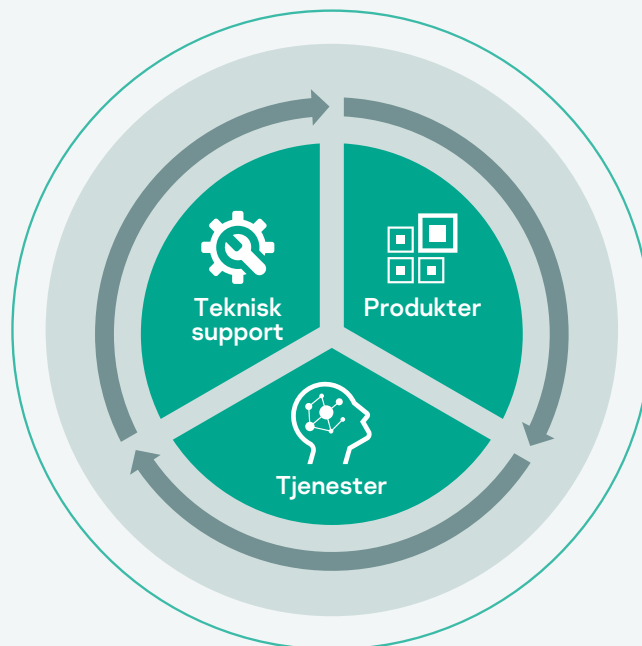
- Høj mængde af manuelle opgaver påkrævet for hændelsesrespons
- For få medarbejdere på IT-sikkerhedsteamet og en mangel på ekspertise på højt niveau
- For mange sikkerhedshændelser at behandle, analysere, fordele og svare effektivt på indenfor en begrænset tidsramme
- Tillid og efterlevelsproblemer ved datadeling efterhånden som digital infrastruktur udvider sit fokus
- Mangel på synlighed og udfordringer ved bevisindsamling til efterbrudsanalyse

Virksomhedsmæssige fordele

- Reduceret finansiel & driftsskade forårsaget af cyberkriminalitet
- Reduceret kompleksitet gennem en simpel, virksomhedsorienteret og administreret grænseflade.
- Reducerede administrative omkostninger gennem opgaveautomatisering og simplificerede sikkerhedsefterlevelsprocesser
- Øget ROI gennem ukompliceret automatisering af arbejdsflows og ingen forstyrrelser til virksomhedens drift
- Mindsket risiko fra avancerede trusler gennem hurtig registrering

En samlet løsning til at starte innovationen mod digital forandring

Kaspersky Threat Management and Defense består af en unik kombination af førende sikkerhedsteknologier, teknisk support og cybersikkerhedstjenester, som alle kan tilpasses til organisations behov samt antage en strategisk tilgang, hvilket leverer samlede processer til beskyttelsen mod avancerede trusler og unikt målrettede angreb.



Produkter

- Kaspersky Anti Targeted Attack Platform
- Kaspersky Endpoint Detection and Response
- Kaspersky Endpoint Security for Business
- Kaspersky Hybrid Cloud Security
- Kaspersky Security for Mail Server
- Kaspersky Security for Internet Gateway
- Kaspersky Private Security Network

Tjenester

- Kaspersky Cybersecurity Training
- Kaspersky Threat Intelligence Portal
- Kaspersky Managed Detection and Response
- Kaspersky Incident Response

Teknisk support

- Kaspersky Maintenance Service Agreement
- Kaspersky Security Account Manager
- Kaspersky Professional Services

Anerkendt til at være den
mest effektive løsning
i industrien



Gartner Peer Insights
**Customers' Choice for
Endpoint Detection &
Response, 2020**

MITRE | ATT&CK®

Registreringskvalitet er bekræftet
af MITRE ATT&CK Evaluation



SE Labs Breach
Response Test:
AAA Awards



ICSA Labs, Advanced
Threat Defense test
(Q3 2019): **100%
registreringsrater
med ingen falske
positive**



Topspiller i Radicati APT Protection
Market Quadrant 2020

Vælg den ideelle balance mellem teknologier og tjenester

Kaspersky tilbyder også en række programmer til at træne færdigheder sammen med data om trusselsefterretninger, der kan berige interne undersøgelsesresultater, for at booste dit teams ekspertise. Vores Managed Detection and Response tjeneste betyder, at dine ressourcer inden for IT-sikkerhed kan gemmes ved at overdrage hændelsesrelaterede behandlingsopgaver til os, eller du kan gå til Kaspersky for at få ekspertvurderinger og ekspertise inden for unik trusselsjagt. Uanset hvad dit forretningsbehov mht. IT-sikkerhed er, både i dag og i fremtiden, så har vi løsningen.

Udvidet forsvar med et bredere perspektiv

Kaspersky Anti Targeted Attack Platform med Kaspersky EDR sikrer grundlæggende flere potentielle trusselsindgangspunkter på både netværks- og slutpunktsniveauer og giver udvidede registrerings- og svarfunktioner. IT-sikkerhedseksperter er bevæbnet med et omfattende værktøjssæt til multidimensionel trusselsregistrering, dybdegående undersøgelser, proaktiv trusselsjagt og et centraliseret modsvar på komplekse hændelser. Den integreres fuldt ud med Kaspersky Endpoint Security for Business, der deler en enkelt agent med Kaspersky EDR, Kaspersky Hybrid Cloud Security og med både Kaspersky Security for Mail Server og Kaspersky Security for Internet Gateway for at give automatiserede svar til komplekse trusler på gatewayniveau. Denne alt-i-en-løsning reducerer betydeligt den tid og indsats, som dit IT-sikkerhedsteam skal bruge på trusselsbeskyttelse takket være maksimal automatisering af forsvarshandlinger på både netværks- og slutpunktsniveauer og kontekstuelle hændelsesrepræsentationer i den enkle webkonsol.

En betroet sikkerhedsløsning, der leverer komplet privatliv

Objektsanalyse foretages på arbejdspladen med ingen udgående dataflow via integration med Kaspersky Private Security Network til større virksomheder med strenge privatlivspolitikker. Dette leverer indgående omdømmeopdateringer i realtid mens virksomhedens data bevares i fuld isolation.

Optimer dit Security Operations Center

For at bekæmpe de mest sofistikerede nutidige cybertrusler og tilpasse sig løbende udfordringer i et omskifteligt trusselsmiljø bør dit SOC (Security Operations Center) være udstyret med avancerede teknologier, som er drevet af trusselsefterretninger, og have professionelle medarbejdere, der har den nødvendige viden og ekspertise. Resultatet er en komplet forsvarscyklus mod de mest komplekse, APT-lignende angreb og målrettede kampagner. Inden for rammerne af Threat Management and Defense tilbyder vi et helt arsenal af avancerede sikkerhedsteknologier og -tjenester til at booste din SOC-effektivitet.

Kaspersky Managed Detection and Response

Hvis du leder efter vidtrækkende ekspertise indenfor trusselsjagt, kan du udvide dine egne ressourcer med færdighederne & erfaringerne fra dine egne trusselsjægere, som vil:

- Gennemgå data indsamlet i dit miljø
- Hurtigt give dit sikkerhedsteam besked, hvis ondsindet aktivitet registrering
- Give råd om, hvordan du svarer og udbedrer

Nyheder om IT-sikkerhedstrusler: securelist.com
Nyheder om IT-sikkerhed: business.kaspersky.com
IT-sikkerhed for små og mellemstore virksomheder:
kaspersky.com/business
IT-sikkerhed for større virksomheder: kaspersky.com/enterprise

www.kaspersky.com

© 2020 AO Kaspersky Lab.
Registrerede varemærker og servicemærker tilhører deres
respektive ejere.



Vi er anerkendte. Vi er uafhængige. Vi er transparente.
Vi har forpligtet os til at opbygge en mere sikker
verden, hvor teknologi kan gøre vores liv bedre. Det er
derfor, at vi gør den sikker, så alle kan få glæde af de
uendelig muligheder, den bringer. Cybersikkerhed for
en mere sikker i morgen.

Få mere at vide på kaspersky.com/transparency



**Proven.
Transparent.
Independent.**