kaspersky BRING ON THE FUTURE

Kaspersky Threat Management & Defense

Het antwoord op het voorkomen van risico's bij cybersec een tijdperk van digitale transformatie

Digitale transformatie is de sleutel tot bedrijfsgroei en institutionele effectiviteit wereldwijd. Maar het beveiligen van de infrastructuur van de digitale organisatie is een enorme uitdaging. Geavanceerde bedreigingen en gerichte aanvallen op unieke netwerkelementen, verborgen en onzichtbaar totdat ze worden getriggerd, dragen bij aan de risicofactoren rond digitale transformatie, waardoor bedrijfsgroei en ontwikkelingsinitiatieven in gevaar komen. Terwijl de technieken die door cybercriminelen worden gebruikt voortdurend evolueren en steeds meer gericht zijn op specifieke omgevingen, vertrouwen te veel organisaties nog steeds op conventionele beveiligingstechnologieën om zich te beschermen tegen huidige en toekomstige dreigingen.

Digitale transformatie: een nieuwe rol voor cybersecurity

Cybersecurity is samen met het naleven van regels en gegevensgebruik een belangrijke strategische prioriteit geworden voor digitale bedrijfsvoering. Organisaties zoeken beveiligingsmethoden met een duidelijke nadruk op bedrijfsbehoeften.

Nieuwe uitdagingen voor bedrijven:

- Veel handmatige taken voor incidentrespons
- Onderbezetting van het IT-beveiligingsteam en een gebrek aan specialistische kennis
- Te veel beveiligingsgebeurtenissen om binnen een beperkt tijdsbestek te verwerken, analyseren, beoordelen en er op effectieve wijze op te reageren
- Problemen met vertrouwen en conformiteitsproblemen met betrekking tot het delen van gegevens wanneer de digitale infrastructuur wordt uitgebreid
- Gebrek aan inzicht en problemen met bewijsverzameling voor analyse na een beveiligingsinbreuk

Zakelijke voordelen

- Minder financiële en operationele schade veroorzaakt door cybercriminaliteit
- Minder complexiteit door een eenvoudige, bedrijfsgeoriënteerde beheerinterface
- Lagere administratiekosten door het automatiseren van taken en vereenvoudigde processen voor beveiligingsconformiteit
- Hoger ROI dankzij naadloze workflow-automatisering zonder bedrijfsprocessen te onderbreken
- Minder risico op geavanceerde dreigingen door snelle detectie

Een samengestelde oplossing voor snellere innovatie bij digitale transformatie

Kaspersky Threat Management and Defense bestaat uit een unieke combinatie van toonaangevende beveiligingstechnologieën, ondersteuning en cybersecuritydiensten die zich volledig aanpassen aan de specifieke kenmerken van de organisatie met een strategische aanpak, waardoor uniforme beveiligingsprocessen tegen geavanceerde bedreigingen en unieke gerichte aanvallen worden geleverd.

Producten

- 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

Services

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

Ondersteuning

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

Bewezen als effectiefste oplossing in de branche

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

Detectiekwaliteit bevestigd via MITRE ATT&CK Evaluation

SE Labs Breach Response Test: **AAA-beoordeling**

ICSA Labs, Advanced Threat Defense test (Q3 2019): **detectiepercentage van 100%, met geen valse positieven**

Topspeler in Radicati APT Protection Market Quadrant 2020

Kies je ideale balans tussen technologieën en diensten

Om de expertise van je team te vergroten, biedt Kaspersky ook een aantal vaardigheidstrainingen en gegevens over dreigingsinformatie waarmee je de interne onderzoeksresultaten kunt verbeteren. Onze Managed Detection and Response-service betekent dat je IT-beveiligingsmiddelen kunnen worden behouden door incident-gerelateerde verwerkingstaken aan ons over te dragen of door Kaspersky te vragen om deskundige beoordelingen en unieke expertise bij de detectie van bedreigingen. Wat je bedrijf nu of in de toekomst ook nodig heeft op het gebied van IT-beveiliging, wij hebben de oplossing.

Uitgebreide bescherming met een breder perspectief

Het Kaspersky Anti Targeted Attack Platform met Kaspersky EDR als kern beveiligt meerdere potentiële dreigingspunten op zowel netwerk- als endpointniveau en biedt uitgebreide detectie- en responsmogelijkheden. De IT-beveiligingsexpert is gewapend met een uitgebreide toolkit voor het ontdekken van multidimensionale dreigingen, diepgaand onderzoek, proactieve dreigingsopsporing en een gecentraliseerde reactie op complexe incidenten. Het is volledig geïntegreerd met Kaspersky Endpoint Security for Business, dat één agent deelt met Kaspersky EDR, Kaspersky Hybrid Cloud Security, en met Kaspersky Security for Mail Server en Kaspersky Security for Internet Gateway, om geautomatiseerde reacties op het niveau van de gateway te bieden voor complexe dreigingen. Doordat dit een alles-in-één oplossing is, zorgt dit ervoor dat uw IT-beveiligingsteams aanzienlijk minder tijd en moeite hoeven te steken in bescherming tegen bedreigingen, dankzij de maximale automatisering van defensieve acties op zowel netwerk- als endpointniveau, en de contextuele weergave van incidenten in één webconsole.

Een betrouwbare beveiligingsoplossing die complete privacy biedt

Voor ondernemingen met een strikt privacybeleid wordt de objectanalyse ter plaatse uitgevoerd zonder uitgaande gegevensstroom via integratie met Kaspersky Private Security Network. Dit levert realtime inkomende reputatie-updates op, terwijl de volledige isolatie van bedrijfsgegevens behouden blijft.

Versterk uw Security Operations Center

Om de meest geavanceerde hedendaagse cyberbedreigingen te bestrijden en u aan te passen aan de voortdurende uitdagingen in een veranderende bedreigingsomgeving, moet uw Security Operations Center (SOC) uitgerust zijn met geavanceerde technologieën, voorzien van informatie over bedreigingen en ondersteund door professionals met alle benodigde kennis en expertise. Het resultaat is een volledige verdedigingscyclus tegen de meest complexe, APT-achtige aanvallen en gerichte campagnes. Binnen het kader van Kaspersky Threat Management and Defense bieden wij een complete serie geavanceerde verdedigingstechnologieën en -diensten om de effectiviteit van uw SOC te vergroten.

Kaspersky Managed Detection and Response

Als u op zoek bent naar uitgebreide expertise op het gebied van dreigingsopsporing, kunt u uw eigen middelen uitbreiden met de vaardigheden en ervaring van onze eigen dreigingsopsporing, die u zullen helpen bij:

- Gegevens onderzoeken die zijn verzameld in je omgeving
- Je beveiligingsteam snel waarschuwen als er schadelijke activiteiten worden gedetecteerd
- Advies geven over respons en herstel

Nieuws over cyberdreigingen: securelist.com
Nieuws over IT-beveiliging: business.kaspersky.com
IT-beveiliging voor het mkb: kaspersky.com/business
IT-beveiliging voor grote bedrijven: kaspersky.com/enterprise

www.kaspersky.com

We hebben ons bewezen. We zijn onafhankelijk. We zijn transparant. Ons doel is een veiligere wereld, waarin technologie onze levens verbetert. We beveiligen deze technologie dus, zodat iedereen overal toegang heeft tot de onbeperkte mogelijkheden ervan. We bieden cyberveiligheid voor een veiligere toekomst.

Ga voor meer informatie naar kaspersky.com/transparency

Proven. Transparent. Independent.