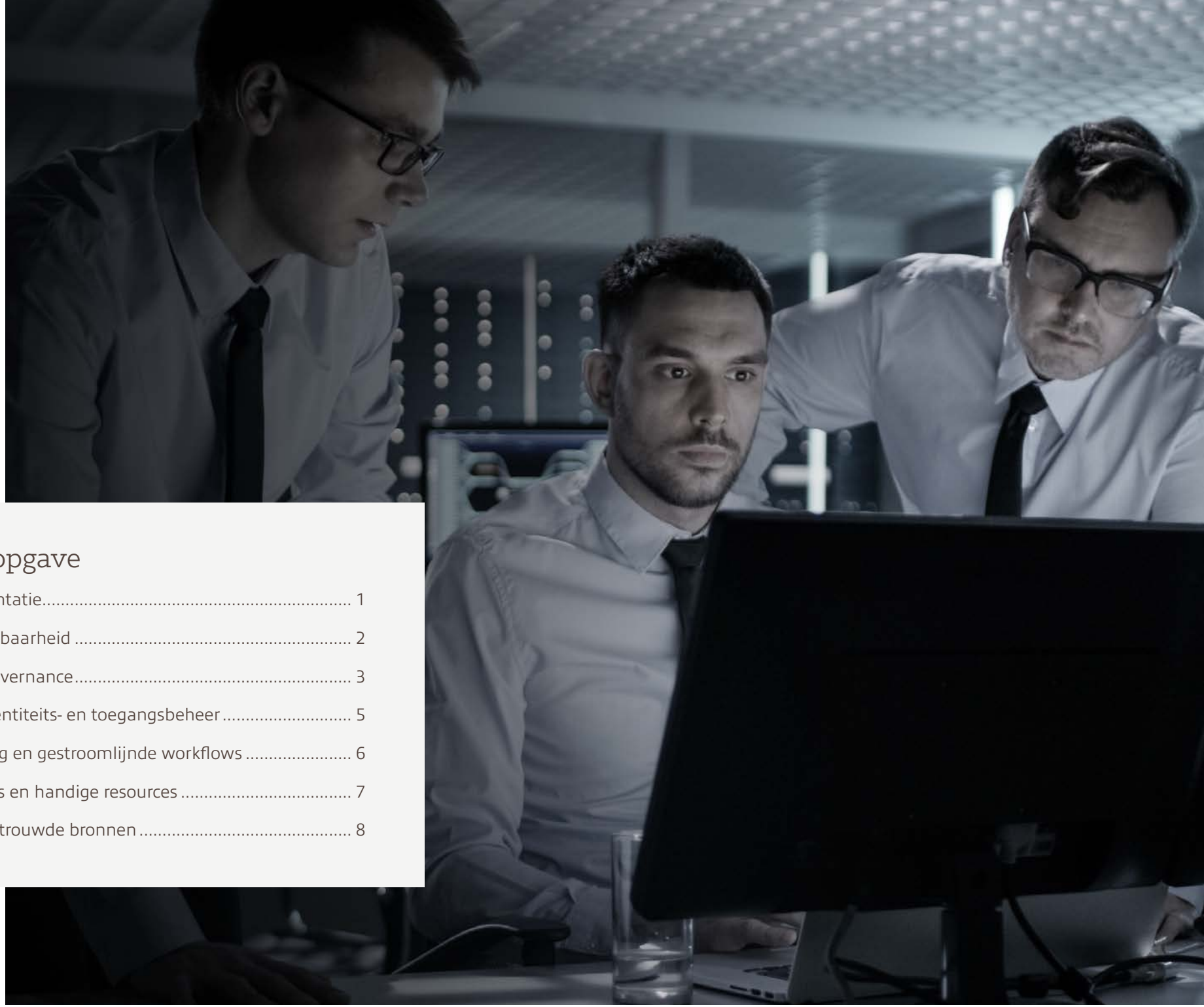
5 kenmerken van een modern beveiligingsprogramma

Insight®



Inhoudsopgave

Een korte oriëntatie

Omdat data exponentieel blijft groeien, is er ook een toename in de aantallen die iets willen bereiken met kwaadaardige aanvallen. Het is nu crucialer dan ooit voor organisaties om hun beveiligingsstrategie te evalueren.

In de eerste helft van 2021 zijn

1767 inbreuken gemeld,

wat heeft geleid tot een blootstelling van **meer dan 18,8 miljard records.**[1]

De gemiddelde kosten waren

$ 1,07 miljoen hoger

bij inbreuken waarbij werken op afstand een factor was bij het veroorzaken van de inbreuk.[2]

De gemiddelde kosten van een data-inbreuk zijn nu

$ 4,24 miljoen.[2]

Soms is het verstandig om een stapje terug te doen. Wat moet een beveiligingsprogramma als doel hebben? Welke doelen zijn realistisch — en welke doelen niet? Hoe moeten beveiligingsinvesteringen worden gedaan en gemeten?

Wij vinden dat er vijf belangrijke kenmerken zijn voor een succesvol en gemoderniseerd beveiligingsprogramma, voor bedrijven van elk type of elke omvang.

[1] Risk Based Security. (Augustus 2021). 2021 Mid Year QuickView Data Breach Report.
[2] Ponemon Institute. (2021). 2021 Cost of a Data Breach Report. Gesponsord door IBM Security.

HOOFDSTUK 1

Volledige zichtbaarheid

IT-omgevingen worden steeds groter. We zien groei in datavolumes, aantal devices, platforms en verkeer. Elke uitbreiding introduceert nieuwe bedreigingsvectoren en extra uitdagingen op het gebied van zichtbaarheid.

Feit:	Overweging:
Wereldwijde datacreatie zal **groeien van 64,2 ZB in 2020 naar 180 ZB in 2025**.[3]	**Hoe worden al deze gegevens gecontroleerd en beveiligd,** met name wanneer ze zich door IT-omgevingen bewegen?
Tegen 2027 zullen er meer dan 41 miljard Internet of Things (IoT)-devices zijn, een duidelijke toename ten opzichte van ongeveer 8 miljard in 2019.[4]	**Welk niveau van zichtbaarheid kunnen we redelijkerwijs nastreven**, gezien deze groei in verbonden devices?
87% van de bedrijven heeft vorig jaar een multicloud-aanpak (met meer dan één public cloud-provider) in gebruik genomen of is begonnen met het gebruik hiervan.[5]	**Hoe maakt u zichtbaarheid eenvoudig, of zelfs mogelijk,** met meerdere platforms van verschillende soorten in dezelfde IT-omgeving?

Toch is volledige zichtbaarheid van cruciaal belang. Wanneer een IT-omgeving hoogwaardige zichtbaarheid biedt en activiteiten worden gecontroleerd, kan dit vele voordelen opleveren.

Ten eerste kunnen aanvalspogingen worden verhinderd en mogelijke schade worden beperkt. Een succesvolle aanval begint meestal met het benutten van één kwetsbaar punt en dringt vervolgens door in meerdere systemen vanaf dat ene beginpunt. Als een inbreuk eerder wordt ontdekt, kan de omvang van het verlies beter worden gecontroleerd. In 2019 was 206 dagen de gemiddelde tijd voor het identificeren van een inbreuk.[2] Denkt u eens aan het aantal records, systemen en gebruikers dat een cyberaanvaller in de loop van meer dan zes maanden zou kunnen bereiken; dit is geen prettige gedachte.

Zichtbaarheid, in combinatie met tools voor monitoring en/of bedreigingsinformatie, draagt ook grotendeels bij aan de effectiviteit van preventie-inspanningen. Gebruikersgedrag bestaat meestal uit patronen, die zich op logische en repetitieve manieren bewegen. Ongebruikelijke activiteiten of bewegingen kunnen duiden op de aanwezigheid van kwaadwillende partijen, zodat IT-beveiligingsmanagers aanvallen kunnen voorkomen en toegang of beleidswijzigingen kunnen implementeren die voorheen onopgemerkte beveiligingsgaps kunnen aanpakken.

[3] Statista. (mei 2022). Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2025.
[4] Newman, P. (maart 2020). The Internet of Things 2020. Business Insider Intelligence.
[5] Marketpulse Research door IDG Research Services. (Februari 2020). The State of IT Modernisation 2020. In opdracht van Insight.

HOOFDSTUK 2

Uitgebreide governance

Veel mensen denken mogelijk aan frameworks zoals COBIT of ITIL wanneer ze de term governance horen. Hoogover draait governance om de manier waarop IT-beslissingen zijn afgestemd op bedrijfsdoelstellingen of -behoeftes. Governance moet ook iets doen aan het ownership en verantwoordelijkheidsgevoel — wie verantwoordelijk is en wie de stakeholders zijn.

Governance is cruciaal voor de beveiliging omdat het organisaties helpt om:

- Beveiligingsdoelstellingen te definiëren en af te stemmen
- Beveiligingsoplossingen te selecteren en valideren
- Training, richtlijnen en andere beveiligingsprogrammering voor gebruikers te organiseren
- Beveiliging onderdeel te maken van gesprekken over adoptie van platforms, netwerkarchitectuur en andere componenten van IT-strategie
- De beveiligingshouding te verbeteren door middel van duidelijk gedefinieerde rollen en processen

Effectieve governance is niet eenvoudig te bereiken, echter. In het meest recente Insight aangevraagde IDG-onderzoek meldden respondenten dat de grootste uitdaging voor IT-modernisering het opzetten van nieuwe governancestrategieën en -processen is voor de IT-modernisering en cloud te ondersteunen.[5]

Een lastig aspect van het bedenken van effectieve governance is, in feite, het toegenomen gebruik van de cloud. Organisaties kunnen al jaren beschikken over praktische governanceframeworks, die alleen betrekking hebben op het datacenter en de duidelijk gedefinieerde perimeter.

Volgens het rapport Flexera 2022 State of the Cloud

89% van de organisaties heeft een multicloud-strategie in gebruik genomen,

en

80% volgen een hybride cloudaanpak door het gebruik van public en private clouds te combineren.[6]

Traditionele governance uitbreiden naar de cloud is essentieel, maar hier is geen vaste formule voor, en vereist investeringen in tijd en middelen.

Dit heeft minimaal gevolgen voor de cloudbeveiliging, of de perceptie ervan. Uit het IDG-onderzoek bleek dat het beheer van public cloudbeveiliging de grootste uitdaging is bij het optimaliseren van cloudervaring en -resultaten, gevolgd door uitdagingen op het gebied van governance en processen.[5]

Door uitgebreide governance op te zetten, inclusief alle platforms, rollen, stakeholders, enz., kan een organisatie ervoor zorgen dat haar beveiligingsactiviteiten robuust, relevant en ondersteund blijven.

[6] Flexera. (2022). 2022 State of the Cloud Report.

HOOFDSTUK 3

Strategisch identiteits- en toegangsbeheer

Iedereen en elk systeem zonder kwaadwillende bedoeling, heeft een identiteit en specifieke toegangsrechten of zou dat moeten hebben. Naarmate IT-omgevingen zich uitbreiden en endpoints zich steeds verder verspreiden, worden identiteits- en toegangsbeheer een centraal onderwerp van beveiligingsgesprekken.

De meeste organisaties hebben Active Directory® en gebruiken verschillende diensten van derden. Dit resulteert in meerdere identiteiten, systemen en oplossingen — en veel complexiteit, vooral wanneer handmatige inspanningen nodig zijn om alles te beheren.

Hier volgen een aantal overwegingen die u moet maken bij identiteits- en toegangsbeheer op beveiligingsgebied:

Denk aan de data.

Hoe gevoelig is dit? Wie heeft er echt toegang nodig? Wanneer en voor hoe lang? Wie is het eerste aanspreekpunt en is dat de beste optie? Het is mogelijk dat organisaties een initiatief voor dataclassificatie als eerste stap moeten ondernemen.

Denk aan uw gebruikers.

Hebt u gebruikerstypen ingesteld? Wanneer hebt u voor het laatst machtigingen geëvalueerd? Hoe verifieert u identiteiten en het geven van toegang? Van verdediging tot zero trust, er zijn veel bruikbare modellen.

Denk aan authenticatie.

Wachtwoorden zijn steeds minder populair. Welke alternatieven hebt u overwogen? Passen mechanismen zoals biometrie bij uw organisatie? Hoe zou u uw huidige authenticatie-aanpak veiliger kunnen maken in de nabije toekomst?

Om het identiteits- en toegangsbeheer strategisch en succesvol te laten verlopen, moeten organisaties alle identiteiten op één locatie bewaren, overwegen om een Cloud Access Security Broker (CASB)-oplossing te implementeren en een gelaagde beveiligingsaanpak implementeren.

HOOFDSTUK 4

Automatisering en gestroomlijnde workflows

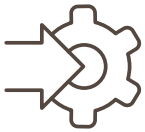
Beveiliging biedt geen ruimte voor fouten. Er kan elk moment van kwetsbaarheden of gaps worden geprofiteerd. Menselijke fouten die leiden tot succesvolle aanvallen zijn onvergeeflijk. Fouten in de beveiliging zijn duur. Ironisch genoeg kan het vermijden van dergelijke kosten ook vrij duur zijn, afhankelijk van de aanpak die u volgt.

Wat bedoelen we? Security Operations Centers (SOC's) moeten worden gemoderniseerd, inclusief toolsets, technologieën, processen/methoden en middelen. In de enquête "The State of IT Modernisation 2020" noemde 57% van de respondenten het upgraden van beveiligingsinfrastructuur en -processen een van de grootste obstakels voor het moderniseren van de IT-werkomgeving.[5] Maar, waar interne resources schaars zijn, moeten organisaties externe partners vinden die cruciale automatisering en andere expertise kunnen bieden.

Automatisering binnen het SOC levert duidelijke voordelen op:

- Snellere detectie-, respons- en herstelmogelijkheden
- Minder fouten vanwege handmatige activiteiten
- Beveiligingsmiddelen worden vrijgemaakt voor strategische prioriteiten
- Betere gebruikerservaringen en tevredenheid

Sommige taken zijn bijzonder geschikt voor automatisering. Neem bijvoorbeeld het reageren op waarschuwingen. In een onderzoek van CRITICALSTART zei 70% van de respondenten dat ze meer dan 10 waarschuwingen per dag onderzoeken, die elk meer dan 10 minuten in beslag nemen om te onderzoeken (cijfers die respectievelijk 45% en 64% hoger waren dan het voorgaande jaar). Waarschuwingsmoeheidis een veelvoorkomende klacht in dergelijke omgevingen, waardoor SOC-professionals waarschuwingen negeren, betalen om meer personeel in dienst te nemen om de last te delen of zelfs hun baan opzeggen.[7]



Door het aantal repetitieve taken van personeel te verminderen en gemeenschappelijke beveiligingsprocessen te automatiseren, kunnen organisaties het moreel verbeteren, een strategischere SOC opbouwen en gemakkelijker een benadering van meerdere lagen voor beveiliging kiezen met minder middelen.

[7] CRITICALSTART. (2019). The Impact of Security Alert Overload.

HOOFDSTUK 5

Effectieve tools en handige resources

Een organisatie is beperkt in wat deze kan doen zonder de juiste tools, technologieën en middelen. Het belangrijkste woord is "juist". Uit een rapport van het Ponemon Institute bleek dat bedrijven gemiddeld 47 verschillende cyberbeveiligingsoplossingen en -technologieën hebben geïmplementeerd.[8] Hetzelfde rapport geeft aan dat meer dan de helft (53%) van de IT-specialisten niet weet hoe goed hun geïmplementeerde cyberbeveiligingstools werken, en slechts 39% zegt dat ze volledige waarde uit hun beveiligingsinvesteringen halen.

Wat is het probleem? Dat zijn er verschillende:

- De tijd of expertise hebben om goede beslissingen te nemen over beveiligingsproducten of -platforms
- Inzicht in de vaardigheden die nodig zijn om beveiligingsinvesteringen te implementeren, in gebruik te nemen, te integreren, aan te passen en te optimaliseren
- Complexe IT-omgevingen (door snelle groei, M&A-activiteit, enz.) met ontelbare aanvalsvectoren
- IT-investeringen afstemmen op budgetten, wat soms leidt tot onfortuinlijke compromissen
- Het verkrijgen van point-oplossingen die elk een beperkt bereik bieden en bijdragen aan toolvermoeidheid
- Belangrijk beveiligingstalent vinden en behouden

IT-directeuren moeten hun risicohouding en mogelijkheden voor het reageren op bedreigingen voortdurend opnieuw evalueren en tegelijkertijd gebruikmaken van het nieuwste beveiligingspakketten Door de afstemming te zoeken met bedrijfs- en brancheleiders, kunnen IT-organisaties ook zorgen voor de buy-in die nodig is om een beveiligingsbewuste organisatie te ontwikkelen en het optreden van schaduw-IT en ander risicovol gedrag te minimaliseren.

Wat kunt u doen om deze zorgen aan te pakken en zinvolle verbeteringen in uw beveiligingsactiviteiten te stimuleren?

[8] Ponemon Institute. (2019). The Cybersecurity Illusion: The Emperor Has No Clothes. Gesponsord door AttackIQ.

Gebruik vertrouwde bronnen

Insight helpt bedrijven zoals de uwe bij het beoordelen van hun beveiligingsomgeving, het ontwikkelen van een uitvoerbaar stappenplan, het implementeren van de optimale oplossingen en het beheren van een eersteklas SOC met alle vijf de beschreven kenmerken. Wij gaan er vanuit dat beveiliging niet alleen een technologie-issue is, maar een zakelijke prioriteit - we combineren technische en advieservaring en intelligentie om uw volledige beveiligingsprogramma uit te breiden.

Een manier waarop we dit kunnen leveren is met Microsoft® Sentinel™, een cloud-native Security Information and Event Management (SIEM)- en Security Orchestration and Automated Response (SOAR)-oplossing die beveiligingsdata verzamelt in de hele hybride onderneming en de kracht van Artificial Intelligence (AI) gebruikt om bedreigingen snel te identificeren en onderzoeken.

Waarom Insight en Microsoft Sentinel?

Maximaliseer de voordelen en capaciteiten van uw beveiligingsinvesteringen

Stem beveiligingsinspanningen beter af op bedrijfsdoelstellingen

Verbeterde beveiliging, zichtbaarheid en controle over uw gehele IT-omgeving.

Versnelling en automatisering van jacht op en detectie van cyberbedreigingen

Draag de taak over van het bewaken van uw netwerk, systemen, applicaties en gegevens

Verminder risico's en maak beveiligingsgerelateerde kosten voorspelbaarder

Over Insight

Meer dan 20 jaar levering van support services

PCI DSS-conform, SOC 2 Type II-gecertificeerd, ISO 27000-gecertificeerd en lid van TSANet en TSIA

Een toonaangevende Microsoft-partner met **18 Gold & Silver-competenties**

Gold Microsoft Partner Microsoft | Azure Expert MSP

Een Azure Expert Managed Services Provider (MSP) en de **grootste Azure-partner**

Onlangs uitgeroepen tot winnaar van de Microsoft Security 20/20 Award voor de categorie Azure Security Deployment Partner of the Year

Wat zegt Microsoft?

Ann Johnson, corporate vice president van Cybersecurity Solutions bij Microsoft, zei: "Door ons Microsoft-beveiligingsportfolio te combineren met de beveiligingsdiensten van Insight, stellen we onze klanten in staat om hun beveiligingsactiviteiten te moderniseren. Cyberbeveiliging is complex, maar hoeft niet ingewikkeld te zijn. Het uitbreiden van onze beveiligingsrelatie met Insight helpt organisaties hun beveiligingsactiviteiten te vereenvoudigen en te schalen als ze groei doormaken."

Over Microsoft Sentinel

- Snel en relatief eenvoudig te implementeren, greenfield of via re-directen van logs
- Flexibel en schaalbaar, waardoor dynamische aanpassingen voor workloads of compliance mogelijk zijn
- Kosteneffectief, zonder kosten vooraf of hardwarevereisten
- Ontwikkeld en consistent verbeterd door IT- en beveiligingsleiders
- Maakt gebruik van de nieuwste, geavanceerde AI- en machine learning-capaciteiten

Haal de tools en expertise in huis die u nodig hebt om alle vijf de kenmerken te ondervangen die in dit ebook worden beschreven. Ga direct aan de slag met Insight en Microsoft Sentinel.

Neem contact met ons op

nl.insight.com

MKT6270_NL