

# Doe meer met minder.

De beveiligingskosten stijgen naarmate het aantal beveiligingsrisico's toeneemt. Tegelijkertijd staan CISO's onder druk om de kosten in de hand te houden.

**82%**

voelt zich onder druk gezet om de kosten te verlagen\*

**#1**

prioriteit om de kosten te verlagen is een betere bedreigingsbeveiliging\*\*

\*Microsoft Pandemic CISO Survey 2020

\*\*Survey of 501 US Security Decision Makers, in opdracht van Microsoft, maart 2022

**Met Microsoft Beveiliging bereik je meer met minder. Hier lees je hoe.**

## Leveranciersbeheer vereenvoedigen.

97% van de ondervraagde organisaties heeft een strategie voor leveranciersconsolidatie of is dat van plan binnen de komende drie jaar.\*

\*Gartner, "Invest Implications: Emerging Tech, Innovatie en nieuwe koopverkeuren leiden de consolidatie van de beveiligingsmarkt", 25 oktober 2022

### Velen wenden zich tot Microsoft. Waarom?



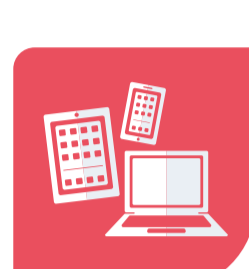
**Beveiliging**



**Naleving**



**Identiteit**



**Apparaatbeheer**



**Privacy**

Microsoft integreert end-to-end oplossingen voor meer dan 50 verschillende categorieën in clouds en platforms.

**60%**

Potentiële besparingen door eliminatie van overbodige mogelijkheden voor klanten die vergelijkbare oplossingen vervangen door Microsoft 365 E5 Beveiliging & Microsoft 365 E5 Naleving.\*\*

**0,-**  
extra kosten

Veel leveranciers vragen een extra vergoeding voor het beheer van cloudbeveiligingspostuur. Met Microsoft Defender voor Cloud is deze mogelijkheid inbegrepen, wat betekent dat er geen extra kosten zijn.

\*\*Besparingen gebaseerd op openbaar beschikbare geschette prijzen voor oplossingen van andere leveranciers en Web Direct/Basic voor Microsoft aanbod

**De Microsoft Cloud is de enige cloud waarmee je kan profiteren van zowel best-of-categorie producten, als best-of-suite oplossingen over de hele tech stack, op elk gebied dat het belangrijkste is voor onze klanten, zodat ze meer kunnen doen met minder.**

— Satya Nadella, Algemeen directeur

## Bedreigingen verminderen met AI en automatisering.

Het aantal en de complexiteit van schendingen op de beveiliging blijven toenemen. Organisaties die hun beveiligingsportefeuillerapport consolideren, melden een verminderd risico op schendingen.

**80%**

hogere kosten wanneer AI en automatisering van de beveiliging niet volledig werd geïmplementeerd\*

\*Ponemon Institute Cost of Breach Data 2021

**34%**

van alle datalekken wordt veroorzaakt door interne bedreigingen\*\*

\*\*Ponemon Institute Cost of Insider Risk, 2020

Met Microsoft Beveiliging kun je bedreigingen en insider-risico's sneller en nauwkeuriger opsporen en erop reageren. In door Microsoft in opdracht van Forrester Consulting uitgevoerde onderzoeken hebben organisaties gemiddeld aanzienlijke besparingen gerealiseerd:



**96%**

96% minder tijd aan het controleren van verdachte activiteiten\*



**88%**

88% minder tijd om te reageren op bedreigingen\*\*



**60%**

60% minder risico op een materiële schending\*\*

\*The Total Economic Impact™ Of Microsoft 365 E5 Naleving, februari, 2021 \*\*The Total Economic Impact™ Of Microsoft SIEM and XDR, augustus 2022

## Operationele efficiëntie verbeteren.

Aanvallen gebeuren en ze kunnen enorme verstoringen en economische schade veroorzaken, vooral bij organisaties die geen sterk zero trust fundament hebben geïmplementeerd.

**150**

toename van ransomware-aanvallen in 2021\*

**1,76**

miljoen hogere kosten zonder volgroeide zero trust geïmplementeerd\*\*

\*Microsoft vuurt terug op CrowdStrike over cyberbeveiliging, Bloomberg Technology, 9 december 2021 \*\*Ponemon Institute Cost of Breach Data 2021

Geïntegreerde werkstromen binnen het Microsoft Security-portfolio verhogen de efficiëntie, wat resulteert in een kosteneffectieve, geconsolideerde omgeving die jou kan helpen:

**1**

Herschik IT-tijd om menselijk kapitaal vrij te maken.

**4**

Minder aanvragen voor het opnieuw instellen van wachtwoorden door self-service mogelijk te maken.

**2**

Bespaar implementatietijd met ingebouwde SIEM.

**5**

Verbetering van de efficiëntie van netwerkgerelateerde IT-werkzaamheden.

**3**

Minder tijd besteden aan beveiligingsbeleid en compliancebeheer.

**6**

Minder tijd besteden aan voortdurende controle.

**Het gaat erom de juiste beveiligingsinvesteringen te doen, niet per se meer te investeren. Ervoor zorgen dat al jouw systemen samenwerken, zodat bedreigingen vroegtijdig worden opgemerkt en snel kunnen worden verholpen.**

— Bret Arsenaault, VP en CISO, Microsoft

## Het Microsoft-verschil: toonaangevende beveiliging.

Wees bedreigingen voor met een allesomvattende benadering van end-to-end, de allerbeste en AI-gestuurde beveiliging.

**43 T**

dreigingssignalen dagelijks geanalyseerd\*

\*FY22 Q4 - Persberichten - Investeersrelaties - Microsoft

**37 miljard**

geblokkeerde e-mailbedreigingen per jaar\*

\*Microsoft Digital Defense rapport 2022

**Meer dan 785.000**

klanten vertrouwen op Microsoft Beveiliging\*

\*Microsoft resultatenrapport vierde kwartaal boekjaar 2022



Meer dan 8.500 Microsoft Beveiligingstechnici en onderzoekers\*



Onderzoeks- en inlichtingenteams van wereldklasse zijn toegewijd aan het verijdelen van geavanceerde cyberaanvallen

\*Verdedigen tegen bedreigingen met de laatste onderzoeksinzichten en trends, Maart 2022, Cyber Signals

**Klaar om te beginnen?**

**Neem vandaag nog contact met ons op voor alle details!**



**Wij zijn er, altijd.**