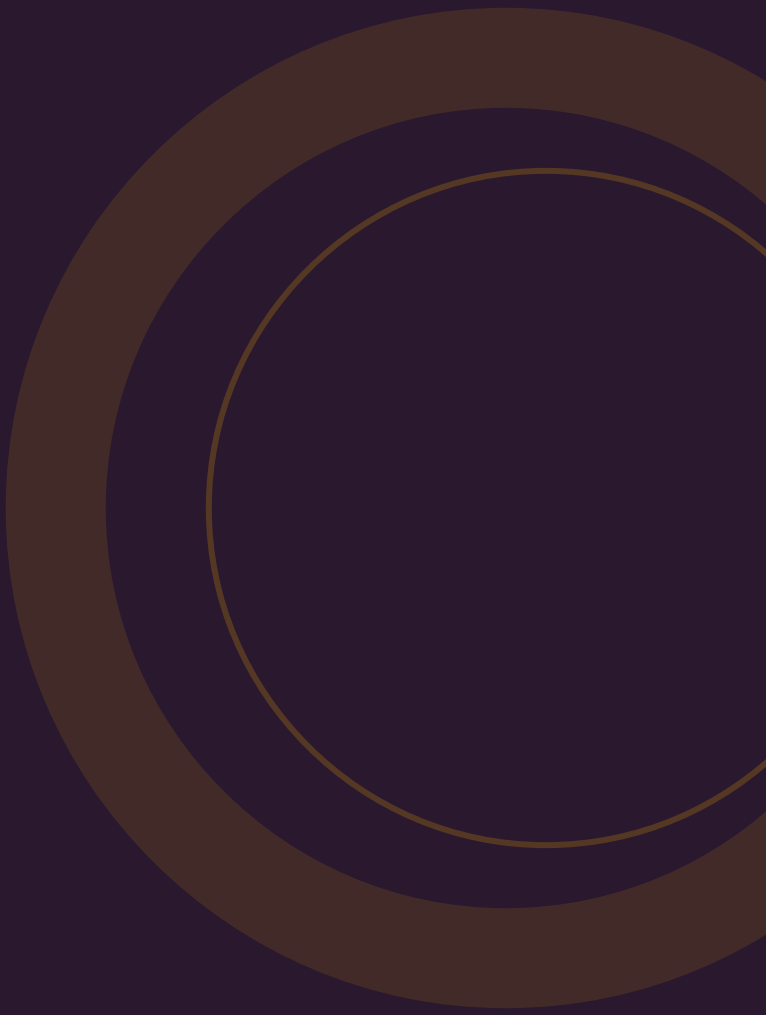
GIDS

De complete gids voor Microsoft 365 Security

Hardening, Conditional Access, Defender, DLP en compliance. Met actuele Nederlandse marktdata.



Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij

Microsoft 365 is het meest aangevallen platform ter wereld.

600M
dagelijkse identiteitsaanvallen op Microsoft-accounts
Microsoft MDDR 2025 [1]

7.000/sec
wachtwoordaanvallen per seconde geblokkeerd door Microsoft
Microsoft [1]

28%
van datalekken begint met phishing of social engineering
Microsoft [1]

30--50%
gemiddelde Secure Score van enterprise M365-tenants
CoreView [2]

3M+
Tycoon 2FA phishing-berichten in feb 2026, gericht op M365
Proofpoint [3]

76%
MFA-gebruik bij NL bedrijven (10-50 pers.) in 2024
CBS [4]

EUR 40--90
per gebruiker/maand totale IT-werkplek incl. M365 en beveiliging
Support-IT [5]

+5--25%
M365 prijsverhoging per 1 juli 2026 -- security wordt gebundeld
Microsoft [6]

1. Wat is Microsoft 365 Security?

Microsoft 365 Security omvat alle beveiligingsmaatregelen gericht op het beschermen van je M365-omgeving: Exchange Online, SharePoint, Teams, OneDrive en Entra ID.

Dit gaat verder dan standaardinstellingen. Het betreft hardening, Conditional Access, Defender-configuratie, Data Loss Prevention en doorlopende monitoring. De gemiddelde M365-tenant scoort slechts 30-50% op Secure Score -- de meeste organisaties laten significante verbeteringen onbenut [2].

VIJF PIJLERS

- **Identity & Access** -- Conditional Access, MFA, Privileged Identity Management
- **Email beveiliging** -- Safe Links, Safe Attachments, anti-phishing
- **Data bescherming** -- Sensitivity labels, DLP, retention policies
- **Device management** -- Intune, device compliance
- **Monitoring** -- Defender portal, audit logging, alerts

2. Waarom is het belangrijk?

600 miljoen dagelijkse identiteitsaanvallen. OAuth-phishing die MFA omzeilt. AI-gegenereerde phishing die steeds overtuigender wordt.

Microsoft blokkeert 7.000 wachtwoordaanvallen per seconde [1]. 28% van datalekken begint met phishing [1]. In februari 2026 werden meer dan 3 miljoen Tycoon 2FA phishing-berichten verstuurd gericht op M365-accounts [3]. OAuth device code phishing is significant toegenomen sinds september 2025.

> **SECURE SCORE GAP**
>
> De gemiddelde enterprise tenant scoort 30-50% op Secure Score [2]. Dat betekent dat meer dan de helft van beschikbare beveiligingsmaatregelen niet is geactiveerd. Elke niet-geconfigureerde maatregel is een potentieel aanvalspad.

3. Het hardeningsproces

M365 hardening duurt 4-8 weken voor een middelgrote organisatie, met doorlopende optimalisatie.

1. **Security Assessment**
   WEEK 1
   Beoordeel huidige M365-configuratie. Check Secure Score, inventariseer Conditional Access policies, controleer MFA-status en admin-rechten.

2. **Identity & Access hardening**
   WEEK 1--2
   Configureer Conditional Access. Verplicht MFA voor alle gebruikers. Stel PIM in voor admin-accounts. Blokkeer legacy authentication.

3. **Email & Data beveiliging**
   WEEK 2--4
   Configureer Safe Links, Safe Attachments, anti-phishing policies. Implementeer DLP en sensitivity labels.

4. **Device management & monitoring**
   WEEK 4--6
   Configureer Intune device compliance. Stel audit logging en alert policies in.

5. **Doorlopend beheer**
   DOORLOPEND
   Monitor Secure Score, review alerts, pas policies aan. Kwartaalreview van alle configuraties.

4. Wat kost het?

TIER	WAT JE KRIJGT	PRIJSINDICATIE
Basis	Eenmalige hardening (Conditional Access, MFA, Defender basis)	EUR 2.000--5.000 eenmalig
Standaard	Hardening + maandelijks beheer + monitoring	EUR 5--10/gebruiker/maand
Premium	Volledig managed: 24/7 monitoring, IR, DLP, compliance	EUR 10--25/gebruiker/maand

> **Let op:** Dit komt bovenop je M365-licentiekosten (EUR 6-55/gebruiker/maand). Microsoft beveiligings-add-ons kosten EUR 1,90-15/gebruiker/maand [7].

5. Selectiecriteria

- **Microsoft-certificeringen** -- Minimaal Security Administrator Associate
- **Ervaring met jouw licentie-niveau** -- Business Premium, E3 of E5
- **Secure Score track record** -- Concrete voor- en na-cijfers
- **Monitoring en alerting** -- 24/7 of business hours?
- **Compliance-kennis** -- NIS2, AVG, ISO 27001

6. Veelgemaakte fouten

1. Standaardinstellingen niet aanpassen

M365 out-of-the-box is niet veilig genoeg. Legacy auth staat open, admin-accounts hebben permanente rechten.

2. MFA niet verplichten

Elke gebruiker zonder MFA is een potentiele ingang voor aanvallers.

3. Geen Conditional Access

Zonder Conditional Access kan iedereen overal inloggen zonder beperkingen.

4. Admin-accounts zonder PIM

Permanente global admin rechten zijn een groot risico. Gebruik just-in-time rechten.

5. Eenmalig hardenen

Zonder doorlopend beheer veroudert je beveiliging door configuratie drift en nieuwe dreigingen.

7. Compliance: NIS2 en regelgeving

M365-beveiliging is een directe invulling van NIS2-zorgplicht: e-mailbeveiliging, toegangsbeheer, audit logging. DLP en sensitivity labels helpen bij AVG-compliance. Per 1 juli 2026 bundelt Microsoft meer beveiligingsfuncties in standaardlicenties [6].

8. Verschil met verwante oplossingen

KENMERK	M365 SECURITY	EDR/XDR	SIEM/SOC
Focus	Cloud-werkplek	Endpoints	Organisatiebreed
Scope	Identiteit, e-mail, data	Laptops, servers	Alle databronnen
Relatie	Primair	Complementair	M365 als databron

9. Trends 2025--2026

1. Security Copilot

AI-beveiligingsassistent in M365 E5 vanaf juli 2026.

2. Passwordless

Passkeys en FIDO2 via Entra ID.

3. Security bundeling

Microsoft voegt beveiligingsfuncties toe aan basisplannen [6].

10. Aan de slag

Begin met een Secure Score check op security.microsoft.com. Vergelijk met het gemiddelde (30-50%) en bepaal welke acties de meeste impact hebben.

DIRECT AAN DE SLAG?

Word vrijblijvend gematcht met aanbieders die passen bij jouw sector, bedrijfsgrootte en budget.

ibgids.nl/word-gematcht

Of neem contact op via info@ibgids.nl

Bronnenlijst

[1] **Microsoft** -- Digital Defense Report 2025. microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2025

[2] **CoreView** -- Secure Score Guide. coreview.com/blog/microsoft-secure-score-a-tactical-guide-to-implementation-configuration-and-optimization

[3] **BleepingComputer** -- M365 OAuth Phishing. bleepingcomputer.com/news/security/microsoft-365-accounts-targeted-in-wave-of-oauth-phishing-attacks/

[4] **CBS** -- Cybersecuritymonitor 2024. cbs.nl/nl-nl/longread/aanvullende-statistische-diensten/2025/cybersecuritymonitor-2024/2-cybersecuritymaatregelen-door-bedrijven

[5] **Support-IT** -- IT-beheer MKB. support-it.nl/kosten-it-beheer-mkb/

[6] **BECS** -- M365 prijsverhoging. becs.nl/microsoft-verhoogt-de-prijzen-van-zakelijke-365-licenties-per-1-juli-2026/

[7] **Microsoft** -- Security Pricing. microsoft.com/nl-nl/security/pricing/small-medium-business

[8] **Microsoft** -- RaccoonO365. blogs.microsoft.com/on-the-issues/2025/09/16/microsoft-seizes-338-websites-to-disrupt-rapidly-growing-raccoono365-phishing-service/

[9] **Expert Insights** -- M365 Statistics. expertinsights.com/email-security/microsoft-365-usage-and-security-statistics-for-2024

[10] **EPC Group** -- M365 Best Practices. epcgroup.net/microsoft-365-security-best-practices-enterprise-guide

[11] **Exodata** -- M365 Hardening 2026. exodata.io/microsoft-365-security-hardening-checklist/

[12] **NCSC** -- Cyberbeveiligingswet. ncsc.nl/over-ncsc/wettelijke-taak/wat-gaat-de-nis2-richtlijn-betekenen-voor-uw-organisatie

[13] **Digitale Overheid** -- Cyberbeveiligingswet. digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cyberbeveiligingswet/

[14] **Hornetsecurity** -- Threat Report. hornetsecurity.com/en/blog/monthly-threat-report/

[15] **Verizon** -- DBIR 2025. verizon.com/business/resources/reports/dbir/