

PERIUM MS365 SCAN

Microsoft 365- beveiliging continu onder controle

Meer dan 150 automatische
configuratiechecks

Direct inzicht in afwijkingen, herstel en bewijs voor
uw normenkaders.

Entra ID Intune Exchange Online SharePoint Teams



Microsoft 365 verandert sneller dan je denkt

Accounts, rechten, policies en apparaten veranderen voortdurend. Daardoor kan een eerder goedgekeurde configuratie ongemerkt afwijken.

Het risico

Handmatige controles kosten tijd en tonen vooral een momentopname. Zonder actuele technische bewijslast loopt sturing achter op de werkelijke situatie.

01 **Configuratie impact**

Nieuwe accounts, instellingen en apparaten veranderen de beveiligingsstatus voortdurend.

02 **Periodieke controle**

Handmatige toetsing vraagt veel capaciteit, is foutgevoelig en veroudert snel.

03 **Verspreide bewijslast**

Technische status en compliance verantwoording (ISO27001, NEN7510, BIO2, DORA, Cbw etc) moeten vaak apart worden samengebracht.

Automatische controle. Direct bewijs.

Perium controleert meer dan 150 Microsoft 365-instellingen en toont live de status per check. Afwijkingen komen direct beschikbaar met herstelstappen, aanbevelingen en bewijs.

Plan scans, vergelijk historische resultaten en volg scores per framework met Perium.

Vergroot je digitale weerbaarheid.



Meer dan 150 checks over jouw Microsoft 365-omgeving

01 Identiteit en toegang

MFA, Conditional Access, sessiebeleid, adminaccounts en legacy authentication.

02 Samenwerking en delen

Exchange Online, SharePoint, Teams, agenda's en externe toegang.

03 Accounts en beleid

Wachtwoordinstellingen, emergency access en user owned apps.

04 Apparaten

Intune-configuratie en device compliance.

05 Bescherming

Phishingmaatregelen, shared mailboxes en andere kritieke beveiligingsinstellingen.

06 Daily scan

Drift control waarmee wijzigingen en afwijkingen automatisch gemonitord worden.

Eén technische controle ondersteunt meerdere normenkaders

De scan koppelt Microsoft 365-checks aan de bekende normenkaders. Zo hergebruik je één actuele uitkomst voor meerdere compliance verplichtingen.

De technische status blijft via Perium centraal zichtbaar, samen met de beoordeling en verbetering van je beheersmaatregelen.

- 01 **ISO 27002**
- 02 **NEN 7510**
- 03 **BIO**
- 04 **NIS2 en Cbw**
- 05 **DORA**
- 06 **CIS Controls**

Veilige configuratie en aantoonbare verbetering

De scan gebruikt Microsoft OAuth2 authenticatie. Voor het uitvoeren van de scans worden geen wachtwoorden gebruikt en is geen permanente toegang nodig.

1

Veilige autorisatie

U geeft via Entra ID de benodigde toegang voor de controle.

2

Automatische scan

De scan toetst de relevante Microsoft 365-instellingen.

3

Afwijking en herstel

Je ontvangt de status, herstelstappen en aanbevelingen.

4

Bewijs en trend

Resultaten worden bruikbaar voor audit, rapportage en historische analyse.

Je houdt zelf de regie over planning, beoordeling en opvolging.

Actuele status en ontwikkeling per controle

8.9 Configuration management 5 checks

40%

31 scans • 31 dagen

48% huidige score



Ensure 'External sharing' of calendars is not available

Details

Non-Compliant

Ensure Sign-in frequency is enabled and browser sessions are not persistent for Administrative users

Details

Compliant

Ensure 'Idle session timeout' is set to '3 hours (or less)' for unmanaged devices (CIS)

Details

Non-Compliant

Enable Conditional Access policies to block legacy authentication

Details

Compliant

Ensure 'User owned apps and services' is restricted

Details

Non-Compliant

Direct zichtbaar

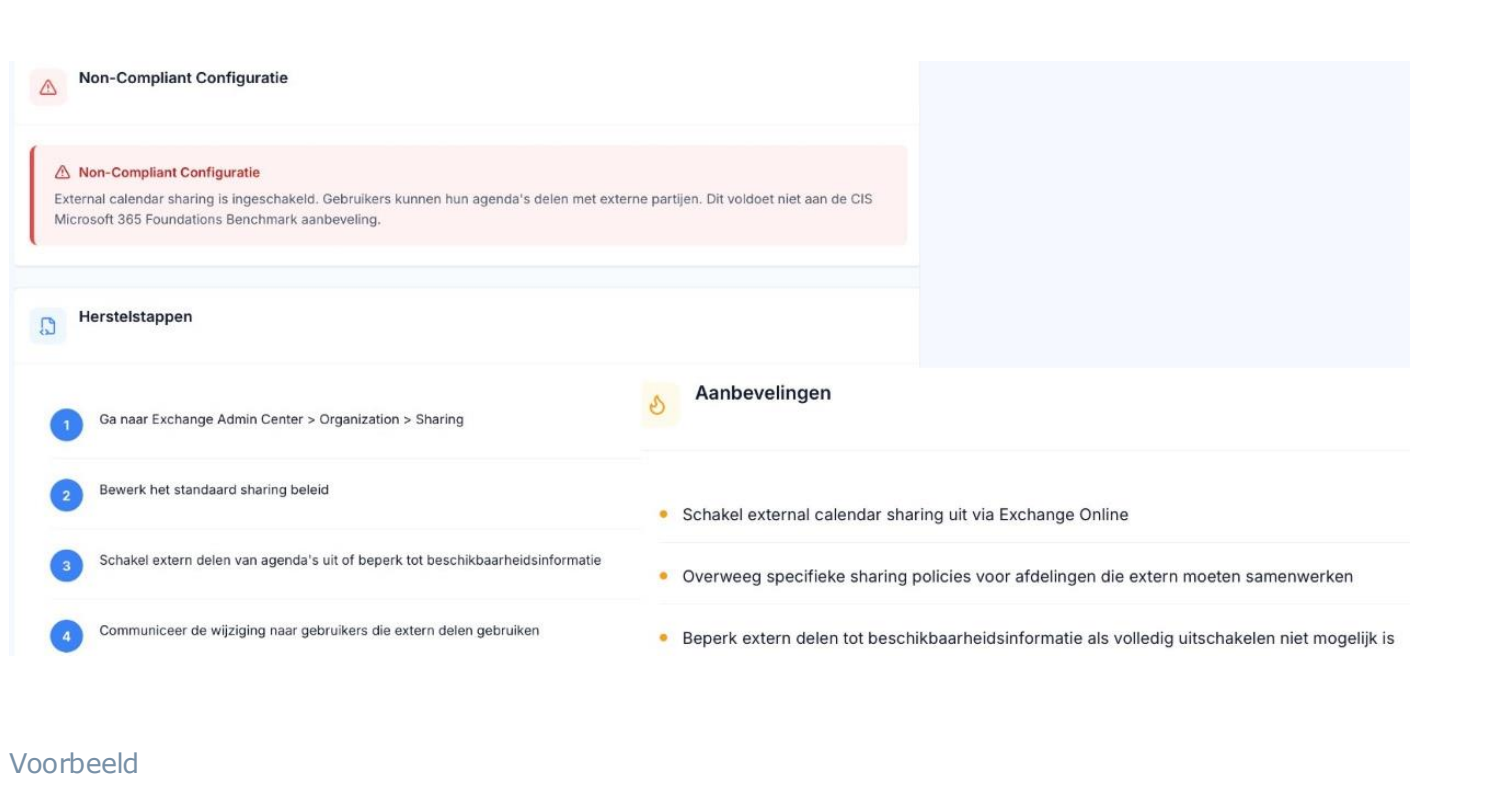
Huidige score en status per check

Historische ontwikkeling over geplande scans

Prioriteiten voor herstel en opvolging

Voorbeeld

Elke afwijking wordt vertaald naar herstel



The screenshot displays a security scan result for a 'Non-Compliant Configuratie'. A red banner at the top indicates the issue: 'External calendar sharing is ingeschakeld. Gebruikers kunnen hun agenda's delen met externe partijen. Dit voldoet niet aan de CIS Microsoft 365 Foundations Benchmark aanbeveling.' Below this, a section titled 'Herstelstappen' (Remediation Steps) lists four actions: 1. Ga naar Exchange Admin Center > Organization > Sharing; 2. Bewerk het standaard sharing beleid; 3. Schakel extern delen van agenda's uit of beperk tot beschikbaarheidsinformatie; 4. Communiceer de wijziging naar gebruikers die extern delen gebruiken. To the right, an 'Aanbevelingen' (Recommendations) section lists three suggestions: 1. Schakel external calendar sharing uit via Exchange Online; 2. Overweeg specifieke sharing policies voor afdelingen die extern moeten samenwerken; 3. Beperk extern delen tot beschikbaarheidsinformatie als volledig uitschakelen niet mogelijk is.

Voorbeeld

01 Duidelijke bevinding

De scan geeft aan welke instelling niet voldoet.

02 Concrete herstelstappen

De specialist ziet waar en hoe de configuratie kan worden aangepast.

03 Gerichte aanbevelingen

De scan ondersteunt een passende keuze voor de organisatiecontext.

Technische bewijslast zonder extra uitzoekwerk

De scan legt per check vast wat deze beoordeelt, welk portaalpad of commando wordt gebruikt en wanneer de instelling compliant is.

Daarmee ontstaat een herhaalbare en uitlegbare controle die specialisten, auditors en management vanuit dezelfde bron kunnen beoordelen.



Bewijslast voor Auditor

WAT TE CONTROLLEREN

Controleer of externe kalenderdeling (external sharing) voor Exchange Online is uitgeschakeld op organisatieniveau.

PORTAL PAD

Microsoft 365 admin center → Settings → Org settings → Calendar → External sharing

POWERSHELL COMMANDO

- `Get-SharingPolicy | Select-Object Name, Domains, Enabled`

COMPLIANT WANNEER

- ✓ External sharing voor Calendar staat op "Off" (uitgeschakeld)
- ✓ Geen sharing policy is geconfigureerd die extern delen van agendagegevens toestaat
- ✗ External sharing staat ingeschakeld of een sharing policy staat extern delen toe

Voorbeeldweergave uit de aangeleverde productpresentatie

Meer grip met minder handmatig werk

Minder tijd kwijt aan terugkerende configuratiechecks

Concrete herstelstappen direct bij iedere afwijking

Herbruikbare bewijslast voor audits en interne toetsing

Historische trends zonder aparte rapportagecyclus

Automatisch delen van scan resultaten voor management, securityteam en management

Direct een NIS2/Cbw readiness check

Actueel inzicht in technische beheersing en prioriteiten

Directe koppeling tussen Microsoft 365 en normkaders

Minder voorbereidingstijd voor audit en toezicht

Gerichte sturing op afwijkingen die aandacht vragen



Maak uw Microsoft 365-beheersing aantoonbaar

Ontdek in een gerichte demo hoe Perium afwijkingen, herstel en auditbewijs samenbrengt in één actuele werkwijze.

Zet onze [ROI Calculator](#) in om direct je besparing te zien.

Plan een demo

perium.nl

hallo@perium.nl

050 - 21 11 729

Atoomweg 6B, 9743 AK Groningen

PERIUM MS365 SCAN

Meer dan 150 checks
Concrete
herstelacties
Direct auditbewijs

Geïntegreerd in Perium en gekoppeld aan meerdere normenkaders.