ACEN

Federaal Planbureau
Analyses en vooruitzichten

REFERENCE CASE - Federaal Planbureau

Een digitale werkomgeving die permanent veilig en compliant blijft

Over Federaal Planbureau

Het Federaal Planbureau is een onafhankelijke federale overheidsinstelling die prognoses en analyses maakt over de economische, sociale en milieuvraagstukken voor de Belgische federale overheid. Op deze manier ondersteunen zij de politieke besluitvorming via objectieve cijfers en feiten.

Met een team van ongeveer 100 medewerkers, waarvan 75 onderzoekers, is de organisatie voor haar werking en complexe econometrische modellen volledig afhankelijk van een stabiele en veilige Microsoft 365-omgeving. Federaal Planbureau is dus een 100% Microsoft-omgeving.

Het IT-team dat verantwoordelijk is om deze Microsoft 365-omgeving draaiende en veilig te houden bestaat uit 8 personen. 4 personen worden fulltime ingezet op het ontwikkelen van tools voor de complexe onderzoeksmodellen. De andere 4 IT-experts zijn verantwoordelijk voor het beheer, het up and running houden en het beveiligen van de volledige infrastructuur.

Federaal Planbureau
Analyses en vooruitzichten

De uitdaging

Naar aanleiding van steeds nieuwe en strengere cybersecurity maatregelen (bv. NIS2) en de toenemende druk van andere overheidsinstellingen was het Federaal Planbureau genoodzaakt hun security te herbekijken en te upgraden naar een managed security-oplossing.

Voor de migratie naar deze managed security-oplossing zag het IT-team van Federaal Planbureau enkele kritische uitdagingen:

NIS2 wetgeving:

Als onafhankelijke overheidsinstantie moet het Federaal Planbureau voldoen aan strikte normen. De noodzaak om aan te tonen dat men "in control" is, was een directe trigger om naar een professionele oplossing te zoeken. Daarnaast is het proactief voldoen aan de NIS 2-richtlijnen een grote meerwaarde voor de compliance, waar Federaal Planbureau zich zwart-op-wit bewijst als een veilige en betrouwbare partner naar alle betrokken partijen.

Hierbij ging het niet louter om het naleven van de wetgeving; het Planbureau hecht er zelf enorm veel waarde aan om deze compliance zwart-op-wit te kunnen aantonen. Alleen zo kunnen zij de rol van een doorlopend veilige en betrouwbare partner garanderen voor alle federale diensten die gevoelige data aan hen toevertrouwen.

Onhaalbare specialisatie:

Het beheer en de beveiliging van een M365-tenant is een fulltime job geworden. "Een policy die je vandaag configureert, kan over twee weken alweer niet up-to-date zijn", Johan Duyck, IT-coördinator bij het Federaal Planbureau. Up-to-date blijven met deze unieke specialisatie is dus een must.

Operationele druk:

Met een team van slechts acht personen was het onmogelijk om zelf een 24/7 monitoring op te zetten zonder de focus op kernactiviteiten te verliezen.

"We beseften steeds meer dat het beheer van M365-omgeving een job op zich is. Je moet zeer gespecialiseerd zijn om de snel veranderende roadmap van Microsoft bij te houden."

Johan Duyck, IT-coördinator bij Federaal Planbureau

Security as a Service: Niet enkel tools, een heel team!

Tijdens de zoektocht naar een gepaste oplossing werden vanuit andere overheidsinstellingen logge en dure oplossingen naar voren geschoven, gericht op duizenden gebruikers. Deze 'bazooka-oplossingen' zijn niet ontwikkeld voor organisaties met een hoge flexibiliteit en gebruikersaantallen zoals het Federaal Planbureau.

In plaats daarvan koos het Federaal Planbureau voor een flexibel en kwalitatief partnership met ACEN. Het partnership steunt op drie pijlers:

1 ACEN managed Microsoft 365

ACEN scant door middel van intelligente tooling de M365-tenant dagelijks op misconfiguraties, ongebruikelijke uitzonderingen (zoals conditional access) en nieuwe security-features. Daarnaast vinden er op regelmatige basis meetings plaats tussen de dedicated ACEN expert en Federaal Planbureau om resultaten te rapporteren, data te analyseren en zo proactief te handelen.

2 24/7 managed SOC

Een gespecialiseerd team van ACEN bewaakt de omgeving dag en nacht, waardoor mogelijke incidenten onmiddellijk worden gedetecteerd en opgevolgd. Alerts worden slim gefilterd en gepriotatiseerd. Op deze manier vermijden we een overload aan meldingen en wordt er snel en concreet gehandeld. Verder is er een concreet incident response plan opgesteld in het kader van een mogelijk incident.

3 Action Pack Units (APUs)

Een flexibel pakket aan service credits die ingezet worden voor proactieve verbeteringen op de opgestelde roadmap, extra consultancy of andere specifieke ad-hoc security-projecten.

Dit vooraf goedgekeurde budgettaire model zorgt voor maximale flexibiliteit en snelheid (de noodzaak om telkens nieuwe offertes op te stellen en/of goedkeuring te vragen aan verschillende decision-makers vervalt). Via deze manier van werken kunnen de experts van ACEN meteen aan de slag zonder tijdverlies, wat in de cybersecuritysector cruciaal is.

"Een Microsoft-omgeving beveiligen is door de constante updates een specialisatie op zich geworden. Met dit model koopt een organisatie geen losse tools, maar de garantie dat hun security-posture 24/7 up-to-date blijft."

Jahirt Ruiz, Cybersecurity Expert at ACEN

Het resultaat? Direct en meetbaar!

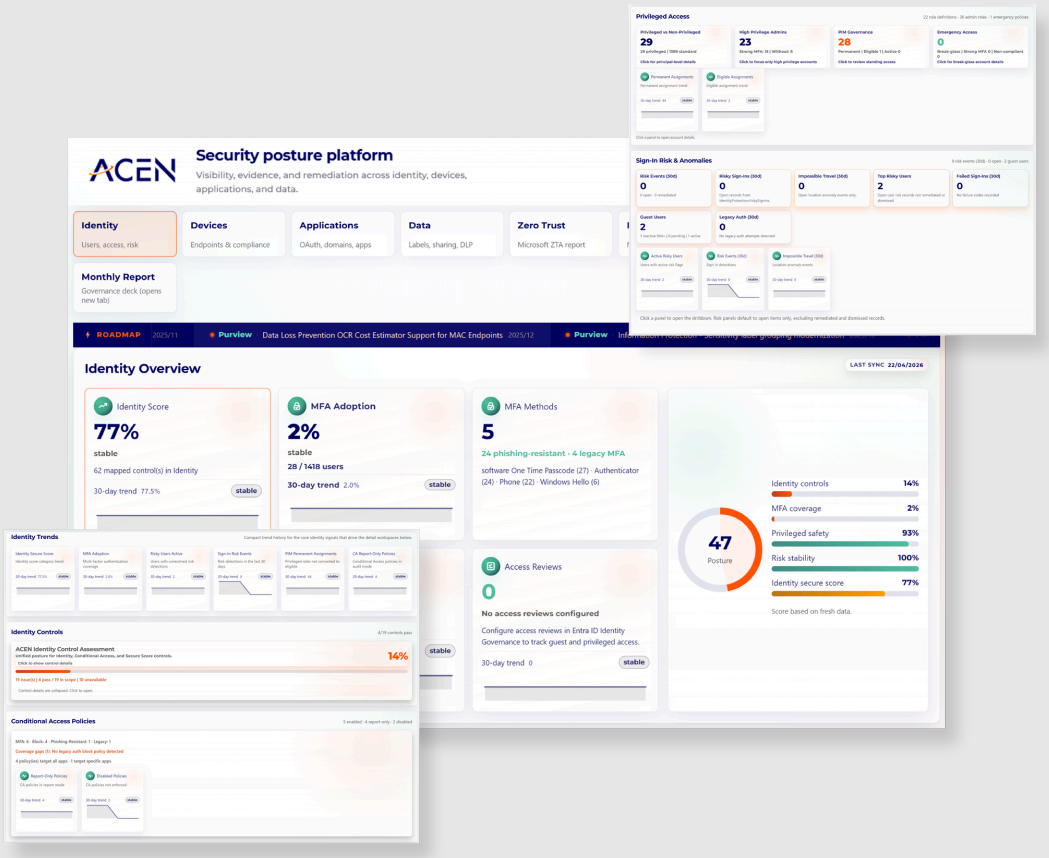
De overstap naar het managed model heeft enkele significante voordelen:

1. Snelle implementatie:

Het implementatietraject verliep in verschillende fasen en was binnen twee maanden volledig afgerond. Dankzij een goede samenwerking (en korte communicatielijnen) met de experts tussen beide teams, heeft de eindgebruiker geen enkele hinder van de implementatie ondervonden tijdens de dagdagelijkse taken.

2. Tijdswinst en ontlasting:

Het interne team wordt niet langer belast met de dagelijkse stress van security-updates. Men heeft nu "een heel team van experten" tot hun beschikking in plaats van een interne medewerker, die niet gespecialiseerd is in cybersecurity.

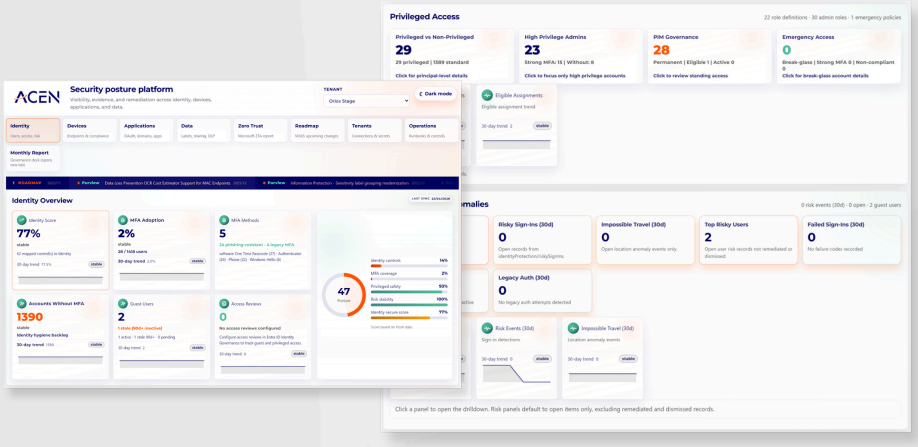


3. Gemoedsrust:

Dankzij het incident response plan en de proactieve monitoring is er een duidelijk gevoel van veiligheid binnen de organisatie. De ACEN-experten staan de klok rond paraat om in te grijpen mocht er toch een incident voorvallen.

4. Compliance-zekerheid:

Federaal Planbureau beschikt vanaf nu over een duidelijke mapping van de bestaande rechten en policies, met meer controle als gevolg. Vanaf nu kan dus zwart-op-wit aangetoond worden dat zij voldoen aan de nodige en noodzakelijke security behoeften voor zowel aan dataleveranciers, andere federale overheidsdiensten als externe partijen. De NIS2-richtlijnen zitten verder ook stevig verwerkt in de cybersecurity roadmap.



ACEN - Een collega op afstand

De samenwerking tussen ACEN en het Federaal Planbureau is gebaseerd op volledig en wederzijds vertrouwen. ACEN beschikt over administratorrechten en kan dus meteen ingrijpen bij een dreiging of incident, maar ook zelfstandig bepaalde configuraties bijsturen na overleg.

De **communicatie tussen beide partijen verloopt vlot via korte lijnen** (zoals een gedeelde Teams-groep), wat de reactiesnelheid drastisch verhoogt ten opzichte van de traditionele ticketing-systemen.

"Ik heb onze directie kunnen overtuigen door aan te tonen dat we met ACEN een team van professionals in huis halen die 24/7 paraat staan. Dat haalt enorm veel druk van mijn eigen team weg."

Johan Duyck, IT-coördinator bij Federal Planning Bureau