

# Cloud Security Benchmark



**valid**

Thrive  
Tech  
Trust

De cloud biedt veel voordelen, zoals schaalbaarheid, flexibiliteit en mobiliteit. Tegelijkertijd maakt cloud computing organisaties kwetsbaar voor cyberaanvallen, die dan ook steeds vaker en met toenemend succes worden gelanceerd. Hoog tijd dus om je weerbaarheid te verhogen en dreiging om te zetten in een kans. Want onderzoek toont aan dat sterke security het vertrouwen van klanten en partners vergroot, waardoor je kunt groeien.



## **Het versterken van je verdediging tegen ransomware, malware en andere cyberdreigingen heeft meer voordelen.**

### **Je kunt bijvoorbeeld:**

- Jouw medewerkers overal en altijd veilig toegang geven tot alle data die ze nodig hebben om hun werk goed te doen. Daardoor kunnen ze optimaal samenwerken.
- Met een goed gevoel gebruik maken van de kansen die moderne technologie biedt.
- Downtime en stilvallen van kritieke processen voorkomen.
- Beter omgaan met strengere eisen die Europese wetgeving stelt aan databescherming, afnemende verzekeraarbaarheid van datadiefstal en beperkte IT-capaciteit.

Maar welke maatregelen moet je precies nemen om risico's zo veel mogelijk te beperken? Waar moet je beginnen om dreigingen tijdig te detecteren en schade te voorkomen?

Lees het in deze brochure of neem contact met ons op.



# Valid Cloud Security Benchmark

Gelukkig is er een kostenefficiënte manier om de antwoorden te vinden op deze vragen: de Valid Cloud Security Benchmark. Deze dienst helpt organisaties die met Microsoft Azure en Microsoft 365 werken, om hun security naar een hoger niveau te tillen. Dit wordt mogelijk gemaakt door de meetbare standaarden van het Center for Internet Security (CIS). Deze gezaghebbende organisatie gebruikt bewezen methodes om organisaties wereldwijd te helpen zich beter te beschermen tegen dreigingen.

De benchmark helpt om kwetsbaarheden te identificeren en biedt inzichten om deze te verhelpen. Een objectieve methode dus om je beveiligingsstatus te beoordelen, risico's te verminderen en een solide basis te leggen voor een effectieve beveiligingsstrategie. Je krijgt grip op security, wat zorgt voor gemoedsrust omdat je kunt vertrouwen op je IT-systemen.



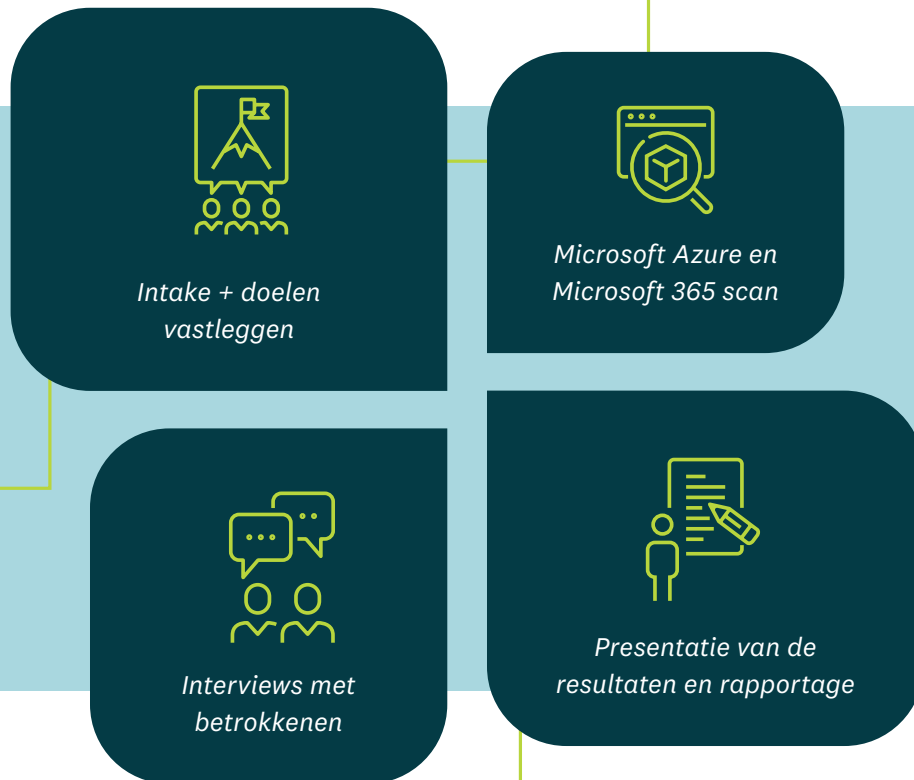
## CIS

Het Center for Internet Security is een non-profit organisatie die zich sinds 2000 richt op het veiliger maken van de digitale wereld. Het biedt richtlijnen en tools om mensen, bedrijven en overheden te helpen om hun IT-systemen beter te beschermen tegen cyberdreigingen.

Het CIS ontwikkelt en publiceert beveiligingsstandaarden, zoals de CIS Controls en de CIS Benchmarks. De Controls zijn een set best practices op het gebied van security, onder meer gericht op beheer van wachtwoorden, toegangsbeheer en monitoring van systemen. Dit zorgt voor een robuuste beveiligingsbasis.

Deze benchmarks zijn gedetailleerde configuratierichtlijnen. Ze dienen om onder meer besturingssystemen en applicaties beter te beveiligen volgens vastgestelde normen en best practices.

# Onderdelen van de benchmark



## Hoe ziet de benchmark eruit?

Het hangt van de specifieke behoeften van jouw organisatie af wat de scope is van de benchmark. Het doel is echter altijd om inzicht te geven in je huidige security status zodat je tot verbetering daarvan kunt komen.

Bij de beoordeling hoort een analyse van je netwerkarchitectuur, firewall configuraties en encryptie-niveaus. Ook beoordelen we detectiesystemen, back-up procedures en methoden voor toegangsbeheer. Hoe goed kun je ongeautoriseerde toegang tot systemen en gegevens voorkomen?

De beoordeling gaat verder dan technologie: we kijken ook naar bestaande beveiligingsrichtlijnen en procedures, naar naleving van wet- en regelgeving en van CIS-richtlijnen voor best practices. Daarnaast evalueren we jouw initiatieven om medewerkers bewust te maken van beveiligingsrisico's. Menselijke fouten zijn namelijk nog steeds de belangrijkste reden voor het slagen van cyberaanvallen.

De interviews helpen om een nog grondiger beeld te krijgen van potentiële risico's en bedreigingen. Zo ben je er zeker van dat er niets over het hoofd wordt gezien. Stakeholders betrekken bij het verbeterproces, vergroot ook het bewustzijn en de kans op steun voor het doorvoeren van maatregelen, en daarna van de acceptatie ervan.

# De voordelen van de benchmark

De benchmark levert een gedetailleerd inzicht in de staat van je cyberdefensie. Je beschikt na afloop over een leidraad voor maatregelen die je kunt nemen om inbreuken te voorkomen en risico's te verminderen. Je kunt hierin prioriteiten stellen.

## Andere voordelen:

- Jouw IT-medewerkers zijn minder tijd kwijt aan incidenten bestrijden en kunnen productiever zijn. Dit biedt hen ruimte om strategisch bij te dragen aan de bedrijfsdoelstellingen.
- Je kunt auditors laten zien dat je controle hebt over security en voldoet aan alle wettelijke eisen.
- Je bouwt vertrouwen en geloofwaardigheid op bij partners en nieuwe klanten, omdat zeer zeker van kunnen zijn dat jouw systemen beschermd zijn volgens de hoogste standaarden.



### De investering

De benchmark helpt je door inzichten te bieden om je beveiliging te versterken en risico's te verminderen. Dit vergt een eenmalige investering van €5.000. Voor het doorvoeren van eventuele verbeterpunten of vervolgacties die uit de benchmark naar voren komen, hanteren we een urenindicatie tegen een vast uurtarief. Het is een investering waard om je beter te wapenen tegen risico's en dreigingen en daarmee hoge kosten en andere schade te voorkomen.

# Valid: jouw benchmark partner

## **Valid helpt organisaties al 25 jaar groeien en bloeien.**

Onze dienstverlening voorziet klanten van (onder andere):

- Een betrouwbaar IT-fundament.
- Relevante data-inzichten.
- Moderne werkplekken.
- Slimme cloud oplossingen.

Ook begeleiden we complexe verandertrajecten. Onze mensen hebben veel kennis en ervaring, ademen technologie, en nemen iedereen mee in begrijpelijke taal. Bovendien zijn we een erkende Microsoft Solutions Partner op verschillende gebieden: van security tot cloud.

Wij helpen je graag met het maken van de juiste keuzes, zodat je een IT-landschap realiseert dat past bij jouw organisatie. Een omgeving die volledig in dienst staat van jouw doelen. Op die manier kun jij je blijven ontwikkelen en ben je altijd klaar voor veranderingen. Dit vraagt om intensieve samenwerking, waarbij vertrouwen een belangrijke rol speelt. Sterker nog: vertrouwen staat aan de basis van alles wat we doen.



### **Meer weten?**

### **Neem contact met ons op**

Hoofdkantoor Valid  
Flight Forum 565  
5657 DR Eindhoven

+31 (0)88 - 900 95 00  
info@valid.nl  
www.valid.nl

**valid**

Trust  
Tech  
Thrive

[valid.nl](https://valid.nl)