FAQ

Nieuwe prijzen Compatible

1. Waarom verandert Compatible haar prijzen?

   Door de snelle ontwikkelingen in de technologie speelt IT een steeds grotere rol in jouw organisatie. De drie belangrijkste externe factoren die van invloed zijn op deze ontwikkelingen zijn de toenemende risico's op cyberaanvallen, de aankomende NIS 2.0-wetgeving, en de opkomst van Artificial Intelligence (AI). Dit brengt bredere en complexere uitdagingen met zich mee, waar we je graag mee willen en moeten helpen. Ons doel is om jou elke dag de beste IT-oplossingen te bieden. Hiervoor is een vernieuwing van onze diensten noodzakelijk, zodat we vooruit blijven lopen op de markt en jouw organisatie daarbij kunnen ondersteunen. Alleen door de prijzen aan te passen kunnen we dit op een duurzame wijze blijven doen.

   Daarom introduceren wij vanaf *1 juli 2024* onze vernieuwde dienstverlening voor al onze klanten, met hogere kwaliteitsnormen, beveiliging als topprioriteit, meer mogelijkheden en volledig gericht op de toekomst.

2. Wat zie ik terug op mijn factuur?

   Op je factuur zul je zien dat een aantal diensten duurder worden en dat er nieuwe onderdelen standaard worden toegevoegd.

   We willen graag transparant zijn over wat dit betekent voor je volgende factuur. Omdat elke omgeving anders van samenstelling is en daardoor de raakvlakken met de verschillende diensten anders zijn, kunnen we de impact hier niet in een eenduidig percentage voor iedereen weergeven. Wil je al vast meer over te weten komen en niet voor een verrassingen komen te staan, neem dan gerust even contact met ons op dan lopen we de verschillende componenten met je door.

De meest in het oog springende aanpassing vind je terug onder de Compatible Managed Security diensten:

+ € 5,75 per gebruiker van een werkplek (verhoging)
+ € 3,50 voor elke e-mail only gebruiker (nieuw)
+ € 1,80 voor elke gedeelde mailbox (nieuw)

Daarnaast zul je zien dat de kosten beter verdeeld worden over de gebruikers en accounts. De reden hiervoor is dat een gebruiker met enkel een mailbox even goed onderdeel is van het geheel dat beschermd moet worden. Ook gedeelde mailboxen waar tot voor kort helemaal niets voor werd doorbelast delen vanaf nu mee in de totale kosten.

Cloud User/Account Support
+ € 0,0 voor de standaard gebruikers (blijft gelijk op € 12,20)
+ € 1,50 voor e-mail only gebruikers (verhoging)
+ € 1,80 voor elke gedeelde mailbox (nieuw)

Een andere wezenlijke verandering is dat we vanaf nu onderscheid maken tussen direct aan gebruikers gerelateerde beveiligingsmaatregelen en maatregelen over de Microsoft 365 als geheel heen. Daarom passen we een nieuwe Tenant Management Fee toe. De hoogte van de fee is afhankelijk van het aantal gebruikers dat een werkplek gebruikt gekoppeld aan de Microsoft 365 omgeving.

1-3 werkplekgebruikers	€ 14,50 (nieuw)
4-10 werkplekgebruikers	€ 29,50 (nieuw)
11-25 werkplekgebruikers	€ 59,50 (nieuw)
26-300 werkplekgebruikers	€ 89,50 (nieuw)

We berekenden al een administratieve licentiemanagement fee door voor alle Microsoft 365 licenties in een omgeving. Deze dienst breiden we uit met een tooling component omdat er voortdurend aanpassingen vereist zijn om licenties efficiënt en snel bij te kunnen plussen en onze zeer onderscheidende service waarbij we ongebruikte maandelijkse Microsoft licenties afschalen op de hernieuwingsdatum. Alleen zo kunnen we blijven voldoen aan de belofte dat je niet betaalt voor wat je niet nodig hebt of niet gebruikt.

We passen de naam aan naar: Licentiemanagement & Tooling

+ € 3,15 Per licentie (verhoging) – de staffel blijft van toepassing

Een belangrijke nieuwe dienst die we voor in ieder geval het actieve e-maildomein van een Microsoft 365 omgeving is E-maildomein security & monitoring. Deze dienst is cruciaal om inzicht te krijgen in wat er gebeurt met je e-maildomein en of en wie er namens jouw organisatie e-mails kan versturen. We hebben een aparte dienstbeschrijving opgesteld waarin we je uitleggen wat de dienst doet en betekent.

+ € 17,- per actief e-mail domein (nieuw)
+ € 5,50 per niet-actief domein (optioneel, zeer aanbevolen!)

Door Compatible beheerde Domeinnamen
Wij beheren namens onze klanten bijna 1.000 domeinnamen. Voor Compatible en klanten heeft dit grote voordelen. Doordat wij direct toegang hebben tot de zogenaamde DNS records kunnen we snel aanpassingen doorvoeren waardoor je digitaal bereikbaar blijft. Deze dienst zorgt ervoor dat je e-mail aankomt, je website bereikbaar is, je kan inloggen op je computer, je veilig mailinglist providers kunt gebruiken die namens jou mailen, etc. etc. De dienst is ook nauw verwant aan de nieuwe E-maildomein Security & Monitoring dienst. We vinden het ook belangrijk dat we een neutrale plek hebben. We verbinden je domeinnaam niet aan een verplichte hosting dienst. Zo ben je vrij om je diensten waar dan ook onder te brengen, wij zorgen ervoor dat je bereikbaar blijft.

De kosten voor de infrastructuur om deze dienst te leveren en te kunnen blijven leveren zijn veel hoger dan wat wij voor deze dienst doorbelasten. We passen de prijs voor de Domeinnamen daarom aan.

x 2 Per domeinnaam (verhoging) – staffels blijven van toepassing

NIS2 – Network & Information Systems 2

3. Wat is NIS2 en waarom is dit zo belangrijk?

De afgelopen jaren zien we dat verschillende ontwikkelingen de veiligheid van onze maatschappij en economie steeds meer onder druk zetten. Denk daarbij aan COVID-19, de Oekraïne-oorlog, en cyberdreigingen. Daarom is er sinds 2020 vanuit de Europese Unie aan de Network and Information Security (NIS2) directive gewerkt. De NIS2-richtlijn richt zich op een verbetering van de digitale en economische weerbaarheid van Europese lidstaten. Deze richtlijn wordt momenteel in nationale wetgeving omgezet.

De richtlijn stuurt op risico's die netwerk- en informatiesystemen bedreigen, zoals cyberbeveiligingsrisico's. De komst van de NIS2-richtlijn moet bijdragen aan meer Europese harmonisatie en een hoger niveau van cybersecurity bij bedrijven en organisaties. Als Managed Service Provider vallen wij onder deze richtlijn en hebben wij zowel zorg- als meldplicht.

4. Waarom heeft NIS2 effect op mijn organisatie?

Als Managed Service Provider zijn wij van Compatible bestempeld als 'essentiële dienstverlener'. In deze hoedanigheid dienen wij te voldoen aan de Europese richtlijn NIS2, en krijgen wij hierbij ketenverantwoordelijkheid. Dit betekent niet alleen dat wij onze interne processen goed op orde moeten hebben, maar ook dat wij aanvullende securitymaatregelen hebben getroffen en blijven treffen die voor jou leiden tot een veiligere omgeving.

De ketenverantwoordelijkheid geldt ook voor jou. Dit betekent dat je verantwoordelijk bent voor de beveiliging van jouw hele toeleveringsketen, inclusief externe leveranciers en partners die toegang hebben tot jouw netwerk- en informatiesystemen. De NIS2-richtlijn legt een grotere nadruk op de beveiliging van deze ketens om ervoor te zorgen dat zwakke plekken bij externe partijen geen bedreiging vormen voor de organisaties zelf. Daarbij zal het ook in toenemende mate een vereiste vanuit de klant worden dat jouw organisatie voldoet aan de NIS2-richtlijn, aangezien ook zij ketenverantwoordelijkheid dragen.

5. Wat houdt zorgplicht in?

De richtlijn bevat een zorgplicht die organisaties verplicht om zelf een risicobeoordeling te doen. Op basis daarvan nemen zij passende maatregelen om hun diensten zoveel mogelijk te waarborgen en de gebruikte informatie te beschermen.

Dit geldt ook voor jou. Je valt wellicht niet direct onder de richtlijn, maar als je levert aan een organisatie die daar wel onder valt en die kans is groot dat zij aan jou vragen om de passende maatregelen die jij hebt genomen bevestigt zodat de keten gesloten blijft.

6. En wat houdt meldplicht in?

De richtlijn schrijft voor dat organisaties incidenten binnen 24 uur bij de toezichthouder moeten melden. Het gaat om incidenten die de verlening van de essentiële dienst sterk (kunnen) verstoren. Een cyberincident moet ook bij het Computer Security Incident Response Team (CSIRT) gemeld worden. Dit team kan vervolgens hulp en bijstand leveren. Factoren die een incident meldingswaardig maken, zijn bijvoorbeeld het aantal personen dat door de verstoring is geraakt, de tijdsduur van een verstoring en de mogelijke financiële verliezen.

7. Meer weten over NIS2

De Nederlandse overheid en veel instanties hebben informatie verzameld om je voor te lichten over NIS2.
Een aantal belangrijke bronnen zijn:

NIS2-richtlijn NIS2-richtlijn - Digitale Overheid

NIS2 Zelfevaluatie NL (regelhulpenvoorbedrijven.nl)

NIS2-Quickscan helpt organisaties bij voorbereiding op nieuwe cyberwet | Nieuwsbericht | Rijksinspectie Digitale Infrastructuur (RDI)

AI – Artificial Intelligence

8. Wat is Artificial Intelligence (AI)?

AI is een geautomatiseerd systeem dat taken uitvoert waar vroeger menselijke intelligentie voor nodig was. AI-systemen werken met in software beschreven algoritmen. De systemen herkennen patronen en nemen dan zelf beslissingen. En net zoals mensen worden ze door te trainen steeds beter.

Een relevant voorbeeld is Microsoft Edge Copilot, de veilige AI-assistent in jouw Edge browser die jouw productiviteit een boost geeft. Meer informatie over Edge Copilot lees je hier. Maar binnen afzienbare tijd zal de Microsoft Copilot niet meer weg te denken zijn uit je dagelijkse werk. Computers krijgen naast de Windows toets straks standaard ook een Copilot toets.

Een heel relevante en bekende speler op het gebied van AI is OpenAI met zijn generatieve AI systeem genaamd ChatGPT. Voor veel mensen is dat nu al dagelijks een enorm goede hulp om productiever te zijn.

9. Wat zijn de positieve gevolgen en gevaren van AI?

Met AI kunnen medewerkers problemen oplossen die voorheen met oude methodes vaak uitdagend zijn. Algoritmes zijn sneller, goedkoper en vaak nauwkeuriger dan mensen. Ze werken 24/7/365 en zijn nooit ziek. Alledaagse taken die voor een medewerker ‘saai’ zijn, kunnen worden geautomatiseerd. AI stelt ons in staat om informatie op te vragen. Een tekst te verbeteren. Een Excelformule te creëren op basis van parameters en voorwaarden die wij invoeren, zonder hiervoor een Excelspecialist te zijn. Slechts enkele voorbeelden waar AI wordt ingezet ter verbetering.

Helaas is er een andere kant van de medaille. AI biedt cybercriminelen nieuwe manieren om bedrijven aan te vallen en data afhandig te maken. Enkele voorbeelden waar we nu al mee te maken hebben:

- Phishing-aanvallen: criminelen gebruiken AI om geloofwaardige phishing-e-mails of berichten te genereren en zo mensen te misleiden en gevoelige informatie te stelen.

- Social engineering: AI wordt gebruikt om overtuigende verhalen te creëren en mensen te manipuleren om gevoelige informatie te onthullen of ongepaste acties uit te voeren.
- Verspreiding van desinformatie: AI wordt gebruikt om nepnieuws, geruchten en valse informatie te verspreiden om het publieke sentiment te beïnvloeden of chaos te veroorzaken.
- Automatische aanvallen: criminelen gebruiken AI-taalmodellen om automatisch spam, haatdragende inhoud of andere schadelijke berichten op sociale media te genereren.

10. Veranderen de uurtarieven?

Nee, diensten afgenomen op nacalculatie blijven gehanteerd op het reeds bekende tarief.

11. Per wanneer wordt mijn factuur aangepast?

De nieuwe dienstverlening wordt automatisch doorgevoerd op de factuur over *juli 2024.*

12. Ik heb nog meer vragen, waar kan ik terecht?

Wij staan voor je klaar om meer vragen te beantwoorden en in gesprek te gaan.

Alle genoemde prijzen zijn Excl. BTW.