



Security in the cloud

Cloud Mail Security



E-mail: enkel openen na screening

Hoeveel e-mails versturen en ontvangen uw medewerkers per dag? Ontelbaar veel! Geen wonder dat cybercriminelen dit medium graag gebruiken om uw bedrijf aan te vallen. Een geloofwaardige afzender nabootsen? Da's een fluitje van een cent voor hen. De onbewuste gebruiker trapt zó in de val. Hoog tijd dus om de criminelen een halt toe te roepen. Met Cloud Mail Security.

Meer geavanceerde aanvallen

E-mailverkeer is de nummer 1 cyberbedreiging voor uw organisatie.

Vroeger waren het standaard spam en phishing e-mails. Nu moet u op uw hoede zijn voor zeer gerichte en geavanceerde aanvallen, waaronder spear phishing, ransomware en Business Email Compromise (BEC).

Gelukkig is er Cloud Mail Security van Proximus om de malafide mails te onderscheppen.

Cloud Mail Security

Cloud Mail Security werkt als een soort buffer. Nog voor de berichten uw mailserver bereiken, analyseert hij al uw e-mails, ook de ongewenste, en stuurt ze "gezuiverd" naar u door. U krijgt dan alleen de legitieme e-mails op uw mailserver. Maar ook e-mails die vanuit uw organisatie vertrekken, worden gescreend: zo worden mails met gevoelige inhoud niet verstuurd zonder versleuteling en kunnen gebruikers niet gaan spammen.

Cloud Mail Security is een oplossing in de cloud. Dat betekent dat ze voor u wordt beheerd, gehost en in real time geüpdatet. U hebt dus geen hardware of specifieke applicaties nodig op uw sites, netwerk of pc's.

Met Cloud Mail Security hebt u de garantie van een totale en externe beveiliging tegen spam en allerlei andere aanvallen, ook de nieuwste zoals spear phishing en BEC. Met deze oplossing beschermt u gebruikers die e-mails met kwaadwillige inhoud per ongeluk openen.





Security in the Cloud Cloud Mail Security



De pluspunten van Cloud Mail Security

- **Bereid uw gebruikers voor op het afwenden van aanvallen** met een brede waaier aan opleidingsmogelijkheden en realistische nabootsing van e-mailaanvallen.
- **Bescherm uw gebruikers tegen onoplettendheid:** bij het aanklikken van gevaarlijke linkjes in een e-mail, bijvoorbeeld, wordt de toegang tot de website geblokkeerd.
- **Stop geavanceerde aanvallen** via de nieuwste beveiligingstechnieken zoals machine learning, behaviour analysis, real-time link following en sandboxing.
- **Win tijd:** geef het volledige beheer uit handen: management, hosting en updates worden gedaan door Proximus.
- **Vermijd extra kosten:** u hoeft geen hardware of software te installeren op uw pc's. Een eenvoudige aanpassing aan het met uw domeinnaam verbonden MX-record (Mail eXchange-record) volstaat om de dienst te activeren.
- **Beveilig zowel on-premise mailservers** als cloud set-ups, zoals Office365 en Gmail Apps.
- **Krijg inzicht in uw e-mailverkeer** en aanvallen via overzichtelijke dashboards.

En de prijs?

Basisaanbod en opties			
Aantal mailboxen Prijs / mailbox / maand:	Basisaanbod Anti-spam en anti-malwarebescherming voor inkomend en optioneel uitgaand mailverkeer.	Optie: ATP Detectie van zero-day aanvallen via sandboxing, behavioural analysis, machine learning en threat intelligence.	Optie: AD-integratie Verfijning van policies op gebruikersniveau door een integratie met Active Directory.
1 – 49	€ 3,63	€ 1,63	Enmalige kost voor hulp op afstand voor installatie en configuratie van deze optie: € 345,00
50 – 99	€ 2,90	€ 1,47	
100 – 249	€ 2,18	€ 1,39	
250 – 500	€ 1,82	€ 1,31	
500 -1000	€ 1,63	€ 1,12	
>1000	Op aanvraag	Op aanvraag	
SLA	Inbegrepen	Inbegrepen	Inbegrepen
Diensten			
Reactive Care Gratis	Assist Vanaf € 258,00 (eenmalig)	Full Care Prijs bepaald volgens uw noden	

Meer info



Surf naar www.proximus.be/security
of contacteer ons op
www.proximus.be/contactpage

