



E-mail & Web Security

Anti-virus en anti-spam oplossing op basis van Symantec.cloud

E-mail zorgt voor een eenvoudige, snelle en goedkope uitwisseling van informatie. Voor veel organisaties is het de voornaamste manier van zakelijke communicatie geworden. E-mail wordt tegenwoordig dan ook terecht gezien als een bedrijfskritische toepassing waarbij een verstoring direct een enorme impact heeft op de dagelijkse gang van zaken. Daarom is ook een hoge bescherming essentieel. Zonder effectieve verdediging riskeren organisaties kostbare verstoringen, datalekken en het verlies van vertrouwen van haar klanten.

Vermindering complexiteit

Claranet biedt met E-mail Security een hoogwaardige oplossing op basis van Symantec technologie. Deze oplossing zorgt voor een optimale bescherming tegen (kwaadaardige) virussen en overlast door spam. De dienst biedt volledige bescherming tegen bekende en onbekende e-mail virussen en heeft een gegarandeerde 99% detectie van spam, vastgelegd in een hoogwaardige SLA. Het helpt organisaties bij het beschermen van berichten tegen virussen, spam, phishing, gerichte aanvallen en bulk e-mail. Daarnaast vermindert het de complexiteit door het gebruik van een centraal platform vanuit een eigen robuuste cloud infrastructuur.

Malware bedreiging

In de afgelopen jaren zijn er steeds meer gerichte aanvallen op verschillende communicatieprotocollen, waaronder e-mail. Zogenaamde malware-programmeurs doen aanzienlijke inspanningen in het ontwikkelen van kwaadaardige software om gaten in de beveiliging uit te kunnen buiten. Bijna één op de 106 e-mails bevat momenteel een vorm van malware bedreiging. Sommige aanvallers gebruiken daarbij zeer gerichte benaderingen die zijn ontworpen om op authenticatie gebaseerde systemen te verslaan. Hierdoor is de inzet van traditionele anti-virus technieken niet voldoende en moeten er extra maatregelen worden genomen. Met de effectieve verdediging van E-mail Security kun je jouw bedrijf beschermen tegen malware zonder hardware of software op locatie.

Toonaangevende e-mail-beveiliging in de cloud beschermt data, gebruikers en netwerken.

Complete beveiliging

Claranet levert met E-mail Security een complete beveiliging van zowel inkomende als uitgaande berichten met een effectieve en accurate anti-malware, anti-spam en content filtering dienst vanuit een wereldwijd cloud-platform. De 99% spamdetectie met slechts 0,0003% valse positieven zorgt dat het netwerk niet volloopt met spam en werknemers hun tijd niet verdoen met het lezen van ongewenste massamails. De 100% beveiliging tegen bekende en onbekende virussen beschermt jouw netwerk en medewerkers tegen nieuwe en opkomende bedreigingen en gerichte aanvallen. De continuïteit is bovendien volledig gewaarborgd door gegandeerde beschikbaarheid van de service. Deze toonaangevende cloudbeveiliging wordt geleverd met de beste SLA's en volledige klantondersteuning zoals je van Claranet mag verwachten.



Meer informatie:

claranet.nl - twitter.com/claranet_nl

Voor het maken van een afspraak:

040 - 239 3300 - verkoop@claranet.nl



Eenvoudig gebruik

Er is geen gebruikerstraining nodig voor het gebruik van E-mail Security. De dienst behoeft geen lokale installatie en is eenvoudig te configureren en te gebruiken. De dienst wordt centraal ingeschakeld om automatisch de inkomende en uitgaande e-mail met bijlagen te scannen. Het biedt alle gebruikers de mogelijkheid om veilig e-mail te ontvangen en te versturen, onafhankelijk van de gebruikte technologie. De infrastructuur en beschermingstechnologieën van E-mail Security worden ontwikkeld en beheerd door een team van experts van Symantec. Je behoudt zelf volledige controle over beleidsregels en serviceprestaties via het webbeheerportal, waarop je ook rapporten kan genereren en e-mails kan traceren.

Met E-mail & Web Security kun je virussen, malware, spam, phishing en gerichte aanvallen blokkeren voordat ze jouw inbox bereiken.

Extra beveiliging

E-mail Security heeft twee additionele modules die in combinatie met anti-virus en anti-spam kunnen worden afgenomen; 'content control' en 'image control'. Met deze modules kan de naleving van beleid op gebied van 'acceptable use'- en/of 'data leakage prevention' voor het e-mailverkeer worden gecontroleerd, door specifieke regels in te stellen voor de controle van inhoud van e-mails en toegevoegde afbeeldingen. Een e-mailbericht dat inbreuk maakt op het beleid van de organisatie kan onderworpen worden aan diverse acties, zoals 'blokkeren/verwijderen' of 'doorsturen naar de IT-afdeling'.

Infrastructuur

De onderliggende infrastructuur van E-mail Security is ontworpen om e-mails met malware bedreigingen te blokkeren vóórdat ze jouw inbox bereiken. De dienst wordt geleverd door middel van een wereldwijde infrastructuur in datacenters verspreid over de hele wereld in de grote internet exchange punten. Redundantie binnen en tussen de datacenters zorgt ervoor dat er een SLA-doelstelling van 100% beschikbaarheid geboden kan worden. De e-mail servers draaien ruim onder hun capaciteit, waardoor er voldoende ruimte over is om onverwachte pieken in het verkeer te kunnen verwerken. De Symantec cloud-infrastructuur verwerkt ruim 7 miljard e-mails per maand van wereldwijd verspreide klanten, variërend van grote multinationals tot MKB-bedrijven en consumenten.

Daarnaast wordt er gebruik gemaakt van Symantec's Global Intelligence Network (GIN), wat bestaat uit meer dan 63,8 miljoen sensoren die duizenden gebeurtenissen per seconde registreren in meer dan 157 landen wereldwijd. En er wordt gebruikt gemaakt van het Symantec 'Probe Network', een systeem van miljoenen nep e-mailaccounts, dat niets anders doet dan het verzamelen van spam en phishing e-mails om zelf hiervan te leren in het beter herkennen van bedreigingen. Het Probe Network heeft een wereldwijde dekking en onderschept 30 miljoen frauduleuze e-mails per dag.

Symantec Skeptic-technologie

Om het hoge serviceniveau te bereiken maakt E-mail Security gebruik van een defensielag, genaamd Skeptic, die volledig in eigen beheer van Symantec is ontwikkeld en wordt beheerd. Skeptic gebruikt heuristische technieken om te bepalen of een e-mail onderdelen bevat van een malware en verzorgt een complexe diepgaande analysescan van de e-mails en bijlagen met behulp van geavanceerde codeanalyse. Het maakt gebruik van meerdere gepatenteerde technologieën en duizenden regels om zowel bekende als onbekende bedreigingen te analyseren en op te sporen. In tegenstelling tot andere commerciële anti-virus oplossingen, kan Skeptic niet worden gedownload en getest door cybercriminelen. Skeptic gebruikt schaalbare server arrays vanuit een robuuste cloudomgeving om de analyse uit te voeren voor de miljarden e-mails per maand. Hierbij wordt gebruik gemaakt van een eigen lerend platform én het Symantec Probe Network; hoe meer verkeer het scant, hoe slimmer het platform wordt.

Web Security

De dienstenbundel is eenvoudig uit te breiden met een module voor professionele bescherming van het internetverkeer tussen jouw organisatie en derden; Web Security. Als een extra beschermlaag tussen het internet en de lokale IT-infrastructuur wordt het wereldwijde cloud-platform van Symantec ingezet om al het internetverkeer te controleren. Met behulp van URL-filtering is het mogelijk om centraal de bedrijfspolicy voor acceptabel surfgedrag van gebruikers aan te passen waarbij bepaalde websites volledig geblokkeerd worden, de toegang wordt beperkt tot bepaalde periodes op een (werk)dag of een maximale bezoekduur ingesteld wordt.

Symantec

Symantec werd in 1982 opgericht door computerdeskundigen met een eigen visie. In die visie veranderde Symantec mee met de technologie. Symantec is wereldwijd marktleider in beveiligings-, back-up- en beschikbaarheidsoplossingen met als voornaamste doel het leveren van oplossingen voor beveiliging, opslag en systeembeheer. De focus ligt op het geven van vertrouwen aan klanten. Symantec is een wereldwijde toonaangevende leverancier en wordt door miljoenen zakelijke en individuele klanten gebruikt.

Garanties en voordelen:

Anti-virus effectiviteit: 100% bescherming tegen bekende en onbekende virussen

Anti-virus accuratie: minder dan 0,0001% valse positieven

Anti-spam effectiviteit: 99% detectie

Anti-spam accuratie: minder dan 0,0003% valse positieven

Beschikbaarheid: 100%

Filtervertraging: scanning en levering van de e-mail in minder dan 60 seconden

24x7 automatische updates

Geen verlies van netwerk-bandbreedte door het filteren van spam en virussen buiten het netwerk

Productiviteit van medewerkers wordt beschermd, geen verloren tijd door het lezen en verwijderen van spam