

Hoe goed is uw e-mail beschermd tegen virussen en spam?

Scannen en filteren van ongewenste e-mail veilig buiten uw bedrijfsnetwerk

Betrouwbare multi-engine VirusBlocking

Geavanceerde SpamFilter

Gebruikersvriendelijke web interface voor het beheren van instellingen

Uitgebreide en overzichtelijke statistieken



CleanPort Introductie

E-mail is als medium voor communicatie niet meer weg te denken uit onze maatschappij. De snelheid en laagdrempeligheid van het gebruik van e-mail brengen enorme voordelen met zich mee. Maar ook grote bedreigingen. Gevaren als virussen en tijdrovende spam kunnen zich snel verspreiden en daarmee uw netwerk besmetten en in voorkomende gevallen uw bedrijf verlammen.

Traditionele anti-virus software is niet berekend op deze snelheid van verspreiding en schiet te kort bij het tegenhouden van nieuwe virussen en het intensieve onderhoud om adequate nieuwe gevaren tegen te gaan. Heeft u er wel eens bij stilgestaan wat ongewenste e-mail u dagelijks kost en welke gevaren het met zich meebrengt?

CleanPort Managed E-mail Filtering is specifiek ontwikkeld voor het veilig maken en effectief houden van uw e-mail. Dit zonder dat u er omkijken naar heeft of extra hoeft te investeren in hardware of software. De dienst werkt op internet level, waardoor uw e-mails veilig buiten uw bedrijfsnetwerk van virussen, spam en andere ongewenste inhoud worden ontdaan.



Virus Protectie

Virusprotectie veilig buiten uw eigen netwerk - door het gebruik van meerdere virusscanners biedt deze dienst een optimale bescherming tegen virussen, trojans en andere gevaren. In de dienst zijn meerdere traditionele anti-virus scanners verwerkt en een in eigen beheer ontwikkelde scanner genaamd ProTAG. Deze intelligente scanner herkent op basis van patronen, waardoor CleanPort ook in staat is om nieuwe virussen direct te detecteren. In tegenstelling tot traditionele oplossingen is het installeren van updates hiervoor niet noodzakelijk. Dit zorgt ervoor dat er eigenlijk geen "window of vulnerability" is wat bij traditionele oplossingen op kan lopen van enkele uren tot enkele dagen. Standaard anti-virus software is namelijk afhankelijk van een update om nieuwe virussen te herkennen.

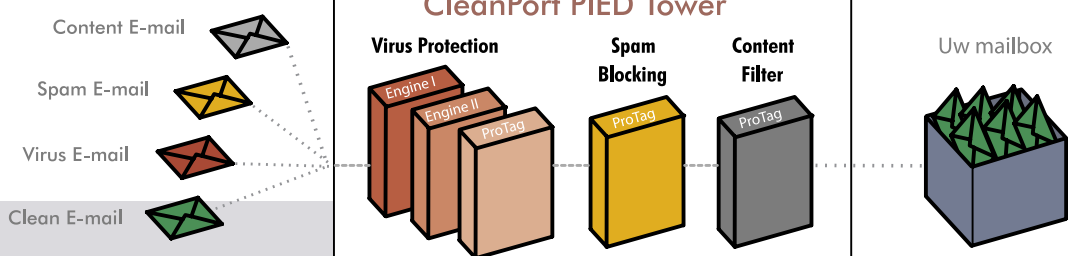
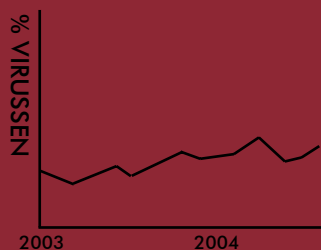
Onderschepte virussen kunnen na keuze direct worden verwijderd of in quarantaine worden geplaatst. Vanuit de quarantaine kunt u ze verwijderen of vrijgeven om ze alsnog in uw mailbox te ontvangen. Na 14 dagen worden ze automatisch uit de quarantaine verwijderd. Deze en andere instellingen en rapportages kunt u naar wens op gebruikers- of domeinniveau instellen. In de statistieken van uw persoonlijke CleanPort MyAccount kunt u zien hoeveel virussen er worden onderschept, per dag, maand en per jaar. Verder vindt u bij de statistieken onder andere een virus top 10. Waardoor u duidelijk inzicht heeft in welke virussen het meeste voorkomen en voor u worden onderschept.

Voor de anti-virus scanners wordt elke 5 minuten gecontroleerd of er nieuwe updates beschikbaar zijn. Deze worden vervolgens via een update mechanisme binnen een minuut over alle mailservers binnen de towers verspreid. De database voor onze ProTAG scanner wordt dagelijks geupdate met nieuwe patronen. De ProTAG scanner is in staat om nieuwe virussen op basis van schadelijke bijlages en objecten, waaronder ActiveX en IFRAMES, te herkennen. Wanneer er een nieuw virus uitbreekt duurt het vaak van enkele uren tot een dag voordat anti-virus software fabrikanten met een update komen, in deze "window of vulnerability" biedt de CleanPort Virus Protection dus al wel protectie via de heuristische ProTAG technologie.

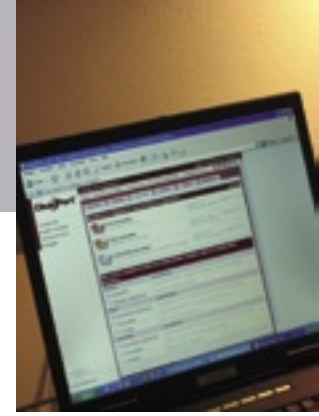
Virussen of andere schadelijke content die door ProTAG worden onderschept geeft CleanPort geen naam, dit om verwarring met de naamstelling van reguliere anti-virussoftware te voorkomen. Deze berichten worden onderschept met als naamgeving "ProTAG". Dit geldt zowel voor de naam in quarantaine als voor de naam in de statistieken, waaronder de Virus top 10.

De hoeveelheid virussen (ten opzichte van het aantal totale mailtjes) kunt u overzichtelijk en gemakkelijk zien in de statistieken.

**1 op de 12 e-mails
bevat een virus**

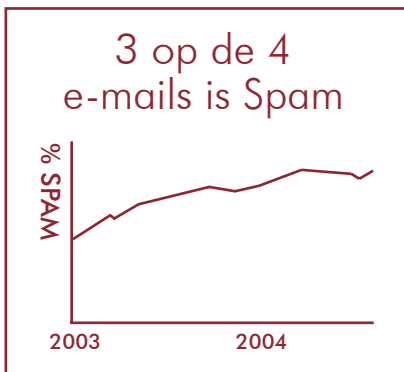


**E-mail zoals
e-mail bedoeld is**



Spam Blocking

De CleanPort Spam Blocking dienst maakt gebruik van heuristische technologie en als aanvulling hierop kunt u white en blacklist gebruiken. De heuristische technologie bepaalt aan de hand van honderden "rules" hoe groot de kans is dat een bepaald e-mailbericht daadwerkelijk spam is. Uit deze controle komt een score tussen de 0 en 100 %. Standaard wordt bij een score van 85% of meer een mailtje als spam gemarkeerd. De gevoeligheid kan elke gebruiker zelf instellen, hiervoor zijn 5 niveaus, waarbij niveau 3 de standaard instelling is. De niveaus zijn als volgt omschreven: "Heel soepel", "Soepel", "Normaal", "Streng" en "Heel Streng". De rules van de heuristische technologie bestaan uit controles op de mail headers en inhoud van het bericht. Waarbij in de headers onder andere wordt gecontroleerd op de afzender en via welke mailservers het mailtje uiteindelijk op de CleanPort tower terecht is gekomen, dit gaat in samenwerking met op internetniveau beheerde (dns)blacklists en onze eigen blacklists.



Voor het controleren van de inhoud van het bericht wordt onder andere Bayesian technologie gebruikt. Deze bekijkt woordcombinaties, wanneer er veel woordcombinaties zijn die vaak in spam berichten worden gebruikt zal dit de totale score verhogen. Wanneer er veel woordcombinaties zijn die niet (vaak) in spam berichten voorkomen zal dit de totale score verlagen. De Bayesian technologie herkent vele talen waaronder de West-Europese, Hebreeuws en Chinees. De CleanPort technologie maakt verder nog gebruik van tientallen andere filters als onderdeel van de Spam Blocking dienst waaronder "URL filters" en "image recognition".

In eigenlijk alle situaties biedt bovenstaande automatische analyse een betrouwbare manier om uw mailbox spam vrij te houden. Mocht u desondanks toch zelf bepaalde afzenders of domeinen specifiek willen doorlaten of blokkeren dan kunt u dit doen met behulp van de white en blacklist mogelijkheden. U geeft dan voor een afzender adres of afzender domein aan of deze wel of niet als spam dient te worden behandeld.

U kunt zelf een keuze maken wat er gebeurt met onderschepte spam berichten, u heeft de keuze uit: in quarantaine plaatsen, direct verwijderen of doorlaten maar het onderwerp van het bericht aanpassen. Het onderwerp wordt dan uitgebreid met *** [CP] SPAM *** waardoor u desgewenst in uw mailprogramma (bijvoorbeeld Outlook) zelf met behulp van regels de spam in een andere folder terecht kunt laten komen. Standaard wordt de spam mail in quarantaine geplaatst.

In de spam quarantaine heeft u de mogelijkheid om mail alsnog in uw mailbox te gaan ontvangen door berichten vanuit de quarantaine vrij te geven. Mocht er perongeluk een mailtje zijn onderschept dat u wel had willen ontvangen dan kunt u dat hier aangeven door het mailtje vrij te geven met de extra knop 'onthoud als niet spam', dit zorgt ervoor dat een vergelijkbaar mailtje de volgende keer gewoon zal worden doorgelaten. U kunt ook zelf berichten uit de quarantaine verwijderen, anders gebeurt dit automatisch na 30 dagen. In de quarantaine kunt u ook zien op basis waarvan een bericht is onderschept, dit kan bijvoorbeeld zijn op basis van heuristische eigenschappen maar ook op basis van het afzenderadres wat u op de blacklist heeft gezet. Elke quarantaine biedt verschillende zoekmogelijkheden om gemakkelijk berichten terug te vinden.

Waarom Managed E-mail Filtering van CleanPort ?

De diensten die CleanPort aanbiedt zijn provider onafhankelijk, hierdoor kan elke organisatie (ook de non-profit sector) gebruik maken van onze diensten.

1 Optimale veiligheid

Door de combinatie van geselecteerde technieken en 24/7 beheer en ontwikkeling bieden de CleanPort Virus Protection, Spam Blocking en aanvullende Content Filter diensten optimale bescherming tegen de gevaren van het gebruik van e-mail. Daarnaast zorgt de CleanPort bescherming ervoor dat u effectief gebruik kunt gaan en blijven maken van e-mail.

3 Eenvoudige setup

Om van de CleanPort diensten gebruik te maken hoeft u geen ingewikkelde langdurige procedures door. De enige twee dingen die u hoeft te doen is de dienst aanvragen en een eenmalige eenvoudige handeling om de dienst te activeren. De rest regelen wij, de dienst werkt voor uw gebruikers transparant, aan de kant van de gebruikers hoeft er niets te veranderen!

2 Geen extra investeringen in hardware of software

De CleanPort dienst wordt aangeboden door middel van een maandelijks abonnementsstarief, u heeft geen extra hardware of software nodig. Door e-mail security te outsourcen maakt u zelfs resources vrij, uw systeem en netwerkbeheerders hoeven zich niet meer met de lastige en dagelijks terugkerende taak van updates en vragen met betrekking tot spam en virus mailtjes bezig te houden..

4 Toegankelijk en inzichtelijk

U heeft zelf 24 uur per dag toegang tot de instellingen voor uw domein(en) via de CleanPort webinterface MyAccount. Met behulp van deze interface kunt u op een gemakkelijke manier instellingen bekijken en wijzigen en tevens met behulp van de dagelijkse rapportage een goed inzicht krijgen in het e-mail verkeer van uw domein(en).

CleanPort in vergelijking met anti-virus en anti-spam diensten die providers aanbieden

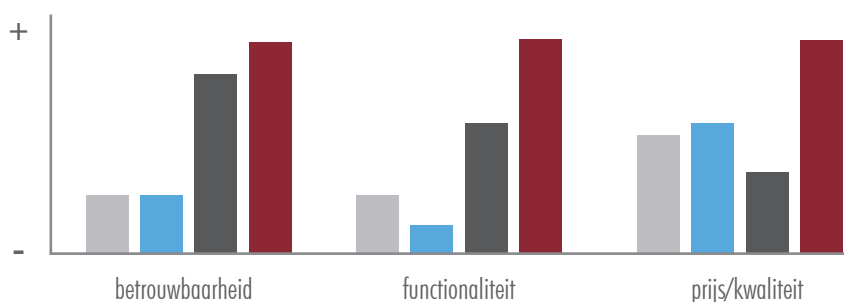
- Meer zekerheid: CleanPort maakt gebruik van meerdere anti-virusscanners
- Uitgebreide statistieken, waarbij providers meestal helemaal geen statistieken ter beschikking stellen
- Elke afzonderlijke gebruiker kan de mogelijkheid worden geboden om persoonlijke instellingen te maken, waaronder de gevoeligheid van de spamfilter en het gebruik van white en blacklists.
- Ten allen tijden toegang tot onderschepte berichten, deze kunnen namelijk in afzonderlijke virus, spam en content filter quarantaines geplaatst worden. Waarbij providers eigenlijk altijd berichten onderschept als virus of spam direct verwijderen. Hierdoor loopt men de kans -vooral bij spam- dat er per ongeluk mail verdwijnt die belangrijk kan zijn
- CleanPort levert de Managed E-mail Security diensten aan miljoenen gebruikers wereldwijd waardoor wij veel meer inzicht hebben in het e-mail verkeer wereldwijd en hierdoor sneller kunnen inspringen op nieuwe virussen en spam technieken
- CleanPort heeft voor elke organisatie een passend model, of u nu een bedrijf met 5 of honderd duizend medewerkers heeft
- CleanPort levert haar diensten wereldwijd aan tientallen providers



Business To You
Secretaris Munniklaan 39
3648 VD WILNIS
Nederland

tel. +31 - (0) 297 - 256569
fax. +31 - (0) 84 - 8712136

e-mail info@b2u.nl
web www.b2u.nl



■ Anti-Virus pakket ■ Provider ■ Managed E-mail ■ CleanPort MEF

CleanPort in vergelijking met andere Managed E-mail Security providers

- Voor elke organisatie een passend model, of u nu een bedrijf met 5 of honderd duizend medewerkers heeft
- Door onze geavanceerde en flexibele software en infrastructuur kunnen wij behalve aan bedrijven ook aan (consumenten) ISP's leveren
- CleanPort biedt de mogelijkheid om op 5 beheersniveau's te beheren, van reseller naar eindgebruiker
- Gebruikersvriendelijke en geavanceerde webinterface, waardoor u uitgebreide instellingen en statistieken kunt beheren, en er nooit mail wordt weggegooid, deze komt immers in een van de drie quarantaines terecht
- 24 uur per dag, 7 dagen per week beheer en support beschikbaar
- Mogelijkheid om onze interface te integreren in bijvoorbeeld uw control pannel of webmail interfaces
- Webinterface in meerdere talen waaronder Nederlands, Engels, Frans en Hebreeuws
- Doordat CleanPort haar diensten in verschillende landen aanbiedt kunnen wij sneller inspringen op ontwikkelingen op het gebied van virussen en nieuwe spam technieken

Deze brochure is met de grootste mogelijke zorg samengesteld. Des ondanks kunnen aan de inhoud van deze brochure geen rechten worden ontleend.



(c) 2004, Copyright CleanPort B.V.
Alle rechten voorbehouden, niets uit deze publicatie mag zonder voorafgaande toestemming van CleanPort B.V. worden gebruikt.