



Managed E-mail security

CleanPort Managed E-mail security

Omdat de hoeveelheid ongewenste E-mail alsmaar toeneemt, zijn standaard software en applicaties tegen SPAM en virussen niet toereikend meer. CleanPort Managed E-Mail Security biedt de meest geavanceerde oplossing van dit moment. CleanPort beschikt over gepatenteerde technologie, en voegt continu zelf ontwikkelde nieuwe technieken en technologieën, zoals bijvoorbeeld Advanced Greylisting en HICAR (Heuristic Character Recognition), toe aan haar oplossing.

CleanPort is geen softwarematige oplossing, maar een gepatenteerde Managed Service. CleanPort wordt dan ook niet op uw PC of uw netwerk geïnstalleerd, maar werkt door het omzetten van het MX-record van uw mailserver. Hierdoor wordt de mail op een veilige afstand van uw eigen bedrijfsnetwerk door CleanPort gefilterd en gescand, wordt ongewenste mail in quarantaine geplaatst, en de overige mail veilig afgeleverd.

Omdat CleanPort iedere dag grote hoeveelheden E-mails voor meer dan tienduizend klanten met in totaal miljoenen eindgebruikers scant, kunnen de kosten voor continue innovatie en support worden gedeeld, zodat de prijs voor CleanPort ook nog eens zeer aantrekkelijk is.

De voordelen van CleanPort Managed E-mail Security op een rij:

1. Geen investeringen nodig in hardware, software en manuren
2. Zeer eenvoudige setup en een gebruikersvriendelijke interface
3. Instelbaar op domein, afdelings- en userniveau
4. CleanPort werkt op veilige afstand en houdt virussen ver weg van uw bedrijfsnetwerk
5. De meest geavanceerde technologie met de heuristische ProTAG en HICAR
6. Bescherming tegen nieuwe virussen en vormen van SPAM
7. Volledige controle via MyAccount over instellingen, rapportage en quarantaine
8. Continu de laatste updates en technologische vernieuwingen zonder daar extra voor te betalen
9. U heeft geen set up kosten, alleen het lage maandtarief per e-mailgebruiker
10. De MyAccount- interface is aan te passen aan uw huisstijl.

E-mail stroom:

Hieronder ziet u een stroomschema van de route die E-mail aflegt van verschillende bronnen naar CleanPort die de mail scant en filtert, om uiteindelijk alleen veilige en gewenste mail af te leveren bij de klant.

**> DNS Server**

Voor elk domein worden er gegevens bijgehouden in DNS servers. Een DNS server maakt een koppeling tussen een hostnaam (bijvoorbeeld: www.uwdomein.nl) en IP adres(sen).

> MX records

Per domein kunnen 1 of meerdere MX records worden ingesteld. MX gegevens geven aan de versturende mail server aan op welke server de e-mail voor een domein moet worden aangeboden. Wanneer u gebruik maakt van CleanPort verwijzen deze MX records naar CleanPort Mail Towers.

Deze mail towers scannen en filteren de e-mail en leveren de schone e-mail af op uw e-mail server.

> Loadbalancer

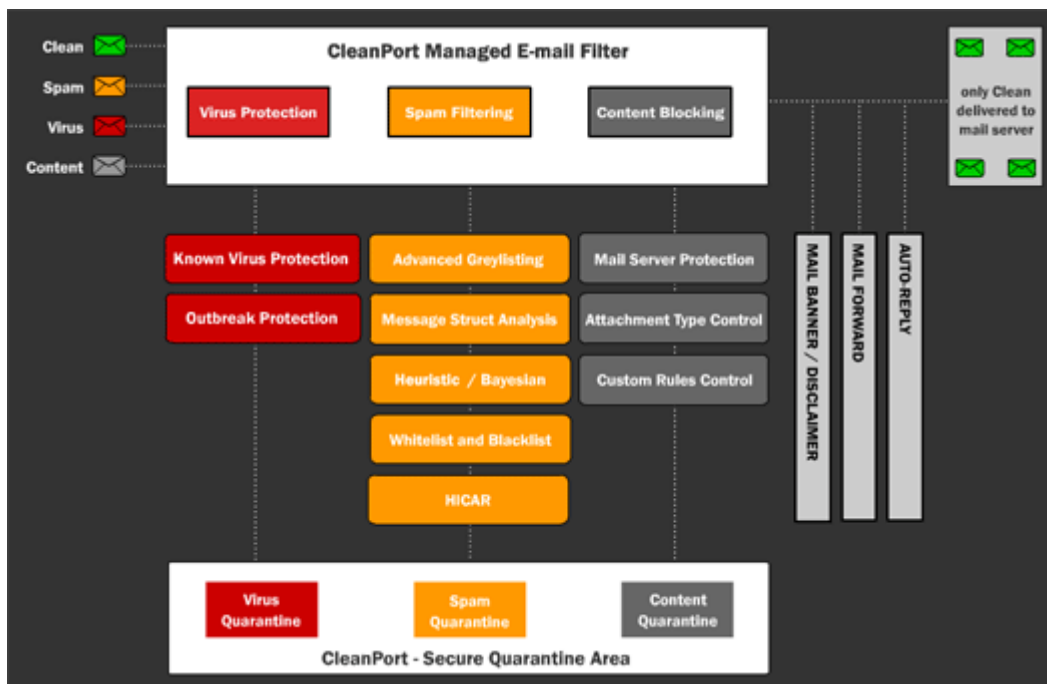
Door gebruik te maken van redundante loadbalancers verdeelt CleanPort de e-mail over een groot aantal mail servers om de doorvoer snelheid continu zo hoog mogelijk te laten zijn.

> Secure Quarantine

E-mails die worden herkend als ongewenst kunnen in Quarantaine worden geplaatst. Elke klant/gebruiker kan toegang krijgen tot de CleanPort webinterface "MyAccount". Met deze inlog kan elke gebruiker of domeinbeheerder o.a. de quarantaine inzien en berichten alsnog vrijgeven.

E-mail filtering:

Het onderstaande schema geeft de verschillende componenten, gepatenteerde technologieën en technieken weer waarmee CleanPort E-mail filtert, scant en blokkeert.



> Known Virus Protection

Multi-engine oplossing: er wordt met meerdere scanners parallel gescand op bestaande virussen.

> Outbreak Virus Protection

Met behulp van een uitgebreide database en geavanceerde patroon herkenning kunnen ook nieuwe virussen worden herkend.

> Advanced Greylisting

Veel spamversturende servers proberen slechts eenmaal een e-mail af te leveren, dit in combinatie met bepaalde patronen maakt het mogelijk nieuwe spam al in een vroegtijdig stadium te herkennen.

> Message Structure Analysis

Op basis van de structuur en headers van e-mail berichten worden verschillende controles uitgevoerd.

> Heuristic / Bayesian

Op basis van de inhoud van een e-mail wordt een mailtje geclassificeerd. Door letter en woordcombinaties kan de inhoud worden gecategoriseerd.

> Whitelist and Blacklist

Er worden een tiental white- en blacklists toegepast om bekende spammers en e-mail signatures te herkennen.

> HICAR Heuristic Image Character Recognition is een door CleanPort ontwikkelde technologie die in staat is om in afbeeldingen versleutelde teksten te herkennen en deze te classificeren.

> Mail Server Protection

Met deze techniek is CleanPort in staat om grote e-mails, zip-of-death en andere gevaren voor uw mailserver tegen te gaan.

> Attachment Type Control

U bepaalt zelf welke type bijlages er wel of niet ontvangen kunnen worden.

> Custom Rules Control

U kunt ook eigen "rules" aanmaken om e-mail die aan de door u opgegeven specifieke voorwaarden voldoet te blokkeren of juist te accepteren.

> Mail Banner / Disclaimer

Het systeem biedt de mogelijkheid om onder elke inkomende of uitgaande e-mail een "handtekening" toe te laten voegen om aan te geven dat de e-mail gescand is. Deze functionaliteit kan ook worden gebruikt om disclaimers onder een e-mail te plaatsen.

> Mail Forward

Naast het afleveren op mail server(s) is het ook mogelijk om mail voor een geheel domein of slechts enkele adressen (tijdelijk) door te laten sturen naar een "extern" e-mailadres.

> Auto-reply

Er bestaat de mogelijkheid om op elk inkomend bericht (tijdelijk) automatisch een bericht terug te laten sturen. Dit kan op gebruikersniveau worden ingesteld.