

Wat zijn de belangrijkste functies voor de Anti-Spam Engine op Cisco e-mail security applicatie (ESA)?

Cisco Anti-Spam kan de breedste reeks bedreigingen wereldwijd stoppen

- Doelstelling om bekende bedreigingen zoals spam, phishing en zombiaanvallen te identificeren, evenals nieuwe en zich ontwikkelende bedreigingen
- Alleen een oplossing om zowel e-mail als web reputatie te combineren om gemengde bedreigingen te detecteren. In tegenstelling tot inhoudelijke technieken zijn deze reputatiesystemen taalkundig agnostisch.
- Realtime toegang tot Sender Base, 's werelds grootste e-mail en web traffic monitoring netwerk, resulteert in nieuwe bedreigingen die worden geïdentificeerd zodra ze beginnen.
- Ontworpen en onderhouden door een team van zeer ervaren veiligheidsdeskundigen. Plaatselijk onderzoekspersoneel in Azië, Europa en Latijns-Amerika draagt bij tot het testen en opleiden van systemen
- Aangedreven door Cisco's unieke Context Adaptive Scanning Engine (CASE), die content-georiënteerde en content-agnostische technieken combineert, en misclassificatie op basis van smalle berichtcontext voorkomt.
- 24x7 ondersteund door het Threat Operations Center om te zorgen voor een analyse van een gesloten lus.

Cisco Anti-Spam biedt geen administratieve overhead

- Instellen en vergeten, met een gebruiksvriendelijke GUI.
- Doorlopende afstemming, training of filtreerschrift zijn niet vereist.
- Hiermee kunnen eindgebruikers zich richten op hun kernactiviteiten in plaats van handmatig berichten opnieuw bekijken.

Cisco Anti-Spam biedt toonaangevende prestaties

- Cisco werkt dynamisch de volgorde bij waarin de regels worden uitgevoerd met ons patentwachten vroege exit-algoritme om onnodig scannen te elimineren.
- Cisco duwt zoveel mogelijk analyse aan de netwerkvolk met netwerk toegelaten scoring, reducerend op-box verwerkingsvereisten.
- Berichten worden één keer gescand vanwege meerdere bedreigingen, waardoor de totale doorvoersnelheid van onze apparatuur wordt geoptimaliseerd.