

SenderBase는 어떻게 작동합니까?

목차

[소개](#)

[SenderBase는 어떻게 작동합니까?](#)

[관련 정보](#)

소개

이 문서에서는 SenderBase의 작동 방식을 설명합니다.

SenderBase는 어떻게 작동합니까?

SenderBase는 이메일 관리자가 발신자의 ID에 대한 객관적 데이터를 제공하여 수신 이메일 스트림을 더 효과적으로 관리할 수 있도록 설계되었습니다. SenderBase는 이메일의 신용 보고 서비스와 유사하며, ISP와 기업에서 합법적인 발신자를 스팸 소스와 구별하기 위해 사용할 수 있는 데이터를 제공합니다. SenderBase는 이메일 관리자가 원치 않는 상용 이메일(UCE)을 시작하는 IP 주소를 안정적으로 식별 및 차단하거나 비즈니스 파트너, 고객 또는 기타 중요한 소스로부터 합법적인 수신 이메일의 신뢰성을 확인할 수 있도록 하는 객관적 데이터를 제공합니다. SenderBase를 고유하게 만드는 것은 이메일 메시지 볼륨에 대한 전역 보기를 제공하고 이메일의 관련 소스를 쉽게 식별하고 그룹화하는 방식으로 데이터를 구성한다는 것입니다. SenderBase는 여러 정보 소스를 결합하여 모든 IP 주소에 대한 "평판 점수"를 결정합니다.

이 정보에는 다음이 포함됩니다.

- 정기적으로 인터넷 이메일을 수신하는 수만 개의 조직에서 제공하는 이메일 볼륨 정보
- SpamCop 서비스에서 받은 스팸 볼륨
- 다른 DNS 기반 차단 목록에 대한 정보

SenderBase의 평판 점수 범위는 -10에서 +10까지입니다. 이는 보내는 IP 주소가 스팸을 보내려고 시도하는 가능성을 반영합니다. 매우 부정적인 점수는 스팸을 보낼 가능성이 매우 높은 발신자를 나타냅니다. 매우 긍정적인 점수는 스팸을 보낼 가능성이 거의 없는 발신자를 나타냅니다. ESA(Email Security Appliance)를 사용하여 이러한 점수를 차단, 제한 및 스팸 필터링 정책과 결합하여 시스템 성능을 가속화하고 오탐을 줄일 수 있습니다.

SenderBase Reputation Service에는 여러 데이터 소스가 포함되므로 매우 부정적인 점수가 발생하여 발신자를 스팸머로 잘못 식별할 가능성이 높습니다. DNS 기반 차단 목록 또는 스팸 보고서가 항상 부정확할 수 있지만, 많은 목록이 동일한 IP 주소를 보고하고 SpamCop가 IP 주소에서 보낸 스팸에 대한 보고서를 많이 갖고 있으면 오탐의 가능성이 크게 줄어듭니다.

관련 정보

- [SenderBase FAQ](#)
- [기술 지원 및 문서 - Cisco Systems](#)