

# Présentation de la réputation Web de Cisco WSA

## Contenu

[Introduction](#)

[Présentation de WBRS](#)

[Utilisation WBRS de SenderBase](#)

[Granularité WBRS](#)

## Introduction

Ce document fournit une vue d'ensemble de la réputation Web de Cisco (WBRS) pour l'appareil de sécurité Web de Cisco (WSA).

Contribué par Josh Wolfer et Stephan Fiebrandt, ingénieurs du centre d'assistance technique Cisco.

## Présentation de WBRS

WBRS est une méthode innovante qui analyse le comportement et les caractéristiques d'un serveur Web et fournit la dernière défense contre le spam, les virus, le phishing et les menaces de logiciels espions.

WBRS utilise une analyse en temps réel sur un ensemble de données vaste, diversifié et mondial afin de détecter les URL qui contiennent une forme quelconque de programme malveillant. WBRS est une partie essentielle de la base de données de sécurité de Cisco, qui protège les clients contre les menaces combinées provenant du trafic de messagerie électronique ou Web.

## Utilisation WBRS de SenderBase

WBRS exploite les données de la base de données de sécurité commune (SenderBase<sup>®</sup> Network) de Cisco, le plus grand réseau mondial de surveillance du trafic web et de messagerie. Il suit plus de 50 paramètres distincts qui sont d'excellents indicateurs de la réputation d'une URL. Grâce à des agents sophistiqués de modélisation de la sécurité et de détection des programmes malveillants, Cisco évalue ces URL en fonction de ces entrées.

Certains paramètres sont les suivants :

- Données de catégorisation des URL

- Présence du code téléchargeable
- Présence de contrats de licence d'utilisateur final (CLUF) longs et confus
- Volume global et modifications du volume
- Informations sur le propriétaire du réseau
- Historique d'une URL
- Âge d'une URL
- Présence de virus/spams/logiciels espions/hameçonnage/listes noires d'attaques
- Types d'URL des domaines courants
- Informations sur l'enregistrement de domaine
- Informations sur l'adresse IP

## Granularité WBRS

WBRS diffère d'une liste noire ou d'autorisation d'URL traditionnelle parce qu'il analyse un large ensemble de données et produit un score très granulaire de -10 à +10, au lieu des catégorisations **bonnes** ou **mauvaises** binaires de la plupart des applications de détection de programmes malveillants. Cette note granulaire offre aux administrateurs une flexibilité accrue ; différentes stratégies de sécurité peuvent être mises en oeuvre en fonction de différentes plages de notation WBRS.