



Spamhaus DBL

Overview

Spamhaus DBL is a real-time database of domains known to be associated with unwanted emails such as spam and phishing attacks. These are often web site domains found in the email body or attachments. This application allows the Sentrion Policy Engine to look up domains in the third-party Spamhaus DBL, blocking unwanted messages that might otherwise reach your employees to rob their productivity and compromise their privacy and security.

Audience

Companies that want an additional layer of protection for blocking unwanted email—particularly phishing attacks. This application is currently available only in Japan.

Key Features and Functionality Overview

Spamhaus DBL is a third-party domain block list that can be queried in real time to identify mail that originates from or links to domains known to be associated with spam. The Sentrion Policy Engine is the industry's premier solution for scanning emails—including the body and attachments—to discover all kinds of suspicious material and deal with it appropriately. Working together, Sentrion and Spamhaus DBL provide an affordable way to keep your end-users safe and productive, while preserving network bandwidth for legitimate business traffic.

Spamhaus DBL for Sentrion allows the Policy Engine to access the Spamhaus database of untrustworthy domains to block up to 90 percent of phishing attacks and other spam, with virtually no false positives. The database is rebuilt and reloaded every two minutes to ensure that new spam domains are blocked before they can do any damage, and that any mistaken listings are swiftly removed. Sixty mirrors strategically located in nations around the world ensure reliability, redundancy and responsiveness.

Spamhaus DBL complements your anti-spam defense by providing an additional, highly effective layer of anti-phishing protection. With the Spamhaus DBL for Sentrion extension and your subscription to the third-party Spamhaus DBL, you get:

- Automatic blocking of emails that contain the domains of spam payload URLs, spam sources and senders, known spammers and spam gangs, and phish, virus and malware-related sites
- Scanning for domains in the message body, such as the disguised URLs that are typically used in phishing attacks or to link users to infected websites
- Up to a 90 percent reduction in the amount of unwanted bulk mail entering your network
- Real-time updates and maintenance, 24x7, to stay ahead of the spammers and keep legitimate domains off the block list

Spamhaus DBL can greatly reduce the amount of junk entering your company—especially the toxic junk that entices employees to disclose personal information, robbing their privacy and ruining their finances. Combined with the standard connection control features of the Sentrion—along with applications such as Enterprise Anti-spam, IP Reputation Services, or Traffic Control with Spamhaus XBL and PBL—Spamhaus DBL becomes part of a complete array of defenses against all kinds of spam. And thanks to the Spamhaus DBL for Sentrion extension, it's managed alongside all your other defenses on a single appliance, simply and affordably.