

Antispam Software Development Kit (SDK)

The challenge

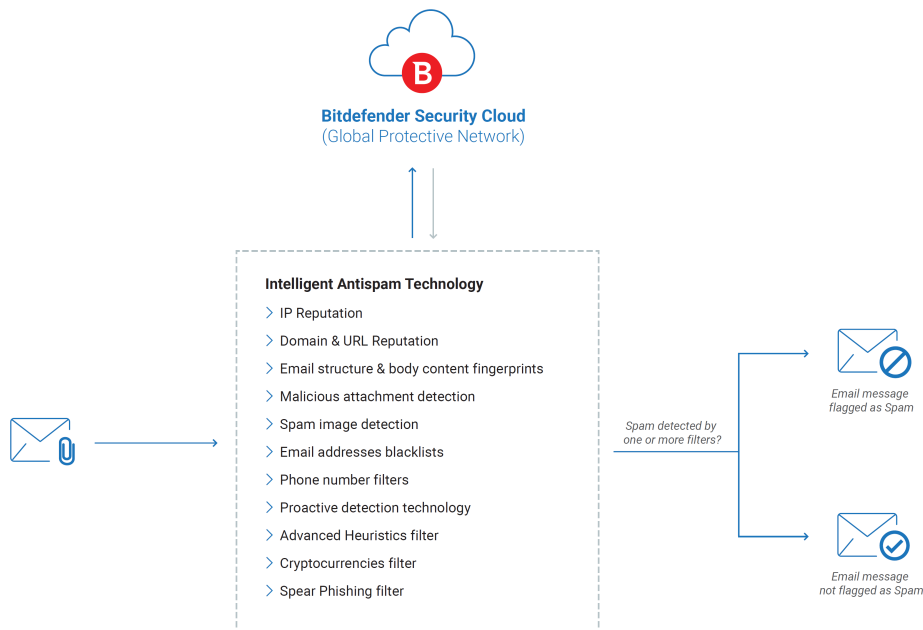
Email remains the primary attack vector for cyber criminals. Billions of spam and phishing messages are circulating around the globe trying to entice users with offers, display inappropriate content, steal confidential information, or mislead people. Not only is the sheer volume of spam emails rapidly increasing, but the number of messages carrying malicious attachments is also on the rise. It is estimated that more than 70% percent of all email sent globally is spam and over two thirds of malware is delivered via malicious email attachments. This makes email the most popular method for attackers to spread malicious code, and it poses a direct threat to users and businesses worldwide.

The solution

Organizations need to adopt a layered approach to email security to gain protection from the increasing risks posed by spam email. A multi-layer, proactive antispam technology with low false-positive rates will prevent exposure to spam and phishing attacks while allowing legitimate emails to reach users and leaving productivity unaffected. The Bitdefender Antispam SDK combines multiple spam and phishing-detection technologies to identify and stop these threats. Using Bitdefender's Intelligent Antispam technology, emails are captured and go through a battery of blacklists and content filtering technologies to identify spam, phishing, extortion scams and malspam attacks.

How the SDK works

The Bitdefender Antispam SDK scans partner-provided email messages stored in a disk file or in process memory, then returns the verdict (spam or not spam). For messages detected as spam, the SDK offers information on why it was detected as spam as well as a spam probability score, which the partner application can use to change the detection threshold. It can also add the specific headers into the email message indicating the spam status.



Intelligent Antispam technology

The Bitdefender Antispam SDK uses a combination of antispam filtering and predictive technologies to effectively detect spam messages in any language and reduce false positives, as well as protect from phishing attacks or malicious links in email attachments.

Components include:

- IP Reputation system: ensures proactive detection of spam emails based on sender's IP address
- Domain and URL Reputation: the message's URLs are extracted and checked against a real-time blacklist
- Email structure, headers and body content fingerprints: spam content is detected using cryptographic hashes
- Malicious attachment detection: an essential layer in detecting messages carrying malware and phishing attachments
- Cryptocurrency address blacklists: cover many types of cryptocurrencies used in extortion scams
- Spam image detection: based on computer vision technologies
- Email address blacklists: ensure detection of a wide range of email scams
- Phone number filter: blocks fraud and spam messages that include phone numbers
- Proactive heuristic detection technology combines complex spam message patterns, advanced heuristic filters and content analysis

- Spear phishing detection based on FROM and Reply-to header content filtering
- Email Classification: based on our detection types and machine learning classification models we can classify an email into:
 - Phishing
 - Malware
 - Extortion
 - Scam
 - Marketing

The SDK utilizes proprietary technologies, including patented detection methods and algorithms, as well as machine learning algorithms.

Detection rate of over 99.9%

Bitdefender's Intelligent Antispam technology is also used by Bitdefender Security for Mail Servers, the only antispam solution to have achieved VBSpam certification in all 59 Virus Bulletin spam tests ever performed. Bitdefender had an average spam detection rate of over 99.9% with zero false positives in the latest 22 consecutive VBSpam tests, and has achieved Virus Bulletin's highest certification, VBSpam+, for 22 tests in a row as of March 2020.

Other features:

- Prevents real-time spam outbreaks using Bitdefender cloud technology; blacklists are updated every second, and detection is replicated around the world via the Bitdefender Cloud
- High efficacy, with an extremely low number of false positives; if one or more filters detect spam characteristics, emails will be flagged accordingly
- Scan modes: scans email message stored in memory or file; can scan by file name or scan file content within the continuous memory buffer; offers full multi-threading and concurrency scan support
- Minimizes device footprint due to Thin Client technology
- No need for signature updates as all detection is completed in the Cloud
- Provides C language bindings; easy portability using the same API for Windows, Linux, and Mac
- All-inclusive SDK with code samples reduces time needed to integrate the SDK into any messaging solution

Specifications

The SDK primarily supports Microsoft Windows and Linux platforms on x86 CPU:

- Microsoft Windows (both 32 and 64-bit): XP SP2 and SP3, 2003 SP1 and SP2, 2008, Vista, Vista SP1, 7, 8, 8.1, 10
- Linux: the 32-bit of the Linux SDK works on any distribution that provides GLIBC 2.3.1 or higher; the 64-bit version of the Linux SDK supports GLIBC 2.3.3 and above, and requires gcc 3.4 or higher
- Mac OS: Mac OS X version 10.7 and above, both i386 and 64-bit architectures

Contact us

For more information about the SDK or any Bitdefender security technology, please reach us at www.bitdefender.com/oem

About Bitdefender Technology Licensing. Bitdefender provides end-to-end cyber security solutions and advanced threat protection to more than 500 million users in more than 150 countries. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and has become a provider of choice for leading Independent Software Vendors (ISVs), hardware vendors, service providers and enterprise organizations looking to integrate security technologies into their products and services. Today, Bitdefender has over 150 technology partners worldwide. More information is available at www.bitdefender.com/oem

Bitdefender®

Founded 2001, Romania
Number of employees 1800+

Headquarters
Enterprise HQ – Santa Clara, CA, United States
Technology HQ – Bucharest, Romania

WORLDWIDE OFFICES

USA & Canada: Ft. Lauderdale, FL | Santa Clara, CA | San Antonio, TX | Toronto, CA

Europe: Copenhagen, DENMARK | Paris, FRANCE | München, GERMANY | Milan, ITALY | Bucharest, Iasi, Cluj, Timisoara, ROMANIA | Barcelona, SPAIN | Dubai, UAE | London, UK | Hague, NETHERLANDS

Australia: Sydney, Melbourne