

Email Threat Protection SDK

The Email Threat Protection SDK is a multi-layered email scanner that can detect sophisticated phishing attempts, malicious attachments, continuously evolving scams, spam and more.

It is powered by an advanced suite of cloud engines, including AI models, generic detection engines and blacklists, all proven to be very effective. Bitdefender's email security suite has earned VBSpam's highest certification possible, with no false positives in every test since 2015.

The SDK is easy to integrate by email security providers, mail hosting companies, or any other partner that needs reliable email security. It comes with comprehensive documentation, code samples, email threat samples, and dedicated technical support.

Features

- ↳ **IP, URL, and domain analysis:** The SDK leverages contextual email threat intelligence to enforce IP, URL or domain blacklists and map spam campaigns in real time.
- ↳ **AI models:** The service uses deep learning models to proactively detect threats. These were trained on diverse email threat feeds, corresponding to different areas, languages and threat types.
- ↳ **Proactive heuristics detection:** A complex engine that combines pattern recognition, AI models, and more for proactive and generic detection of diverse, obfuscated campaigns.
- ↳ **Deobfuscation engines:** Multiple filters use patented fingerprinting algorithms and computer vision technologies to detect evasion techniques and ensure detection for sophisticated email attacks.
- ↳ **Phone and crypto wallet blacklists:** filters that detect blacklisted phone numbers and crypto wallets, very effective against scams, extortion, or charity fraud.

How the Email Threat Protection SDK works

The SDK provides several functions in C that partners can call to request scans on MIME files from disk or memory. When the scan function is called, the SDK extracts relevant data from the email and sends it to the Bitdefender cloud via an SSL-secured connection. There, the data goes through a battery of blacklists and AI-powered filters to identify email threats.

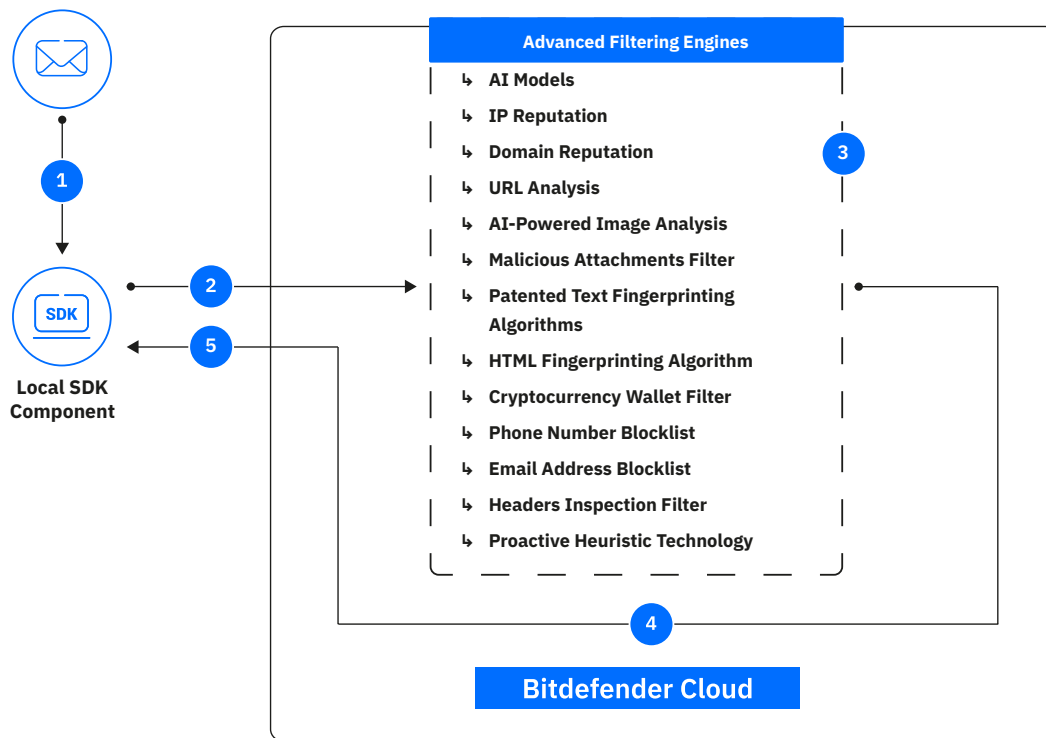
At-A-Glance

Bitdefender's Email Threat Protection SDK is an award-winning email security solution that can detect spam, phishing attempts like Business Email Compromise (BEC), elaborate email scams, and plenty more known or emerging email threats.

Benefits:

- ↳ **Advanced Threat Detection:** The SDK maintains a 99,9% detection rate thanks to a vast range of features, heuristics, data correlation mechanisms, and carefully trained deep learning models.
- ↳ **Lightning-Fast Results:** A verdict and associated threat context are available milliseconds after the scan function is called.
- ↳ **Easy-to-Integrate:** The SDK comes with code samples, email threat samples to test your application, comprehensive documentation, and support for common OS and architectures.
- ↳ **Minimal Footprint:** Scanning is done in the cloud, and the submission process only uses a few Megabytes of memory on the local device.
- ↳ **Language Independent:** Bitdefender's email security solution can identify threats in any language because it is continuously trained on diverse email threat feeds.

The verdict is returned as a bitmask combination that provides a detection result (spam or clean) and classification categories: phishing, malware, extortion, scam, marketing and others.



- 1 Local SDK component extracts data from the MIME file.
- 2 Local SDK component sends that encrypted data to the Bitdefender cloud via an SSL-secured connection.
- 3 The advanced email filtering engines process that data to identify threats.
- 4 The service generates a bitmask combination providing a detection result.
- 5 The function returns the bitmask combination, threat context, and a threat probability score in milliseconds.

Free evaluation

Evaluating the Bitdefender Email Threat Protection SDK is free of charge and includes technical support.

Contact us

For more information regarding the Email Threat Protection SDK please reach us at <https://www.bitdefender.com/oem/contact-us.html>

