

Online Threats SDK

The Online Threats SDK scans URLs and HTML content to determine if a page is malicious. Detections are further categorized as phishing, fraud, malicious, miner, or PUA, depending on the partner's license. The SDK uses several offline filters to analyze HTML content, and it queries Bitdefender's URL Status Service to access real-time threat intelligence about web content. Pages can be scanned from memory, or as files on disk, and a verdict is returned in milliseconds.

Features

- ↳ **Reliable detection rate:**
The Online Threats SDK uses patented fingerprinting technologies and threat intelligence to detect malicious pages.
- ↳ **Next-gen scanner:**
The SDK's filters use deep learning and other advanced detection technologies to scan HTML content.
- ↳ **Flexible deployment:**
The SDK comes with native support for 32-bit and 64-bit platforms, and it supports multiple operating systems with the same API.
- ↳ **Full multithreading and concurrency scan support:**
All scans are run in a partner thread context, allowing separate affinity and priority settings for each scan.

At-a-Glance

The Online Threats SDK is a powerful scanner that can detect malicious URLs and HTML content. It's lightweight, fast and easy to integrate via a simple API. Despite the low footprint, the SDK maintains a high detection rate, and low false positives.

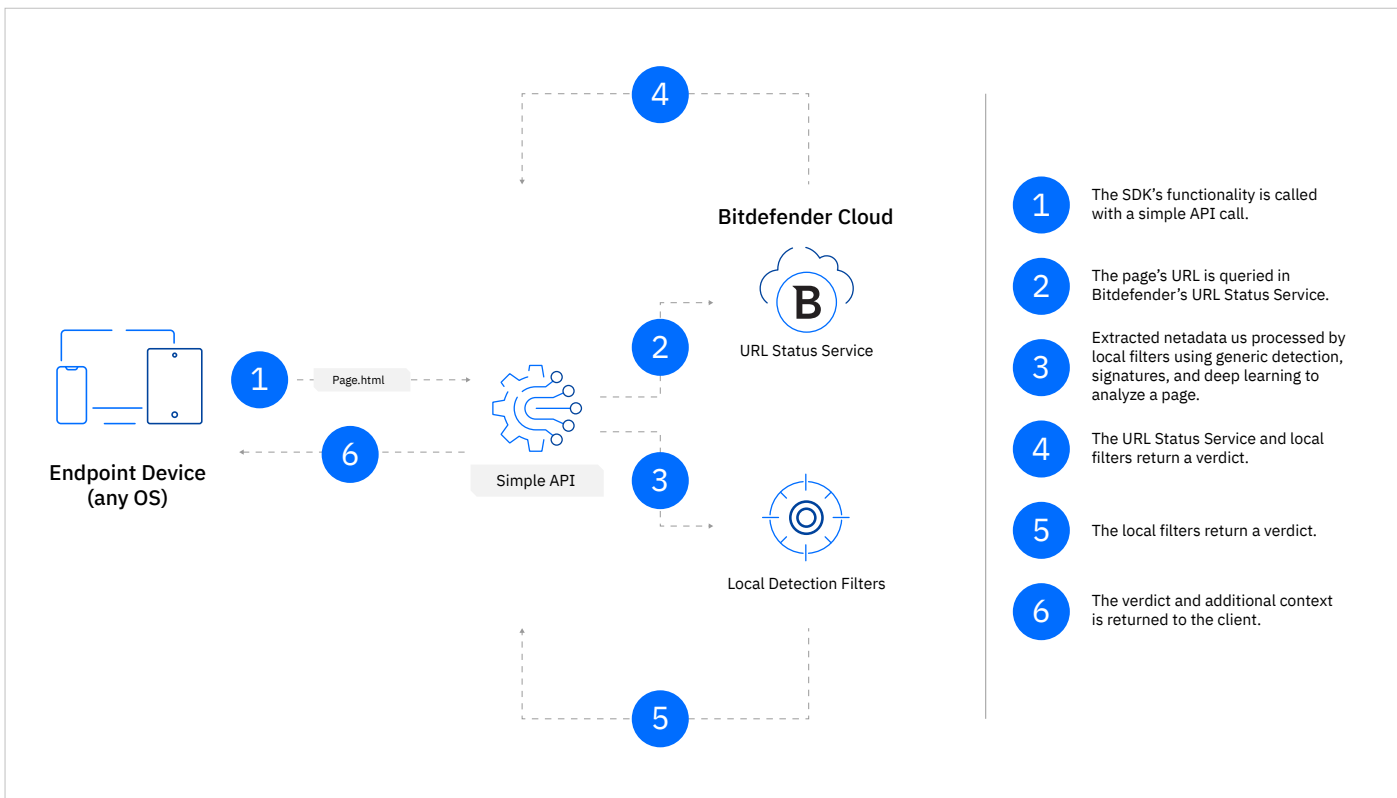
Key Benefits

- ↳ **Proven Effectiveness:**
The technology powering this SDK is used extensively in Bitdefender products and licensed by dozens of partners.
- ↳ **Small footprint:**
The local component of the SDK only needs a few megabytes of memory.
- ↳ **Quick Verdicts:**
The SDK is partially cloud based, reducing the local database size and providing a verdict in milliseconds.
- ↳ **Easy to integrate:**
The SDK comes with comprehensive documentation, code samples, and tech support from an experienced team.

How The Online Threats SDK Works

The SDK's functionality is available to partners via a simple API, compatible with multiple operating systems. To trigger a scan, partners need to provide HTML content stripped of any encodings, either from memory, a file location on disk, or a URL.

Once a scan is triggered, the SDK queries our URL Status Service to see if the page's URL is known to be malicious. On top of that, it extracts data from the HTML page and sends it through a battery of local filters built on proprietary fingerprinting technology. These filters use generic detection, signatures, and deep learning to analyze a page and return a verdict with additional context.



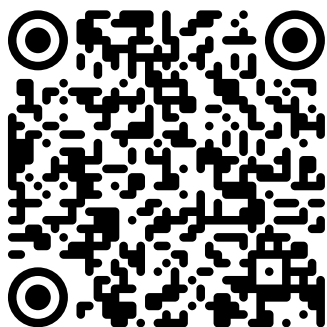
FREE Evaluation

Evaluating the Bitdefender Online Threats SDK is free of charge and includes technical support.

Contact us

For more information regarding the Online Threats SDK please reach us at:

<https://www.bitdefender.com/oem/contact-us.html>



Bitdefender is a cybersecurity leader delivering best-in-class threat prevention, detection, and response solutions worldwide. Guardian over millions of consumer, business, and government environments, Bitdefender is one of the industry's most trusted experts for eliminating threats, protecting privacy and data, and enabling cyber resilience. With deep investments in research and development, Bitdefender Labs discovers over 400 new threats each minute and validates around 40 billion daily threat queries. The company has pioneered breakthrough innovations in antimalware, IoT security, behavioral analytics, and artificial intelligence, and its technology is licensed by more than 150 of the world's most recognized technology brands. Launched in 2001, Bitdefender has customers in 170+ countries with offices around the world.

For more information, visit <https://www.bitdefender.com>

All Rights Reserved. © 2025 Bitdefender.

All trademarks, trade names, and products referenced herein are the property of their respective owners.

Romania HQ

Orhideea Towers
15A Orhideeor Road,
6th District,
Bucharest 060071

T: +40 21 4412452

US HQ

6301 NW 5th Way,
#4300,
Fort Lauderdale,
FL, 33309

T: +1 954-776-6262