

Reputation Threat Intelligence Feeds & Services

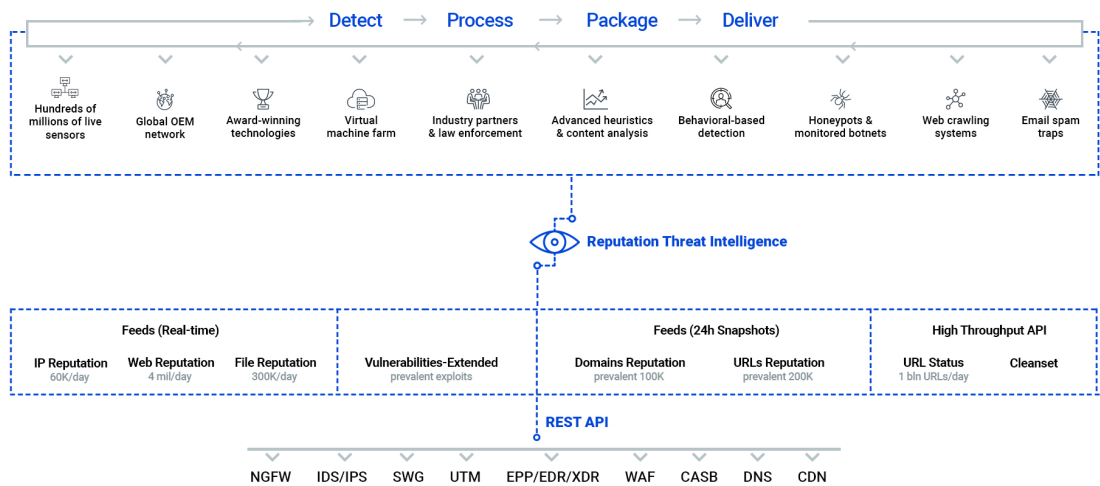
Real-time, highly curated threat data for security solution vendors

Reputation Threat Intelligence, also named tactical, technical or operational TI, is a continuous stream of indicators (IPs, URLs or file hashes) used mostly for machine-to-machine detection and blocking of cyber threats.

Bitdefender Reputation Threat Intelligence enables security solution vendors, enterprises and other organizations to augment their detection and filtering efficacy and enhance their solutions by using large quantities of updated IoCs delivered in real time.

In the current information-based economy, it's increasingly valuable to quickly and automatically ingest as many validated IoCs as possible, to be able to defend against new emerging perils at multiple levels, even before fully understanding their severity or prevalence, relying on the breadth of visibility and expertise of established players in the market such as Bitdefender.

Bitdefender Reputation Threat Intelligence Feeds and Services provide actionable IoCs such as malicious domains, file hashes and IP addresses collected from a wide variety of proprietary and partnership sources, delivered quickly with a minimum of context to help prioritization.



Key Benefits:

- Delivers real-time, high-quality threat information from a diversity of sources such as Bitdefender’s network of hundreds of millions of endpoints, deep web monitoring, web crawling systems, sandbox analyzer services, advanced heuristic and content analyzers, email spam traps, honeypots and monitored botnets, as well as industry and OEM partners.
- Covers a wide area of IoCs, including all typology of malicious domains, IPs, URLs and filehashes (such as Malware, Phishing, Fraud, Spam, PUA, unwanted). The data is automatically curated to remove duplicate entries, categorize threats, reduce false positives, update reputation and add useful context. Super vised automated processes ensure the data is accurate and actionable.
- Seemingly integrates into any platform or infrastructure in minutes. The platform-agnostic approach is compatible with M2M (machine-to-machine) systems familiar with consuming RESTful APIs delivering structured formats, packed using wire-efficient compression and delivered real-time in a stream-like manner.

Bitdefender Reputation Threat Intelligence portfolio consists of Feeds and API query services:

Feeds	APIs
Web Reputation (real-time)	URL Status
File Reputation (real-time)	Cleanset
IP Reputation (real-time)	
Domains-Reputation (24h snapshot)	
URLs-Reputation (24h snapshot)	
Vulnerabilities-Extended (6h snapshot)	

Reputation Threat Intelligence Feeds

Dedicated for prevention and detection use cases, the feeds contain real-time updated IoC, with a low rate of false positives.

Backend Systems for XDR/EDR/EPP, NGFW, UTM, WAF, DNS Security, IDS/IPS, CDN and CASB integrate threat MRTI (machine readable threat intelligence) feeds to administer dynamic blacklists/whitelists of IoC, effectively stopping the propagation of new malware strains and increasing their effectiveness against new strains ("known unknown" malware that was already detected).

Bitdefender Reputation Threat Intelligence feeds contain large quantities of highly accurate (low FPs) threat data and are delivered in real time, in a simplified format to allow rapid, precise and convenient ingestion into the customer's security systems.

Features

- Contains malware domains, IP addresses, URLs and file hashes seen in the live sensors.
- The information is presented in JSONL format, prepared for MRTI integration scenarios, and it contains an unlimited quantity of records.
- Update in real-time with new entries are permanently added.
- Large quantities of indicators, typical quantities are 150,000-200,000 entries per hour (3.6 million-4.8 million per day).
- Each indicator in the feed is reported in a maximum 5 minutes from the moment of detection.
- Data stays available for the last 7 days, for convenience. It can be read in multiple calls of intervals of a maximum of 1 hour (because of the quantity of data).

Benefits

- Easy to access and consume, token-based authentication, data delivered via a typical REST API.
- The interrogation API offers 2 parameters from and to, allowing a custom read of the data, from 7 days ago, up to the present moment, with 1s resolution.
- Delivered as deltas, to simplify processing of the consumer.
- Gzip-compressed by default, reducing the data transfer needed to 1/4 of the original.

Threat Intelligence Services

Bitdefender Reputation Threat Intelligence cloud services are low-latency, high-throughput, distributed query services that can cope with large quantities of concurrent requests to respond to multiple end-users around the globe.

The services are customized for multiple automated use-cases where there is a need to quickly and reliably verify the reputation of customers' IoCs with an external reputation provider.

In addition to the Reputation Threat Intelligence Feeds and Services, Bitdefender delivers first-hand Advanced Threat Intelligence to businesses and SOC (Security Operations Centers) via integration with third-party reputable TIPs (threat intelligence platforms). Bitdefender Labs correlate hundreds of thousands of selected Indicators of Compromise (IoCs) and turn them into actionable, real-time insights into the latest threats. For more information check [Advanced Threat Intelligence datasheet](#).

FREE evaluation

Evaluating the Bitdefender Reputation Threat Intelligence Feeds & Services is free of charge and includes technical support.

Contact us

For more information 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 hundreds of millions of 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