OEM Datasheet

Bitdefender
BUILT FOR RESILIENCE

Reputation Threat Intelligence Feeds & Services

IP Reputation Feed

The IP Reputation Feed, part of the Bitdefender Reputation Threat Intelligence Feeds & Services portfolio, delivers stream-like MRTI (machine-readable threat intelligence) on malicious IPs detected by live sensors. As the data in the feed is updated permanently, security solutions such as NGFW, SWG, WAF, CASB, DNS filters, EDR/EPP Backends, UTM, IDS/IPS and IOT management use it to increase detection and filtering efficacy.

Bitdefender, a global security solutions provider with hundreds of millions of sensors covering B2B, B2C and the OEM ecosystem, can capture emerging threats in real time and further share the intelligence with partners to increase the defender's capabilities.

Features

Furthermore, Bitdefender IP Reputation Feed includes a set of key information for each IoC delivered, enabling customers to effectively parse the data, classify and prioritize it based on customized criteria in order to narrow down the relevant data for the business.

- **Tags** - contains indications regarding the type of threat or particularity of the attacks exposed by the respective IP
- **Severity and Confidence** - for assessing the level of threats and confidence of the verdict, useful for filtering
- **Ports and Protocols** - further disseminate what ports and protocols are used from the respective IP in its malicious activity
- **Countries** - contain up to 5 countries, associated with the IP, useful for country-level rules
- **Domains** - domains resolving to the IP, 5 of the most recent ones
- **Popularity** - has values from 1 to 5 (5 being the most popular). Useful for showcasing the prevalence of attacks that can influence the priority of counter-rules at customers
- **First_seen, timestamp, and TTL** - fix the temporal activity of the malware and advise for how long to consider this detection.
- If the popularity of an IP changes an additional updated record is sent

At-a-Glance

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.

The data is delivered in real time, enabling customers to increase detection and filtering efficacy and enhance their solutions by using large quantities of updated IoCs.

Key Benefits

- Large quantities of indicators, typically 2,000-3,000 entries/hour (48,000-72,000/day)
- Update in real time, new entries are permanently added
- Each indicator reported in a maximum of 5 minutes from the moment of the detection
- Data available for the last 7 days, accessible in multiple calls at convenient intervals
- The information is presented in JSONL format, prepared for MRTI (Machine Readable Threat Intelligence) integration scenarios, and contains an unlimited quantity of records

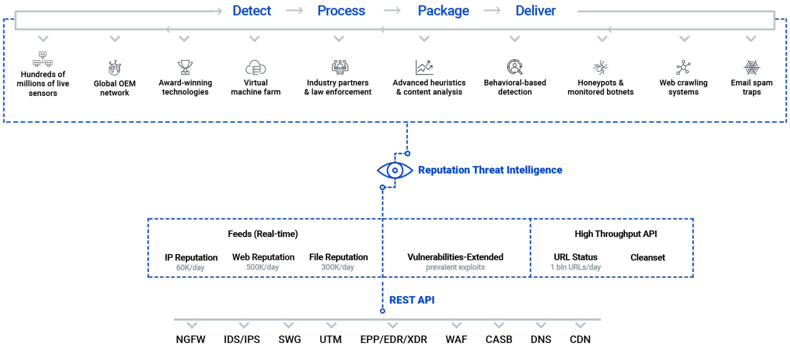
Reputation Threat Intelligence Feeds

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.

In addition to the Reputation Threat Intelligence Feeds and Services, Bitdefender delivers first-hand Operational and Tactical Threat Intelligence to organizations and SOCs (Security Operations Centers) via integration with third-party reputable TIPs (threat intelligence platforms), SIEMS and SOARs. 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 regarding the Reputation Threat Intelligence Feeds & Services please reach us at www.bitdefender.com/oem

Bitdefender
BUILT FOR RESILIENCE

3945 Freedom Circle
Ste 500, Santa Clara
California, 95054, USA

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.