Bitdefender

DATASHEET

Bitdefender Threat Intelligence IP Reputation Feed

Threat actors can hijack, use, and ditch IP addresses in a matter of hours. IP filtering systems need real-time information to keep up with an attacker's infrastructure, which is why Bitdefender's IP Reputation Feed delivers addresses in under 5 minutes from when they're first seen by our sensors.

The feed delivers this data via stream-like MRTI (machine-readable threat intelligence). Any security solution that filters traffic based on IP address can use it to expand visibility, and stop incoming attacks.

Bitdefender's intelligence is pulled from hundreds of millions of sensors covering the B2B, B2C and OEM ecosystems. That's why the IP Reputation Feed can deliver large quantities of indicators extracted in real time, usually between **80,000-100,000 per day**.

Features

- **IP Reputation:** The feed contains IP addresses associated with malicious activity, both IPv4 and IPv6. The indicators include TTLs, first and last seen dates, as well as confidence and severity scoring.
- **Real-time data:** IP addresses we see in the wild make their way to the IP reputation feed in under 5 minutes.
- **Added context:** Indicators are delivered alongside useful context, such as what ports and protocols are used, countries associated with the IP, domains resolving from the IP, popularity score, and more.
- **Flexible format:** The information is presented in JSONL format, prepared for machine-readable integration scenarios.
- **Large quantities of validated indicators:** The feed usually delivers between 80,000 to 100,000 indicators per day.

Reputation Threat Intelligence Feeds

Bitdefender's IP Reputation feed includes valuable information about each indicator. These include:

- Tags – indications regarding the type of threat or particularity of the attacks exposed by an IP address.
- Severity and Confidence scores - 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 by the respective IP.
- Countries - contains 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 score - useful for showcasing the prevalence of attacks that can influence the priority of counter-rules.

At-A-Glance

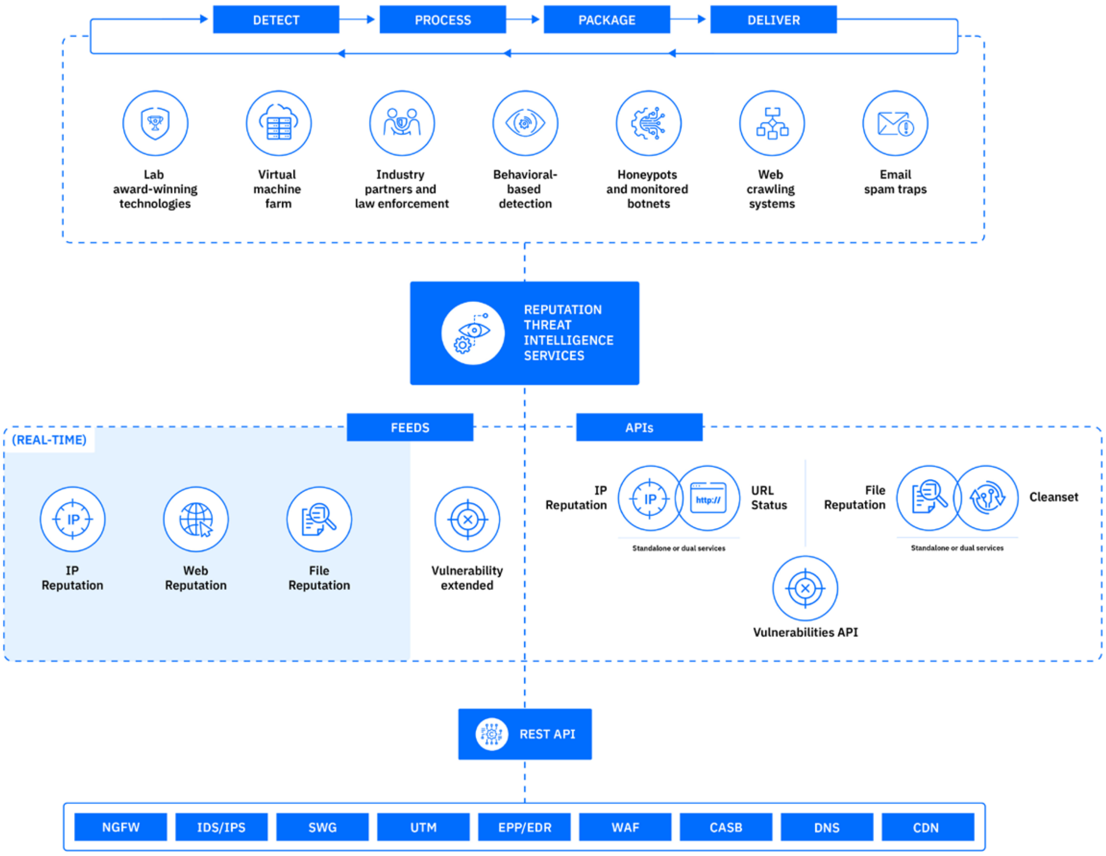
Bitdefender's IP Reputation feed draws on global telemetry to deliver real-time intelligence on large quantities of malicious IP addresses. All IoCs come with actionable threat context, and they take less than 5 minutes to get from detection to inclusion in the feed.

Benefits

- **Large quantities and fast delivery:** The IP Reputation feed delivers 80,000-100,000 indicators per day, which are processed in less than 5 minutes from detection.
- **Actionable threat context:** Indicators are delivered alongside threat context that enables better filtering, country-level rules, alert triage, and more.
- **Guaranteed interoperability:** The feeds can be consumed in Bitdefender's proprietary JSON format, and they're also available in TI platforms, or Bitdefender's TI Portal.
- **Unparalleled visibility:** Bitdefender's telemetry encompasses over 500 million worldwide sensors, offering unparalleled visibility into malicious IP addresses.

- First_seen, timestamp, and TTL – help fix the temporal activity of malicious activity and advise for how long to consider this detection.

Bitdefender Reputation Threat Intelligence Feeds and Services provide actionable indicators such as malicious IP addresses, domains, file hashes and URLs. The IP Reputation feed can be complemented by other feeds and services, to further augment detection and prevention.



FREE evaluation

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

Contact us

For more information regarding the Reputation Threat Intelligence Services visit our website: bitdefender.com/oem/threat-intelligence-feeds-services.html or reach us at:

Bitdefender is a global cybersecurity leader protecting over 500 million systems in more than 150 countries. Since 2001, Bitdefender innovation has consistently delivered award-winning security products and threat intelligence for the smart connected home, mobile users, modern businesses and their networks, devices, data centers and Cloud infrastructure. Today, Bitdefender is also the provider of choice, embedded in over 38% of the world's security solutions. Recognized by industry, respected by vendors and evangelized by customers, Bitdefender is the cybersecurity company you can trust and rely on.