Bitdefender

DATASHEET

IP Blocklist

Automated Prevention and Detection

Automated blocklists don't need a high volume of indicators. They need vetted, high-confidence IoCs. Otherwise, false positives can interrupt crucial workflows.

That's why Bitdefender built the IP Blocklist. It's based on a large dataset of malicious IPs, but filtered to only include indicators with a high IP reputation score. These indicators:

- Pose a severe risk to your attack surface
- Have a high confidence score attributed by our Labs team
- Are popular – they show up in recent attacks
- Have additional threat context that informs indicator relevance (whether it's an indirect verdict, from a cloud provider, honeypot, etc)

The IP Blocklist can be integrated with a few simple API calls, and it's useful for any automated filtering use case. It can improve the efficiency of NGFWs, UTMs, routers, and more appliances sitting at the edge of your network.

Features

- **Active IoCs only**: The feed only includes popular IP addresses associated with critical threats.
- **Exclusion of low-risk activity**: Only IPs connected with spam, phishing or fraud activity are filtered.
- **Flexible format**: The information is presented in JSONL format or CSV, prepared for machine-readable integration scenarios.
- **Customizable feed**: By default, only IPs with a minimum IP reputation score of 50 (out of 100) are included. However, partners can change the value for this parameter and the type of threat context they want to see in responses from Bitdefender.

Threat Intelligence APIs

Bitdefender's IP Blocklist returns actionable information on known malicious IP addresses, including:

- **Tags –** indications regarding the type of threat or particularity of the attacks exposed by an IP address. These tags include "Access Attempt," "Crawler" "Command Injection," and more.

At-A-Glance

Bitdefender's IP Blocklist draws on global telemetry to deliver real-time intelligence on indicators queried by partners. All queries return IoCs with high confidence scores, minimizing false positives and improving automated blocklists.

Benefits

- **Quantity and quality:** The IP Blocklist is built by processing 80,000-100,000 indicators per day. Malicious IPs make their way to our datasets n less than 5 minutes from detection, but only high-confidence, active indicators are further disseminated in the IP Blocklist.
- **Optimized for blocklist:** API calls return high-confidence IoCs, making it perfect for automated detection and prevention use cases.
- **Easy Integration:** The REST API service is easy to query, simplifying integration of the IP Blocklist into your workflows.
- **Unparalleled visibility:** Bitdefender's telemetry encompasses over 500 million worldwide sensors, offering unparalleled visibility into malicious IP addresses.

- **Severity, Confidence and IP reputation scores –** for assessing the level of threats, the confidence of the verdict, and popularity of the indicator. The IP Reputation Score can also be used for automated filtering.

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

Here's what a JSON response from the IP Blocklist will look like:

```
ip, tags, confidence, severity, ip_reputation_score
165.154.120.89, "['Scanner', 'InvalidFileAccess', 'Phishing']"'Phishing' ]",99,99,89
101.36.108.158, "['Scanner', 'InvalidFileAccess']",99,99,89
152.32.132.203, "['Scanner', 'InvalidFileAccess', 'Phishing']"'Phishing']",99,99,89
185.97.113.40, "['CommandInjection', "AccessAttempt', 'Phishing']", 99,99, 89
162.219.216.183, "['AccessAttempt', 'Phishing']", 99,99,89
165.154.206.223, "['Scanner', 'CommandInjection', 'InvalidFileAccess', 'Phishing']"
89.248.163.217, ['Scanner' ],99,99,89
```

Partners can customize responses to only include:

- The raw IP addresses, with no additional context
- Indicators along with tags.
- Indicators along with tags and reputation scores, as seen in the screenshot above.

FREE evaluation

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

Contact us

For more information on Bitdefender Threat Intelligence Services visit our website: bitdefender.com/oem/threat-intelligence-feeds-services.html or reach us at: https://www.bitdefender.com/oem/contact-us.html

17122025: Bitdefender-OEM-IPBlocklist-datasheet-brand300-en_EN