Bitdefender

DATASHEET

# Bitdefender File Feed

Bitdefender's award-winning anti-malware solutions act as a global network of over 500 million malicious file sensors. That's how Bitdefender captures the malicious files used by threat actors in real time.

This intelligence is available to SOCs, and other security teams that need reliable context on the artefacts they notice in their infrastructure. With the Bitdefender File Feed, the malicious files detected on real-life endpoints are delivered in under 5 minutes from detection.

## Features

- **File Reputation:** Ingest file hashes associated with malicious content recently observed in the wild.
- **Indicator metadata:** Bitdefender attributes multiple scores to malicious files. These include severity, confidence, and popularity, to help triage alerts, inform investigations, and threat hunting exercises.
- **Actionable context:** When available, indicators are delivered alongside crucial threat context, including the type of threat, or related indicators.
- **Real-time data:** Malicious artefacts we identify in our telemetry are processed by Bitdefender Labs and included in the File Reputation feed in under 5 minutes.
- **Customizable feed:** Partners can customize queries to the file feed, for example, to only include high confidence indicators. Responses can also be adjusted based on time stamp, file format, and partners can choose to exclude related indicators, revoked entries, or suspicious files.

## At-A-Glance

Bitdefender File Feed is a continuously updated feed that delivers newly identified malicious or suspicious file hashes, along with a risk assessment, detection timestamps, and the regions where they were observed.

## Benefits

- **Easy to customize:** Security professionals can filter data from the File Feed to only ingest relevant addresses, based on their confidence, timestamp, file format, and whether the entry was revoked, or labeled as suspicious.
- **Actionable threat context:** Indicators are delivered alongside threat context unique to Bitdefender, such as threat types, related indicators to malicious files, and more.
- **Interoperability:** The feeds can be consumed in Bitdefender's proprietary JSONL format or ingested from third-party TI platforms like Splunk.
- **Real-world visibility:** Bitdefender's telemetry encompasses over 500 million worldwide sensors, offering visibility into malicious file hashes observed in the wild, based on real endpoint activity rather than synthetic data.

Bitdefender

DATASHEET

# Bitdefender File Feed Overview

Bitdefender File Feed delivers high quantities of malicious hashes in a customizable JSON format. Entries include:

| | |
|---|---|
| **Indicator metadata** | ↳ severity (risk level)<br>↳ confidence (certainty of classification)<br>↳ popularity (prevalence of the file)<br>↳ file_format (e.g., “Windows executable”, “Document / JSON”)<br>↳ file_size<br>↳ file_names (when available) |
| **Threat context (when available)** | ↳ threat_label (for example: “Gen:Variant.Application.HackTool.96”)<br>↳ threat_type (for example: “passwordstealer”)<br>↳ threat_family (for example: “lummastealer”)<br>↳ mitre_attack (list of MITRE techniques associated with the file)<br>↳ exploited_vulnerabilities (list of exploited vulnerabilities)<br>↳ suspicious_entry (only included when the event is flagged as suspicious)<br>↳ affected_countries<br>↳ affected_industries<br>↳ tags (optional tags, like “OSINT”) |
| **Telemetry timestamps and indicator lifecycle** | ↳ first_seen<br>↳ timestamp (most recent sighting)<br>↳ TTL (time-to-live of the indicator) |
| **Related indicators (when available)** | related_indicators, including their:<br>↳ type (example – file, ipv4)<br>↳ relationship (example file_modifies_file<br>↳ last_seen<br>↳ SHA1, SHA256, MD5 hash of the file<br>↳ tags specific to indicator type |
| **Similar Files** | ↳ sha256 (hash of the similar file)<br>↳ tlsh (hash to measure similarity)<br>↳ distance (TLSH distance or a similar metric)<br>↳ percentage_similarity |

The feed can be consumed via simple API calls, with data delivered in a structured JSONL format. To support broader interoperability, Bitdefender provides translation scripts for commonly used formats such as STIX and MISP. The web feed is also available in third-party TI management solutions, like Splunk, OpenCTI, and more.

## FREE evaluation

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

## Contact us

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



11022026-Bitdefender-OEM-FileFeed-datasheet-brand319-en_EN