Bitdefender

DATASHEET

Reputation Threat Intelligence Services

File Reputation API

Part of the Bitdefender Reputation Threat Intelligence Services portfolio, File Reputation API allows the submission of file-hashes to obtain reputation details for these files, where available. It is meant to be called by all customers in machine-to-machine (M2M) use cases to check in real time if some file-hashes are flagged for malicious activities and need further blocking actions.

Bitdefender, a global leader in security solutions, operates an extensive sensor network comprising hundreds of millions of units across B2B, B2C, and the OEM ecosystem. This wide-reaching network enables Bitdefender to swiftly detect emerging threats in real-time and share this intelligence with partners, bolstering defenders' capabilities against potential security risks.

Features

- ↳ A File Reputation API request returns a verdict, whether malicious or unknown. If the file is malicious and known to Bitdefender, the API will also provide additional details such as threat family, time and date of first encounter, and many more.
- ↳ The API supports several file-hash formats, including SHA256, SHA1, and MD5.
- ↳ The information is presented in JSONL format.
- ↳ The abstract database is updated in real-time, new entries are permanently added, and existing entries and their time-to-live are updated permanently, based on the information of the last known malicious activity.
- ↳ The database contains millions of active malicious file-hashes. These file-hashes are constantly updated to track the evolving patterns of malicious activity carried out by attackers.
- ↳ It provides vetted information, used also in a variety of Bitdefender and partner products.
- ↳ Works seamlessly together with the File Reputation Feed, to cover both surveillance of the file-hashes of interest and what is new from Bitdefender.

At-a-Glance

The File Reputation API is a cloud-based service that allows submissions of file-hashes and responds with their status: either malicious or unknown. If the file is malicious the reply will confirm its status and provide additional threat context

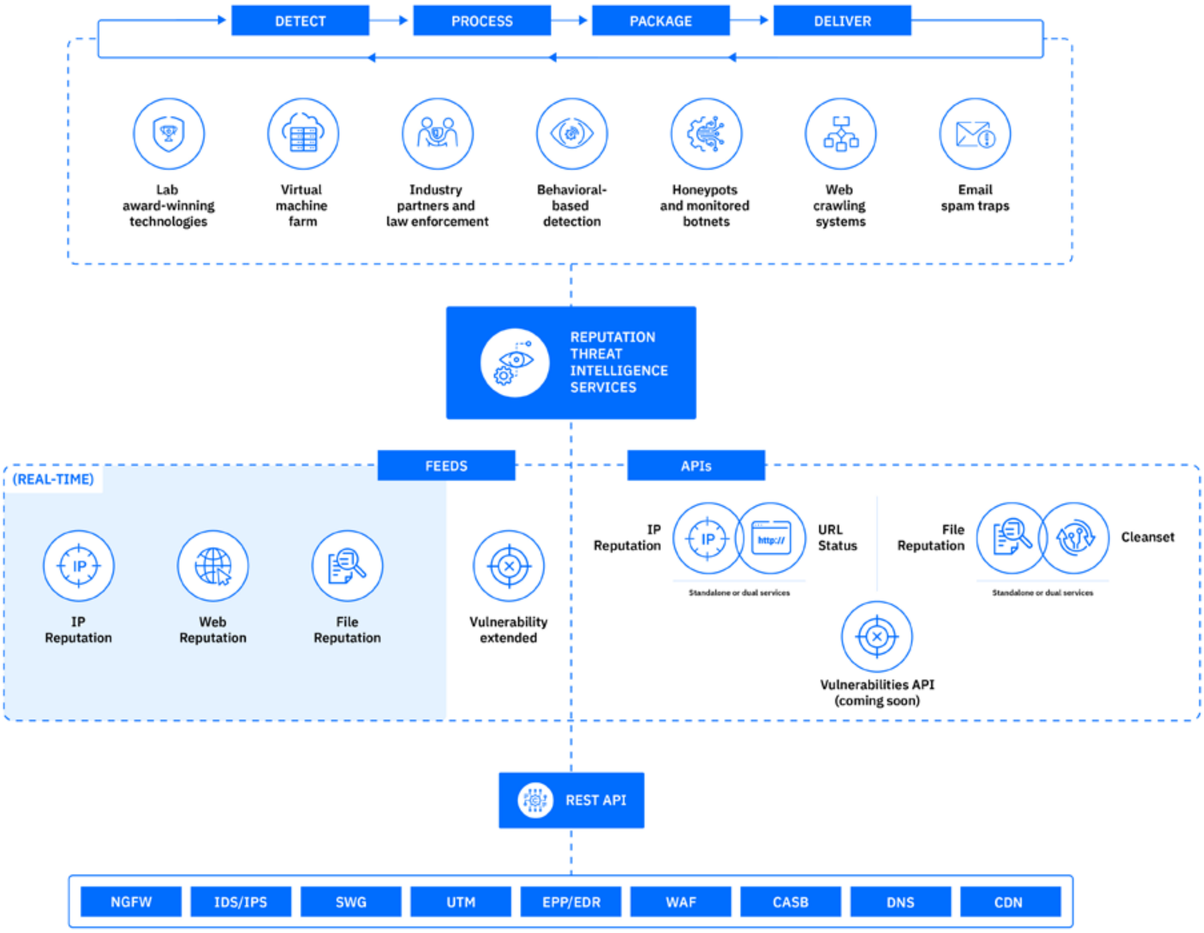
Key Benefits

- ↳ **Rapid Threat Detection:** enables rapid detection of known malicious file-hashes allowing for timely response and mitigation.
- ↳ **Automated Security Operations:** enables automation of security operations, such as scanning files for known threats during file uploads or downloads. This reduces the burden on security teams and helps streamline incident response processes.
- ↳ **Enhanced Incident Response:** When a security incident occurs, it provides valuable context about known malicious files involved in the attack. This information enables security teams to respond effectively by identifying compromised systems, containing the threat, and restoring operations.
- ↳ **Proactive Defense:** By regularly querying File Reputation API, organizations can proactively identify and mitigate potential threats before they cause harm. This proactive approach helps prevent security incidents and reduces the likelihood of successful cyberattacks.

Reputation Threat Intelligence APIs

Bitdefender Reputation Threat Intelligence APIs are cloud-based services featuring distributed query services with low-latency and high throughput capabilities. These services are designed to efficiently handle a significant volume of simultaneous requests, catering to various consumers across the globe. They are well-suited for numerous automated use-cases where a swift and dependable assessment of the reputation of customers' IoC is essential.

Reputation Threat Intelligence APIs are part of the broader Bitdefender Threat Intelligence Services portfolio.



FREE evaluation

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

Contact us

For more information regarding the Reputation Threat Intelligence Services please reach us at https://www.bitdefender.com/oem/contact-us.html