

Reputation Threat Intelligence Services

Vulnerabilities API

Part of the Bitdefender Reputation Threat Intelligence Services portfolio, Vulnerabilities API lets partners submit a CVE, CVSS, Product, or Vendor to query vulnerabilities and their associated IoCs. API calls return information about known vulnerabilities, emerging vulnerabilities discovered in real time by our sensors, and threat context pulled from Bitdefender's telemetry, such as CVEs currently being exploited or what vulnerabilities are being used by threat actors.

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 lets us mix OSINT data about vulnerabilities with context from live systems and deliver unique insights to partners that want to understand their threat surface, configure systems, manage patches, or harden security in any other way.

Features

- ↳ Easy to access and consume, token-based authentication, data delivered via a typical REST API.
- ↳ Rich, actionable context that enables quick risk assessment and mitigation.
- ↳ The abstract database is updated every 6 hours, new entries are added all the time, and existing entries are updated continuously.
- ↳ Every vulnerability comes with CPE qualifiers to optimize configuration management.

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 automated and manual use-cases where a swift and dependable assessment of threats or vulnerabilities is essential.

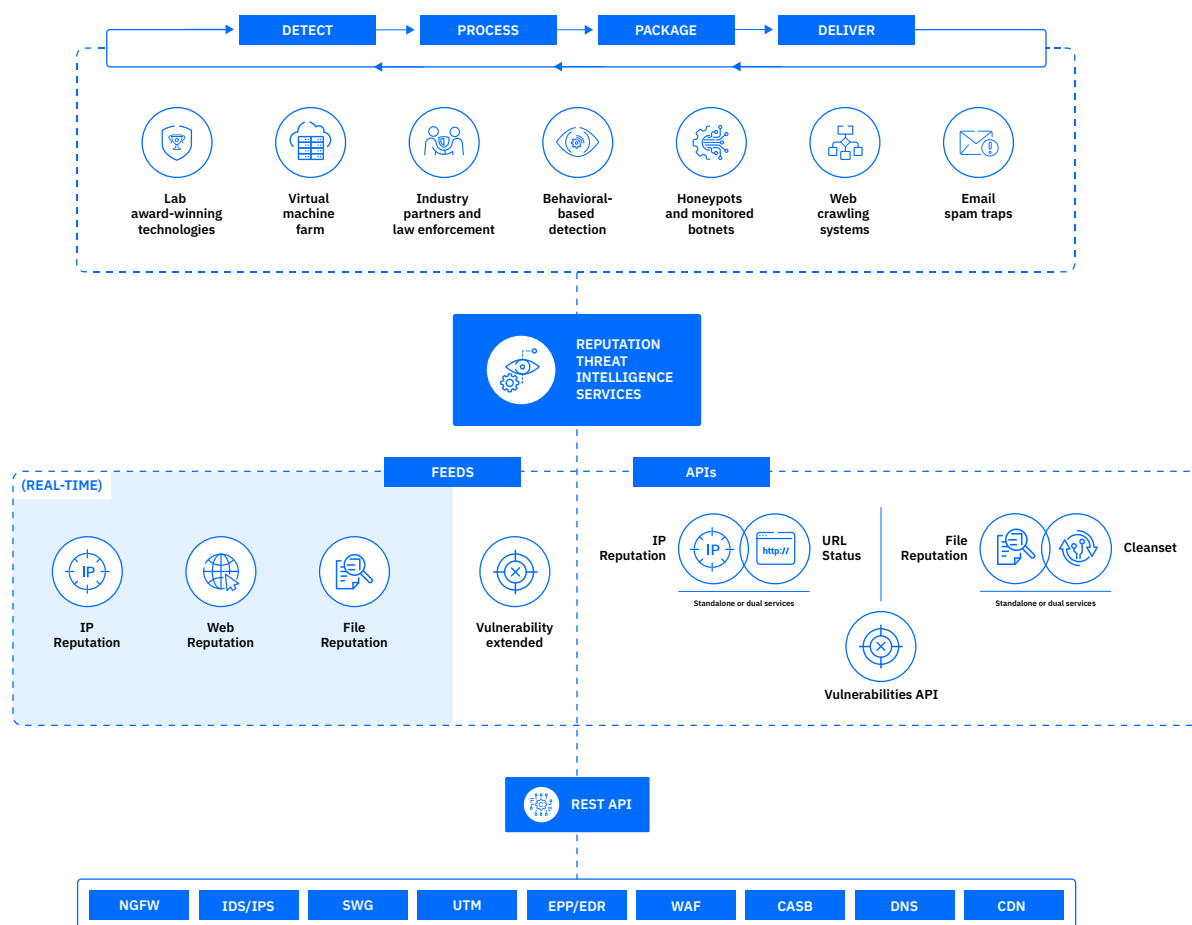
Reputation Threat Intelligence APIs are part of the broader Bitdefender Threat Intelligence Services portfolio.

At-a-Glance

The Vulnerabilities API is a cloud-based service that can be queried about products, vendors or CVEs and returns information on known or emerging vulnerabilities. These are packaged with actionable context from Bitdefender's telemetry, enabling quick patching, configuration management, automated filtering, and other security hardening tasks.

Key Benefits

- ↳ **Threat Context in Real Time:** Acquire intelligence on emerging vulnerabilities to expedite incident response and patching.
- ↳ **Automated Security Operations:** The service enables automation of security operations, such as service configuration, compliance management or patching. This reduces the burden on security teams and helps streamline investigations.
- ↳ **Actionable IoCs:** The API provides actionable IoCs for all queries, like file hashes, known weaknesses and CVSS scores.
- ↳ **Easy Integration:** The service is a straightforward API, returning information in JSON format, making it easy to integrate into any SIEM or SOAR.



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 visit our website: bitdefender.com/oem/threat-intelligence-feeds-services.html or reach us at:

