Bitdefender

All Rights Reserved. © 2023 Bitdefender. All trademarks, trade names, and products referenced herein are the property of their respective owners.

DATASHEET

Mar 2023

Bitdefender Operational Threat Intelligence

Contextual, Real-Life Insights into the Global Threat Landscape

Security professionals need to protect their business assets from known and emerging cyberattacks. Relying mostly on internal telemetry that has limited value, makes it difficult to understand the impact of prevalent cyber-threats. This translates into a limited capability to detect and mitigate threats that have bypassed the prevention layers and to reduce their business impact.

While organizations struggle with limited capabilities, threat actors become more and more knowledgeable, constantly improving their tools and methods, which makes it even more difficult to stay on top of evolving threats.

In many situations, Bitdefender is at the forefront of such threats by collecting and curating anonymized telemetry from millions of sensors around the globe, from its product presence in B2B, B2C and OEM, as well as other sources such as honeypots, web scanning tools, dark web, work with law enforcement.

Bridging the Visibility Gap

Operational Threat Intelligence resolves a long-standing blind spot for security analysts, offering global visibility into unique, evasive malware, APTs, zero-days and C&Cs that are difficult to catch.

The Bitdefender Intelligence Portal allows quick access to the Threats Database. Additionally, the Intelligence feeds and services can be integrated in minutes in any platform or infrastructure.

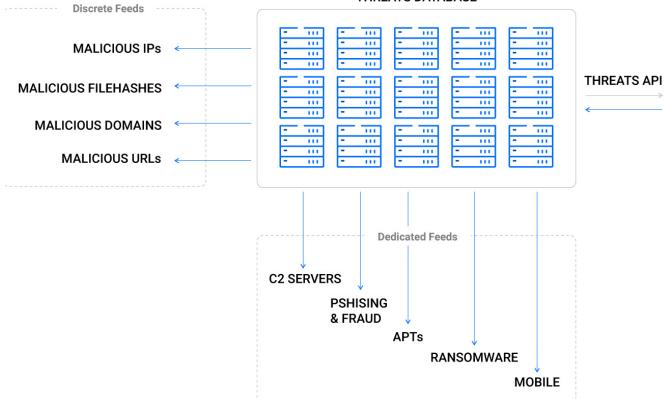
At-a-Glance

Bitdefender Operational Threat Intelligence enables security analysts to gain access to global threat information and better understand sophisticated attacks. The solution delivers current real-life threats and IoCs together with enriched context, supporting Threat Hunting, Incident Response and Forensic Analysis.

The threat information is enriched with Actor and Threat Family attribution, carefully following their activity across multiple geos and industries, extracting their TTPs and IoCs using a multitude of award-winning tools such as behavioral detection, Sandbox and machine learning. Furthermore, threats include scoring and confidence index.

Key Benefits

- → Extends visibility outside the customers' environment into the global threat landscape
- → Enables alert triage and increased security operations efficiency
- → Reduces the investigation and response time by providing the necessary context around threats to gain visibility and understanding of the root cause
- → Strengthens your customers' trust and helps you defend them against sophisticated attacks
- → Available through the user-friendly Bitdefender Intelligence Portal and alternatively as APIs /Feeds for automation
- → Feeds deliver novelties and updates of existing threats via multiple formats, STIX included



THREATS DATABASE

Bitdefender is a cybersecurity leader delivering best-in-class threat prevention, detection, and response solutions worldwide. Guardian over millions of consumer, business, and government environments, Bitdefender is one of the industry's most trusted experts for eliminating threats, protecting privacy and data, and enabling cyber resilience. With deep investments in research and development, Bitdefender Labs discovers over 400 new threats each minute and validates around 40 billion daily threat queries. The company has pioneered breakthrough innovations in antimalware, IoT security, behavioral analytics, and artificial intelligence, and its technology is licensed by more than 150 of the world's most recognized technology brands. Launched in 2001, Bitdefender has customers in 170+ countries with offices around the world.

Romania HQ Orhideea Towers 15A Orhideelor Road, 6th District, Bucharest 060071 T: +40 21 4412452 F: +40 21 4412453 US HQ 3945 Freedom Circle, Suite 500, Santa Clara, CA, 95054

bitdefender.com