ADVANCED THREAT INTELLIGENCE

Contextual insights into the global threat landscape

Bitdefender Advanced Threat Intelligence is an enterprise security service that enables Security Operations Centers (SOCs) to easily integrate **real-time threat knowledge** into their existing infrastructure and **better understand** sophisticated attacks. The solution delivers **up-to-date, contextual intelligence** on URLs, IPs, domains, certificates, files, Command and Control servers and Advanced Persistent Threats to Managed Security Service Providers (MSSPs), Managed Detection & Response (MDR) companies, IT security and investigation consultancies and large enterprises that need to block ingenious threats.

The solution, powered by a **massive install base**, helps partners maintain **global balance** and capture the threat landscape inside and **outside the United States**, with Indicators of Compromise (IoCs) that cover both English-speaking and non-English sources.

> "By 2022, 20% of large enterprises will use commercial threat intelligence (TI) services to inform their security strategies, which is an increase from fewer than 10% today."
>
> *Gartner Market Guide for Security Threat Intelligence Products and Services*,
> Craig Lawson, Ryan Benson, Ruggero Contu,
> 19 February 2019

Cyber-Threat Intelligence Labs Expertise

Sophisticated threats are among the main concerns of enterprises today. As **environments grow more complex**, malware actors find innovative ways to infiltrate overlooked entry points in the network, hiding behind the scenes to wreak havoc without making a full-blown appearance. **Advanced Threat Intelligence** solves security operations challenges by providing extensively curated insights on complex cyber-threats.

Bitdefender Cyber-Threat Intelligence Labs analyze and block more than **half a million IoCs daily** with multiple technologies, including a virtual machine farm that **executes hundreds of thousands of malware samples** and collects **URL information** on the websites cyber-criminals leverage to download or upload malicious components.

This living database of knowledge lets Security Operations Centers **understand sophisticated threats** such as zero-day and evasive malware, block them before they even make an impact, and accelerate **incident response and forensics**.

Accurate Indicators of Compromise

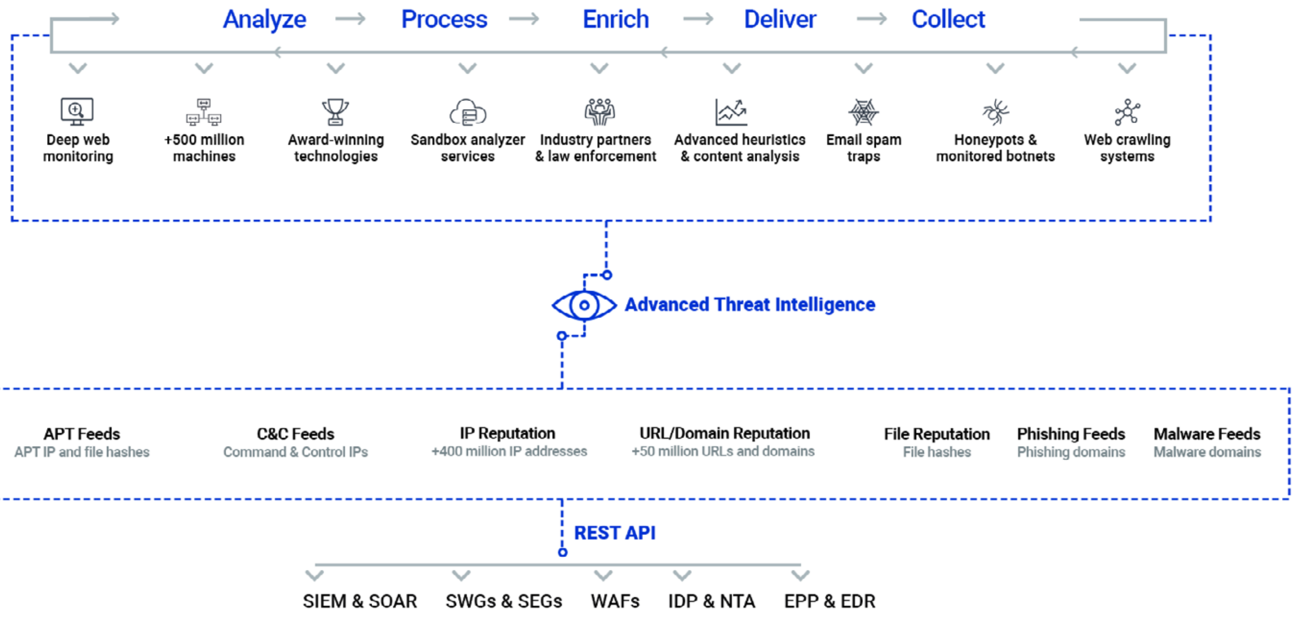
The Bitdefender engines are based on a **combination of extensive knowledge repositories**, open sources, email spam traps, honeypots, botnet monitoring, extensive collaboration with industry partners and law enforcement agencies, and other, more unconventional, sources. Our Labs continuously collect and analyze intelligence from the **dark web**, with **6.5 million onions** (including duplicates) seen by our servers, as well as **7 million onion visits**.

To keep threat intelligence **up to date**, our Labs use cross-analysis techniques and **clean up data daily**, turning large volumes of information into meaningful insights. Sources include:

- The entire Bitdefender technology stack: award-winning anti-spam, anti-phishing and anti-fraud technologies, Sandbox Analyzer, Network Traffic Security Analytics, etc.
- IoCs identified and processed by Bitdefender's global install base
- Web crawling systems
- Email traps, honeypots and data from monitored botnets
- Advanced heuristics techniques and content analysis
- Internal virtual machine farm that executes more than 200,000 malware samples per day
- Data shared with industry partnerships and law enforcement agencies

Advanced Threat Intelligence Architecture

Advanced Threat Intelligence resolves a long-standing blind spot for SOC managers and analysts, offering global insight into unique, evasive malware, APTs, zero-days and C&Cs that are hard to catch, and it does so in a platform-agnostic format compatible with any SIEM familiar with consuming a REST API. The service can be integrated in minutes on any platform or infrastructure.



Key Benefits

- Improves decision-making with accurate, real-time data on IPs, URLs, domains, files, APTs, C&C servers and more
- Accelerates incident response and forensic capabilities to mitigate the latest sophisticated threats
- Strengthens your customers' trust and helps you defend them against attacks before they wreak havoc
- Detects targeted, evasive and zero-days attacks across the world
- Augments your security capabilities with the expertise of Bitdefender Labs, a global R&D leader in cyber-security tests
- Decreases time-to-value by seamlessly integrating into your existing architecture

Key Features

Reputation Services

Advanced Threat Intelligence lets security analysts easily detect and understand malicious, phishing or fraudulent URLs and domains, IPs, files and file certificates. It captures the entire Bitdefender technology stack and turns Indicators of Compromise into actionable data. Insights into the latest threats include information on the threat name as recognized by the security industry, family, type and version (e.g. trojan, APT).

Unique, Curated Feeds

Bitdefender offers insights into hard-to-catch Advanced Persistent Threats and Command & Control servers, including their IPs, domains, and files. It enables Security Operations Centers to detect and block sophisticated attacks and reduce false positives.

Insight into the Deep & Dark Web

Harvesting data from the Deep & Dark Web comes with risks of compromise and extra precaution is needed when navigating such sites. By leveraging the skills of our highly specialized team, Bitdefender Advanced Threat Intelligence is able to incorporate streams of information which is otherwise ignored.

Continously updated data

Our team of 800+ security R&D engineers ensure our threat intelligence data doesn’t miss anything. The highly sophisticated machine learning models developed internally are able to detect zero-day threats faster than any competitor, keeping you up to date with the latest attack vectors.

Easy integration via a light REST API

Bitdefender allows organizations to easily consume threat intelligence data and integrate it within minutes on any platform or infrastructure. The services are platform-agnostic and compatible with any SIEM, SOAR or other security tools familiar with consuming APIs.

File Reputation	Certificate Reputation	IP Reputation	URL/Domain Reputation	APT IP Feeds	APT Domain Feeds	C&C Feeds	Phishing Feeds	Malware Feeds
Hashes (md5, sha)	Hashes (md5, sha)	IP addresses	DNS domains and URLs	APT IPs	APT Domains	C&C Server IPs	Phishing domains	Malware domains
Files that are known to be part of threats or attacks	Certificates known to sign files that are part of attacks	Known to contain some sort of threat, such as botnet C&Cs or DoS attacks	Known to spread malware, phishing and other threats	IPs behind highly targeted cyber-attacks (APTs)	Domains hosting Advanced Persistent Threats	Command & Control server IPs that are hard to catch	Domains associated with phishing threats	Domains associated with malicious threats
ATI Services	ATI Services	ATI Services	ATI Services	ATI Feeds	ATI Feeds	ATI Feeds	ATI Feeds	ATI Feeds

Free Evaluation

Bitdefender Advanced Threat Intelligence includes a no-fee proof-of-concept with complementary technical support.

You can request a demo by e-mail at oemsales@bitdefender.com or by phone at +1-650-437-6581.

Bitdefender is a global security technology company that provides cutting edge end-to-end cyber security solutions and advanced threat protection to more than 500 million users in more than 150 countries. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a provider of choice in both hybrid infrastructure security and endpoint protection. Through R&D, alliances and partnerships, Bitdefender is trusted to be ahead and deliver robust security you can rely on. More information is available at http://www.bitdefender.com.

FOR MORE INFORMATION VISIT: bitdefender.com/business