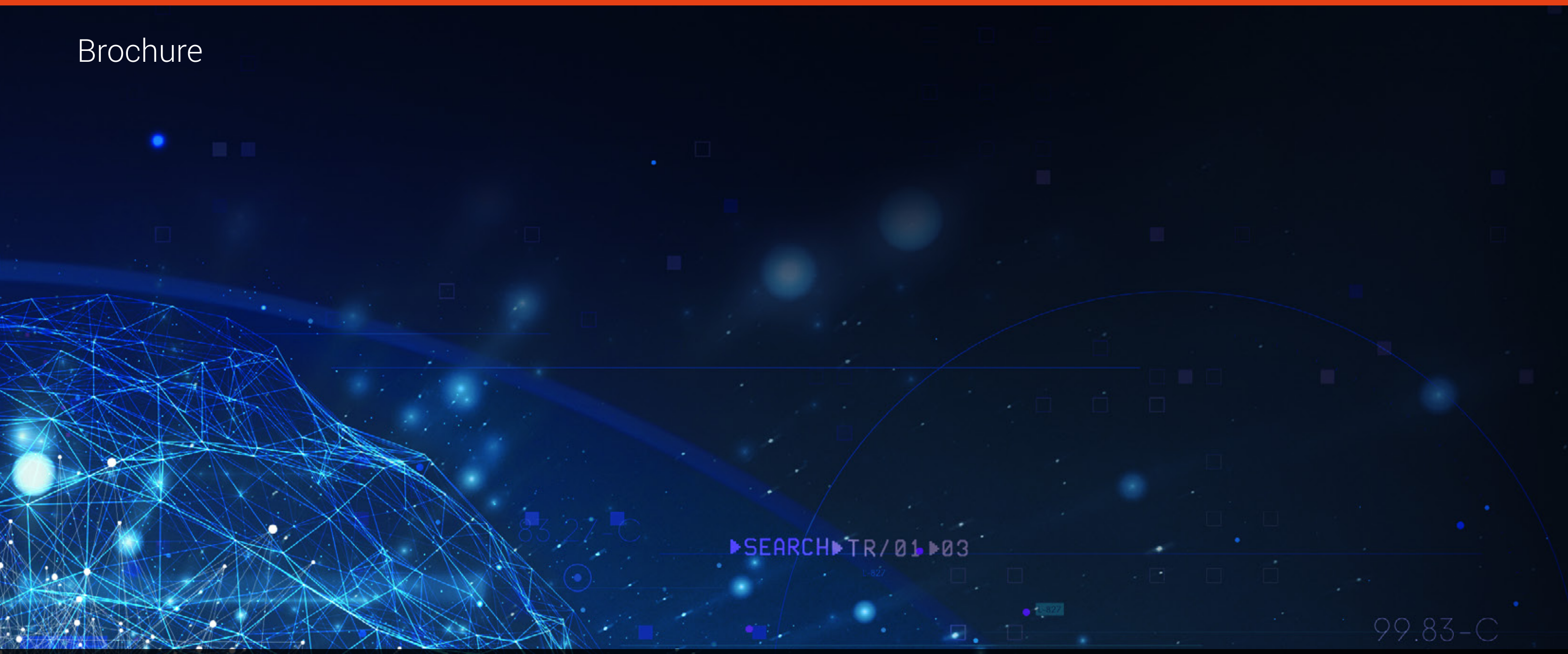
Brochure



Bitdefender®

Advanced Threat Intelligence

Differentiate and Win with the World's #1-Rated Security

1. Security Operations Challenges

1.1 Global Scale. Global Threats.

From technical specialists to team leaders and business architects, security experts today must cover many areas. They need to monitor, research and analyze threats as they occur, protecting enterprise networks and helping them scale operationally as they achieve higher business goals. But most of all, security leaders need to be brilliant forecasters, constantly predicting shifts of a market growing in both complexity and vulnerability.

Unfortunately, as digital services become critical to business growth, their ecosystems offer cybercriminals new opportunities to thrive. Cybercrime costs climbed 12% last year and the phenomenon is now so prevalent that the 2019 World Economic Forum Global Risks Report has included cyberattacks and data fraud among the top five risks CEOs are most likely to face.

Cybercrime has grown in both volume and sophistication, the latest attack vectors targeting not only large enterprises, but also third-party services and smaller, less-protected suppliers. In fact, business growth and the complexity it brings are now two of security's biggest challenges.

Global expansion makes today's business environments less centralized and more reliant on external actors, from SaaS providers to cloud platforms and IoT devices, as well as a myriad of other useful, yet vulnerable, bits of infrastructure.

1.2. One Infrastructure. Countless Vulnerabilities.

Impressive growth needs laser-focused security. Whether you're a vigilant CISO, an informed product manager or a seasoned security analyst looking to protect enterprise infrastructure (yours or a customer's), your problem is most likely the same: too many potential threats and too little time to understand them.

While malware is by far the costliest type of attack for organizations, more insidious threats are always waiting to take your security operations by surprise. Malicious insider attacks, ransomware, spear phishing, and web-based and DDoS attacks have all grown in frequency and proportion. And these are just surface threats, the ones that make headlines.

Others run undetected, and their goal is not to damage infrastructures but to expose them. We name only a few cyber-crime instruments, including:

- **Zero-day vulnerabilities:** exploits in hardware and software systems that have yet to become publicly known. Such exploits can take years to detect, a timeframe in which multiple parties might use them for nefarious purposes. If they run unpatched for too long, they're often called "n-day threats".
- **Advanced Persistent Threats (APTs):** highly targeted cyber-attacks means not to get in and out as quickly as possible, but to gain access to resources and remain undetected.
- **Command & Control:** servers used to coordinate attacks against internal and external systems or to steal data from a network. Cloud-based services are often prime targets, as this makes C&C servers more difficult to detect.
- **Cryptojacking**: a relatively new form of malware that makes use of personal or enterprise infrastructure for cryptomining and can easily blend in with your regular network bandwidth. Cryptojacking doesn't harm your software, but it does damage your hardware and productivity.
- **Evasive malware**: advanced malware that can hide its tracks as it infiltrates networks. Most targeted attacks against enterprises rely on evasive techniques that allow them to stay undetected for long periods.

What makes these attacks so special? The fact that either no attack signature exists, or they are incredibly hard to detect. This means signature-based tools fall flat in searching for them. It's these types of attacks that make organizations highly sensitive to the decreasing effectiveness of traditional network security and heuristics-based detection.

Aside from these vulnerabilities, security executives and analysts also face other business environment challenges that put even more pressure on enterprise infrastructure:

- **The lack of compliance**, which drains the resources of SOCs and other vendors who are now required to also deal with the numerous regulatory issues of their markets.
- **Cumbersome, manual processes**, with security data scattered across the organization, difficult to collect and analyze. This also exposes the human element, one of the most vulnerable pieces in the security puzzle.
- **Poor expertise** generated by the global cybersecurity skill shortage. This issue is also related to the ever-growing role of the SOC, in which detection and response have become instantaneous tasks, and where detecting a threat means nothing without understanding its nature.
- **Accelerated growth** and the accelerated integration of new partners and technologies means that keeping up with these changes as a security provider is already difficult. However, making employees keep up with security is even harder.

In this challenging landscape, security experts find themselves wearing too many hats, as they deal with endless threats and growing complexity.

2. The Solution

2.1 Threat Intelligence – The New Expert on Your Team

The first step in fighting an enemy is understanding it. It's also the most important step, as way too many companies prefer to invest in damage control rather than prevention. Threat intelligence is like having an additional team of analysts, constantly showing your most vulnerable spots and telling you when the next attack might occur.

Cyber-threat intelligence consists of a stream of tightly organized, refined and curated information about all potential and current cyber threats that could endanger your company's finance, infrastructure or data. Its main purpose is to help organizations understand the risk of external threats and to fully prevent them.

To use a more complex definition: threat intelligence is a stream of evidence-based knowledge that includes context, mechanisms and indicators, as well as implications and action-oriented advice about an existing or emerging threat.

A threat intelligence platform can gather, filter and analyze data and provide the results in standard formats so you can include it in a variety of security applications and systems.

There are multiple classifications of threat intelligence feeds, usually pertaining to the areas they cover. Some solutions cover only specific threats (such as DDoS attacks), while others aim to cover all core assets of a company, from hardware and software systems to onboarding procedures and business partner connectivity. Many of these platforms use a crowd-sourced model, combining human and technical intelligence to provide quick, actionable insights.

The most common classification of TI is that pertaining to its scope. Tactical, strategic, and operational threat intelligence are terms often used to define the same product or product suite in the context of when, how, and on what it is used.

- Strategic threat intelligence is mostly focused on identifying constant threats to an organization's main assets. This includes infrastructure, but also employees, customers, and partners. Strategic threat intelligence is less a question of tools, as it is a question of mindset – it's information-centric and focused on intention, rather than specific action.
- Tactical threat intelligence is the main type of TI that SOCs and IT departments use as it is a real-time operation focused on detecting and preventing currently active threats at a certain moment in time.
- Operational threat intelligence goes beyond tactical TI by focusing on the vulnerabilities themselves and the attacker's tools, rather than their damage. It's often used by forensic investigators and incident responders in combination with other tools.

No matter the scope of threat intelligence, its final objective is the same: to help your company understand and provide predictive remedies for the kind of threats that typical security procedures can't cover.

2.2 How Can Threat Intelligence Help Your Business?

What kind of information can you expect threat intelligence to provide? You can, for example, find out if your company's connection to a certain IP can be classified as suspicious. You can also find out if one of your partners is running any type of malicious activity through their website or online platforms. If a vulnerability is out in the wild, you can be promptly notified that your business platforms are at risk. The same goes for more common threats.

Another area where threat intelligence is crucial is the creation of an "incident response team", either inside an enterprise, or through an outside partner such as MSSP. An incident response team is not necessarily tied to a past or potential security breach, but it can also be used as an evaluation tool for the company's assets. For example, many managers seem to think that their physical assets and infrastructure are more valuable than their data. However, by using TI and finding out what attackers are really after in your market sector (and it's usually a type of data) your incident response team can be properly equipped to stop potential intruders.

Threat Intelligence can easily recognize threat actors as well as tactical indicators (a process called trailing). While not equivalent to network intrusion detection systems (NIDS) or other ready-made security solutions (including antivirus software), threat intelligence can be used as a complementary solution, as it doesn't just recognize patterns. It also shows you the extent of the attack, its source and the vulnerabilities that caused it, and it helps you clear any remains of malicious infrastructure. Threat Intelligence is actionable information, not raw data.

As a security professional, you'll easily find out what areas you should direct your security spending to and what improvements can be made to your architecture. Incident prevention, zero-day attack rumors, and the search for leaked data are also covered. The same goes for business and competitive intelligence that might threaten the position of your business or your security programs. Threat anticipation will be a part of your routine.

2.3 What Makes Effective Threat Intelligence

Now that you know how threat intelligence can benefit your company, you're probably wondering: how do I choose the best vendor? What should I look for when choosing a Threat Intelligence solution?

One of the first things you should bear in mind when choosing such a platform is that only information that's associated with a context and is delivered in an actionable format can be considered "intelligence". The context itself is what sets intelligence apart from mere data, as it provides the instructions that make information usable. Intelligence always has a purpose.

The journey of a piece of information from data to intelligence usually starts with a SIEM scanning the business environment for potentially useful data, from logs to transactions. The data is then fed into the Threat Intelligence platform, were it is processed, cleaned and enriched. The resulting information is then contextualized and delivered in a format in which the right people can use it to anticipate attacks.

Basing their predictions of a continued increase in connected endpoints, Global Market Insights forecast that the threat intelligence market is set to increase from $4bn in 2018 to $13bn by 2025. This means there will be many names to choose from. However, best-in-class threat intelligence services provide a few easily recognizable features:

- **Context:** The context itself sets intelligence apart from mere data, as it provides the instructions that make information usable.
- **Accuracy:** The specifics of each vulnerability set intelligence apart from post-event detection.
- **Integration:** Threat intelligence should come in a multitude of formats and easily integrate into the existing system of your SOC.
- **Alignment:** A good threat intelligence solution should be tailored to your company and aligned to your business goals.
- **Timeliness:** Prevention is a time-dependent action, so response speed is always critical.

3. Our Offer

3.1 Bitdefender Advanced Threat Intelligence – A Unique Approach

Supported by 18 years of experience, based on innovative technology, and fed by hundreds of millions of sensors, Bitdefender's new Advanced Threat Intelligence services eliminate long-standing blind spots for security analysts and enable them to thrive in the increasingly dangerous and complex world of cybercrime.

Our solution delivers real-time insights into the cyber-threat landscape to Managed Security Service Providers (MSSPs), Managed Detection & Response companies (MDRs), security consulting and investigations firms, and large enterprises with a Security Ops Center (SOC) that need to block and understand ingenious attacks and threat actors.

From evasive malware, APTs, zero-day threats and Command & Control servers to the reputation of files, URLs, domains and IPs, security analysts can get access to an accurate, up-to-date collection of real-world data.

Our unique, platform-agnostic approach, compatible with any SIEM familiar with consuming a REST API, lets other security professionals integrate our cyber-threat intelligence in minutes on any platform or infrastructure.

Here are just a few of the features that make our Advanced Threat Intelligence services stand out:

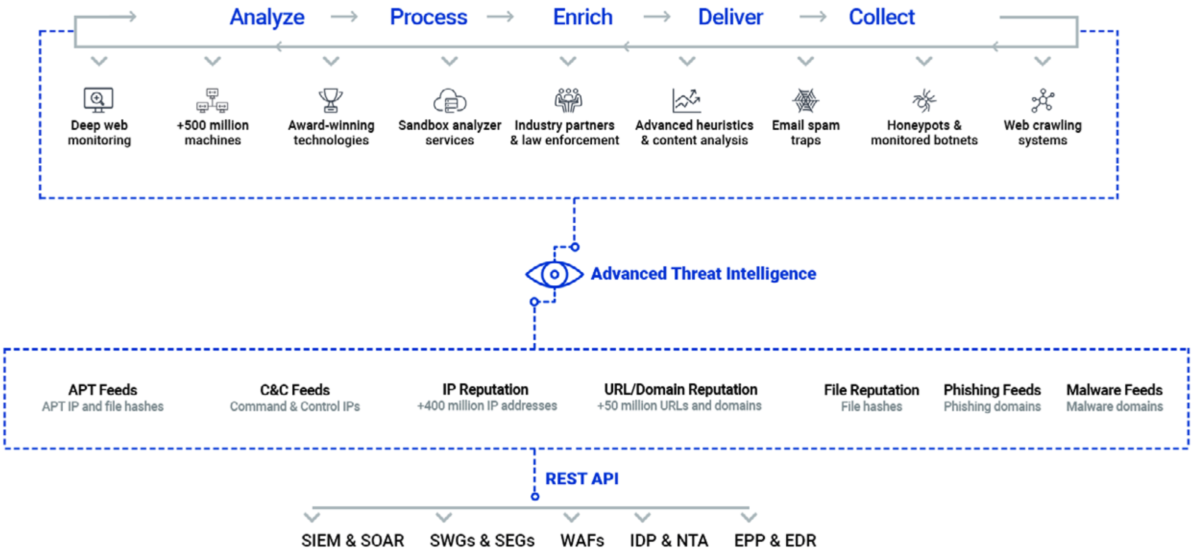
- **Source Quality.** Our engine is based on a combination of extensive knowledge repositories, open sources, traps, honeypots and botnet monitoring, and is backed by prolific collaboration with industry partners and reputable law enforcement agencies. Our virtual machine farm executes hundreds of thousands of malware samples daily and collects URL information on countless websites.
- **Contextualization.** We offer global insight into unique, evasive malware, APTs, zero-days and C&Cs that are hard to catch and that SOC analysts often lack visibility into.
- **Expertise.** More than 800 security experts in Bitdefender Cyber-Threat Intelligence Labs analyze and block approximately 600,000 IoCs daily using multiple technologies, including machine learning, advanced heuristics and content analysis.
- **Accuracy and Performance**. Bitdefender is a global cybersecurity and antivirus software leader protecting over 500 million systems in more than 150 countries.
- **Global View.** As compared to most competitors, our threat intelligence is globally balanced. Our data captures the threat landscape in the US, EMEA and APAC.
- **Technology Licensing Leader.** With more than 150 Technology Partners worldwide, Bitdefender is the provider of choice, used in over 38% of the world's security solutions evaluated by independent testing organizations.
- **Integration.** We disseminate our threat intelligence in a form organizations can easily consume. Our services can be integrated in minutes on any platform or infrastructure.
- **Ease of use.** All queries are processed through the Bitdefender Cloud infrastructure, which eliminates resource requirements on the client's end, in addition to management overheads.

3.2 What We Can Do for Your Business

Our products constantly achieve the industry's highest detection rates due to the expertise of our laboratories and our global networks. We build our intelligence from the over 500 million systems we protect in more than 150 countries. Our cloud-based infrastructure processes over 11 billion requests and over 6 TB of data per day, allowing effective, globally balanced detection of cybersecurity threats.

By using our Advanced Threat Intelligence platform, you can:

- Gain real-time visibility into the reputation of files, IPs, domains and URLs.
- Get a handle on global intelligence and detect targeted, evasive and zero-days attacks across the world.
- Improve decision-making and perfect your business architecture with a service that integrates seamlessly into your existing security architecture through light REST-based API.
- Accelerate incident response and forensic capabilities with contextual, actionable indicators.
- Grow your customers' trust and defend them against attacks even before they are launched.
- Augment your security capabilities by leveraging the expertise of Bitdefender Labs, a global R&D leader in cyber-security tests.
- Increase time-to-value by seamlessly integrating Advanced Threat Intelligence into your existing security architecture.
- Get end-to-end visibility into complex Indicators of Compromise.



Here are just a few of the numbers behind our Threat Intelligence offering:

- Up to 2 million pieces of malware analyzed daily
- URL Reputation services alone detect and block over 50 million malicious URLs
- 12,000 domains with malware found and added in the repository on a daily basis
- 46,800 URLs with malware or spam per day
- 2,800 new IP records with malware added per day
- 2.7 billion entries in our file reputation database
- 1.06 Petabytes of searchable file data
- Information on 143 million unique IPs

We can help:

- Enterprises that want better visibility into the threat landscape and the ability to discover IOCs (Indicators of Compromise) in real-time.
- Managed Security Service Providers and MDR companies whose clients are targeted by sophisticated threat actors.
- Security Operations Center and security consulting companies who want to improve their offer with highly specialized products.

3.3. Why Bitdefender

500+	50+	800+	150+	100+
Million Systems Protected	Billion URLs Blocked	Engineers & Researchers	Technology Partners Worldwide	New Patents Since 2015

Bitdefender has a strategic focus on technology licensing, a long and proven history of partnerships, and one of the broadest portfolios in the industry, including over 20 SDKs, APIs, and advanced technologies. Our award-winning services can enhance your products and services with security capabilities and best-in-class protection, along with extensive business and technical support.

For 18 years, Bitdefender has consistently produced award-winning business and consumer security technology. We've become the provider of choice for leading Independent Software Vendors (ISVs), hardware vendors, service providers and marketing companies looking to integrate security technologies into their products and services.

Today, Bitdefender technology is present in over 38% of the world's security solutions and has over 150 technology licensing partners worldwide. Our solutions are proven and recognized by independent test labs, our teams have issued hundreds of patents over the past three years and our SDKs and APIs work across all operating systems and hardware platforms. For more than half a million systems, Bitdefender is the provider of choice.

Request a Trial

Bitdefender Advanced Threat Intelligence is a best-in-class solution that will ease the burden on your security operations. It also includes a no fee proof-of-concept with complementary technical support.

It will allow you to improve decision-making, accelerate incident response and boost your forensic capabilities by using accurate and contextual threat indicators. In time, our TI solution will help grow your customers' trust and allow you to offer them new packages. Furthermore, our solution will augment your security capabilities by getting a complete view of the security landscape, inside and outside the US.

All you have to do is request an evaluation by e-mail at oemsales@bitdefender.com or by phone at +1-650-437-6581.

Bitdefender is a global cybersecurity and antivirus software leader protecting over 500 million systems in more than 150 countries. Since 2001, Bitdefender innovation has consistently delivered award-winning security products and threat intelligence for people, homes, businesses and their devices, networks and cloud services. Today, Bitdefender is also the provider-of-choice, used in over 38% of the world's security solutions. Recognized by industry, respected by vendors and evangelized by our customers, Bitdefender is the cybersecurity company you can trust and rely on. Bitdefender is a global cybersecurity and antivirus software leader protecting over 500 million systems in more than 150 countries. Since 2001, Bitdefender innovation has consistently delivered award-winning security products and threat intelligence for people, homes, businesses and their devices, networks and cloud services. Today, Bitdefender is also the provider-of-choice, used in over 38% of the world's security solutions. Recognized by industry, respected by vendors and evangelized by our customers, Bitdefender is the cybersecurity company you can trust and rely on. http://www.bitdefender.com.

Bitdefender-Whitepaper-ADVThreatIntel-CREAT3637-en_EN