WHITEPAPER OEM

web version only / English version only

Bitdefender Antimalware Engine

Technologies Drive Success

Contents

Reality, recognition, performance

The reality is that threat actors will never stop honing the techniques and tools they use to breach systems. In your arsenal, you need advanced, reliable tools to protect against the full range of cyber threats. You need multiple layers of advanced components and technologies to deliver consistent industry-leading detection, accuracy and performance for known and unknown threats. You also must deliver it across hybrid-, multi-cloud environments, IoT, embedded devices, and wherever your customers need to go.

In this document, we describe how Bitdefender solves these challenges in order to deliver value to your organization, whether you are looking to protect endpoints, gateways, cloud infrastructures, from the basic endpoint level to a global footprint across various business environments.

Award Winning Antimalware

- Protection against known and unknown malware, including viruses, Trojans, worms, ransomware, advanced persistent threats, spyware, adware, etc.
- 99.9% detection consistently demonstrated in third-party tests
- High-speed scanning, full multi-threading architecture
- Small footprint, low memory and processing requirements
- Fast and easy integration into partner applications and services
- Multiple SDKs available, optimized for various use cases
- Support for multiple OSes (Windows, Linux, Mac)
- Used by Bitdefender consumer and business products
- Multiple awards from independent testing organizations such as AV-Comparatives, AV-TEST

Experience with antimalware products, especially those preloaded on a newly acquired machine, shows users that they slow down a system significantly. However, this is not true for all antimalware solutions. The Bitdefender detection logic has been designed with real-life usage scenarios in mind, where end-user experience is just as important as protection.

Bitdefender has excelled at delivering highly effective antimalware by focusing on efficacy and performance simultaneously. We have honed our engine development with OEM relationships on IoT devices with extremely limited resources such as routers and printers. In addition, optional modules such as SmartScan implement intelligent optimization algorithms that speed up the scanning process without compromising the malware detection rate.

Simply put, we are experts at fitting a lot of antimalware prowess into a small space.

Advancing engine components and tech

Antimalware continues to advance, yet the view of present-day antimalware is influenced by the latest-and-greatest. It is tempting to conclude that the newest approach is the best, and therefore, only method required to secure endpoints. Adopting new methods is important, but focusing on only the new technologies creates an incomplete picture of what is required to deliver a robust, performant and, above-all, useful, antimalware engine.

In this section, we outline why signatures, generic detection, heuristics, and emulation continue to advance.

Signature-based detection

Antimalware signatures are snippets of code from malware samples used by antimalware programs to perform pattern-matching. Signatures are useful for a number of reasons:

- A new signature can be created and added to the engine in a matter of minutes. A generic detection requires study of the malware family, writing the detection, and testing it – a process that takes at least a few hours.
- Applying signatures is faster process than running the generic detections. Applying 10,000 signatures is significantly faster than applying 100 generic detections, which increases performance for users.
- Signatures are compact; adding even a large set increases the engine size trivially.
- As they are based on malware content, signatures are highly precise and accurate in terms of detection. They almost never produce false positives, which results in a better-quality security product.

Ultimately, signatures are reactive. Antimalware vendors need a sample of the malware to develop a signature and then push it to users – and this creates a vulnerability window.

However, not all signature-based detection is equal. The Bitdefender engine uses key aspects of an examined file to create a static fingerprint of known malware. Knowing this, attackers frequently mutate their creations to evade detection by changing the signature of the file. However, Bitdefender “signatures” are a combination of small hashes on certain parts of malware code rather than a full hash on the file. Thus,our signatures can detect even completely mutated files, as long as the actual malware code part remains unmodified.

While Bitdefender delivers a next-generation engine that uses a variety of technologies for malware detection, signatures are and will continue to remain a part of the engine and produce a solid bulk of detections.

Generic detection

Generic detection is useful for discovering all samples (including those unknown) of a known malware family. It is a type of detection used by the antimalware engine for identifying files with malicious characteristics. Generic detection extracts the key characteristics of one or a few samples of a malware family and creates a “one size fits all” detection rule to catch as many variants of the same family of the same vulnerability, as possible.

- Generic detection is responsible for the detection of all strains of malware belonging to a specific malware family or subfamily.
- It is very useful in detecting polymorphic or metamorphic malware, which are impossible to handle based on signatures only.
- Unlike single-file detections, generic detections look for broadly similar code or behavioral patterns in dozens or even hundreds of suspect programs or files, to efficiently determine their potential for causing harm.

Heuristics-based detection

Heuristic detection is responsible for the detection of previously unknown zero-day malware. It provides outstanding proactive detection capabilities against new malware variants, new malware families, and against unknown vulnerabilities and exploits. Rather than relying on signatures or binary or code fingerprints, heuristic detection relies on complex algorithms that specify patterns and behaviors indicating that an application may be malicious. Inevitably, malicious software attempts to perform actions in a context that legitimate applications do not. Examples of suspicious behavior include attempting to drop files or disguise process injection (executing code in another process's memory space).

- Files are first checked against the Bitdefender Signature Database. If no signature is matched, the file is sent to the heuristic engine to be observed.
- Heuristic detections occur during a milliseconds-pause as an application launch, allowing the code to be executed in a virtual environment that is isolated – sandboxed – from the real computer. If suspicious behavior is observed, the program execution is blocked.
- In other words, heuristic detection is the logic that analyzes the output of generic signatures (static) and emulator (dynamic) code analysis when it is not clear if the binary is malware.
- Heuristic detection is thus based on the output of the emulator and is effective in detecting new malware.

Emulation

Emulation is the antimalware engine's ultimate weapon against polymorphic malware and for broader, yet accurate, proactive detections. With every replication step, polymorphic malware changes the encryption method and key with which it encrypts the original virus code, but the original virus code/body stays the same. Bypassing encryption and peeking under the surface allows our generic detection to spot any polymorphic malware family.

Emulation means the engine simulates a virtual computer – its CPU, memory, operating system API and resources—and simulates execution of a suspect file in this virtual environment. The suspect file's code is disassembled, just as an operating system would, but the instructions have an effect on only software-simulated, safe data structures. This disassembly helps us gain a high level of insight into the suspect file, allowing for an accurate threat prediction.

An emulator must account for the many features of the simulated computer and operating system, such as processes and threads, files, and anti-debugging and anti-emulation techniques.

To deal with obfuscated binaries, the Bitdefender antimalware engine uses emulation as follows.

- It checks files by running them in a virtual environment inside the Bitdefender engine, designed to emulate the behavior of an actual computer. If any specific file exhibits suspicious, malware-like activity, the engine reports the file as malicious. If not, the file is declared clean, and the process is allowed to run.
- The output of the emulation also powers malware detections, notably the heuristics-based detection.
- The engine has a full machine code emulator for x86/x64 platforms, as well as a full emulator for JavaScript and VBScript languages.
- These emulators are confined and have no access to the actual file system or Internet, and thus will not leak information.

Enriching engine components and tech

The market is awash with perspectives declaring the components and technologies described above as elements of the past. Consistently achieving top-ranked third-party results for efficacy and performance must mean the Bitdefender is on top of – indeed, ahead of –the complete antimalware story.

Machine Learning Algorithms

Machine Learning (ML) significantly improves detection time for modern threats by analyzing massive amounts of data significantly faster than any human could. When trained to accurately detect various types of malware behavior, ML yields a high detection rate, for both known and unknown samples. Incorporating machine learning into both static (file-based) and dynamic (behavior-based) malware analysis sharply accelerates detections of new malware samples. This offers protection from even previously unknown threats – APTs, zero-day attacks and ransomware.

Bitdefender has been training ML algorithms for years - Perceptrons, Neural Networks, Centroids, Binary Decision Tree and Deep Learning, to name a few. Some focus on specific malware families, others on new malicious files, and more are built to minimize false positives. They complement one another, as well as traditional heuristic and signature-based detection.

For instance, Neural Networks are among the most popular implementations of ML algorithms that are designed to increase malware detection rates using repeated training sessions on popular malware categories. Allowing these algorithms to extract features from existing malware samples or families enables them to learn to predict future malware based on shared similar features.

Cloud-sourced detection

Bitdefender's antimalware engine combines formidable local capabilities with cloud-based updates, meant to bolster detection as well as reduce the rate of false positives. The engine leverages Bitdefender Threat Intelligence, which is fueled by hundreds of millions of threat sensors around the world. Our malware labs and research teams use massive data feeds, continuously crunched by advanced Machine Learning, and ultimately human curation, to create updates for Bitdefender Antimalware Engine components. This means that an endpoint in one part of the world receives the benefit of detections across a vast network encompassing the rest of the world.

Comprehensive Inspection

File format analyzers and parsers

- The Bitdefender antimalware engine analyzes a large number of file formats, from various executables to Microsoft Office documents, Flash files and MP4 videos, etc. An analyzer in the engine determines if the file format is supported. Another parser is responsible for extracting the relevant data for the engine.
- Unlike traditional file format parsers, the Bitdefender engine streamlines analysis by extracting only the required data, rather than parsing the entire file. For example, analyzing PDF files and Microsoft Office documents requires only the parts which contains scripts.
- Streamlined analysis also expands the ability of the Bitdefender engine to deal with damaged or altered file formats, and also expands capabilities to cover new versions not yet officially supported. Some applications will try to open damaged files, even if an antimalware engine cannot, which leaves a security gap.
- File format parsers must correctly deal with damaged or altered file formats, including handling the new, unsupported versions of the file format. Parsers are carefully designed so they attempt to extract the necessary data even from slightly damaged files (because some applications would open those files). They are also designed to handle completely damaged files, which would likely crash the original application.

Un-archivers and archivers

- The Bitdefender engine scans inside the most common type of archives and packed files.
- The engine unpacks a wide variety of archive formats, including all modern archivers and a number of old archivers that are no longer supported. The latter are still necessary as many third-party test organizations and individual researchers have test collection malware using these older archives.
- In engine terminology, an archive is a file that can contain one or more other files. This definition includes not only traditional archives such as ZIP or RAR, but also disk images like ISO or DMG, install packages such as InstallShield or MSI, and even multi-part MIME documents.
- As with file parsers, the Bitdefender engine can also handle damaged archives, and will try its best to unpack the file even from a damaged archive, so that it can be scanned. The Bitdefender antimalware archive algorithms are built around the concept of "in-depth scanning," which means they can be configured to scan embedded archives down to any depth. The engine can extract an archive embedded in another archive (embedded in another archive...) as long as there is enough disk/ memory to store the unpacked objects.
- The Bitdefender engine can also pack (i.e. create) a number of archives, as this is necessary for the disinfection or deletion of files inside the archives.

Executable unpackers

Runtime packers are used to minimize the download size of an executable file, but in many cases they are also used to add an obfuscation layer over the program code. Once initiated, the executable runs a decoder loop that opens the packed section and then transfers execution (in memory) to the unpacked section. Seeing a runtime-packer in use is not enough evidence to classify a program as malicious, because benign legitimate applications also use packers. Nonetheless, the presence of a packer can raise a yellow flag in an anti-malware engine. When other suspicious behaviors are encountered, the combination results in a heuristic classification as malware.

As most malware binaries are packed, this is an extremely important feature of the antimalware engine.

- The Bitdefender engine can unpack a large variety of packed executables by using either emulation or generic unpackers.
- The engine will try to use generic unpackers for the packers it recognizes (such as UPX). For the packers it does not recognize or for which it has no generic unpacker, it will use emulation. This is extremely useful as it means that, if malware writers start to use a new packer, technology licensing partners do not need to wait until Bitdefender creates an unpacker for it.

Driving Your Success

Attackers will continue to be creative in leveraging every tool at their disposal to succeed. Organizations will also continue to pursue business goals with on-premises, outsourced, and multi-, hybrid-cloud configurations, complicating the lives of security practitioners. While complexity seems inevitable, the Bitdefender Antimalware Engine is highly flexible, performant and robust. As we have detailed here, there is plenty of complexity under the hood, but we take care of it so our partners can focus on their success.

While going down that road, note that the Bitdefender Antimalware Engine is available for integration in multiple SDK variants. This eases implementation at the endpoint, network, perimeter, gateway, and on cloud-based platforms. It can also be complemented by a wide range of other Bitdefender technologies to harden security, protect against additional threat vectors, and respond to additional market demands.

About Bitdefender Technology Licensing

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 180 of the world's most recognized technology brands. Launched in 2001, Bitdefender has customers in 170+ countries with offices around the world. For more information, visit https://www.bitdefender.com/oem.

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