# Advanced Threat Control (ATC) SDK

## The need for multi-layer security

The constant emergence of new cyber threats has left traditional security mechanisms insufficient and unreliable at offering adequate defense. With over 12 million new and variant strains of malware coming out each month, tracking and mitigating each threat has become enormously challenging. Compounding the problem, both malware and the mechanisms used to deliver it have become increasingly sophisticated. Ransomware, in particular, is of major concern.

Ransomware attacks have tripled in frequency and have proven to cause extensive damage, including loss of sensitive data, operational downtime, lost productivity and reputational harm. Many new variants of ransomware are successful because they use different attack vectors, files and vulnerabilities and are often polymorphic by design. This has allowed attacks to elude many antimalware solutions, which have mostly relied for detection on signatures for known families of ransomware.

As threats grow more frequent and sophisticated, organizations need multi-layer protection solutions that go beyond traditional signature detection technologies and even the standard heuristic scanning.

## Advanced Threat Control SDK

Bitdefender's Advanced Threat Control (ATC) SDK employs a proactive dynamic technology based on advanced heuristics methods to detect zero-day threats in real time. An on-execution protection layer, the SDK augments Bitdefender's comprehensive pre-execution detection technologies, and enables organizations to add an extra layer of protection that drastically reduces the risk of new or evasive malware compromising a system.

Operating on a zero-trust assumption, the ATC SDK permanently monitors active applications and processes for any signs of malicious behavior. It relies on actual behavior characteristics instead of signatures or binary or code fingerprints, letting the SDK consistently detect new ransomware variants, other zero-day threats and file-less attacks.

## How the SDK works

The ATC SDK continuously monitors processes running in the operating system using filters in user mode and kernel model, and hunts for any suspicious signs or abnormal behavior. Unlike other heuristic scanners, the SDK monitors processes for as long as they are active so it cannot be defeated by the delaying tactics of some advanced malware. This constant, real-time monitoring also prevents malware from exploiting or hijacking already-trusted applications.

Processes are monitored for malware-like actions such as copying or moving files in System or Windows folders or limited access disk locations; executing or injecting code in another process's space to run with higher privileges; self-replication; creating an auto-start entry in the registry, accessing or executing illegal operations in registry locations that require elevated privileges; dropping and registering drivers; or ransomware-specific actions like removing backup files / shadow copies or generating encryption keys and more.

As legitimate applications sometimes perform one or more of these actions, the SDK does not determine a process to be malicious based on any single action. It looks for behavior specific to malware and assigns a score for each process based on its action and context. This is important because a process may not indicate malicious intent when analyzed individually, but collective analysis will provide the insight needed to make a determination. When the overall score for a process reaches a given threshold, the process is reported as harmful or malicious, then terminated.

Zero trust,
Always monitor running processes

Maintain process ledger
based on process behavior

Process is terminated when
given threshold is reached

## Leveraging signatures and heuristics with collective intelligence and machine learning

- The SDK leverages Bitdefender's Cloud – Bitdefender Global Protective Network (GPN) – to get information about newly discovered threats. A central threat intelligence Cloud that is always up to date and can be accessed by any system also greatly reduces the need for local signature databases that slow down computers.
- Bitdefender's Global Protective Network (GPN) performs 11 billion queries per day, and uses reflective models and advanced machine learning algorithms to extract malware patterns, ensuring real-time protection against any threat.

## Key features and benefits

Proactive, dynamic protection technology based on continuous monitoring of processes' behavior:

- High efficacy against ransomware, zero-day exploits and advanced persistent threats (APTs);
- Detects advanced attacks early and prevents breaches, reducing incident response costs and efforts;
- Awarded technology – Bitdefender had an average detection rate of 99.9% in 2019 Real-World Protection tests by AV-Comparatives; and won the "Product of the Year" award after scoring "Advanced+" in all 7 tests conducted in 2019;
- Intelligent performance optimization for application and process monitoring ensures low system impact;
- Designed to facilitate remediation / cleanup of detected malware;
- Acts as an additional or last layer of defense against known and unknown threats, complementing Bitdefender's lineup of antimalware technologies.

## Specifications

Seamless integration process, using C interface bindings; allows integration via dynamic linked library; • Supports systems/endpoints running on Windows 7 and higher (x86/x64).

## FREE evaluation

Evaluating the Bitdefender Advanced Threat Control SDK is free of charge and includes technical support.

## Contact us

For more information about the SDK or any Bitdefender security technology, please reach us at www.bitdefender.com/oem

**About Bitdefender Technology Licensing.** Bitdefender provides 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 has become a provider of choice for leading Independent Software Vendors (ISVs), hardware vendors, service providers and enterprise organizations looking to integrate security technologies into their products and services. Today, Bitdefender has over 150 technology partners worldwide. More information is available at www.bitdefender.com/oem

Bitdefender®

**Founded** 2001, Romania
**Number of employees** 1800+

**Headquarters**
Enterprise HQ – Santa Clara, CA, United States
Technology HQ – Bucharest, Romania

**WORLDWIDE OFFICES**
**USA & Canada:** Ft. Lauderdale, FL | Santa Clara, CA | San Antonio, TX | Toronto, CA
**Europe:** Copenhagen, DENMARK | Paris, FRANCE | München, GERMANY | Milan, ITALY | Bucharest, Iasi, Cluj, Timisoara, ROMANIA | Barcelona, SPAIN | Dubai, UAE | London, UK | Hague, NETHERLANDS
**Australia:** Sydney, Melbourne