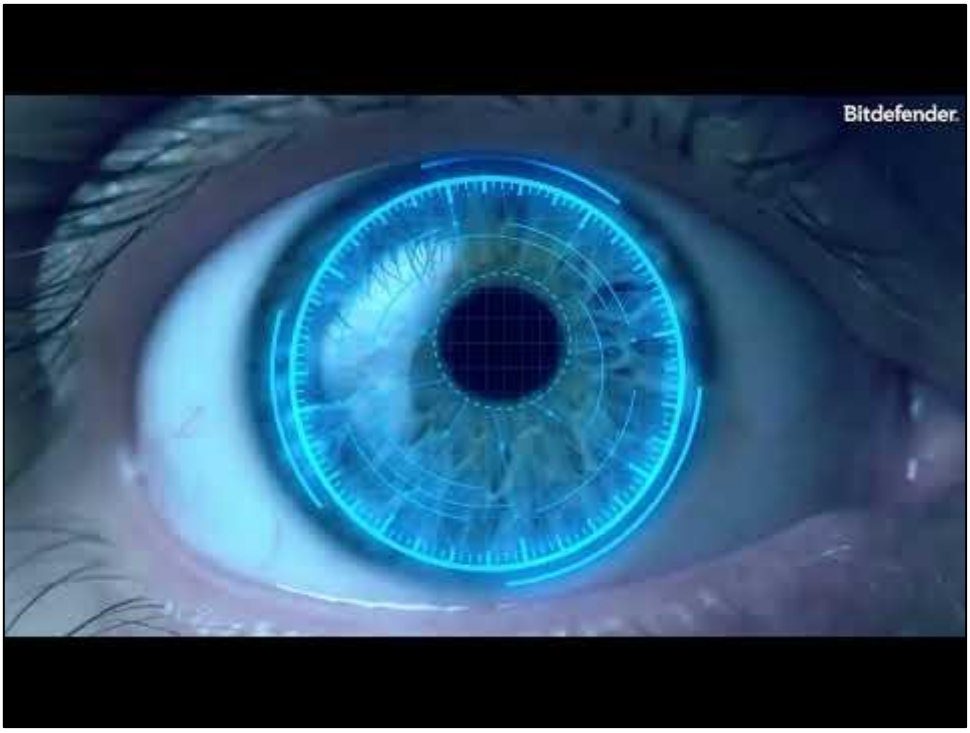
What is Bitdefender Advanced Threat Defense and What does it do?

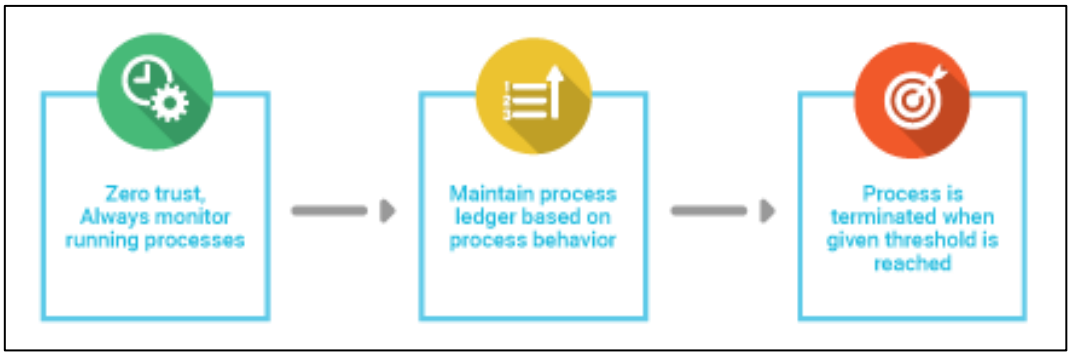
This article is a step-by-step guide to help you get started with Advanced Threat Defense quickly. We'll also cover the module's key features to help you understand how it works and why it's great to use the Advanced Threat Defense feature included in Bitdefender products. Additionally, we'll highlight tips to help you manage its settings.

What is Bitdefender Advanced Threat Defense?

Advanced Threat Defense is Bitdefender's innovative take on detecting ransomware and zero-day threats in real time using advanced heuristic methods. This method is different from traditional malware detection, which involves identifying malware using the virus signature database.



How does Bitdefender Advanced Threat Defense work?



Bitdefender Advanced Threat Defense identifies anomalies in apps' behavior and correlates different suspicious behaviors to significantly improve detection.

Bitdefender Advanced Threat Defense continuously monitors the applications and processes running on your computer. It monitors suspicious activities such as copying files to important Windows operating system folders, executing or injecting code into other processes, multiplying them, changing the Windows registry, or installing drivers.

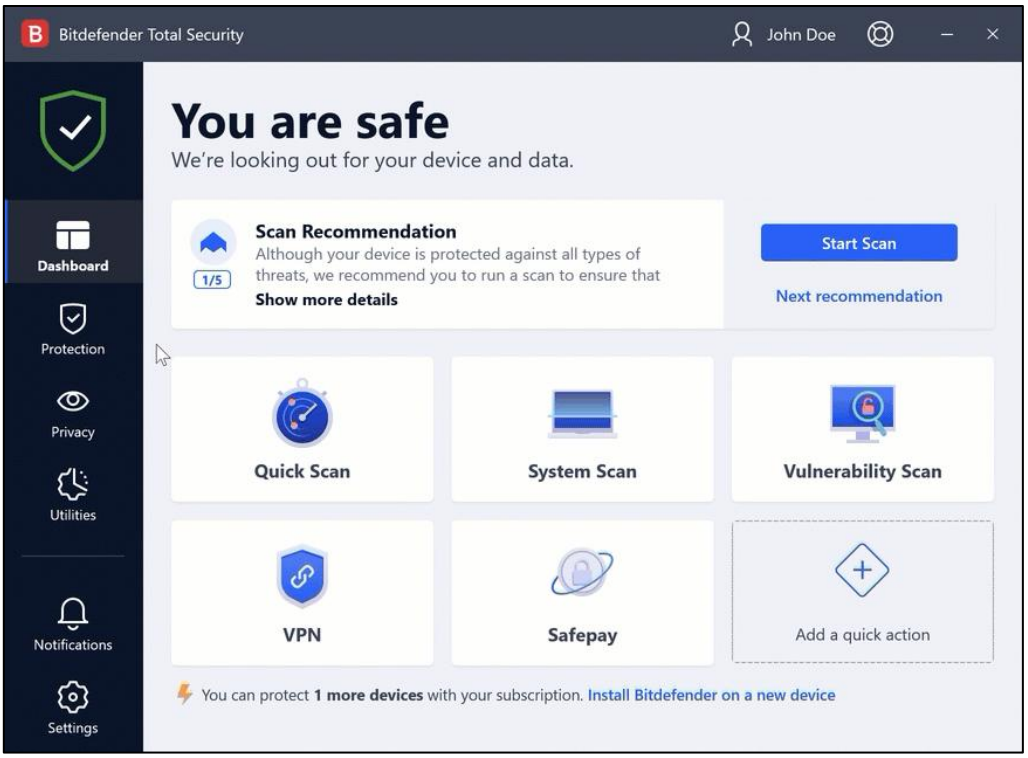
Each action is scored, and every process receives a danger score. If the overall score for a process reaches a certain threshold, Bitdefender makes the decision to block that application that 99% of the time turns out to be malware. Thanks to the score-based rating system, the number of false positive detections is very low and the detection of threats, even if they are very new, is extremely effective.

Turning on or off Advanced Threat Defense

To keep your system protected from ransomware and other threats, we recommend you disable Advanced Threat Defense for as little time as possible.

To enable or disable this feature:

1. Click Protection on the navigation menu on the Bitdefender interface.
2. In the ADVANCED THREAT DEFENSE pane, click Open.
3. Go to the Settings tab and click the switch next to Bitdefender Advanced Threat Defense.



Finding apps blocked by Advanced Threat Defense

With the Advanced Threat Defense module enabled, even the most sophisticated attacks are blocked in real-time before the malware reaches the computer.

As a safety measure, you will be notified each time threats and potentially malicious processes are detected and blocked. You can check which applications have been detected by Advanced Threat Defense in the Notifications window, on the left-hand side of the Bitdefender interface.

To check at any time the list of detected malicious attacks:

1. Click Protection on the navigation menu on the Bitdefender interface.
2. In the ADVANCED THREAT DEFENSE pane, click Open.
3. Go to the Threat Defense window. The attacks detected in the last 90 days are displayed here. To find details about the threat type, the path to the malicious process, or if the disinfection has been successful, simply click on its name.

You can exclude trusted apps, so they are not blocked if they perform threat-like actions by following the steps from this article – How to stop Advanced Threat Defense from blocking a process.

What's the Exploit Detection feature?

To further enhance your protection against zero-day threats, we have integrated an Exploit Detection feature directly into the Advanced Threat Defense module. A way used by hackers to breach systems is to take advantage of bugs or vulnerabilities present in computer software (apps or plugins) and hardware. To make sure that your device stays away from such attacks, that normally spread very fast, Bitdefender uses the newest anti-exploit technologies.

The Exploit detection option is enabled by default.

Turning on or off Exploit Detection

To turn on or off the Exploit Detection feature in Bitdefender:

1. Click Protection on the navigation menu on the Bitdefender interface.
2. In the ADVANCED THREAT DEFENSE pane, click Open.
3. Go to the Settings tab and click the switch next to Exploit Detection to turn the feature on or off.