Incorrect Detection: Report a False Positive or False Negative detection to Bitdefender Labs

Fill out the form below to report an incorrect detection to Bitdefender Labs. For example, if you think Bitdefender has incorrectly classified as dangerous, phishing, fraudulent etc. a website or file you trust (false positive). Or that it missed a threat (false negative). Once confirmed, false alarms are corrected within hours.

What is a False Positive?

In cybersecurity, a false positive detection or false alarm refers to a situation where security software incorrectly identifies a harmless file or website as a threat. It occurs when a program or webpage performs an action that appears to the antivirus program to be a virus-like activity. We strive to reduce false-positive reports to a minimum. However, Bitdefender may on occasion mistakenly flag a safe website or a legitimate file as a false positive threat.

What is a False Negative?

A false negative refers to a situation where security software fails to detect an actual threat. Bitdefender detects about 99.51% of viruses in the wild, so it is possible, although very unlikely, that a virus will get past its filters. This is mainly because new malware is released continuously and there is a time gap between when a virus is created and when we add detection for it. Other situations concern PUA/PUP programs installed with the user's consent in bundled packages, which do not trigger an alert because the user has accepted the license agreement to use them.