avast business
powered by AVG and Avast

A Closer Look:

CyberCapture

Our proprietary, cloud-based CyberCapture technology, available in every tier of Avast Business Antivirus, detects morphed, yet unknown files, in real-time and protects you from zero-second attacks. CyberCapture provides a competitive advantage against threats and a front-line defense for zero-day attacks.

Stops zero-second attacks
Server polymorphism, where one malware sample targets a single user before the code morphs into a new sample and attacks the next user, enables fast cyberattacks targeting a maximum number of victims. These zero-second attacks, which are difficult to prevent using traditional protection methods, are stopped by CyberCapture.

Identifies, isolates, analyzes, and protects against malware
In developing CyberCapture, we focused on shortening the time between malware discovery and the deployment of a detection. CyberCapture identifies, isolates, and quickly determines whether unknown files are potentially harmful and then analyzes them in real-time in the cloud.

Detects Locky and other ransomware strains
We first used CyberCapture to identify Locky ransomware, a form of malware delivered by email with a Microsoft Word attachment that contains malicious macros. CyberCapture catches malware in this form, and other types of threats, early and automatically.

The competitive advantage

CyberCapture is unique due to the variety, type, and volume of new malware it can continually identify. It is constantly gathering intelligence on new viruses, analyzing over 10,000 new files each day to protect businesses and their end users against the latest threats.

This means it continues to organically improve as it is used and will continue to demonstrate increased performance.

Let's take a closer look at CyberCapture.

What is CyberCapture?
CyberCapture is a cloud-based, smart, file scanner feature in Avast Business Antivirus products. It detects and analyzes rare, suspicious files. If you attempt to run a suspicious file, CyberCapture will lock the file from your PC and send it to our Avast Threat Lab where it will be analyzed in a safe, virtual environment.

What conditions trigger CyberCapture?
CyberCapture is triggered when you run or download suspicious files from the Internet that CyberCapture has not previously encountered.

How does CyberCapture work?
CyberCapture works by seizing, or 'capturing,' any low prevalent or low reputation files – files that have not been seen by users – for deeper analysis in a safe cloud environment.

If a user downloads a suspicious file from the Internet and, according to our Avast threat database, it has never been seen before by any of our users, it will be put into an isolated environment where it can be observed and behavioral data will be collected. Before the user can run the suspicious file, CyberCapture locks the file from the PC and sends it to our Avast Threat Lab for analysis.

How are suspicious files analyzed?
Rather than relying on the latest virus definition updates, CyberCapture immediately isolates suspicious files in a safe environment and automatically establishes a two-way communication channel between the user and our Avast Threat Lab for analysis. Files are uploaded via an encrypted connection for privacy and to ensure hackers cannot access the files.

To analyze and fully dissect the file, we clear away the malware creator's false code and misdirection to observe the binary level commands inside the malware and understand the instructions hidden there.

What happens after the initial analysis?
Based on the initial inspection of the suspicious files, CyberCapture can decide if more analysis is required.

In this case, files are further analyzed by our machine learning and behavior analysis systems. Once this analysis is completed, the user is notified and the file is either released back to the user and can be run, or if it is identified as malicious, it is quarantined so it can no longer execute on a user's system and infect the network.

How long does it take to analyze a file?
The analysis process typically takes 5-10 minutes. In certain cases, it will not be possible for our detection engines to make a reliable decision about the files and our experienced Avast Threat Lab analysts will manually analyze the file. If manual testing is required, it may take up to two hours.

During that time, the file is still contained in the "capture" stage and cannot cause any harm. Once the analysis is complete, the user is notified about the result and the file is either quarantined or determined safe and released from the capture and allowed to run.

Avast threat protection at work

Our hundreds of millions of users provide a continual stream of data that helps us quickly identify and destroy any threat – and predict future ones. Day and night, our immense cloud-based, machine-learning engine is evolving and learning, making our solutions smarter, faster, and growing more powerful by the second.

- **1.5 billion malware attacks** blocked monthly
- **300 million new files** checked monthly
- **200 billion URLS** checked monthly
- **30 million** executable files analyzed
- **500 million** visits to malicious websites blocked
- **128 million ransomware attacks** blocked last year

About Avast Business

Avast Business provides integrated, cloud-based endpoint and network security solutions to protect small and medium businesses from the growing threat of downtime, lost revenue, and reputational damage caused by cyberattacks. Backed by the largest, most globally dispersed threat detection network, the Avast Business layered security solutions make it easy and affordable for businesses to secure, manage, and monitor increasingly complex IT environments.

For more information, visit: **www.avast.com/business**.