Sandbox

Our Sandbox feature, available in every tier of Avast Business Antivirus, provides the ability to analyze potential threats and vulnerabilities in a secure, virtual environment isolated from the rest of the network. IT teams can test potential malware, understand exactly how it works before it invades networks and devices, and gain important insights to continually improve their security defense.

Enables safe testing and insights

Tests suspicious files, applications, URLs, or new code in a safe, virtual space to protect users and networks from cyberthreats.

Improves protection against zero-day threats

Enables inspection and analysis of potential or emerging threats without risk of infection, including malicious zero-day threats.

Protects remote or traveling users

Keeps remote workers and on-the-go employees secure, on or off company networks, regardless of location.

The competitive advantage

Integrated into our Avast Business Antivirus products, Sandbox is an easy-to-use, always-available tool that reduces risk to users, regardless of their location, by testing and analyzing suspicious files, applications, and URLs in a safe environment. Sandbox works alongside and shares its observations with our proprietary CyberCapture file scanning feature, enabling IT to better determine malicious and non-malicious behavior and continually improve threat protection.

Let's take a closer look at Sandbox.

What is Sandbox?

Sandbox provides a safe environment for opening suspicious files, running untrusted programs, or downloading URLs, without interfering or affecting the device. As an easy-to-use tool, it tests and categorizes software as "safe" or "unsafe," or tests code and applications before release. Sandbox allows IT to observe and analyze what potential malware is doing, gaining greater insights about new threats and vulnerabilities – without introducing risks to the network.

When is Sandbox used?

Sandbox can be used anytime, for any situation, to safely examine a file or code, while keeping it isolated from a PC and the company network.

How does Sandbox work?

Sandbox is pre-loaded in all Avast Business Antivirus products. It can be run on-demand or automatically. You can also specify certain applications that should always be deployed in Sandbox. To run Sandbox, simply right click the file or URL you wish to test and select 'Run in Sandbox' and then choose the menu option, 'Always run in Sandbox,' or 'Run a single instance of Sandbox.' This will open a file explorer and from there you can choose what you wish to run in the virtualized environment. Once the Sandbox mode starts, you will see details of anything currently running in the Sandbox. When running in Sandbox, an arrow will indicate that this is within the Sandbox environment.

Once you have completed testing in Sandbox mode, press 'Close All' to end the testing. Sandbox will be restored to its original state and any downloaded files or changed browser settings will be automatically deleted. After testing, if everything proves safe, you can move any file, application, or URL to a computer or device without introducing risk. Files identified as potential malware, or requiring additional analysis, are automatically sent to CyberCapture for in-depth analysis.

What is the difference between Sandbox and CyberCapture?

Sandbox has the ability run suspicious files in a safe virtual environment for initial testing and sends its findings to CyberCapture – a cloud-based file scanner feature in Avast Business Antivirus products. CyberCapture is designed to automatically detect and analyze rare, suspicious files and uses machine learning and behavior analytics to do a deeper analysis on potential malware. If malware is detected, CyberCapture quarantines and stops it so it can no longer execute on a user's system and infect the network.

What is unique about Sandbox?

Sandbox is integrated into our Avast Business Antivirus products for quick access and intuitive use. It provides a safe, effective, and affordable tool for testing in a virtual environment, protecting users across the entire network regardless of user location.

Users also benefit from the integrated technology and functionality of more than 13 Avast Business Antivirus features working together to detect and stop threats, continually making our endpoint protection solutions smarter.

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 delivers all-in-one cybersecurity solutions for today's modern workplace, providing total peace of mind. Avast provides integrated, 100% cloud-based endpoint and network security solutions for businesses and IT service providers. Backed by a globally dispersed threat detection network, the Avast Business security portfolio makes it easy and affordable to secure, manage, and monitor complex networks. Our easy-to-deploy cloud security solutions are built to offer maximum protection businesses can count on. For more information about our cloud-based cybersecurity solutions, visit **www.avast.com/business**.