What is a sandbox and how does it sandbox a program?

Many browsers today are designed to automatically run in their own sandbox without user settings.

Sand boxes created because playing with sand are very interesting, but we don't want it to follow from the yard to the house. If you've ever been on the beach, you'll know how much sand is and how hard it is to remove it. Then, the sand is in the hallway, in the laundry room and in your bathroom.

In the computer world, many similar problems exist with programs. Programs running on your computer share the resources of that computer. All your programs use the same static storage media as the drive, the same memory and a central processor (CPU). When common resources like these are shared, you may encounter problems. A program takes up your entire computer, because it writes data to all parts of the drive, accesses memory from all areas and sends requests to the CPU, along with all other programs. We keep the sand in the box just like the reason we sandbox computer programs: To place programs within the scope of management.

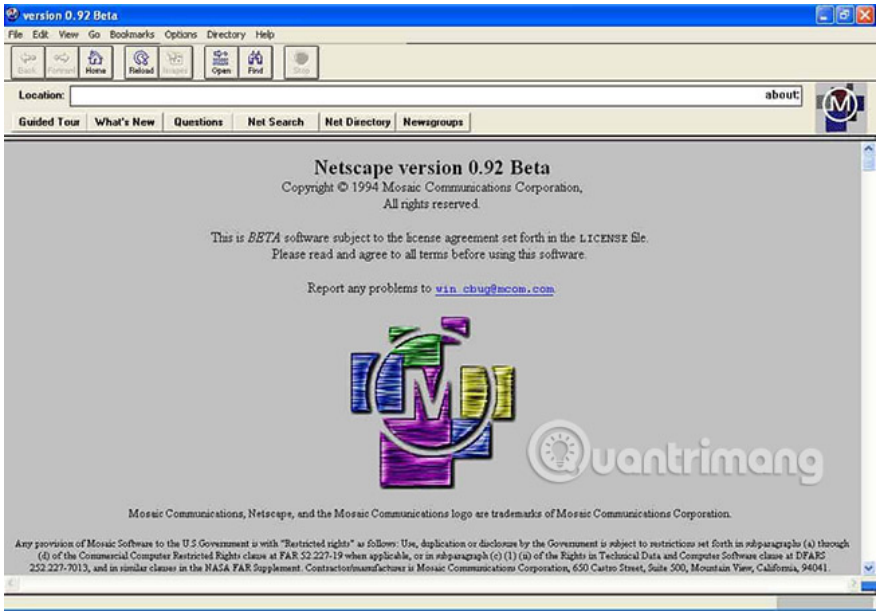
Basic computer design facilitates the sharing of this resource. By allowing programs to share resources, the computer seems to have many tasks and is doing a lot of work at the same time. This is exactly the kind of behavior we often require from computers, phones, tablets and smart watches for years. But these capabilities can cause unwanted side effects. Programs may perform poorly and fail or cause other programs to fail. They can rely on a number of other applications on the computer, applications that conflict with the needs of other programs, and more and more malicious programs try to access areas outside the limits to do so. bad things.

What is a sandbox and how does it sandbox a program?

1. Browser sandbox
2. Manual sandbox
    1. Virtual machine
    2. VirtualBox
    3. Parallels
    4. Sandboxie
    5. Qubes OS
3. Problems can occur with non-sandbox programs
    1. Programs conflict with each other
    2. Programs with different dependencies
    3. Malicious programs

Browser sandbox

The global network (www) was launched in 1989, and the first truly popular browser, Mosaic, brought the Internet into a popular culture. The web is designed to share documents, never designed to support what we have now: An Internet-based distribution system, where software runs on the cloud. The conflict between design and practical use has created numerous opportunities for bad guys, using web browsers as a mechanism for distributing malware.



The boundary between the end of the physical desktop and the starting point of the Internet is unclear. Most of the programs we run today are partly or entirely dependent on an Internet connection to work directly. With Internet connectivity constantly operating in the background, it is clear that the programs we use to access the Internet become a very attractive attack target. The first goal is the famous web browser. In fact, in 2016, Internet Sucuri security company eliminated more than half a billion malicious requests targeting websites and browsers over a 30-day period.

Because browsers are so rich and always turned on, they deserve special attention. Many browsers today are designed to automatically run in their own sandbox without user settings.

1. Google Chrome has been sandboxed from the beginning.
2. Mozilla Firefox takes longer to deploy the sandbox, but it is now almost 100% complete.
3. Internet Explorer introduced some sandbox levels in 2006 with IE 7 and Microsoft Edge sandbox all current processes.
4. Apple's Safari browser also runs web pages in separate processes.

If you are running a strange browser or want to be more separate between your operating system and browser, you can consider the manual sandbox options listed in the next section.

Manual sandbox

While browsers are a crucial weakness in any operating system, it doesn't mean they are the only weakness. Any application has the potential to be poisoned and therefore any computer can be enhanced by using the sandbox. Manual sandbox is the process of configuring your system, so that an application sandbox can be fully accessible

to your system.

1. 7 best Sandbox apps for Windows 10

Virtual machine

Desktop virtualization has come a long way in recent years and is now quite easy to install and use virtual machines. A virtual machine is as its name implies, is an unrealistic "machine". It is really just a software. The most common use of a virtual machine is to install a copy of the operating system on it and run that virtual machine on your computer, as if it were a physical machine. This type of operation provides a lot of useful things for security, because programs can only access resources within the virtual machine. If a malware infects your system, it will only be able to infect the virtual machine. This limits the negative effects it can cause. You can even run alternate operating systems in a virtual machine such as running a Linux distribution in a virtual machine on a Windows PC.

There are many virtualization applications, each targeting a specific type of use. The best and most popular desktop virtualization applications that users can handle are VirtualBox and Parallels.

Virtualization consists of two main parts. The term **'host'** refers to the actual physical computer running virtualization software. The term **'guest'** refers to the operating system running in the virtualized application.

VirtualBox

VirtualBox is owned by Oracle and has clients for all major operating systems. After installing VirtualBox, you can create a virtual machine using the **New** button **.** You will need to provide the means to install the operating system because VirtualBox does not come with that. Linux distributions that are easily found on the Internet, such as **distrowatch.com** and proprietary operating systems like Windows, will need a CD for easy installation.

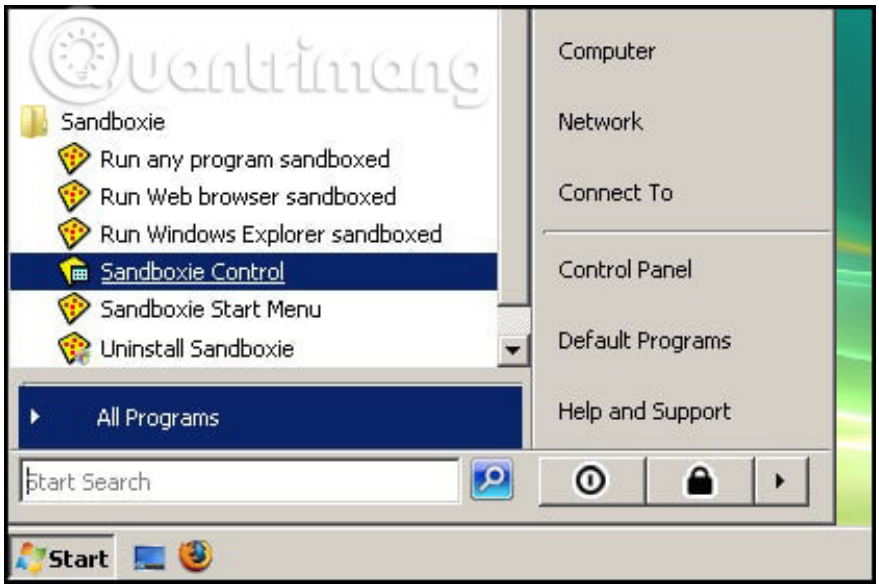
1. Installing Ubuntu in VirtualBox does not need DVD or USB

Parallels

Parallels is very similar to VirtualBox, but it only runs on macOS and is specifically built to run Windows in virtual machines. If you're looking for that combination (running Windows on your macOS desktop), Parallels might be the best solution for you. Parallels is not free, but there is a free 30-day trial package.

1. Install Windows on Mac with Parallels Desktop 9

Sandboxie

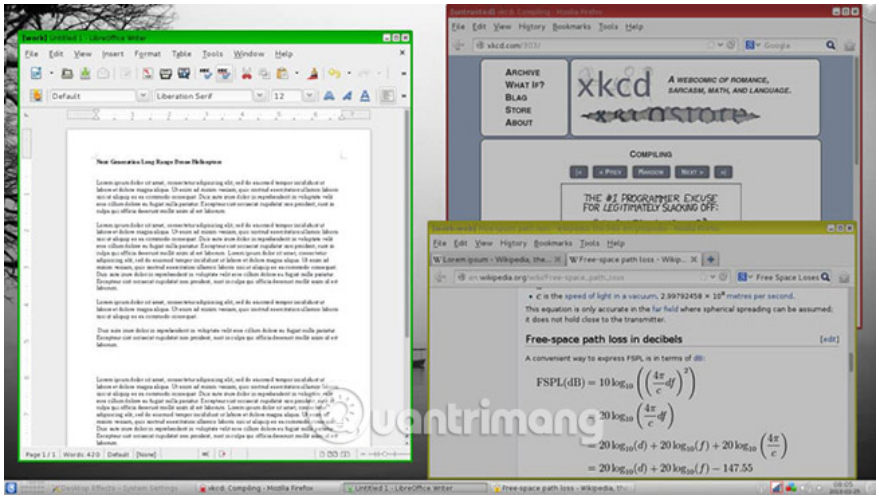


Sandboxie's motto is 'Trust No Program' (Don't believe any program). It only runs on Windows and requires programs to run separately from the underlying operating system. The Sandboxie control panel is used to specify specific programs that run in the sandbox. The biggest threat-prone programs, such as browsers and email programs, are listed as configuration options by default and other applications can be added as needed.

The data inside Sandboxie is destroyed when a sandbox is closed, but Sandboxie can be configured to keep important data unchanged. The folder containing the web browser's email and bookmarks is an example of the data that might exist when deleting the sandbox.

Sandboxie is designed for home users and is quite cheap.

Qubes OS



QubesOS (pronounced "Cubes") deserves a special candidate for virtualization. Qubes uses Xen hypervisor instead of VirtualBox. It launches several guest operating systems and each operating system separately. This allows individual sandbox applications, each in its own virtual machine, instead of having to sandbox the entire guest operating system. The special difference of QubesOS is that, Xen plays its own operating system, there is no 'host' operating system running behind it.

Taking the time to your system sandbox can create a solid defensive step against a variety of malware and help somewhat for software development. There cannot be a completely healthy Internet usage environment, but isolating your vulnerable applications may be helpful.

Problems can occur with non-sandbox programs

Programs conflict with each other

In the first days, the CPU distributed resources on a first come, first served basis. This is fine when our computers do not have to do many things, but today, more complex methods of resource allocation are used. The CPU drastically protects the boundaries of the resources they have allocated and, if a program tries to access unspecified resources, programs or other programs may fail.

Running a program in a sandbox allows the system to pre-allocate resources, such as memory and disk space, before the program requires anything. This ensures that the resources are available to the program whenever it needs it, and also ensures that no other program can use those resources.

Programs with different dependencies

Each program has several versions. Very few programs are perfect in all aspects when first released. That's why users must constantly update updates. Devices always inform users that updates need to be applied or new versions of the programs already available. It is important to allow these updates to take place as soon as possible, as many of these updates relate to security or performance issues. Turning off updates on updates often makes your device less secure and runs in a less-than-ideal state.

Below the main applications used and interactive every day is a set of assistance programs. These programs exist to help the main application run properly. We humans are rarely aware of these programs, but the main program cannot function without them. These help programs are called developer dependencies. Like any other program, these dependencies are constantly updated and changed. That's what makes things so complicated.

If a main program uses a specific function that the dependency itself has, but this dependency is upgraded and suddenly no longer functions, the main application will stop working. The main application does not get the expected results from that dependency. In many cases, the dependency error is so unexpected that the main application will immediately encounter an unexpected problem. The main application developer may not be alerted to changes to dependencies, so it is difficult to explain such situations and handle it skillfully.

Most programmers do their best to ensure backward compatibility, which means that even if the newer version of the application has no functionality in the past, it will still handle requests for functionality. that skillfully, so that other applications depend on it incessantly. However, some exceptions are notable as Java and Python are known to be very difficult to work on when upgrading. In the Linux world, the famous 'dependent hell' refers to the problems inherent with major system updates. In some cases, dependency programs have their own dependency levels, and they are not unprecedented in an upgrade situation, when it cannot meet all dependencies. For example, if the Puppy Vet Tracker program needs version 2.0 of some dependent programs, but the Daily Star Wars Quote program needs version 1.0 of the same dependency program, it cannot respond to that request. both programs.

Developers often encounter this problem and the sandbox is a way to solve it. Creating a sandbox and installing a Puppy Vet Tracker into it will allow the dependency program to be upgraded to version 2.0. The main computer system will still use version 1.0 of the dependent program, and so users can still receive their daily Star Wars quotes. Mutually beneficial.

Malicious programs

Consider a situation in which an application shares your computer with all other running programs. Some programs running on your computer may contain sensitive information. Perhaps you have legal documents, budget spreadsheets or password managers open and those applications are storing some data in memory. Existing malicious programs always probe around areas of the computer, where other programs are active, to see if any vulnerabilities can be found. In recent years, resource allocation has become better, so the program does not have to access data in specific designated areas, but hacking techniques, such as trying to read the memory assigned to the chapter submission, can still work.

The secret to successfully deleting data (deleting data from your system) is always based on tricking computer users into installing malware. This is usually done with social engineering or phishing techniques and can result in all files being stolen.

Sandbox programs can provide very powerful protection against malicious programs. When a program is sandboxed properly, it can only access the memory and disk space assigned to it. Therefore, opening sensitive documents in a sandbox will often prevent the possibility that malicious programs will attack them, because documents are not in the same memory space as malicious programs. It can be said that hackers who want to break into sandboxes share a common goal. That is to escape the virtual environment and this is considered a serious attack that Microsoft recently paid a sum of $ 105,000 to a group of white hat hackers who have demonstrated that this is possible when used. Edge browser.

See more:

1. Analyze Malware actions with the Joebox Online Sandbox
2. Answer these 5 questions before clicking on any link
3. Analyze Malware actions