

STU Tech • Blog • What is Sandboxing, And Why Do We Need It?

14 October 2022 • Admin

**Sandboxing in Cyber Security** refers to running software or accessing a file in an environment isolated from your computer system. Therefore, any malware won't harm your system. In this blog post, you will learn why we need **sandboxing**.

## Why is Sandboxing important?

Say you get an email with a PDF attachment. The sender is a stranger, however, you know that the PDF is crucial. In such cases, **sandboxing** may be the best choice. You can safely open the PDF in a sandbox and verify its credibility.

Cyber threats are increasing day by day. You may not know which software you can trust and which is safe. If you only allow trusted software and files to run on your system, your computer will be secure. However, often you may find the need to run untrusted software. And **sandboxing** cyber security tools allow you to run any file without worrying about their credibility.

Sandboxing cyber security tools are essential to protect your network from zero-day threats. Zero-day threats are threats you know nothing about before an attack.



## How is Sandbox implemented?

You can implement sandbox in different ways.

1. User-level isolation: the application inside the sandbox interacts with the environment with system calls. You can then specify the permitted system calls.
2. Sandboxed sandbox: each application gets a unique ID. That ID is the kernel's responsibility or the process level to ensure security between apps and the OS.
3. Isolated environment: the software components of the sandbox do not interact with the operating system. You can not access applications installed outside the sandbox. Moreover, all the changes are temporary.

## What are the different types of Sandboxing?

There are several types of **Sandboxing**.

**Full-System Emulation:** This **sandboxing** type simulates host machine's CPU and memory. The environment uses emulated devices.

**Integrated with Operating System:** The **sandboxing** security functionality is a part of the operating system. For example:

- Security, groups, and Linux namespaces from the kernel features in Linux for implementing **sandboxing**.
- Android uses a Linux user ID to implement complete application **sandboxing**.
- Apple App sandbox is available for Mac and required for all applications distributed via Mac Store.
- Windows has an in-built sandbox for process-level users.
- **Full Virtualization:** This sandbox type uses the same hardware without emulation. However, it creates barriers in the virtual environment, but these environments use the same physical devices.
- **Browser-Based:** You can run harmful apps online in a sandbox. The online website loads in a different environment in the Sandbox type. This way, you can secure your system from malicious code.

## Pros and Cons of Sandboxing

As with everything, **sandboxing** also has pros and cons. So let's look at **sandboxing's** pros and cons.

**Pros:**

- You can test new software in a controlled environment.
- Protects the system from malicious software.
- Restricts unauthorized access.
- You can safely visit any website using a browser-based sandbox.
- Cons:**
- People may become careless; it is not great as sandboxes have faults.
- There may be a security gap that malicious software can attack.
- Malicious programs can identify that it is a sandbox and take action if you trust it. Then they can harm your computer once you remove them from the sandbox.

## Sandboxing Use Cases

**Sandboxing** has mainly two uses: software testing and cybersecurity.

- **Software Testing:** Using a sandbox, you can safely test your application. It would be a controlled environment where you can negotiate any mistake. You can also run two incompatible programs in separate sandboxes.
- **Cyber Security:** As a sandbox is isolated or needs permissions to interact with the operating system, you can run suspicious programs in it. Additionally, you can research various malware in a sandbox. Understanding their vulnerabilities would be beneficial for learning how to detect them. Again, after creating an antimalware solution, you can test it in a sandbox. Therefore, a **sandbox in security** is essential.

## FAQ

What is an example of sandboxing?

An example of **sandboxing** would be running a virtual machine running a Linux operating system on Windows. The virtual machine will utilize the hardware of your computer. However, it will not have any direct access to it. But you can connect a USB drive directly to the virtual machine, bypassing the operating system. This way, you won't expose your OS to any harmful program on the USB drive.

Why is it called sandboxing?

**Sandboxing** comes from the practice of letting children play with sand in a box. You will then ensure that children don't make the house dirty. All the sand will remain in the box. And children can play with sand as long as they are in the box.

Is sandboxing a type of malware?

No, **sandboxing** is not a type of malware. On the contrary, it may protect you from malware. It is an environment where you can run software or access files without letting it affect the OS. That means you can test any suspicious program in a sandbox to ensure it's safe.

Why is sandboxing used?

**Sandboxing** enables users to run programs isolated from the operating system. There can be numerous reasons for using sandbox technology. For example, you may need to test two different, incompatible programs simultaneously. Or you may need to test a dangerous-looking file. You can also test changes in a sandbox before making them in the real world. This way, your errors won't affect your computer system.

What is sandboxing technology?

Sandboxing technology enables users to create a virtual environment separated from the OS. There are several ways to implement this. For example, the operating system's code may have some features that allow creating software in an isolated environment. Or you could use third-party **sandboxing** software. You may even have a complete virtual machine running a separate operating system.

## Leave a Reply

Your email address will not be published. Required fields are marked \*

☐ Show my name, email, and website in this browser for the next time I comment.

Search Here

## Categories

- > Network Integration (1)
- > Road Mapping as a Service (2)
- > Optical Fiber (2)
- > Optical Interconnect Technology (2)
- > RAN Service (2)
- > EdgeCloud Infrastructure Networks (2)
- > Access Cables (2)
- > Modern Network Infrastructures (2)
- > Fiber Deployment (2)
- > EdgeClouds (2)
- > 5G Technologies (2)
- > Network Services and Infrastructures (2)
- > Data Center Networks (2)
- > Fiber (1)
- > Edge Data Centers (1)
- > Cyber Security (2)
- > Cloud Migration (1)
- > Cloud Managed Services (1)
- > Connectivity and Optical Interconnect (1)
- > Digital Transformation (1)
- > 4G/5G Service Management (1)
- > Network Software Products (2)
- > Customer Management (2)
- > Optical Fiber Splicing (2)
- > STU Stories (1)
- > SD-WAN Technology (2)
- > SD-OT Technology (2)
- > Access Technologies (2)
- > SD-WAN - SD-WAN Network Management Software (2)
- > Culture with Real STU (2)
- > CSPs - Communications Service Providers (1)
- > CSP Sustainability Culture and Life at STU (1)
- > Data Center and Analytics (1)
- > Internet and IT Infrastructure (2)
- > Fiber Deployment and Implementation (1)
- > Managed Services (2)
- > OGC - Optical Fiber Cables (2)
- > Other Topics (2)

## Recent Post



**The Evolution of Edge Technologies in Data Centers**

August 5, 2022

[Read More >](#)



**An Overview of Network Services**

August 5, 2022

[Read More >](#)



**A Look at Modern Data Center Design and Architecture**

August 5, 2022

[Read More >](#)



**The Evolution of Edge Technologies in Data Centers**

August 5, 2022

[Read More >](#)

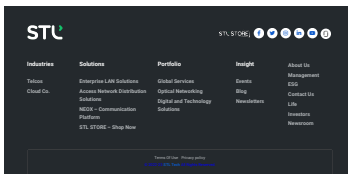


**An Overview of Network Services**

August 5, 2022

[Read More >](#)

## Latest Blogs



STU Tech • Blog • What is Sandboxing, And Why Do We Need It?

14 October 2022 • Admin

**Sandboxing in Cyber Security** refers to running software or accessing a file in an environment isolated from your computer system. Therefore, any malware won't harm your system. In this blog post, you will learn why we need **sandboxing**.

**Why is Sandboxing important?**

Say you get an email with a PDF attachment. The sender is a stranger, however, you know that the PDF is crucial. In such cases, **sandboxing** may be the best choice. You can safely open the PDF in a sandbox and verify its credibility.

Cyber threats are increasing day by day. You may not know which software you can trust and which is safe. If you only allow trusted software and files to run on your system, your computer will be secure. However, often you may find the need to run untrusted software. And **sandboxing** cyber security tools allow you to run any file without worrying about their credibility.

Sandboxing cyber security tools are essential to protect your network from zero-day threats. Zero-day threats are threats you know nothing about before an attack.

Importance of Sandboxing

How is Sandbox implemented?

You can implement sandbox in different ways.

1. User-level isolation: the application inside the sandbox interacts with the environment with system calls. You can then specify the permitted system calls.

2. Sandboxed sandbox: each application gets a unique ID. That ID is the kernel's responsibility or the process level to ensure security between apps and the OS.

3. Isolated environment: the software components of the sandbox do not interact with the operating system. You can not access applications installed outside the sandbox. Moreover, all the changes are temporary.

What are the different types of Sandboxing?

There are several types of Sandboxing.

Full-System Emulation: This sandboxing type simulates host machine's CPU and memory. The environment uses emulated devices.

Integrated with Operating System: The sandboxing security functionality is a part of the operating system. For example:

Security, groups, and Linux namespaces from the kernel features in Linux for implementing sandboxing.

Android uses a Linux user ID to implement complete application sandboxing.

Apple App sandbox is available for Mac and required for all applications distributed via Mac Store.

Windows has an in-built sandbox for process-level users.

Full Virtualization: This sandbox type uses the same hardware without emulation. However, it creates barriers in the virtual environment, but these environments use the same physical devices.

Browser-Based: You can run harmful apps online in a sandbox. The online website loads in a different environment in the Sandbox type. This way, you can secure your system from malicious code.

Pros and Cons of Sandboxing

As with everything, sandboxing also has pros and cons. So let's look at sandboxing's pros and cons.

Pros:

You can test new software in a controlled environment.

Protects the system from malicious software.

Restricts unauthorized access.

You can safely visit any website using a browser-based sandbox.

Cons:

People may become careless; it is not great as sandboxes have faults.

There may be a security gap that malicious software can attack.

Malicious programs can identify that it is a sandbox and take action if you trust it. Then they can harm your computer once you remove them from the sandbox.

Sandboxing Use Cases

Sandboxing has mainly two uses: software testing and cybersecurity.

Software Testing: Using a sandbox, you can safely test your application. It would be a controlled environment where you can negotiate any mistake. You can also run two incompatible programs in separate sandboxes.

Cyber Security: As a sandbox is isolated or needs permissions to interact with the operating system, you can run suspicious programs in it. Additionally, you can research various malware in a sandbox. Understanding their vulnerabilities would be beneficial for learning how to detect them. Again, after creating an antimalware solution, you can test it in a sandbox. Therefore, a sandbox in security is essential.

FAQ

What is an example of sandboxing?

An example of sandboxing would be running a virtual machine running a Linux operating system on Windows. The virtual machine will utilize the hardware of your computer. However, it will not have any direct access to it. But you can connect a USB drive directly to the virtual machine, bypassing the operating system. This way, you won't expose your OS to any harmful program on the USB drive.

Why is it called sandboxing?

Sandboxing comes from the practice of letting children play with sand in a box. You will then ensure that children don't make the house dirty. All the sand will remain in the box. And children can play with sand as long as they are in the box.

Is sandboxing a type of malware?

No, sandboxing is not a type of malware. On the contrary, it may protect you from malware. It is an environment where you can run software or access files without letting it affect the OS. That means you can test any suspicious program in a sandbox to ensure it's safe.

Why is sandboxing used?

Sandboxing enables users to run programs isolated from the operating system. There can be numerous reasons for using sandbox technology. For example, you may need to test two different, incompatible programs simultaneously. Or you may need to test a dangerous-looking file. You can also test changes in a sandbox before making them in the real world. This way, your errors won't affect your computer system.

What is sandboxing technology?

Sandboxing technology enables users to create a virtual environment separated from the OS. There are several ways to implement this. For example, the operating system's code may have some features that allow creating software in an isolated environment. Or you could use third-party sandboxing software. You may even have a complete virtual machine running a separate operating system.

Leave a Reply

Your email address will not be published. Required fields are marked \*

Enter Name Enter Email

Enter Message

Show my name, email, and website in this browser for the next time I comment.

Enter Your Comments

Post Comment

Search Here

Search

Categories

Network Integration (1)

Road Mapping as a Service (2)

Optical Fiber (2)

Optical Interconnect Technology (2)

RAN Service (2)

EdgeCloud Infrastructure Networks (2)

Access Cables (2)

Modern Network Infrastructures (2)

Fiber Deployment (2)

EdgeClouds (2)

5G Technologies (2)

Network Services and Infrastructures (2)

Data Center Networks (2)

Fiber (1)

Edge Data Centers (1)

Cyber Security (2)

Cloud Migration (1)

Cloud Managed Services (1)

Connectivity and Optical Interconnect (1)

Digital Transformation (1)

4G/5G Service Management (1)

Network Software Products (2)

Customer Management (2)

Optical Fiber Splicing (2)

STU Stories (1)

SD-WAN Technology (2)

SD-OT Technology (2)

Access Technologies (2)

SD-WAN - SD-WAN Network Management Software (2)

Culture with Real STU (2)

CSPs - Communications Service Providers (1)

CSP Sustainability Culture and Life at STU (1)

Data Center and Analytics (1)

Internet and IT Infrastructure (2)

Fiber Deployment and Implementation (1)

Managed Services (2)

OGC - Optical Fiber Cables (2)

Other Topics (2)

Recent Post

The Evolution of Edge Technologies in Data Centers

August 5, 2022

Read More >

An Overview of Network Services

August 5, 2022

Read More >

A Look at Modern Data Center Design and Architecture

August 5, 2022

Read More >

The Evolution of Edge Technologies in Data Centers

August 5, 2022

Read More >

An Overview of Network Services

August 5, 2022

Read More >

A Look at Modern Data Center Design and Architecture

August 5, 2022

Read More >

STU Tech • Blog • What is Sandboxing, And Why Do We Need It?

14 October 2022 • Admin

Sandboxing in Cyber Security refers to running software or accessing a file in an environment isolated from your computer system. Therefore, any malware won't harm your system. In this blog post, you will learn why we need sandboxing.

Why is Sandboxing important?

Say you get an email with a PDF attachment. The sender is a stranger, however, you know that the PDF is crucial. In such cases, sandboxing may be the best choice. You can safely open the PDF in a sandbox and verify its credibility.

Cyber threats are increasing day by day. You may not know which software you can trust and which is safe. If you only allow trusted software and files to run on your system, your computer will be secure. However, often you may find the need to run untrusted software. And sandboxing cyber security tools allow you to run any file without worrying about their credibility.

Sandboxing cyber security tools are essential to protect your network from zero-day threats. Zero-day threats are threats you know nothing about before an attack.