**Reference:** [**https://www.techopedia.com/**](https://www.techopedia.com/)

[**https://www.hysolate.com/**](https://www.hysolate.com/)

**OS Security. Antiviruses**

## What Does Operating System Security (OS Security) Mean?

Operating system security (OS security) is the process of ensuring OS integrity, confidentiality and availability.  
  
OS security refers to specified steps or measures used to protect the OS from threats, viruses, worms, malware or remote hacker intrusions. OS security encompasses all preventive-control techniques, which safeguard any computer assets capable of being stolen, edited or deleted if OS security is compromised.

OS security encompasses many different techniques and methods which ensure safety from threats and attacks. OS security allows different applications and programs to perform required tasks and stop unauthorized interference.  
  
OS security may be approached in many ways, including adherence to the following:

* Performing regular OS patch updates
* Installing updated antivirus engines and software
* Scrutinizing all incoming and outgoing network traffic through a firewall
* Creating secure accounts with required privileges only (i.e., user management)

## What are Common OS Security Threats?

Here are a few of the most common threat vectors that can affect an operating system.

### Malware

Malware is short for malicious software, which encompasses a range of attack vectors such as viruses, worms, trojans, and rootkits. Malware is injected into a system without the owner’s consent, or by masquerading as legitimate software, with the objective of stealing, destroying or corrupting data, or compromising the device.

Malware can also replicate, allowing it to spread further in a corporate network and beyond. Malware attacks often go undetected by the target user, allowing for the quiet extraction of sensitive data. In other cases attackers silently “herd” compromised devices into botnets and use them for criminal activities such as distributed denial of services (DDoS) attacks.

### Denial of Service Attacks

A Denial of Service (DoS) attack is intended to clog a system with fake requests so it becomes overloaded, and eventually stops serving legitimate requests. Some DoS attacks, in addition to overwhelming a system’s resources, can cause damage to the underlying infrastructure.

Modern DoS attacks are waged by a distributed network of thousands or millions of bots (automated agents)—this is known as distributed denial of service (DDoS), and can be extremely difficult to mitigate due to its huge scale.

An example of a DoS attack is the repeated use of system requests in a tight loop, or a “syn flood” in which the attacker sends a large number of network requests, requiring the server to acknowledge each one, and exhausting its resources.

### Network Intrusion

Network intrusion occurs when an individual gains access to a system for improper use. There are several types of network intrusion depending on the type of intruder:

* Careless insiders—authorized users who neglect to follow security policies or best practices, causing exposure of sensitive assets.
* Malicious insiders—authorized users who misuse their privileges for malicious indigence.
* Masqueraders—external individuals who pose as legitimate users, exploiting the account or credentials of an authorized user to gain access to the system.
* Clandestine users—attackers who penetrate the system by gaining supervisory control and going around access controls.

### Buffer Overflow

The main function of a buffer is to temporarily store data. Each buffer has a capacity of data it can hold. During a buffer overflow attack, the buffer or other temporary data stores are overflowing with data. When the buffer overflows, the program attempting to write the data may overwrite other memory locations containing important information.

Threat actors look for buffer overflow vulnerabilities, which they can exploit to inject scripts that help them hijack the system or crash it.

## How Can You Ensure Operating System Security?

Here are a few ways you can improve operating system security in your organization.

### Authentication Measures

Authentication involves matching an identified user with the programs or data they are allowed to access. All operating systems have controls that can be used to verify that users who run a particular program are authorized to do so.

You can use the following techniques to authenticate users at the operating system level:

* + Security keys: keys are provided by a key generator, usually in the form of a physical dongle. The user must insert the key into a slot in the machine to log in.
  + Username-password combinations: The user enters a username that is registered with the OS, along with a matching password.
  + Biometric signatures: The user scans a physical attribute, such as a fingerprint or retina, to identify themselves.
* Multi-factor authentication: Modern authentication systems use multiple methods to identify a user, combining something the user knows (credentials), something they own (such as a mobile device), and/or a physical characteristic (biometrics).

### Using One-Time Passwords

One-time passwords offer an additional layer of security when combined with standard authentication measures. Users must enter a unique password generated each time they log in to the system. A one-time password cannot be reused.

Examples of one-time passwords include:

* Network passwords: An application sends a one-time password to the users via a registered email address or mobile phone number. The user must enter this password to log in to the computer.
* Random numbers: The user receives a card with listing numbers that correspond to matching letters. The OS requires the user to enter the numbers that match a set of randomly generated letters.
* Secret keys: The user receives a device that generates secret keys. The user then enters the secret key into the OS system, which identifies the user credentials associated with the key.

### Virtualization

Virtualization enables you to abstract software from hardware, effectively separating the two. The main advantage of virtualization is that it introduces a high level of efficiency and flexibility, while providing greater security coverage. There are many types of virtualization, including desktop, application, network, server, storage, and OS virtualization.

What is OS virtualization?

OS virtualization enables you to multiple isolated user environments using the same OS kernel. The technology that creates and enables this type of isolation is called a “hypervisor”, which serves as a layer located between the device and the virtualized resources.

The hypervisor manages the virtual machines (VM) running on the device (typically 2-3 Vms). Each VM is used for each user or each security zone. There are several types of VMs that can run alongside each other. Here are the three main categories:

**Fully locked-down VM**

Should be used to provide access to sensitive data and corporate systems, such as IT environments, payment systems, and sensitive customer data.

**Unlocked, open VM**

Should be used to provide unrestricted access to non-corporate resources. For example, full web browsing sessions, installation of applications, and use of external devices.

**Semi-locked-down VM**

Should be used to provide access to standard corporate applications and resources, such as office documents, company email, and internal services.

Advantages of OS virtualization

Each type of VM is limited to the actions allowed by design. Any further action is restricted. This keeps the environment secure. The hypervisor runs below the OS of the device and splits the device into multiple VMs running locally with their own OS—effectively isolating users.

Because the users are isolated, the devices remain secure. This ensures that employees and third parties can gain access to company resources without endangering company resources.

Another major advantage of OS virtualization is that none of the virtualized environments can directly access the network. Instead, connectivity is enabled via an invisible, virtualized network layer that implements network segmentation directly on the endpoint device.

## Testing and Validating Operating System Security

Securing an operating system or any software is an ongoing process that requires constant testing. Depending on the risk and priority of a system, security posture tests may take place on a monthly, weekly or daily basis. Here are a few testing methods you can use.

### Vulnerability Assessment

Vulnerability assessment involves testing for weaknesses that may be lying undetected in an operating system. Identifying vulnerabilities allows you to identify possible vectors for an attack so you can better understand the risk to your system.

As part of a continuous process, vulnerability assessment attempts to stay on top of newly exposed vulnerabilities by locating, classifying and prioritizing them according to severity and impact. This process usually combines manual tasks with automated tools.

The following are some of the typical methods used for OS vulnerability assessment:

* Scanning for known vulnerabilities
* Scanning the software and applications on an operating system
* Scanning for malware
* Scanning for missing patches and updates
* Patch testing
* Port scanning

### Penetration Testing

Penetration testing, or pentesting, is a security assessment strategy that uses vulnerability assessment to identify how an attacker may successfully exploit vulnerabilities in the system. The penetration testing method involves simulating an exploit to evaluate system security.

Penetration testing helps discover vulnerabilities beyond the obvious, and seeks to identify the methods an attacker may use to exploit them. Security teams can leverage the insights provided by pentesting to put in place effective security measures.

There are three types of penetration testing, each of which provides different types of insights into operating system security and potential for exploitation:

* White Box: The penetration tester has full technical knowledge of the system being tested.
* Grey Box: The pentester has limited technical knowledge of the system being tested.
* Black Box: The pentester doesn’t have any prior technical knowledge of the system being tested.

## Antiviruses

An antivirus product is a program designed to detect and remove viruses and other kinds of malicious software from your computer or laptop.

Malicious software - known as malware - is code that can harm your computers and laptops, and the data on them. Your devices can become infected by inadvertently downloading malware that's in an attachment linked to a dubious email, or hidden on a USB drive, or even by simply visiting a dodgy website.

Once it's on your computer or laptop, malware can steal your data, encrypt it so you can't access it, or even erase it completely. For this reason it's important that you always use antivirus software, and keep it up to date to protect your data and devices.

Several different companies build antivirus software and what each offer can vary but all perform some essential functions:

* Scan specific files or directories for any malware or known malicious patterns
* Allow you to schedule scans to automatically run for you
* Allow you to initiate a scan of a particular file or your entire computer, or of a CD or flash drive at any time.
* Remove any malicious code detected –sometimes you will be notified of an infection and asked if you want to clean the file, other programs will automatically do this behind the scenes.
* Show you the ‘health’ of your computer