Learn 10 Critical Steps to Protect your Servers

Global Institute of Technology

Contents

Is security real?

Information is like gold nowadays, and hackers are gold miners. Because of the vital role they play, servers keep confidential company data and information.

An unsecured server is vulnerable to all kinds of threats and data breaches.

Security vulnerabilities can lead to loss of complex data or loss of ability and control that could affect the entire organization.
f you do not protect your servers, you are on a dangerous path as personal information such as bank accounts, contact information, or social security may be compromised.

If you do not know how to protect your servers, this article describes some of the server security tips you can use to protect your servers.

Establish and Use a Secure Connection

When connecting to a remote server, it is essential to establish a secure channel for communication. The best way to do this is to use the SSH (Secure Shell) protocol. Unlike a previously used telnet, SSH access encrypts all data transmitted over the transmission.

You must install the SSH daemon and have an SSH client, on which you can issue commands and manage servers to gain remote access using the SSH protocol.

By default, SSH uses port 22. Everyone knows this, including hackers. Most people do not construct this minor detail. However, changing the port number is a simple way to reduce the chances of hackers attacking your server. Therefore, SSH's best practice is to use port numbers from 1024 to 32,767.

SSH (Secure Shell) Protocol

The secure shell, sometimes referred to as the secure socket shell, is a protocol that allows you to securely connect to a remote computer or server using a text-based interface.

Once the secure SSH connection is established, the shell session will start, and you can manipulate the server by typing commands into the client on your local computer.

Computer and network administrators use this protocol extensively, as well as anyone who needs to manage the computer remotely in a more secure manner.

To test if a client is available on your Linux based system, you must:

1. Load an SSH terminal. You can search for "terminal" or press CTRL + ALT + T on your keyboard.
2. Type Ssh and press Enter on the terminal.
3. If the client is installed, you will receive an answer like:

```
username@host:~$ ssh

usage: ssh [-1246AaCfGgKkMNnqsTtVvXxYy] [-b bind_address]
[-c cipher_spec]
```

```
[-D [bind_address:]port] [-E log_file] [-e escape_char]
[-F configfile] [-I pkcs11] [-i identity_file]
[-J [user@]host[:port]] [-L address] [-l login_name] [-m mac_spec] [-
O ctl_cmd] [-o option] [-p port] [-Q query_option] [-R address] [-S
ctl_path] [-W host:port] [-w local_tun[:remote_tun]]
[user@]hostname [command]


username@host:~$
```

Telnet

Telnet is vulnerable to cybersecurity attacks because it does not have encryption methods compared to modern SSH.

What is Telnet?

Telnet is a client-server protocol that precedes the TCP protocol. Network protocol allows a user to sign in to another computer on the same network over a TCP / IP connection.

The client machine that runs the telnet client connects to a CLI on the remote device, usually a dedicated platform.

Telnet is lightweight and fast, making it a preferred option in some application cases:

- Initial network hardware configuration.
- Remote access to trusted internal networks.
- Test for open or used ports.
- Adjust mail and web servers.
- Checks port sharing.

How Does Telnet Work?

The telnet protocol creates a communication path through a virtual terminal connection. Distributes data in-band with telnet control information over the Transmission Control Protocol (TCP).

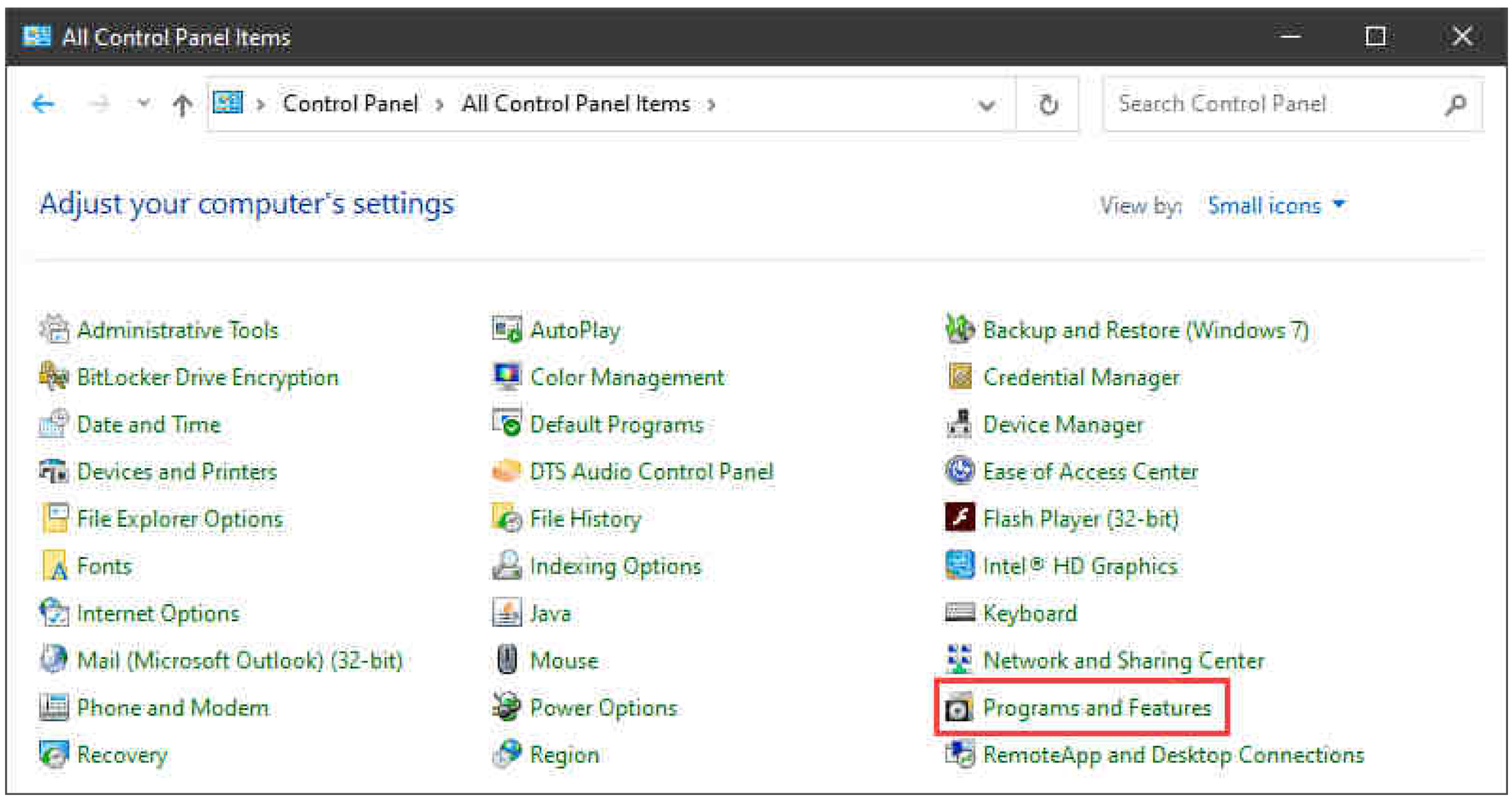
Unlike other TCP / IP protocols, telnet provides a sign-in screen and allows you to log in as the actual user of the remote device when establishing a connection on port 23. This type of access provides direct control with all privileges such as the holder of credentials.

Telnet comes with a command that can be accessed from the command line in Windows. The telnet command is also available for MacOS and Linux operating systems.

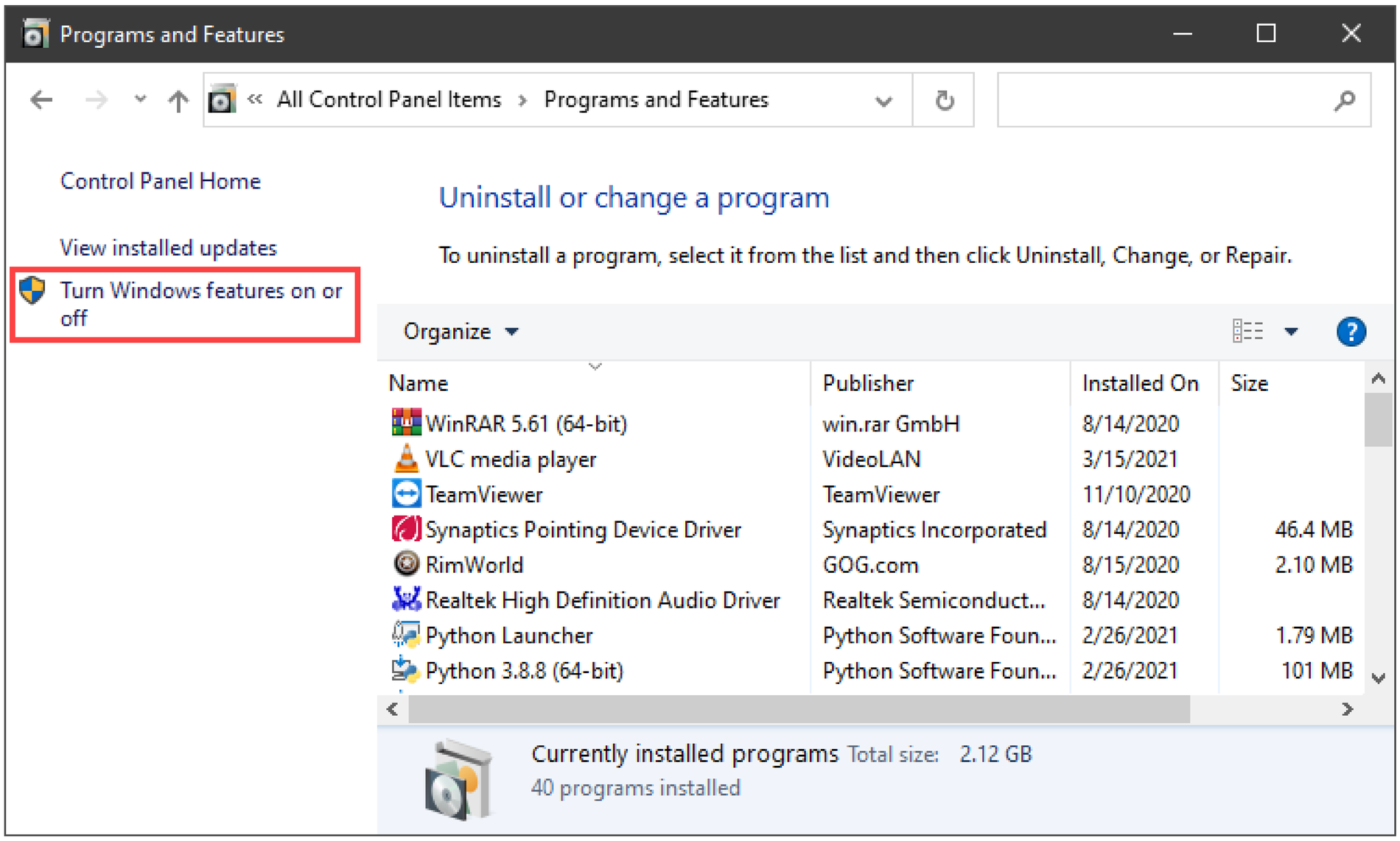
How to Enable Telnet on Windows 10?

Option 1: Enable Telnet using GUI

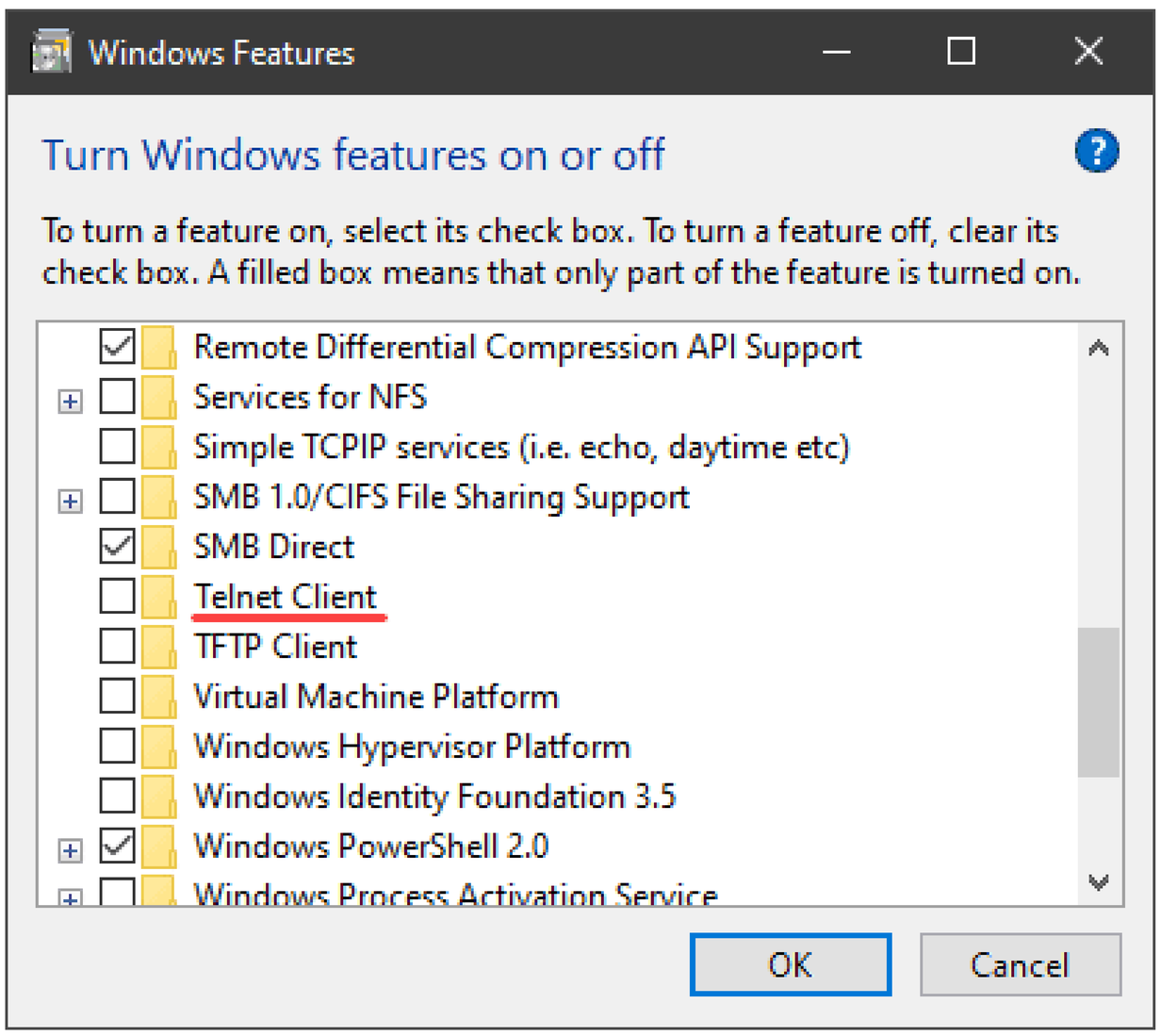
1. Open the Programs and Features options in Control Panel:



2. Click the Turn Windows features on or off setting:



3. Locate the Telnet Client option on the list, select it and click OK to install the feature:



4. When Windows completes the requested change, click Close.

5. Open the command prompt and run telnet to open the Microsoft Telnet Client:

```
Welcome to Microsoft Telnet Client

Escape Character is 'CTRL+]'

Microsoft Telnet>
```

Option 2: Enable Telnet Using Command Prompt

1. In the command prompt, run:

   pkgmgr /iu:"TelnetClient"

2. Restart the command prompt and run telnet to open the Microsoft Telnet Client.

3. Run quit to exit the client:

```
Welcome to Microsoft Telnet Client

Escape Character is 'CTRL+]'

Microsoft Telnet> quit

C:\Users\User>
```

Use SSH Keys Authentication

Instead of a password, you can authenticate an SSH server using a pair of SSH keys, a better alternative to traditional logins. The keys carry many more bits than a password and are not easily cracked by most modern computers. The popular RSA 2048-bit encryption is equivalent to a 617-digit password.

The key pair consists of a public key and a private key.

The public key has several copies, one of which remains on the server, while others are shared with users. Anyone that has the public key has the power to encrypt data, while only the user with the corresponding private key can read this data. The private key is not shared with anyone and must be kept secure. When establishing a connection, the server asks for evidence that the user has the private key, before allowing privileged access.

Authenticate an SSH server using a pair of SSH keys

Set up your first SSH keys :

Use SSH keys for authentication when connecting with your server or between your servers. They can greatly simplify and enhance the security of your login process. When the keys are activated properly they provide a secure, fast and easy way to access your cloud server.

Follow our guide and learn how to set up your first SSH keys for authentication using OpenSSH.

1. Create a new key pair on a terminal with the next command

The key generator prompts for the location where the key is stored and the file name. Enter a new name or use the default by pressing Enter.

```
ssh-keygen -t rsa
```

2. Create a password for the key when prompted (optional)

This is a simple password that will protect your private key if it gets into the hands of anyone. Enter the password you want or proceed without a password. Press Enter twice. Note that some automation tools cannot open password-protected private keys.

3. Copy the public part of the key pair to your cloud server using the following command

Replace username and server with the server address where you want to use your username and key authentication.

```
ssh-copy-id -i ~/.ssh/id_rsa.pub user@server
```

Enter your user account password for that SSH server when prompted.

You can now authenticate your server with the key pair, but this time you will need to enter the password each time you connect.

4. Set SSH Agent to save keys to avoid re-entering passwords for each login (optional)

Enter the following commands and enter the private SSH key to start the agent.

```
ssh-agent $BASH
ssh-add ~/.ssh/id_rsa
```

Type the current password of your key when prompted. If you have saved a private key somewhere other than the default location and name, you must specify it when adding the key.

Then, you can connect to your cloud server using the authentication keys and open the key by repeating the last 2 steps once for each system restart.

Privileged access

In this article, you will learn what privileged access management is by implementing PAM and how to manage security risks.

What is Privileged Access Management?

Privileged access management implements at least privileged policies. It empowers companies to reduce the threat of security attacks and data breaches.

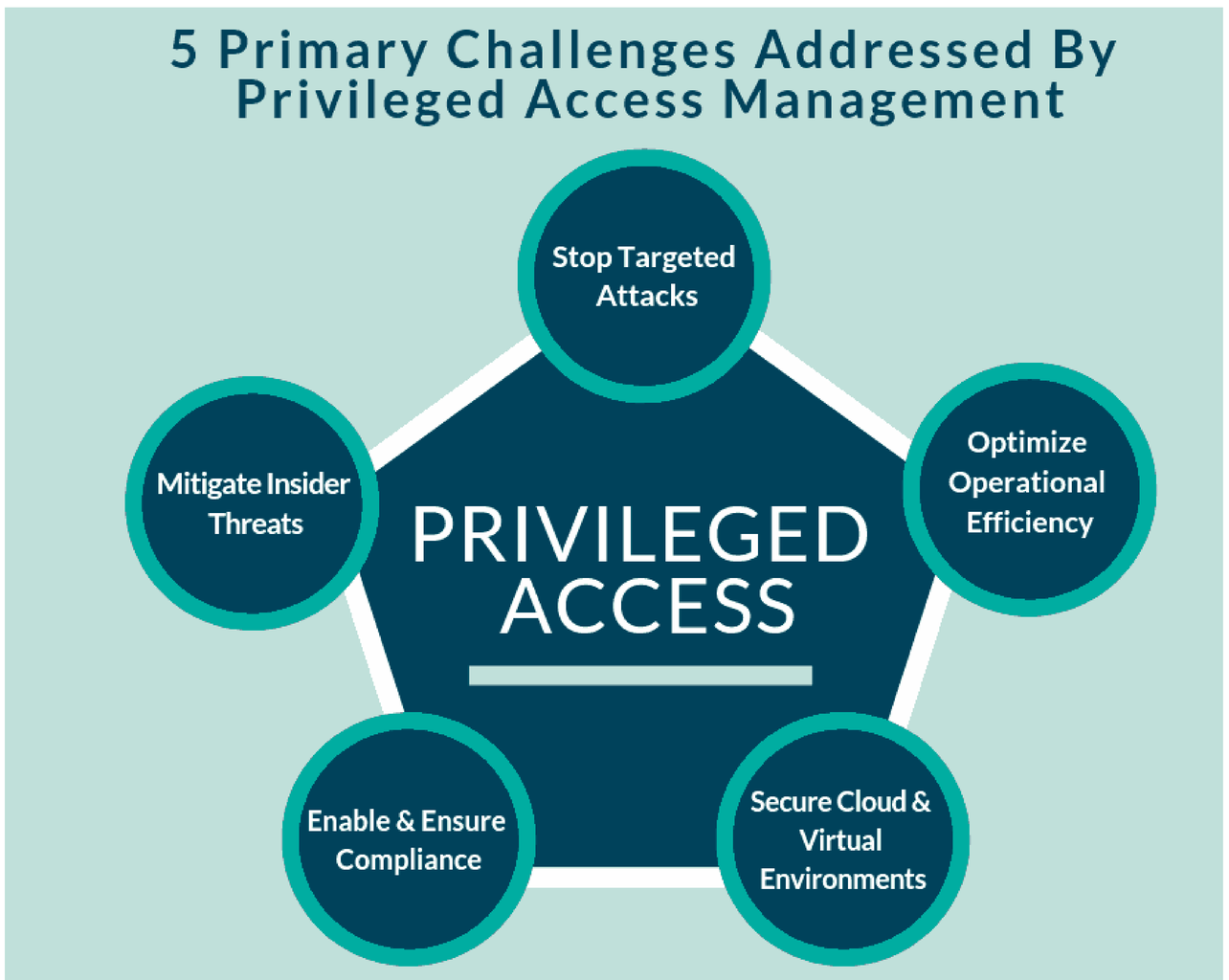
Privileged Access Management is often referred to as "Privilege Session Management" or "Privileged Account Management".

Privileged security provides the power to protect your data and information technology systems.

PAM acts as a secure repository or repository that protects your data and networks. With privileged user management, users can access only the data required for their work. ID groups set these parameters. This prevents users from accessing other systems and information.

A business can assign unauthorized access to another employee’s funds to the company. Another employee may be involved in installing the software.

For example, a business may have one or two employees with administrator access to the Microsoft Exchange server. Setting up email security protocols is achieved through administrator access. Only those users can delete the email account or set up a new one.



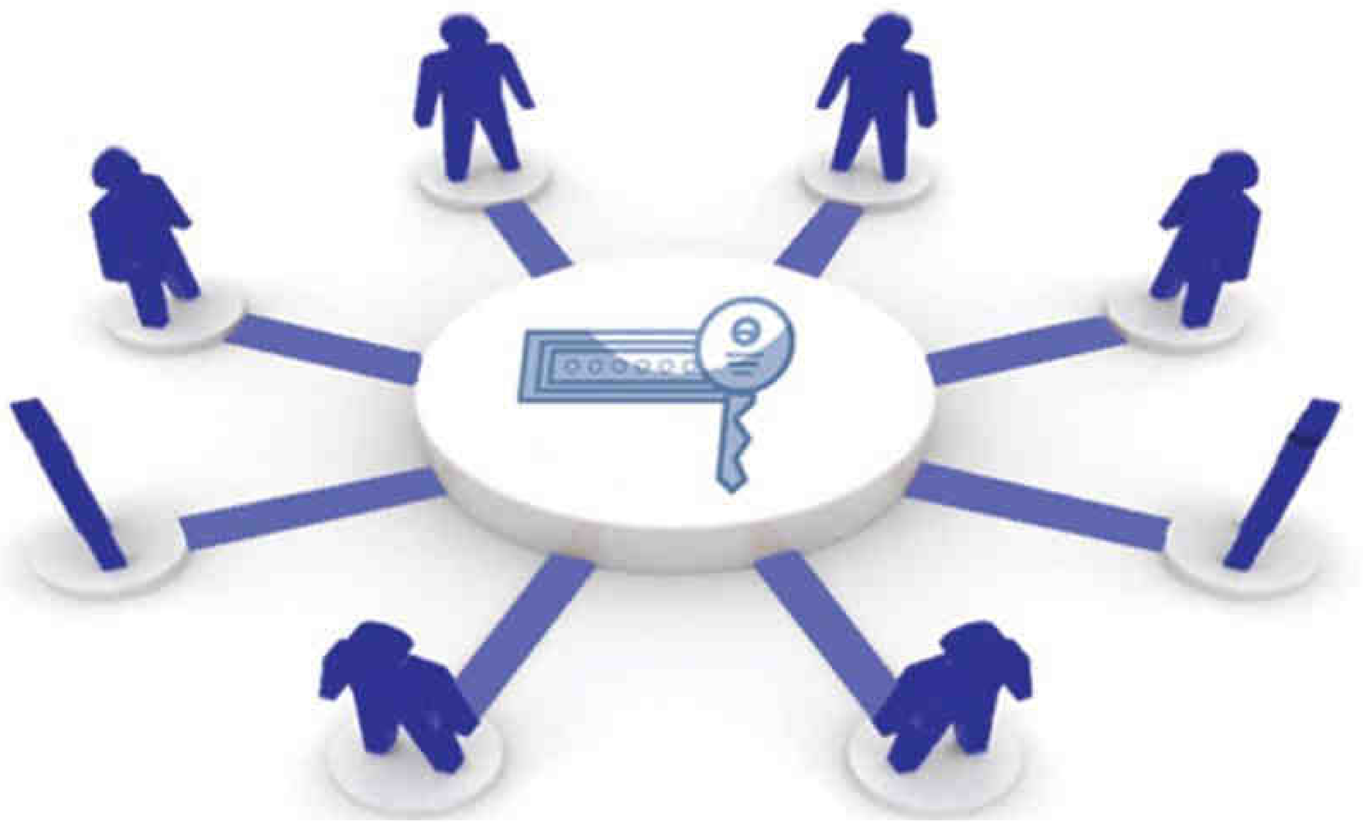
Benefits of Privileged Access Security

- Many companies are concerned about data security. Cybercrime cost businesses more than $ 600 billion last year.

- In the past, companies have had limited success in increasing cybersecurity. To succeed in preventing cyber attacks, a company must have a central strategy to protect vital systems. They need real-time network control.

- PAM Security provides a single management solution for many cybersecurity needs. It protects complex systems. This restricts access to your data. This gives you a more secure solution for storing and accessing credentials. This provides security without deceiving employees.

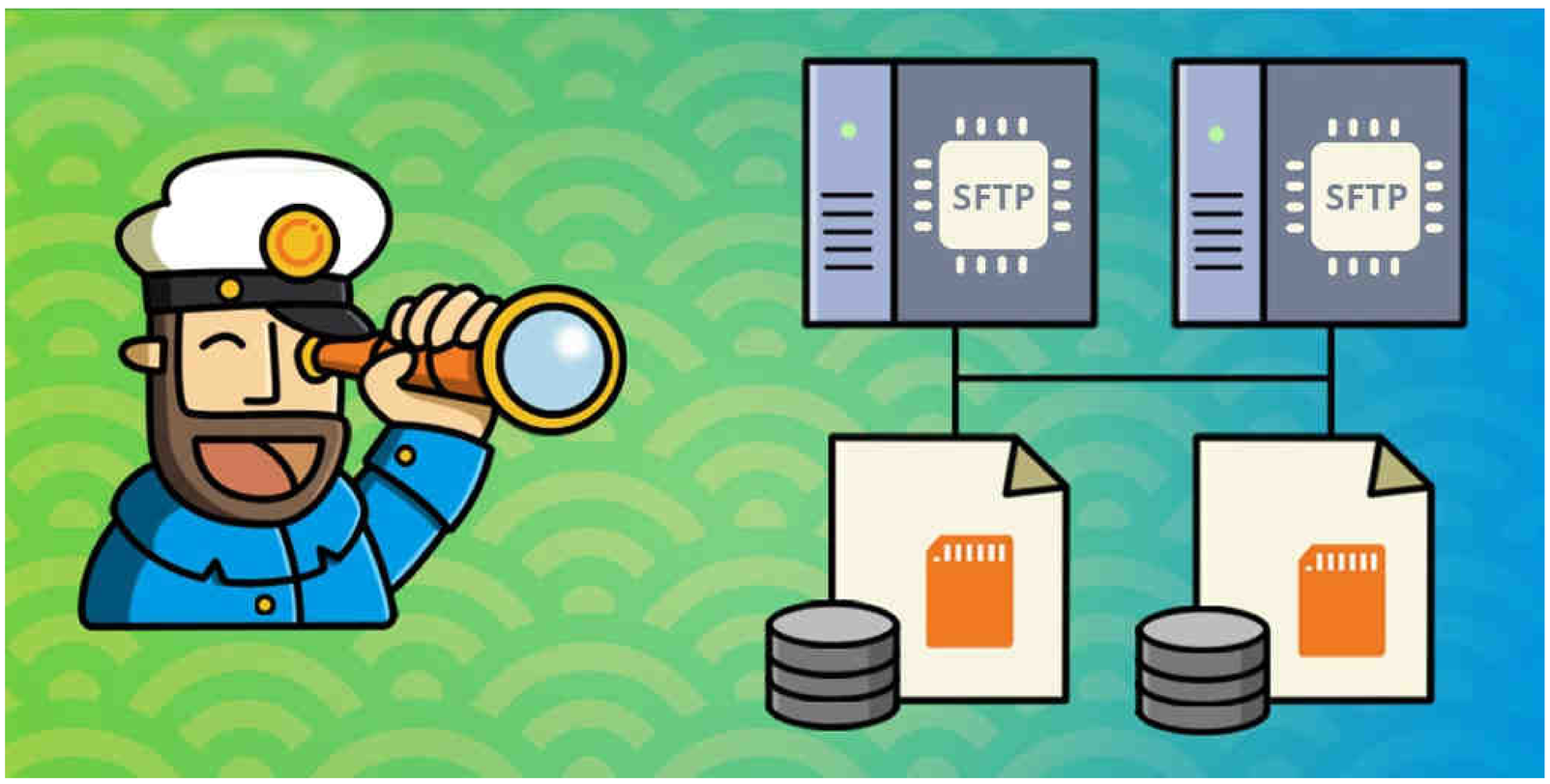
- Businesses use PAM to reduce the risk of data breaches. This increases security and restricts access to key systems.



Secure File Transfer Protocol

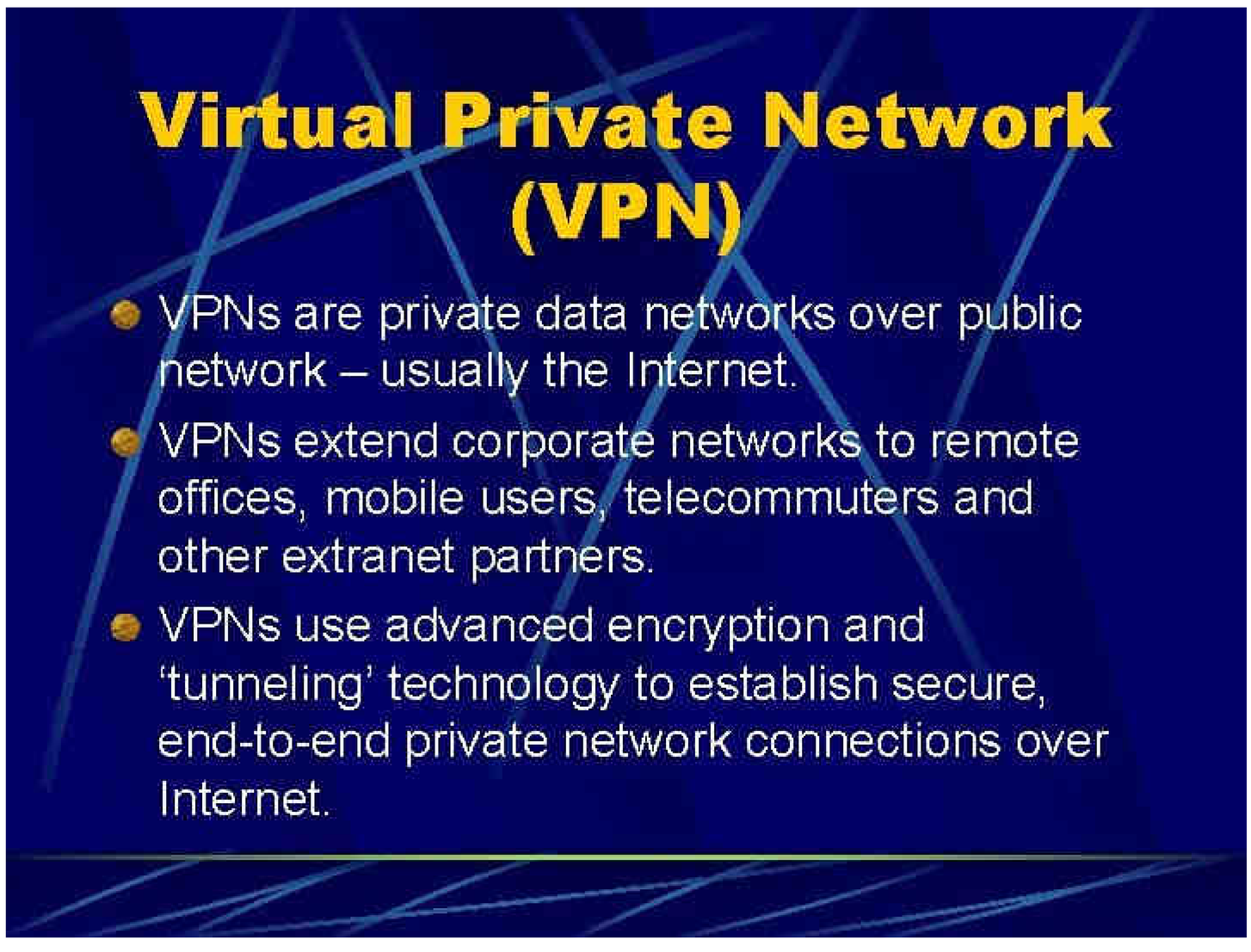
It is important to use File Transfer Protocol (FTPS) to transfer files from the server without the risk of hackers compromising or stealing data. It encrypts data files and your authentication information.

FTPS uses both a command channel and a data channel, and the user can encrypt both. Note that it only protects files during the transfer. Once they reach the server, the data is no longer encrypted. For this reason, encrypting files before sending them adds another layer of security.



Use Private Networks and VPNs

Private networks use a private IP to establish isolated communication channels between servers in the same range. It allows multiple servers under one account to exchange information and data in public space without exposure.



Attacks from malicious users

Cyberattack is the deliberate exploitation of computer systems, networks and technology-based companies. These attacks use malicious code to change computer code, data, or logic. You can compromise your data and culminate in the devastating effects of promoting cybercrime such as information and identity theft. A cyberattack is also known as a computer network attack (CNA).

Bear phishing is an email aimed at a specific individual or organization that wants unauthorized access to sensitive information. These hacks are not carried out by random attackers but are often carried out by trade secrets, financial gain or military intelligence.

Malware Attacks

Malware is a code that could stealthily compromise a compromised computer system without the user's permission. This broad definition includes many specific types of malicious software (malware) such as spyware, ransomware, command and control.

Many well-known businesses, states and criminal actors have discovered the use of malware.

Malware differs from other software in that it spreads over a network, causing changes and damage, being undetectable, and persistent in the infected system. This can destroy a network and bring the performance of the machine to its knees.

Monitor Login Attempts

Using anti-hacking software to monitor login attempts is one way to protect your server against rogue attacks. These automated attacks use trial and error methods and try every combination of letters and numbers to gain access to the system.

Anti-hacking software monitors all log files and detects suspicious login attempts. If the number of attempts exceeds the prescribed rule, the anti-intrusion software blocks the IP address for a certain period of time or indefinitely.

protect your server against brute force attacks

A brutal attack is one of the simplest and least sophisticated hacking methods. As the name implies, ruthless attacks are not subtle. The theory behind such an attack is that if you make countless attempts to guess the password, you will eventually be correct.

The attacker aims to gain forced access to the user account by trying to guess the username/email and password. Typically, a large-scale attack using a hacked account involves stealing sensitive data, shutting down a computer, or a combination of all three.

Creating this type of attack activation code does not take much imagination or knowledge, and there are even widely available automated tools that can submit several thousand password attempts per second.

How to Identify Brute Force Attacks

A brutal attack is easy to identify and investigate. You can find them by looking at your Apache access log or Linux log files. This attack will leave a series of failed login attempts, as seen below:

```
Sep 21 20:10:10 host proftpd[25197]: yourserver (usersip[usersip]) - USER theusername (Login failed): Incorrect password.
```

Brute Force Attack Prevention Techniques

Let’s explore other ways to prevent a brutal attack.

- Restrict failed login attempts
- Make the root user inaccessible via SSH by editing the sshd_config file
- Do not use the default port, just edit the port line in your sshd_configfile
- Use the captcha
- Limit logins to a specific IP address or range
- Two factor recognition
- Personal login URLs
- Monitor server logs

Server Password Security

When it comes to server security, make sure you use password best practices. The first step is to create clear password policies and rules that all members of the server must follow.

You must enable a minimum character length for passwords, set password complex guidelines, complete session time for inactivity, and use a multi-factor authentication strategy.

Establish password requirements

The first thing to do is set the password requirements and rules that all members of the server must follow.

Do not allow blank or default passwords. Execute the minimum password length and issue. Keep the lockout policy. Do not store passwords using reversible encryption. End session time for inactivity and enable two-factor authentication.

Set a password expiration policy

Setting the password expiration date is another common practice when installing requirements for users. The password can last for weeks or even months, depending on the level of security required.

Password Don’ts

If you want to maintain a secure server, there are some things to avoid when obtaining passwords. First, be careful where you store passwords. Do not write them down on pieces of paper and wrap them around the office.

It is generally advised not to use personal information such as your date of birth, hometown, nicknames and other things that may link you and the user to the password. These are very easy to guess, especially those who know you personally.

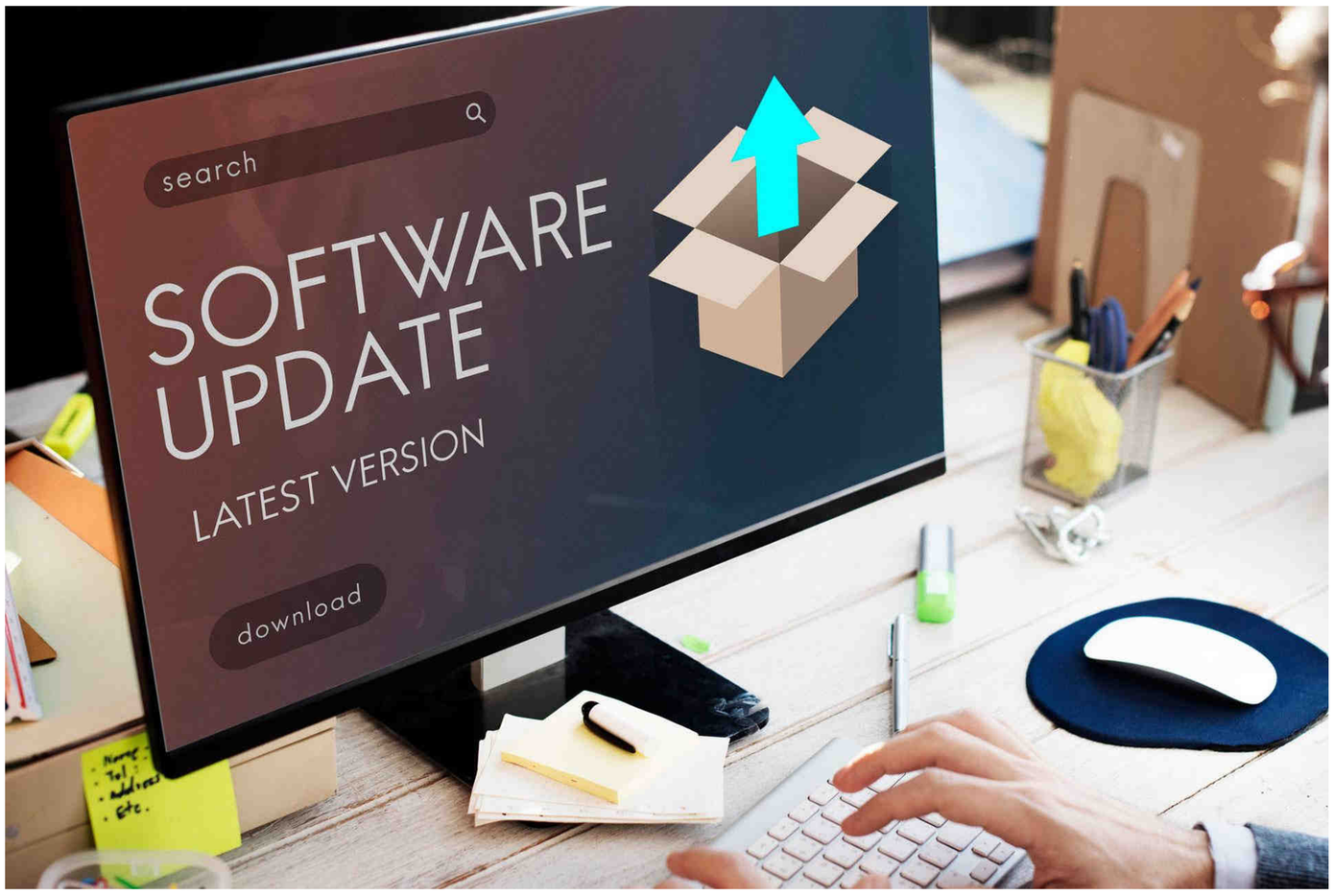
Passwords containing only simple dictionary words are easy to break, especially by dictionary (rogue) attacks. Keep in mind the same danger, try to avoid repeating rows of characters in the same password.

Finally, do not use the same password for multiple accounts. By recycling passwords, you run a significant risk. If a hacker gains access to one account, all other accounts with the same password may be at risk.

Update and Upgrade Software Regularly

Regularly updating the software on a server is an important step in keeping it safe from hackers. Outdated software is already being explored for its vulnerabilities, which could expose hackers to exploit and harm your computer. If you keep everything updated, make sure it is updated to protect itself in the first row.

Automatic updates are a way to guarantee that no updates are forgotten. However, allowing the system to make such changes automatically can be dangerous. Before updating your production environment, it is a good idea to explore how innovation works in a testing environment.



Hide Server Information

Try to provide as little information as possible about the basic infrastructure. The less known about the server, the better.

Also, it is a good idea to hide the version numbers of any software you have installed on the server. Often they, by nature, reveal the exact release date that can help hackers when looking for vulnerabilities. It is usually easy to remove this information by deleting it from the HTTP title of its greeting banner.

Set Up and Maintain a Firewall

Protect your server by controlling and restricting access to your computer.

It is essential to use CSF (ConfigServer and Firewall) to tighten security on your server. It only allows specific key links and locks access to other services.

Set up the firewall during the initial server setup or when making changes to the services provided by the server. By default, a common server runs different services, including public, private, and internal services.

- **Public services** are usually operated by web servers that allow access to a website. Anyone can access these services on the Internet, often anonymously.
- **Private services** are used when dealing with the database control panel. In such a case, the same point should be accessed for the selected number. They have authorized accounts with special privileges within the server.
- **Internal services** are never disclosed to the Internet or the outside world. They are only accessible from the server and only accept local connections.

Back Up Your Server

Although the previously mentioned steps are designed to protect your server data, it is important to have a system backup in case something goes wrong.

Save encrypted backups of your sensitive data offsite or use the cloud solution.

Whether you have automated backup jobs or do them manually, make sure you make a habit of this precaution. Also, you should check the backups, check the detailed backup. This should include "intelligence tests" that administrators or end-users check for data recovery consistency.

Configure Your Computer to File Backups

You should always have a file backup and have a restore strategy. You never know when a hacker might succeed in breaking into your servers.

In the event of such a breach, the backup file may be your savior.

Regular backup of your data allows you to recover all the information that your server had before the data breach took place.

So, for the sake of your data, you need to make sure that you make sure to back up the data.

You should also carefully consider where to store your backup files.

You can choose to keep the files locally or in the cloud, which is a safe approach.

Update, update, update!

It is essential to be up-to-date on security fixes related to all software and operating systems in server security. Server systems and software technologies are so complex that some of the security vulnerabilities they carry can easily go unnoticed.

As you increase your knowledge on preventing cybercrimes, threats are also continuously evolving. Either you want to be equipped in the current cyber threats or pursue a career in the Cybersecurity industry, Global Institute of Technology Services offers a free live Demo class.

Join our class to learn the foundation of Cybersecurity and get certified!

Join Our Demo Class

https://gitservices.com/

Global Institute of Technology