Security

Top 10 Most Secure Linux Distros for Personal Use

5 months ago • by Prateek Jangid

It is no secret that everyone looks for a secure operating system that offers top-notch privacy. If you are using a system that is not secure enough, anyone can access your system and exploit your data, such as photos, videos, files, and sensitive financial information. Linux systems offer fantastic privacy and security as compared to other OS, like Windows or Mac. So, it is best to go for a Linux system for better security. But, there is an extensive list of secure Linux distros, and it can be difficult to choose one.

Several different kinds of secure Linux distros exist, and each is developed for unique usages, including spy-level security, personal use, organizational usage, and more. So, if you want standard security and privacy, you can use the Linux distros that are best for personal use. This article will help you to choose the best Linux distro for your personal usage needs. The following sections include complete information about the top 10 most secure Linux distros available for personal use.

Linux Kodachi

Linux Kodachi is a lightweight Linux distro based on Xubuntu 18.04 and developed for running from a USB or DVD. Kodachi is one of the most secure Linux distros available for personal use, offering an anonymous, anti-forensic, and secure system to users. For even tighter security, Linux Kodachi filters all network traffic by VPN, or Virtual Proxy Network, and a Tor network to obscure your location. This Linux distro also works to remove all activity traces after you use it. Kodachi is based on the stable distribution Linux Debian, with customized features from Xfce for higher stability, security, and singularity.

Kodachi also has a support system for a protocol, DNScrypt, and utility for encrypting a request for the OpenDNS server through elliptical cryptography. As mentioned previously, Kodachi also has a browser-based system on the Tor Browser, in which you can eliminate any uncertain Tor modules.

Pros and cons of Linux Kodachi

Pros	Cons
Contains various pre-installed programs.	Many users complain about the narrow service, as Kodachi is based on Xubuntu.
Offers a powerful security system.	

Provides speedy network access.	
Is highly stable.	

2. Qubes OS

Qubes OS is one of the most secure Linux distros available. Many users recommend this distro for a high-level privacy system. Qubes is a security-oriented operating system (OS) that offers the compatibility to run other programs on a computer/laptop. This Linux distro works for isolating the user's files from malicious activities and malware without affecting the data. Qubes OS provides top-notch security through compartmentalization, through which you can compartmentalize different tasks in the securely isolated compartment known as Qubes.

The Qubes operating system uses the RPM package manager to work on any desktop environment without consuming an excessive amount of resources. Most importantly, Qubes is an open-source operating system, so the source codes are easily available online. We recommend that you use Qube OS if you need advanced security, but it is a bit of an advanced operating system for new users.

Pros and Cons of Qubes OS

Pros	Cons
Users can perform application separation with a sandboxed virtual machine, assuring that any malicious script or apps cannot be passed to system applications.	Only recommended for advanced users.

Offers a higher level of separation through the Internet by forcing all Internet traffic via the Whonix Tor gateway.	It is difficult to test Qubes OS because it does not work well in a virtual machine.

3. Whonix

Whonix is based on the Debian GNU/Linux to offer outstanding security and advanced level privacy. This distro is one of the most secure Linux distros if you want something different in your system's security. Whonix is different because it does not have a live system rather than running on a virtual machine, particularly where it is isolated from the primary operating system to eliminate the DNS leakage risk.

There are two specific parts to Whonix. The first part is Whonix Gateway, which works as the Tor gateway. The second part is Whonix Workstation, an isolated network that works to route all connections via the Tor gateway. This Linux distro will work well if you need a private IP address for your system. As mentioned earlier, Whonix is based on Debian, so it utilizes two different VMs (virtual machines) that make it a little bit resource hungry.

Pros and Cons of Whonix

Pros	Cons

Uses VirtualBox technology to ensure that many people can use this distro easily.	Is somewhat resource hungry because it requires a high-end system for proper use.
Is easy to set up and use because it does not require special knowledge.	Anonymity in Whonix is offered in the workstation virtual machine only, and users can forget it easily.

4. Tails (The Amnesic Incognito Live System)

Tails, or The Amnesic Incognito Live System, is a security-centric system based on Debian. It is one of the most secure Linux distros available for personal use because it was designed for protecting your identity by keeping your activities anonymous. Tails forces incoming or outgoing traffic through a Tor network and block all traceable connections. Tails was first released in 2009 for personal computers.

Tails is one of the most secure Linux distros available for personal use. It does not require any space in your hard disk, as Tails only needs space in the RAM, but it will be erased once a user shuts down the system. Hence, the default desktop environment of Tails is Gnome, and it can be used via a pen drive to save all the RAM data.

Pros and Cons of Tails

Pros	Cons
Is an easy-to-use Linux distro.	Must be used as the live boot OS.
You can quickly start browsing anonymously.	Sometimes, users misplace the flash drive, which can create major issues.

Is packaged with a TOR Browser.	TOR is a bit problematic, as it is compressed for Tails.
Offers a secured space to save passwords.	

5. Kali Linux

Kali Linux is based on Debian and was created to offer an amazing penetration Linux distro for ethical hacking, security experts, digital forensics, and network security assessments. This distribution is one of the best and most secure Linux distros for personal, providing users with packages of tools like Foremost, Wireshark, Maltigo as-Aircrack-ng, Kismet, and more. These packages offer various benefits to users, such as exploiting a victim application, checking the targeted IP address, and performing a network discovery.

You can use Kali Linux via a USB stick or DVD, so this distro is quite easy to use, like the Tails distro mentioned earlier in the list. Kali Linux is compatible with both 32- and 64-bit systems. Apart from that, the basic requirements of Kali Linux are 512 MB of RAM and 10 GB of hard disk space. According to multiple surveys, developers consider Kali Linux to be one of the top-ranked and most secure Linux distros available.

Pros and Cons Kali Linux

Pros	Cons
An open-source distribution that can be accessed easily.	Can make the system a bit slower than usual.

Inxluswa multi-language support.	Users face software-related issues.
Allows users to locate different binaries easily.	Sometimes, Kali Linux corrupts the system.

6. Parrot Security OS

Parrot Security OS was developed by FrozenBox and is based on a Debian distribution. Released in 2013, this Linux distro was created for ethical hacking, working anonymously, and penetration testing. This Linux distro was specifically designed to test authorized simulated attacks on the computer system, which can be beneficial for assessing system vulnerabilities. As mentioned earlier, Parrot Security OS is an open-source and free GNU distribution made for security researchers, developers, penetration testers, privacy enthusiasts, and forensic investigators.

Parrot Security OS comes with a portable laboratory that works to protect your system from security-related issues while using the Internet, gaming, or browsing. This Linux distro is distributed as a rolling release (frequently providing updates and applications), so it offers some core applications, including Parrot Terminal, MATE, Tor Browser, and OnionShare, as its default desktop environment.

Pros and Cons Parrot Security OS

Pros	Cons
Offers a large number of tools.	It is not minimalistic.
The widgets are very easy to use.	It has shortcut-related issues.
Does not require the GPU to run correctly.	
Has a sleek UI, and things are easy to navigate.	

7. BlackArch Linux

BlackArch is based on Arch Linux, and it is a lightweight Linux distro designed for penetration tester, security researchers, and computer experts. This Linux distro provides multiple features, combined with 2,000+ cybersecurity tools that users can install according to their requirements. BlackArch can be used on any hardware, as it is a lightweight Linux distro and also a new project, so many developers prefer to use this distro nowadays.

According to the reviews, this Linux distro can compete against many reliable OS due to the variety of features and tools for experts that it offers. Users can choose between different desktop environments, including Awesome, spectrwm, Fluxbox, and Blackbox. BlackArch is available in the DVD image, and you can also easily run it from a pen drive.

Pros and Cons of BlackArch Linux

Pros	Cons
Offers a large repository.	It is not recommended for beginners.
It is a suitable choice for professionals.	Sometimes, the system becomes slower while using BlackArch.
It is better than ArchStrike.	
It is based on Arch Linux.	

8. IprediaOS

IprediaOS is a privacy-centered Linux distro based on Fedora. If you are looking for a platform to browse, email, and share files anonymously, then IprediaOS is a good choice for you. Along with privacy and anonymity, IprediaOS also provides stability, computing ability, and amazing speed. Compared to other Linux distros, IprediaOS is much faster, and you can run this distro

smoothly even on older systems.

The Ipredia operating system is security-conscious, and it is designed with the minimalist ideology of shipping with vital applications. IprediaOS seeks to transparently encrypt and anonymize all traffic by sending it through an I2P anonymizing network. The basic features of IprediaOS include I2P Router, Anonymous BitTorrent client, Anonymous email client, Anonymous IRC client, and more.

Pros and Cons of IprediaOS

Pros	Cons
Can be used on an older system.	Sometimes, users face performance-related issues.
Provides anonymous email client services.	
Provides anonymous email client services.	

9. Discreete

Discreete Linux is based on Debian, and it was developed to offer protection from trojan-based surveillance by isolating working from a location with secured data. Discreete was formerly known as UPR (Ubuntu Privacy Remix), so it is a trusted and secure Linux distro that will protect your data. You can use this OS via CD, DVD, or USB drive, as it cannot be installed on the hard drive, and all networks are deliberately disabled when Discreete runs in the system.

Discreete is one of the unique Linux distros in terms of security, and it was developed for everyday computer activities, such as gaming or word processing. As we have mentioned above, Discreete disables the Internet connection while working to separate the data and cryptographic keys to remain protected from non-trusted networks.

Pros and Cons of Discreete

Pros	Cons
It is best for everyday work.	Disables the network when a user works on it.
You can use it via DVD, CD, or USB drive.	

10. TENS

The full form of TENS is Trusted End Node Security. TENS was developed by the United States Department of Defense's Air Force Research Laboratory. This Linux distro does not need administrator privileges for running without installation and storing it in the hard drive. TENS consists of an Xfce desktop, and it is customized to look like a Windows XP desktop. Everything about the appearance of TENS is similar to Windows, including the application names and placements.

This Linux distro is available in two editions. The first edition of TENS is a Deluxe edition that includes various applications, like LibreOffice, Evince PDF reader, Totem Movie Player, Thunderbird, and so on. The other edition of TENS is the regular edition that includes an encryption app and some other useful apps.

Pros and Cons of TENS

Pros	Cons
Offers great security and privacy.	The look of TENS
Provides two different editions for users.	Exhibits performance-related issues.

Conclusion

This article provided a list of the top ten most secure Linux distros for personal use. All the distros discussed in this article offer amazing features and anonymity to the user. We have included these Linux distros according to user reviews and features, but the list position of

each distribution is completely random. Privacy, security, and anonymity are important for performing specific computer-related tasks, and any of these Linux distros would be a great choice for keeping your information safe from malicious threats.

ABOUT THE AUTHOR

Prateek Jangid

A passionate Linux user for personal and professional reasons, always exploring what is new in the world of Linux and sharing with my readers.

View all posts

RELATED LINUX HINT POSTS

- **How to disable password login on Linux**
- **MAC Flooding Attack**
- **Smurf Attack**
- **Introduction to Cryptography**
- **Bluetooth Security Risks**
- **Best Certifications for Cyber Security**
- **Symmetric Vs. Asymmetric Key Ciphers**

Linux Hint LLC, editor@linuxhint.com
1210 Kelly Park Cir, Morgan Hill, CA 95037