

Forum:[Hack Forums](#)

Thread: [Tails OS vs Qubes OS - Stay hidden from any Agency!](#)

Network Bytes - *October 14, 2014, 6:50 pm*

I am pretty sure some of you guys have heard about Tails OS, the OS Edward Snowden used to stay hidden from NSA.

Recently it has come to my attention that there is another OS that is known for security, this is called Qubes OS.

Now, I have read a lot about both of these Operating systems, and they are not to be confused with each other, as they both stand for two different things.

There is this blog where they post information about staying hidden from any agency and what not, they have taken the time to compare both Tails OS and Qubes OS.

At the end they summarize and conclude which OS should benefit for you and they state the following:

Quote:Qubes vs Tails?

Qubes and Tails have fundamentally different use-cases. They're both very important, and I use both operating systems every day.

Tails is for staying anonymous. When you use it on a computer, it doesn't leave a trace that it was ever booted. It changes your MAC address before you connect to a network, and it forces all traffic to go over the Tor network, ensuring that you don't make a technical mistake and accidentally leak your IP address. When you use the web browser that comes with Tails, your traffic looks exactly like the traffic of all other Tor users.

Qubes is for staying secure while still being able to use a wide variety of software that might contain zero day vulnerabilities, but it's not for staying anonymous. Qubes supports cool networking tricks, like making an AppVM where all traffic is forced to go through Tor, but this doesn't incorporate most of the anonymity tricks that Tails excels at.

Bottom line

For maximum security, I would recommend that people use Qubes on their computer for all their everyday, non-anonymous needs: checking email, chatting, using social media and browsing the web, developing software, doing research, writing articles. Since you do all of this work in AppVMs that run Linux (and optionally some of it in AppVMs that run Windows), you get the latest and best tools to work with, and it's simple to install new software. For more sensitive needs where anonymity is important, you can use Tor Browser Bundle inside of an AppVM.

And for the most sensitive needs, as the NSA journalists explained, you should boot to Tails.

Take a look at this article to read more about it:

<https://freedom.press/blog/2014/04/operating-system-can-protect-you-even-if-you-get-hacked>

Tails OS: <https://tails.boum.org/>

Qubes OS: <https://qubes-os.org/>