# Security By Isolation – A quick peek at Qubes OS

## Introduction

In today's digital age, security is paramount. Today, we will explore a unique operating system - Qubes OS - designed with an innovative approach to security by isolation.

Mattia Coffetti

Mattia (Mzkk_) Coffetti 🔍 | LinkedIn

"If you're serious about security, @QubesOS is the best OS available today. It's what I use, and free."

— Edward Snowden, whistleblower and privacy advocate

"SecureDrop depends on Qubes OS for best-in-class isolation of sensitive workloads on journalist workstations. Providing journalists with a sane way to handle untrusted content from unknown sources is part of our job, and Qubes gives us the tools we need to do that job well."

— Freedom of the Press Foundation, non-profit dedicated to supporting free speech and public-interest journalism

"When I use Qubes I feel like a god. Software thinks that it's in control, that it can do what it wants? It can't. I'm in control."

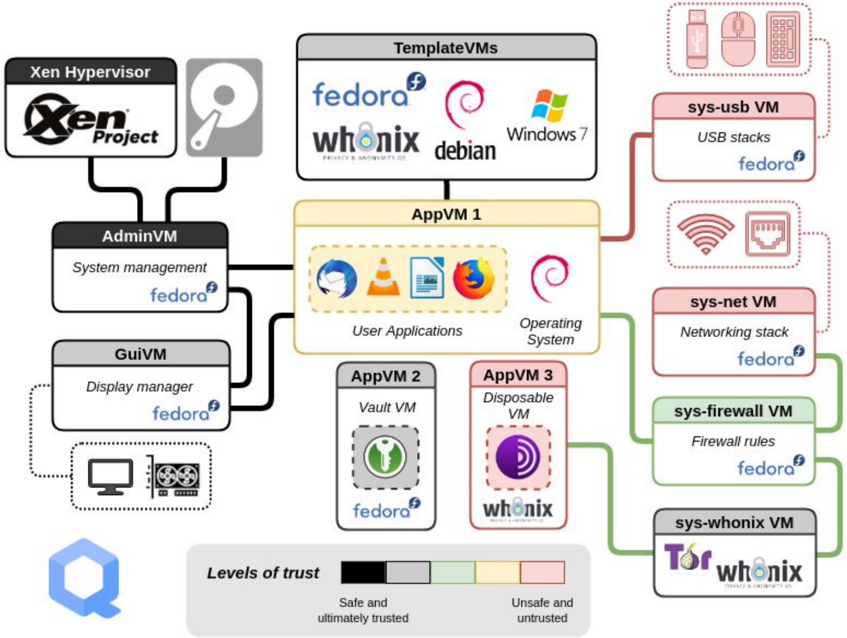
— Micah Lee, Director of Information Security at The Intercept, advisor to DDoSecrets

"Qubes OS gives us greater confidence in the security of systems being used to remotely access our servers, mainly because powerful physical and logical privilege separation between workspaces allows our engineers to select appropriate degrees of isolation for different processes."

— Let's Encrypt, non-profit, world's largest certificate authority

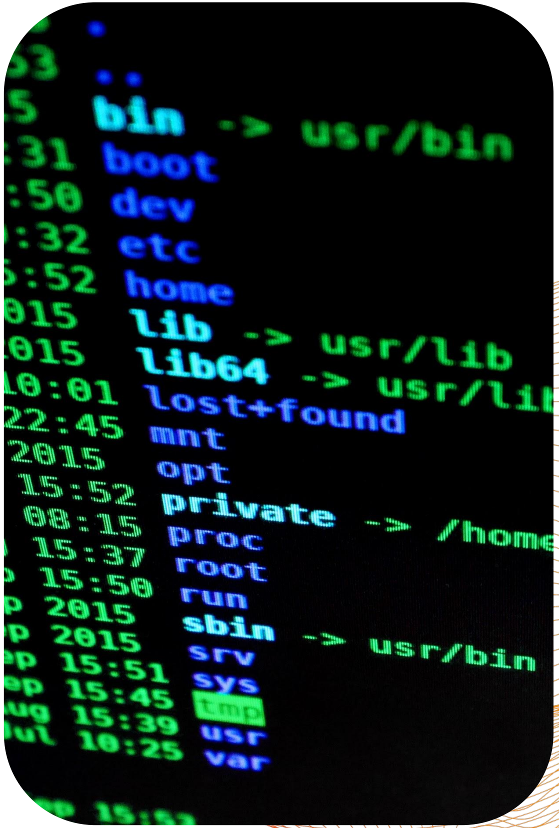
# Overview of Qubes OS

- A high-security operating system that uses the Xen hypervisor to partition the operating system and applications into separate isolated components, or "qubes".
- Compartmentalization strategy offers a high degree of protection against malware spread.
- If an application within a qube becomes infected, the malware is unable to spread outside of that particular domain.



# Security by Isolation

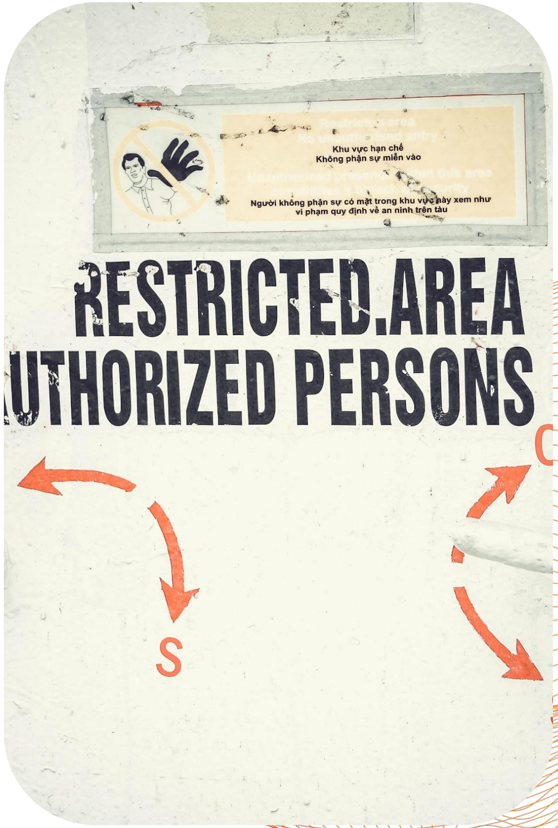
- Running each application within separate, sandboxed virtual machines referred to as "qubes".
- Ensures that each qube only has the potential to affect applications within the same qube.
- Provides protection against even risky applications affecting trusted ones or writing to the underlying file system.



```
      .
3     ..
5     bin -> usr/bin
:31   boot
:50   dev
:32   etc
:52   home
015   lib -> usr/lib
015   lib64 -> usr/li
0:01  lost+found
22:45 mnt
2015  opt
 15:52 private -> /home
 08:15 proc
 15:37 root
 15:50 run
p 2015 sbin -> usr/bin
p 2015 srv
ep 15:51 sys
ep 15:45 tmp
ug 15:39 usr
ul 10:25 var
```

# Security by Isolation - Qubes

- Qubes operate on a template system, allowing multiple qubes to be based on a single template without the risk of one qube compromising its template or other qubes based on it. This architecture provides robust security, limiting the damage of any potential attack to just one qube.
- Qubes OS also incorporates "helper" qubes for specific services, such as internet connectivity or USB access, and a management qube for automatic housekeeping tasks. All these types of qubes are also template-based, offering flexibility and security.


Khu vực hạn chế
Không phận sự miễn vào
Người không phận sự có mặt trong khu vực này xem như
vi phạm quy định về an ninh trên tàu
RESTRICTED.AREA
UTHORIZED PERSONS
S

# Security by Isolation - Glossary

## dom0

**Domain** zero. A type of **admin qube**. Also known as the **host** domain, dom0 is the initial qube started by the Xen hypervisor on boot. Dom0 runs the Xen management toolstack and has special privileges relative to other domains, such as direct access to most hardware.

## app qube

Any **qube** that does not have a root filesystem of its own. Every app qube is based on a **template** from which it borrows the root filesystem.

## disposable

A type of temporary **app qube** that self-destructs when its originating window closes. Each disposable is based on a **disposable template**.

## domU

Unprivileged **domain**. Also known as **guest** domains, domUs are the counterparts to dom0. In Xen, all VMs except dom0 are domUs. By default, most domUs lack direct hardware access.

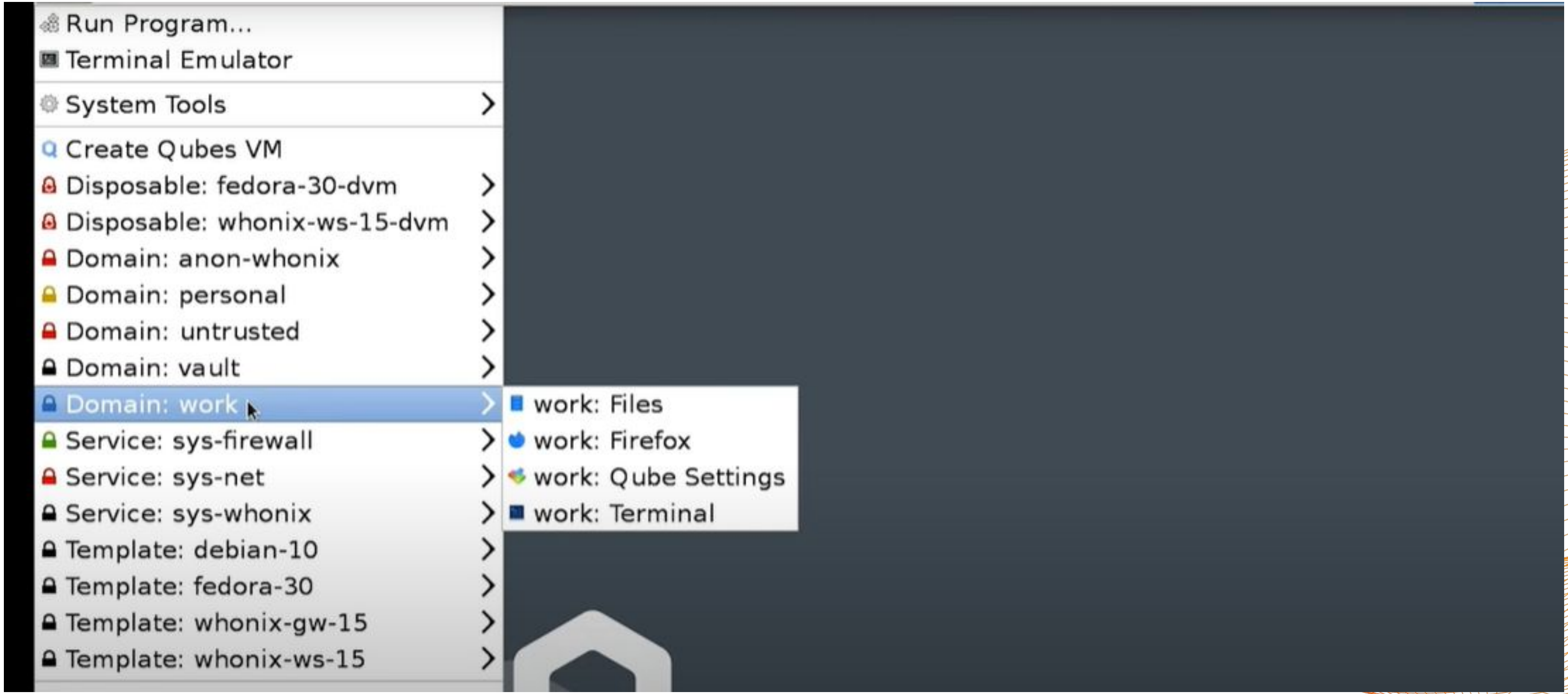
## service qube

Any **app qube** the primary purpose of which is to provide services to other qubes. `sys-net` and `sys-firewall` are examples of service qubes.

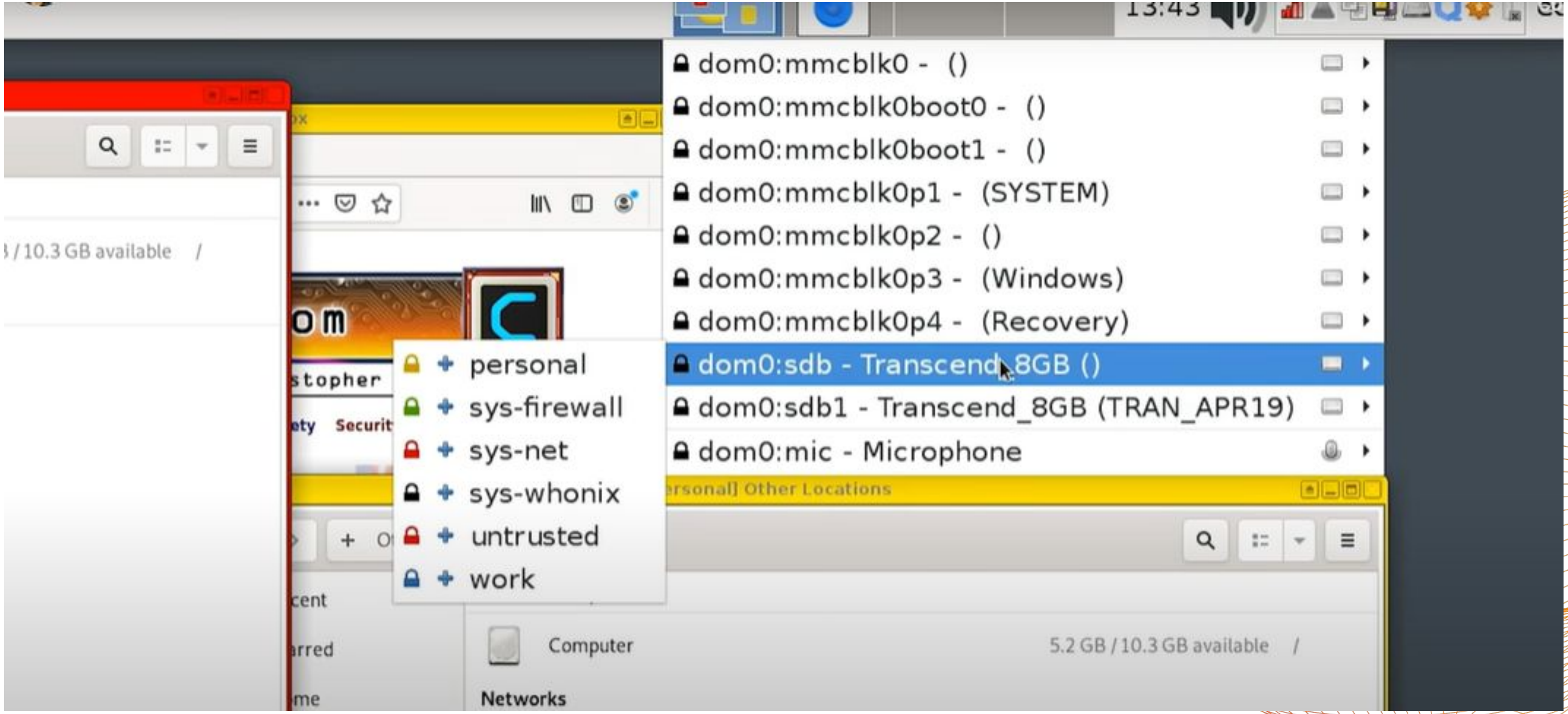
## template

Any **qube** that shares its root filesystem with another qube. A qube that is borrowing a template's root filesystem is known as an **app qube** and is said to be "based on" the template. Templates are intended for installing and updating software applications, but not for running them.

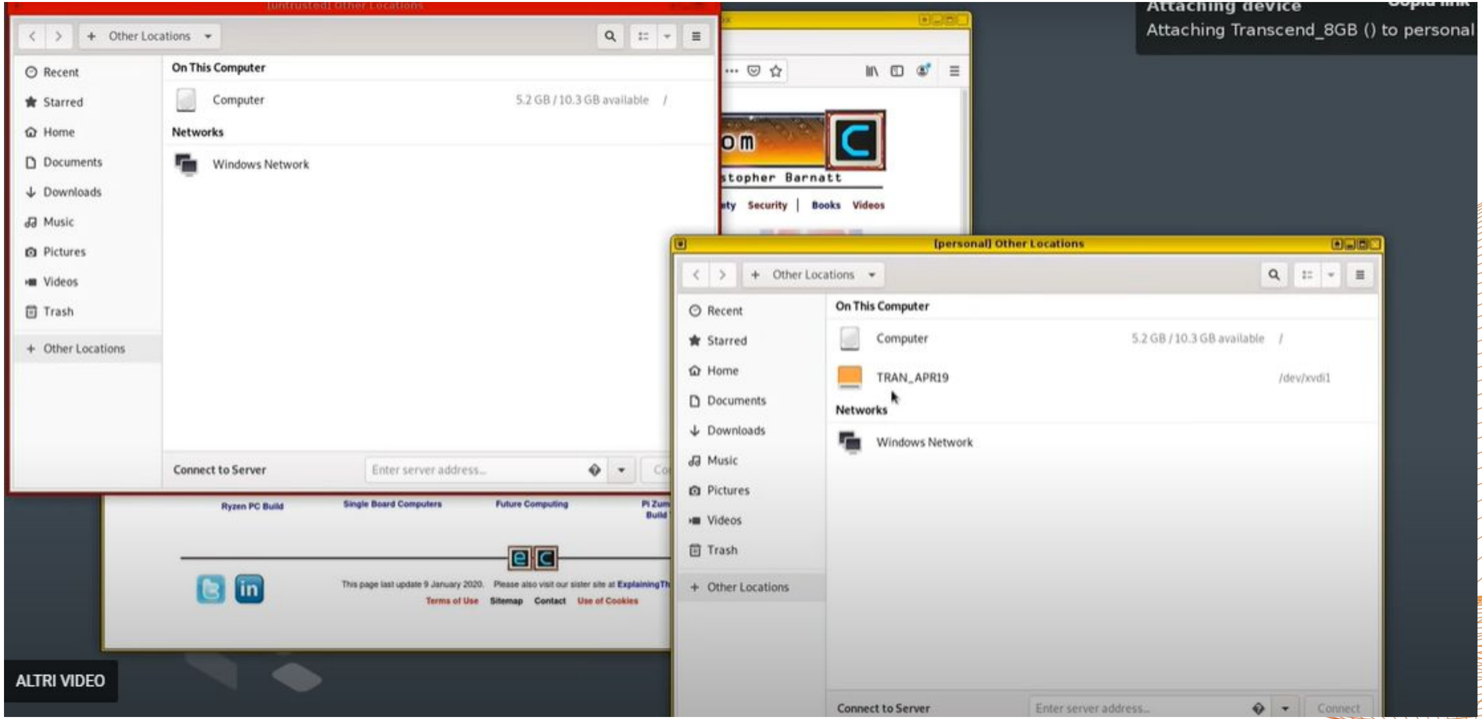
# Security by Isolation - How to run App Qubes



# Security by Isolation - External drive access



# Security by Isolation - External drive access

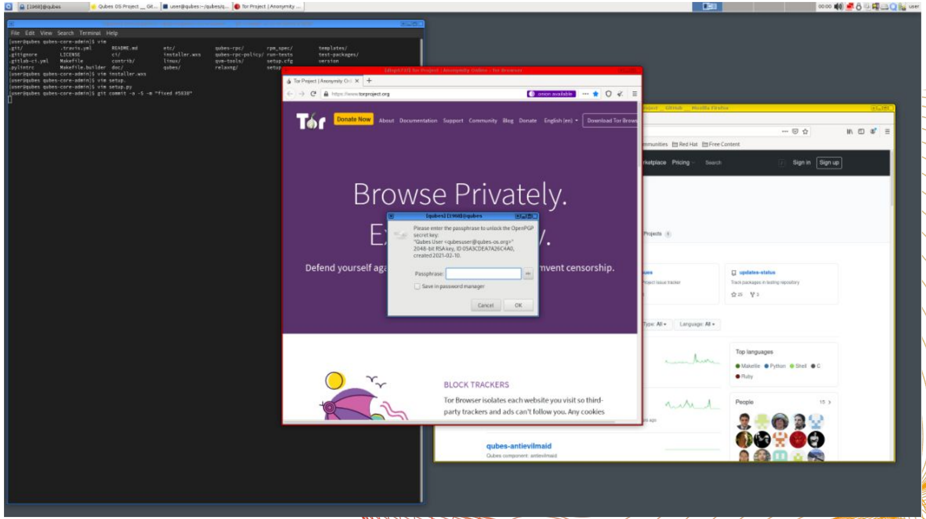


Attaching device

Attaching Transcend_8GB () to personal

# Security by Isolation - Labels

It is always clearly visible to which domain a given window belongs. Here it's immediately clear that the passphrase-prompting window belongs to some domain with the "blue" label. When we look at the titlebar, we see "[qubes]", which is the name of the actual domain. Theoretically, the untrusted application (here, the red Tor Browser running in a DisposableVM) beneath the prompt window could draw a similar looking window within its contents. In practice, this would be very hard, because it doesn't know, e.g., the exact decoration style that is in use. However, if this is a concern, the user can simply try to move the more trusted window onto some empty space on the desktop such that no other window is present beneath it. Or, better yet, use the Expose-like effect (available via a hot-key). A malicious application from an untrusted domain cannot spoof the whole desktop because the trusted Window Manager will never let any domain "own" the whole screen. Its titlebar will always be visible.



```
[user@qubes qubes-core-admin]$ vim
.git/           .travis.yml      README.md       etc/            qubes-rpc/        rpm_spec/        templates/
.gitignore      LICENSE          ci/             installer.wxs   qubes-rpc-policy/ run-tests        test-packages/
.gitlab-ci.yml  Makefile         contrib/        linux/          qvm-tools/        setup.cfg        version
.pylintrc       Makefile.builder doc/            qubes/          relaxng/          setup
[user@qubes qubes-core-admin]$ vim installer.wxs
[user@qubes qubes-core-admin]$ vim setup.
[user@qubes qubes-core-admin]$ vim setup.py
[user@qubes qubes-core-admin]$ git commit -a -S -m "fixed #5838"
```

[qubes] [1968]@qubes

Please enter the passphrase to unlock the OpenPGP secret key:
"Qubes User <qubesuser@qubes-os.org>"
2048-bit RSA key, ID 05A3CDEA7A26C4A0,
created 2021-02-10.

Passphrase:

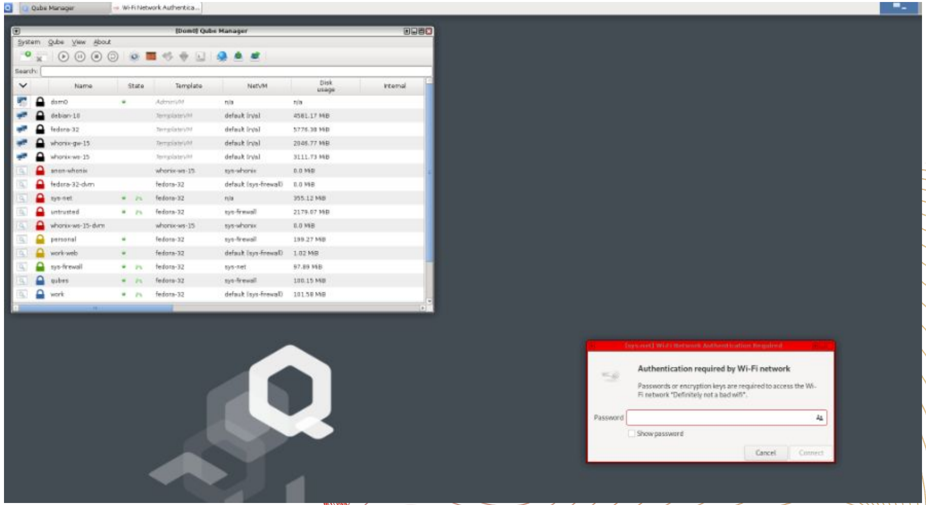
□ Save in password manager

Cancel OK

Tor Browser isolates each website you visit so third-party trackers and ads can't follow you. Any cookies

# Security by Isolation - Network stack

All the networking runs in a special, unprivileged NetVM. (Notice the red frame around the Network Manager dialog box on the screen above.) This means that in the event that your network card driver, Wi-Fi stack, or DHCP client is compromised, the integrity of the rest of the system will not be affected! This feature requires Intel VT-d or AMD IOMMU hardware (e.g., Core i5/i7 systems)



| Name | State | Template | NetVM | Disk usage | Internal |
|---|---|---|---|---|---|
| dom0 | ● | AdminVM | n/a | n/a | |
| debian-10 | | TemplateVM | default (n/a) | 4581.17 MiB | |
| fedora-32 | | TemplateVM | default (n/a) | 5776.38 MiB | |
| whonix-gw-15 | | TemplateVM | default (n/a) | 2046.77 MiB | |
| whonix-ws-15 | | TemplateVM | default (n/a) | 3111.73 MiB | |
| anon-whonix | | whonix-ws-15 | sys-whonix | 0.0 MiB | |
| fedora-32-dvm | | fedora-32 | default (sys-firewall) | 0.0 MiB | |
| sys-net | ● | fedora-32 | n/a | 355.12 MiB | |
| untrusted | ● | fedora-32 | sys-firewall | 2179.07 MiB | |
| whonix-ws-15-dvm | | whonix-ws-15 | sys-whonix | 0.0 MiB | |
| personal | ● | fedora-32 | sys-firewall | 199.27 MiB | |
| work-web | ● | fedora-32 | default (sys-firewall) | 1.02 MiB | |
| sys-firewall | ● | fedora-32 | sys-net | 97.89 MiB | |
| qubes | ● | fedora-32 | sys-firewall | 100.15 MiB | |
| work | ● | fedora-32 | default (sys-firewall) | 101.58 MiB | |

[sys-net] Wi-Fi Network Authentication Required

**Authentication required by Wi-Fi network**

Passwords or encryption keys are required to access the Wi-Fi network "Definitely not a bad wifi".

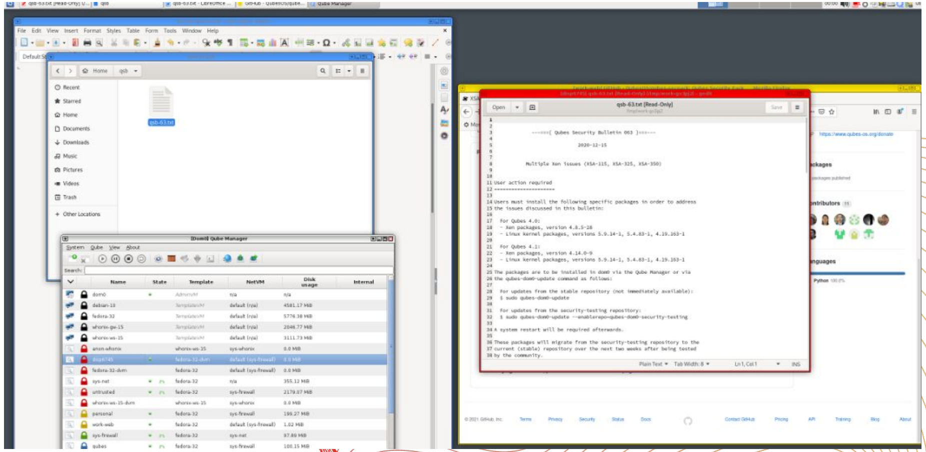
Password

□ Show password

Cancel Connect

# Security by Isolation - Disposable VM’s

Qubes’ unique DisposableVMs (DispVMs) allow the user to open any file in a disposable VM in a matter of seconds! A file can be edited in a disposable VM, and any changes are projected back onto the original file. Currently, there is no way to mark files to be automatically opened in a disposable VM (one needs to right-click on the file and choose the “View in DisposableVM” or “Edit in DisposableVM” option), but this is planned for the R2 Beta 3 release.



| Name | State | Template | NetVM | Disk usage | Internal |
|---|---|---|---|---|---|
| dom0 | ● | AdminVM | n/a | n/a | |
| debian-10 | | TemplateVM | default (n/a) | 4581.17 MB | |
| fedora-32 | | TemplateVM | default (n/a) | 5776.38 MB | |
| whonix-gw-15 | | TemplateVM | default (n/a) | 2046.77 MB | |
| whonix-ws-15 | | TemplateVM | default (n/a) | 3111.73 MB | |
| anon-whonix | | whonix-ws-15 | sys-whonix | 0.0 MB | |
| disp6745 | ● | fedora-32-dvm | default (sys-firewall) | 0.0 MB | |
| fedora-32-dvm | | fedora-32 | default (sys-firewall) | 0.0 MB | |
| sys-net | ● | fedora-32 | n/a | 355.12 MB | |
| untrusted | ● | fedora-32 | sys-firewall | 2179.07 MB | |
| whonix-ws-15-dvm | | whonix-ws-15 | sys-whonix | 0.0 MB | |
| personal | ● | fedora-32 | sys-firewall | 199.27 MB | |
| work-web | ● | fedora-32 | default (sys-firewall) | 1.02 MB | |
| sys-firewall | ● | fedora-32 | sys-net | 97.89 MB | |
| qubes | ● | fedora-32 | sys-firewall | 108.15 MB | |

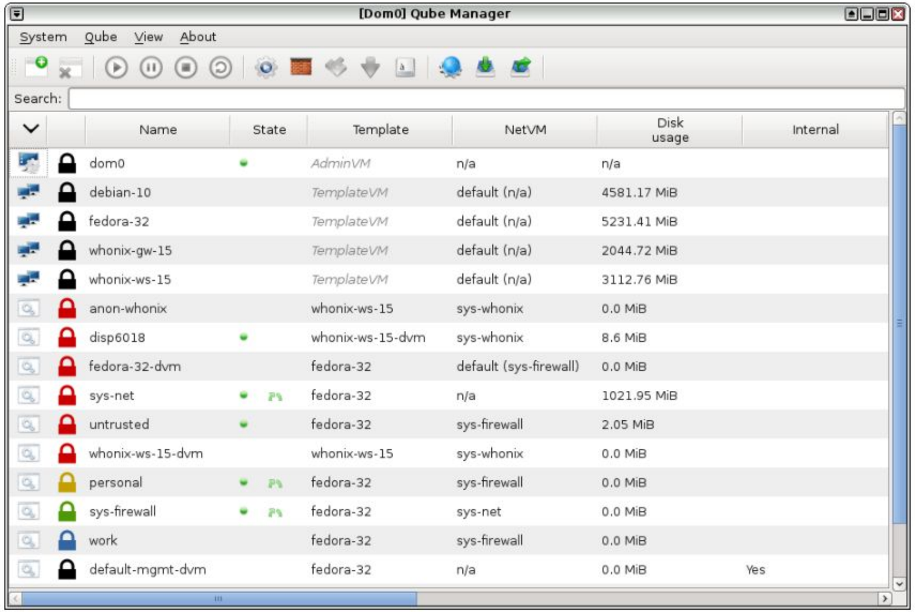
qsb-63.txt (Read-Only)

```


              ---===[ Qubes Security Bulletin 063 ]===---

                             2020-12-15


           Multiple Xen issues (XSA-115, XSA-325, XSA-350)


User action required
=====================

Users must install the following specific packages in order to address
the issues discussed in this bulletin:

  For Qubes 4.0:
  - Xen packages, version 4.8.5-28
  - Linux kernel packages, versions 5.9.14-1, 5.4.83-1, 4.19.163-1

  For Qubes 4.1:
  - Xen packages, version 4.14.0-9
  - Linux kernel packages, versions 5.9.14-1, 5.4.83-1, 4.19.163-1

The packages are to be installed in dom0 via the Qube Manager or via
the qubes-dom0-update command as follows:

  For updates from the stable repository (not immediately available):
  $ sudo qubes-dom0-update

  For updates from the security-testing repository:
  $ sudo qubes-dom0-update --enablerepo=qubes-dom0-security-testing

A system restart will be required afterwards.

These packages will migrate from the security-testing repository to the
current (stable) repository over the next two weeks after being tested
by the community.
```

# How Many cubes i need?

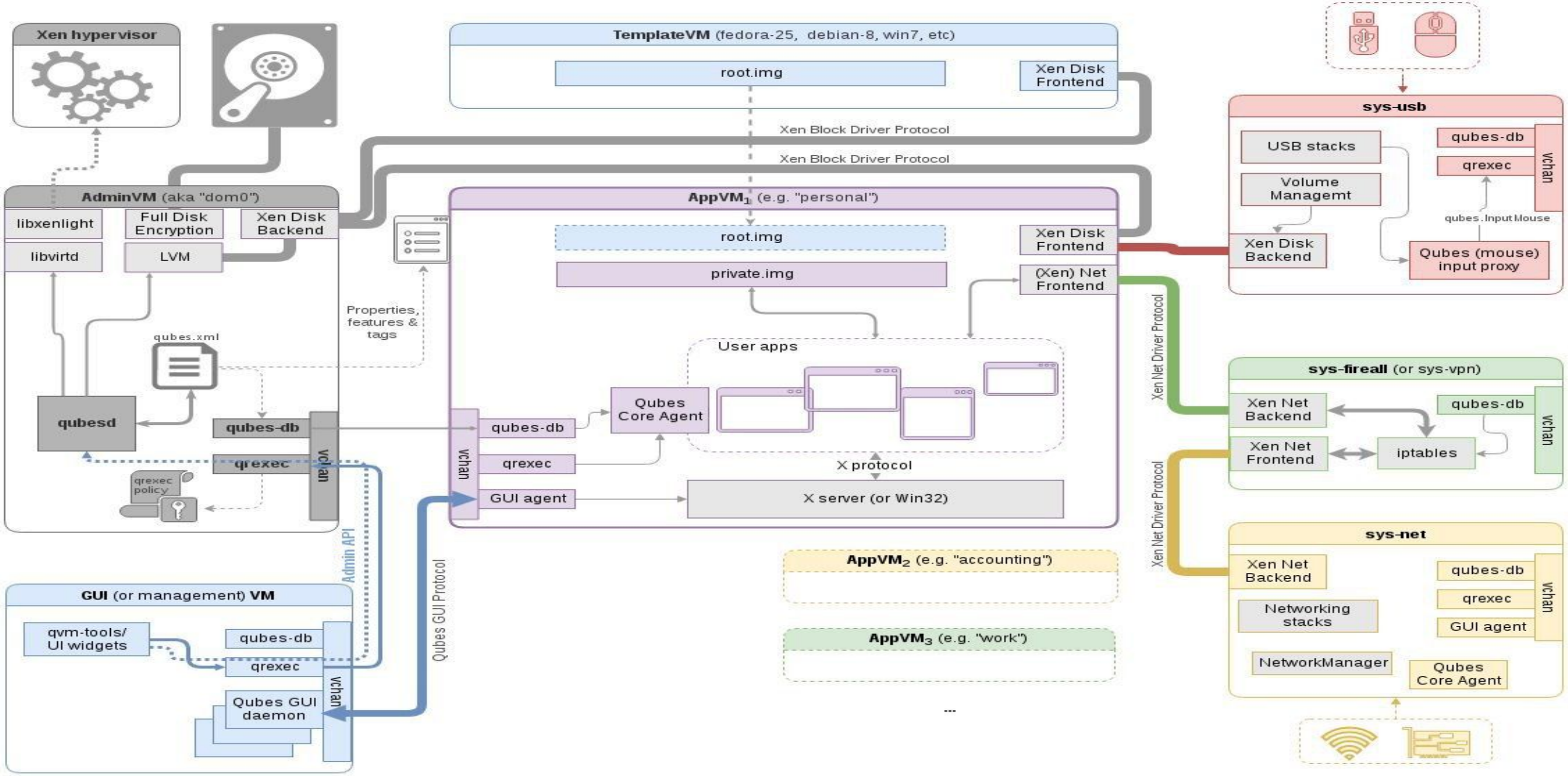
That's a great question, but there's no one-size-fits-all answer. It depends on the structure of your digital life, and this is at least a little different for everyone. If you plan on using your system for work, then it also depends on what kind of job you do.

It's a good idea to start out with the qubes created automatically by the installer: `work`, `personal`, `untrusted`, and `vault`. If and when you start to feel that some activity just doesn't fit into any of your existing qubes, or you want to partition some part of your life, you can easily create a new qube for it. You'll also be able to easily **copy any files** you need to the newly-created qube.



| Name | State | Template | NetVM | Disk usage | Internal |
|---|---|---|---|---|---|
| dom0 | ● | AdminVM | n/a | n/a | |
| debian-10 | | TemplateVM | default (n/a) | 4581.17 MiB | |
| fedora-32 | | TemplateVM | default (n/a) | 5231.41 MiB | |
| whonix-gw-15 | | TemplateVM | default (n/a) | 2044.72 MiB | |
| whonix-ws-15 | | TemplateVM | default (n/a) | 3112.76 MiB | |
| anon-whonix | | whonix-ws-15 | sys-whonix | 0.0 MiB | |
| disp6018 | ● | whonix-ws-15-dvm | sys-whonix | 8.6 MiB | |
| fedora-32-dvm | | fedora-32 | default (sys-firewall) | 0.0 MiB | |
| sys-net | ● | fedora-32 | n/a | 1021.95 MiB | |
| untrusted | ● | fedora-32 | sys-firewall | 2.05 MiB | |
| whonix-ws-15-dvm | | whonix-ws-15 | sys-whonix | 0.0 MiB | |
| personal | ● | fedora-32 | sys-firewall | 0.0 MiB | |
| sys-firewall | ● | fedora-32 | sys-net | 0.0 MiB | |
| work | | fedora-32 | sys-firewall | 0.0 MiB | |
| default-mgmt-dvm | | fedora-32 | n/a | 0.0 MiB | Yes |

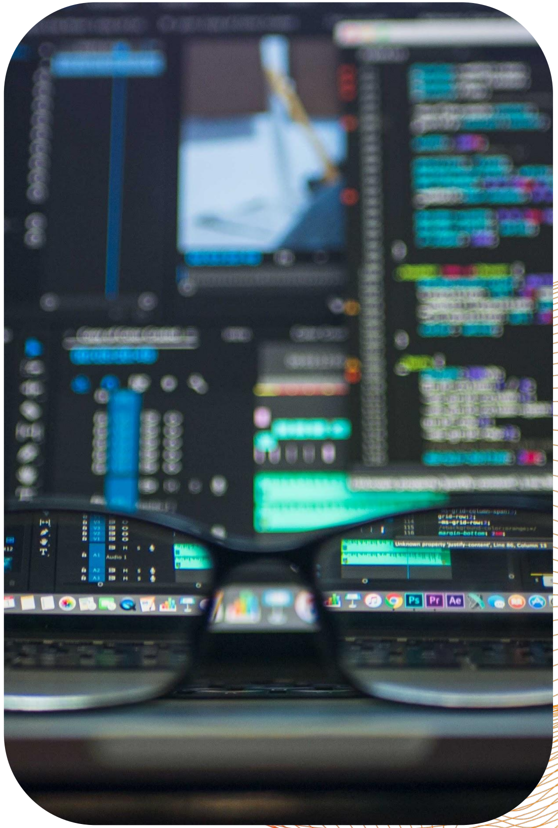
# In-depth view of Qubes OS



# Vmapps communication and networking docs Qubes OS

https://www.qubes-os.org/doc/qrexec/

https://www.qubes-os.org/doc/networking/

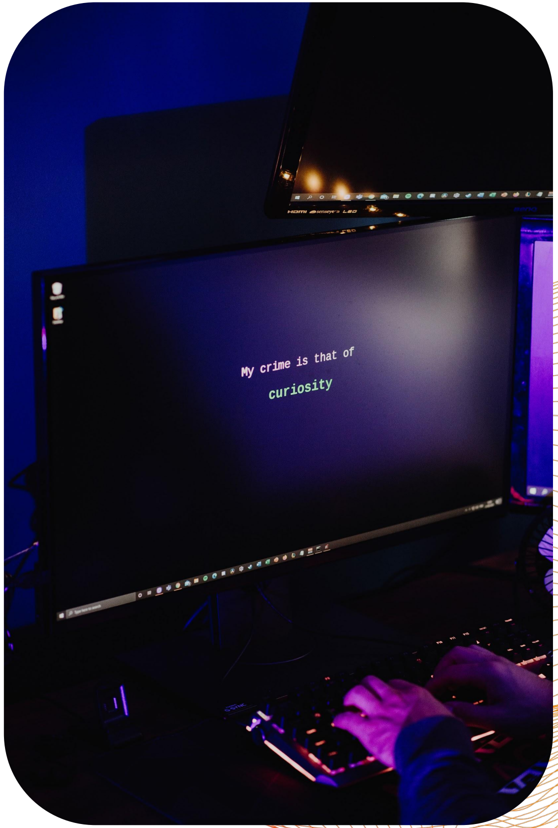


# Privacy and Anonymity

- Offers robust privacy features, including an integrated Whonix gateway and workstation running in separate qubes.
- Enables safe and easy internet use over the Tor network, providing significant anonymity online.

# Qubes OS vs Tails.

- Tails focuses on privacy and anonymity, while Qubes OS emphasizes security through isolation.
- Tails is typically used as a live, disposable system, while Qubes OS is designed to be installed as the primary operating system on your machine.
- Both offer unique advantages, and the choice between them depends on your specific needs for security, privacy, and usability.



# Conclusion

- Qubes OS offers a unique approach to operating system security by isolating applications and operating systems into separate "qubes".
- Its integration with the Tor network through Whonix also enables enhanced privacy and anonymity.
- While Tails offers similar privacy features, its emphasis on being a live, disposable system sets it apart from Qubes OS.
- Both offer unique advantages, and the choice between them depends on your specific needs for security, privacy, and usability.

# Thank you for your time and attention 🙂

https://www.qubes-os.org/

https://www.hacklabg.net/

https://www.nohat.it/

Mattia Coffetti

Mattia (Mzkk_) Coffetti 🔍 | LinkedIn

HACKLAB BITM

COMPUTER SECURITY CONFERENCE NO HAT

# Presentazione associazione

2023

# L’associazione

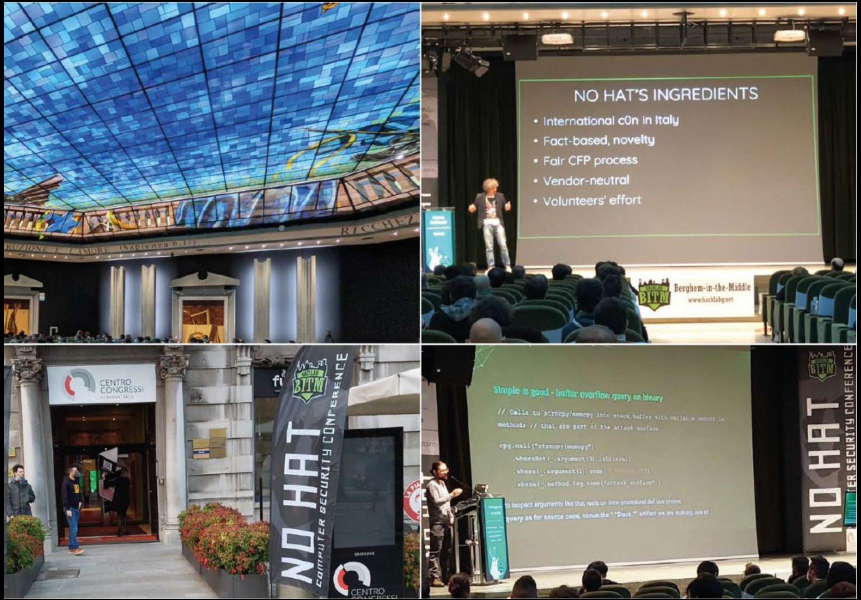
**“Berghem-in-the-Middle ETS”** l’**HackLab di Bergamo** è un’**Associazione senza fini di lucro** fondata nel luglio 2018 da un gruppo di appassionati e professionisti di sicurezza informatica e di informatica in generale: www.hacklabg.net

L’Associazione è animata dalla passione per tutto quello che concerne la sicurezza informatica e ha lo scopo di:

- diffondere la cultura della privacy e della sicurezza informatica
- essere punto di ritrovo per professionisti, studenti e appassionati di privacy e sicurezza
- sensibilizzare gli utenti alle tematiche della privacy e dell’anonimato

L’associazione **Berghem-in-the-Middle** organizza la conferenza annuale di sicurezza **«No Hat»** (www.nohat.it)**.** Dopo 4 edizioni di successo, è ora riconosciuta tra le maggiori conferenze di Security a livello nazionale, e ha ottenuto rilevanza Europea grazie all’alto livello dei contenuti presentati da ricercatori e specialisti della scena internazionale.

# No Hat 2022



- 9 talk con speaker internazionali
- 530 partecipanti in presenza
- 350+ visualizzazioni uniche dell'evento in streaming
- 17 sponsor
- 300+ litri di birra, 500+ caffè

www.nohat.it/2022

## No Hat 2023 : 21 ottobre