SYNACKTIV

The Good, the Bad, and the Secure

A pentester's journey daily driving Qubes OS

Pierre Milioni at Pass the SALT

2023/07/03

Whoami?

SYNACKTIV

- **Pierre Milioni (*@b1two_*)**
  - Pentester at Synacktiv
- **Working at Synacktiv**
  - Offensive security
  - 140+ ninjas: pentest, reverse engineering, development, CSIRT
  - 6 locations: Paris, Rennes, Lyon, Toulouse, Lille (very soon) & remote
  - We are hiring! → *apply@synacktiv.com*

Introduction

SYNACKTIV

- **Pentesting**
  - Audit systems & report vulnerabilities
  - Never ending flow of new missions
    - New environments
  - Large community
    - Lots of tools, lots of *poc* → lots of dependencies

Introduction

SYNACKTIV

- **Unsafe environment**
  - Unthinkable to audit everything
  - Exposed to multiple vulnerabilities

Introduction

SYNACKTIV

- **Need of a confined environment**
  - Containers & namespaces
    - Partial isolation
    - Docker, LXC/LXD, Podman, ...
  - Physically separated workstation
    - Full isolation
    - Not practical
  - Virtual machines
    - Strong isolation
    - VirtualBox, VMware, qemu/kvm, Qubes OS

Introduction

SYNACKTIV

- **In the end…**
  - Virtual machines w/ Qubes OS
    - Decent security
    - Implements handy features
    - Good community

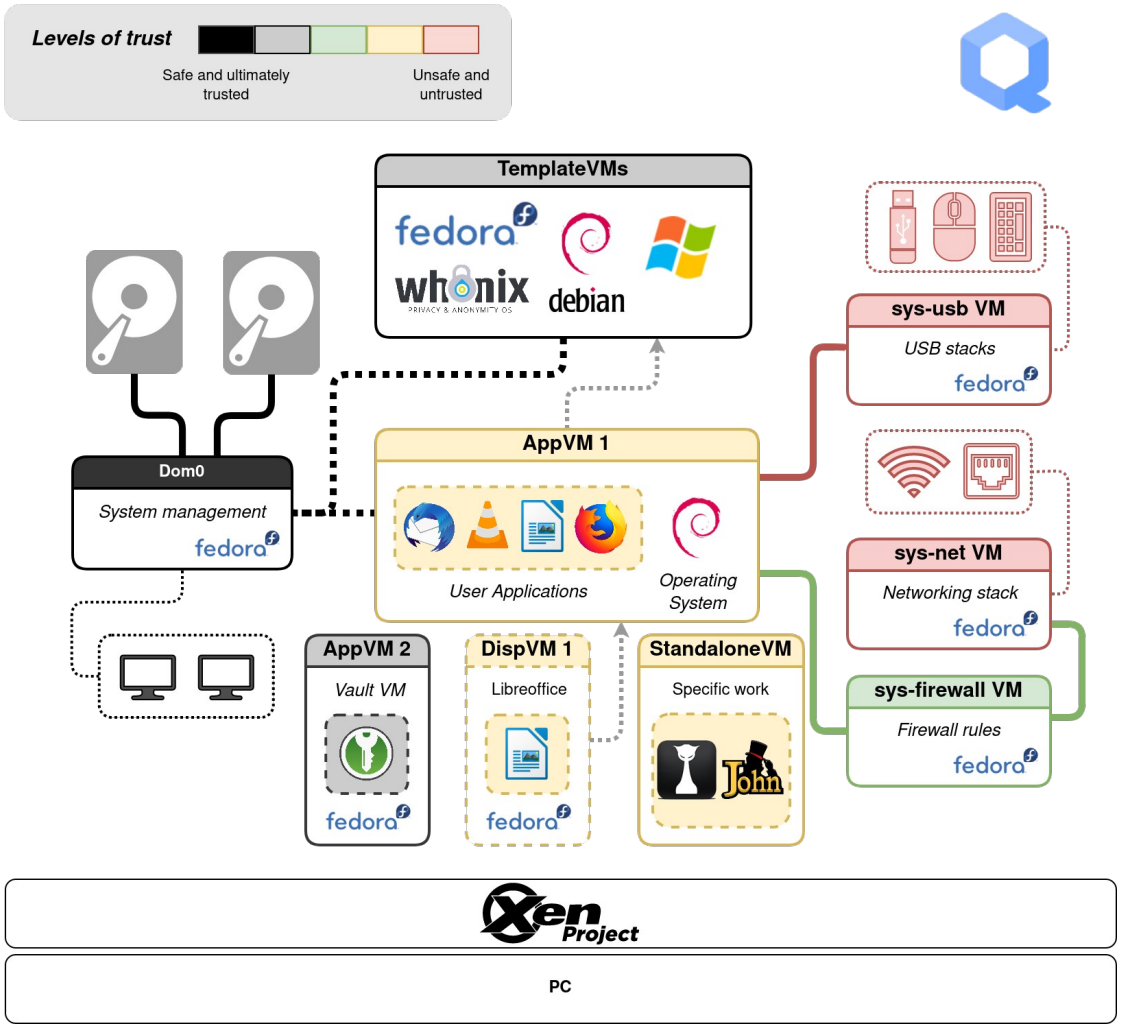
Introduction

SYNACKTIV

- **In the end…**
  - Virtual machines w/ Qubes OS
    - ~~Decent security~~
    - ~~Implements handy features~~
    - ~~Good community~~
    - Looked fun

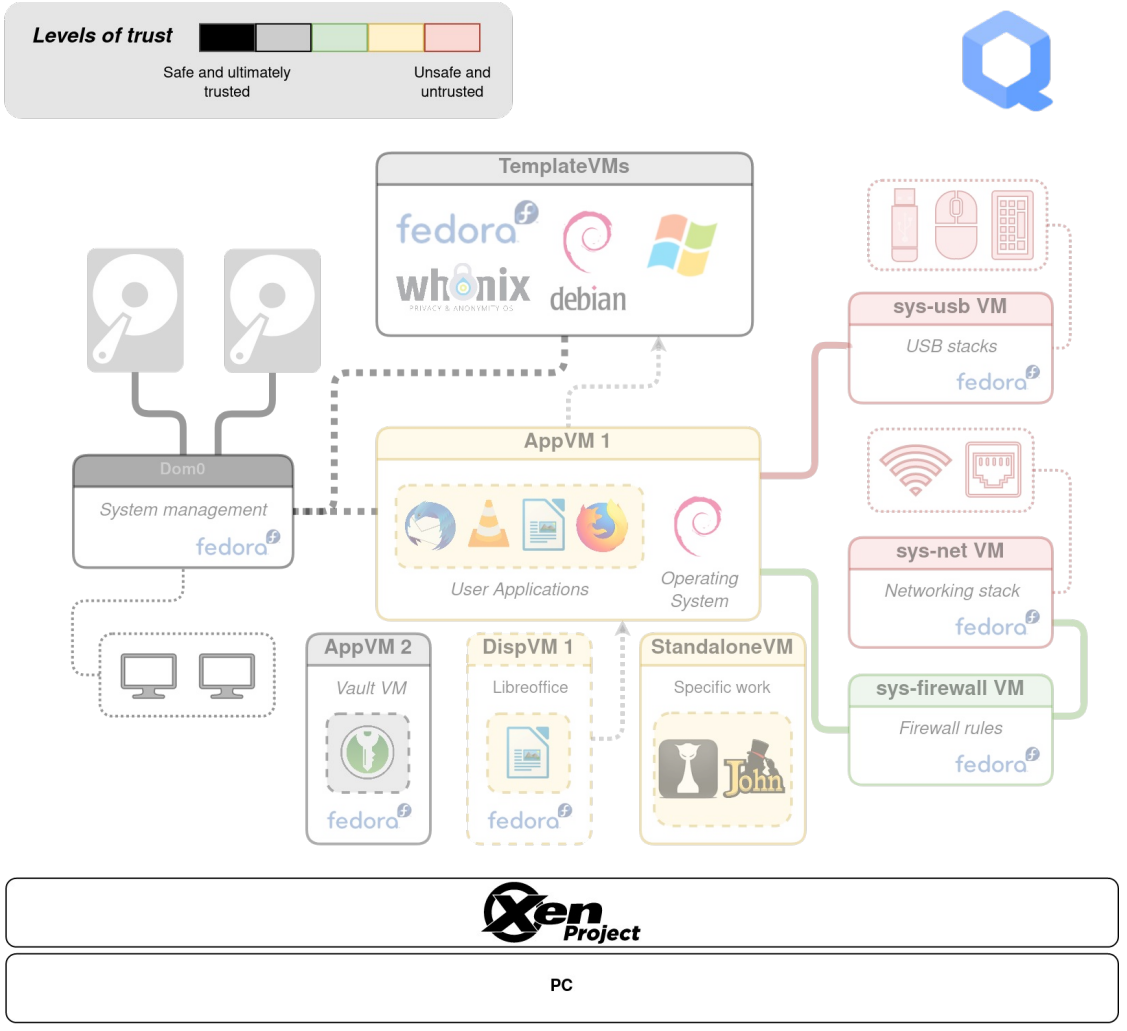
Exploring Qubes OS

SYNACKTIV



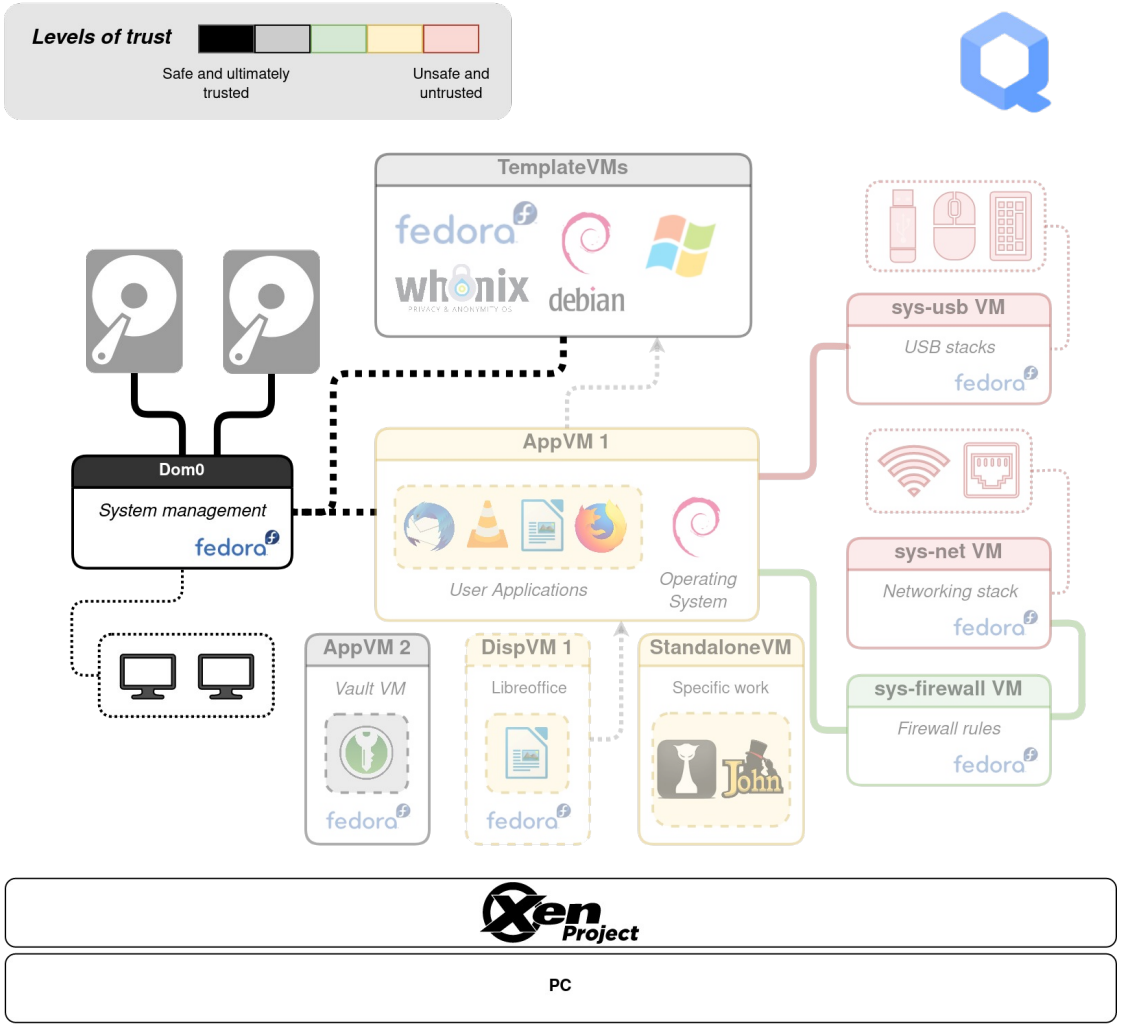
Exploring Qubes OS

SYNACKTIV



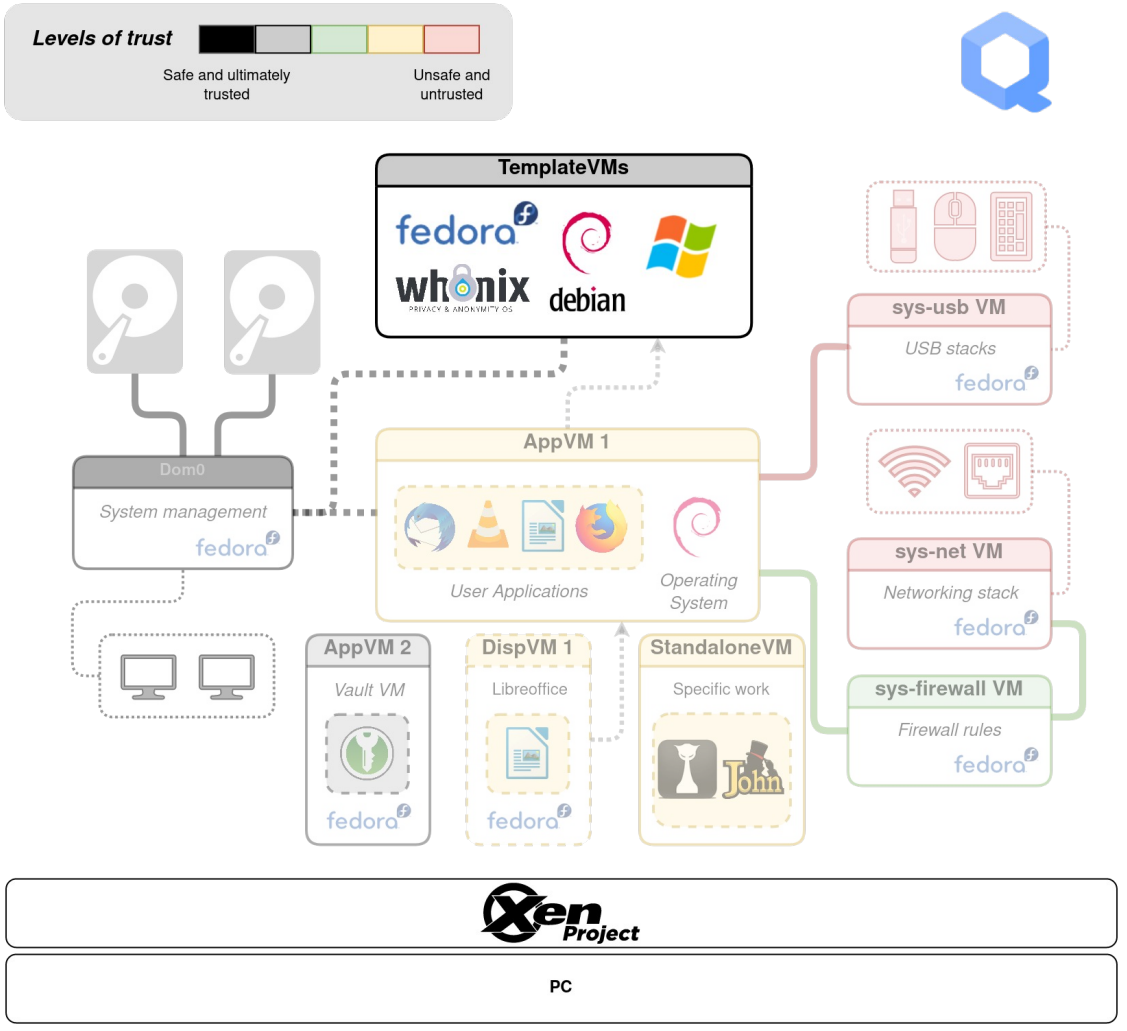
Exploring Qubes OS

SYNACKTIV



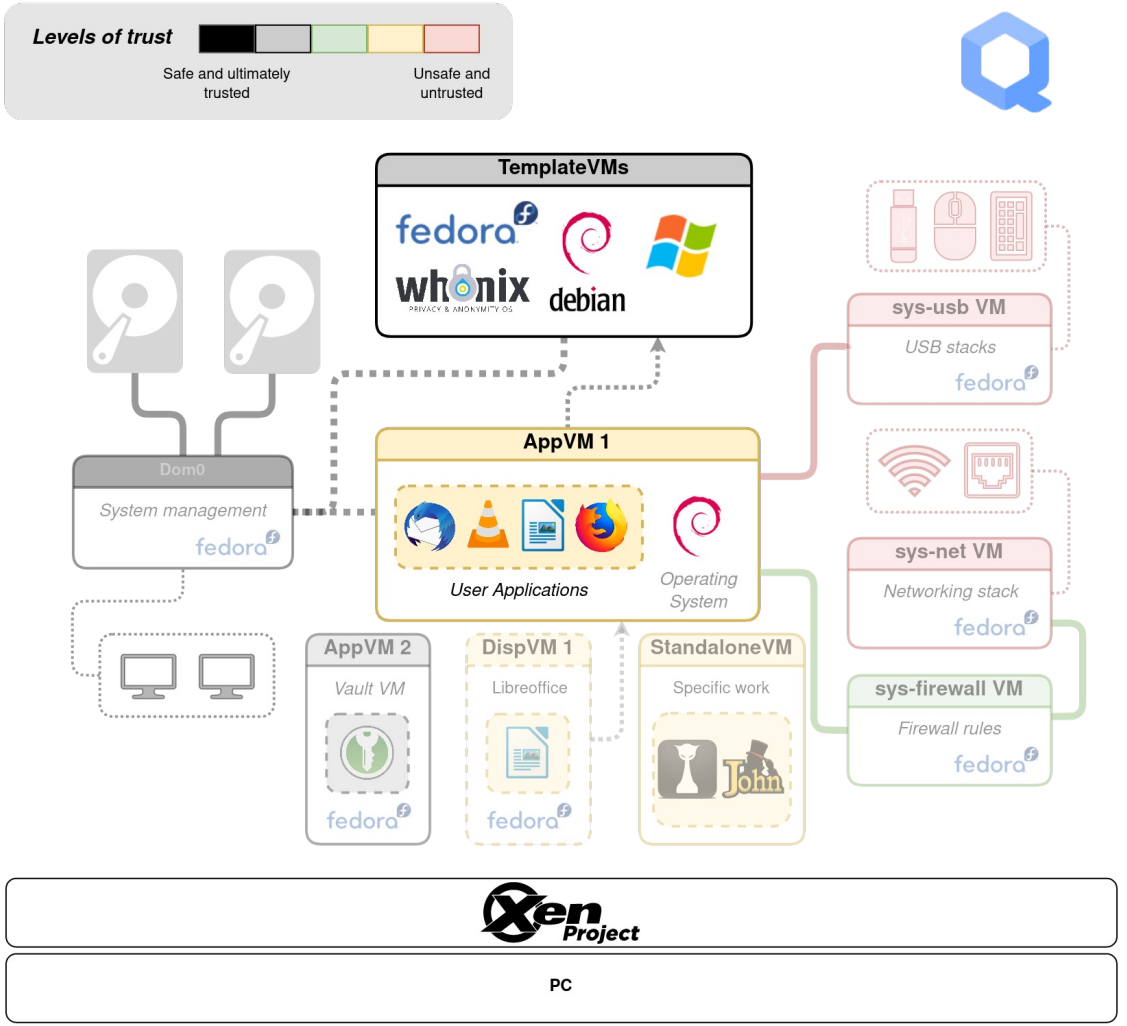
Exploring Qubes OS

SYNACKTIV



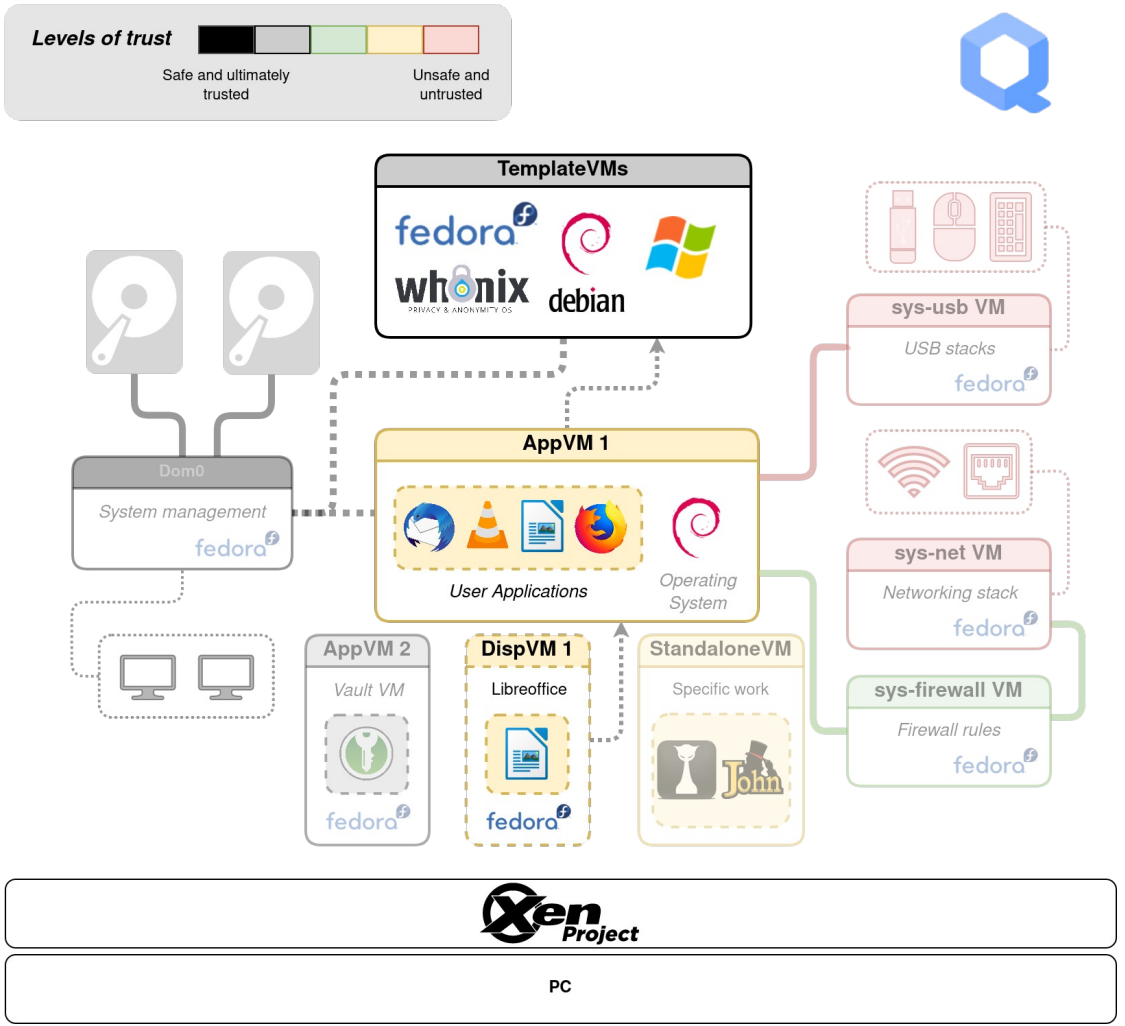
Exploring Qubes OS

SYNACKTIV



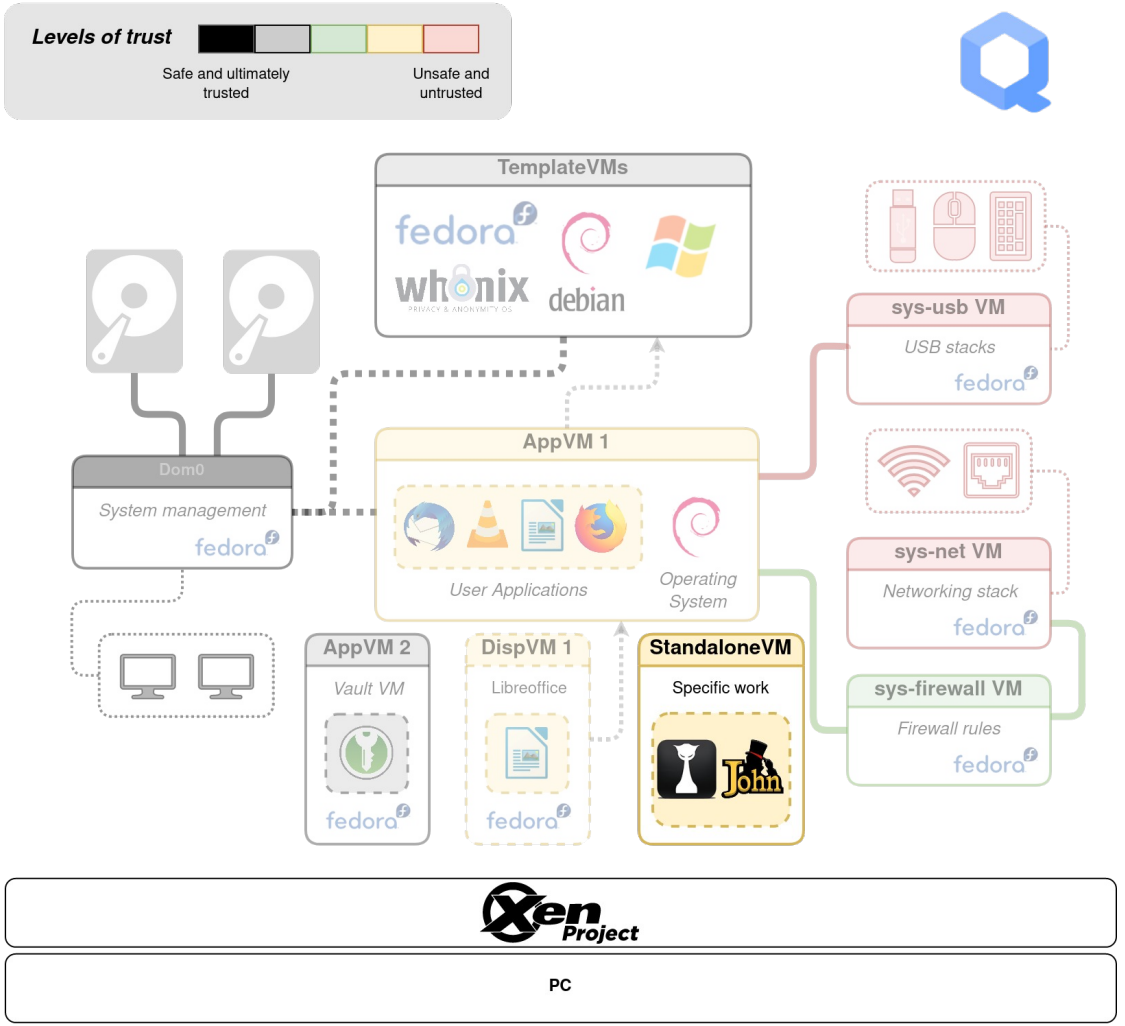
Exploring Qubes OS

SYNACKTIV



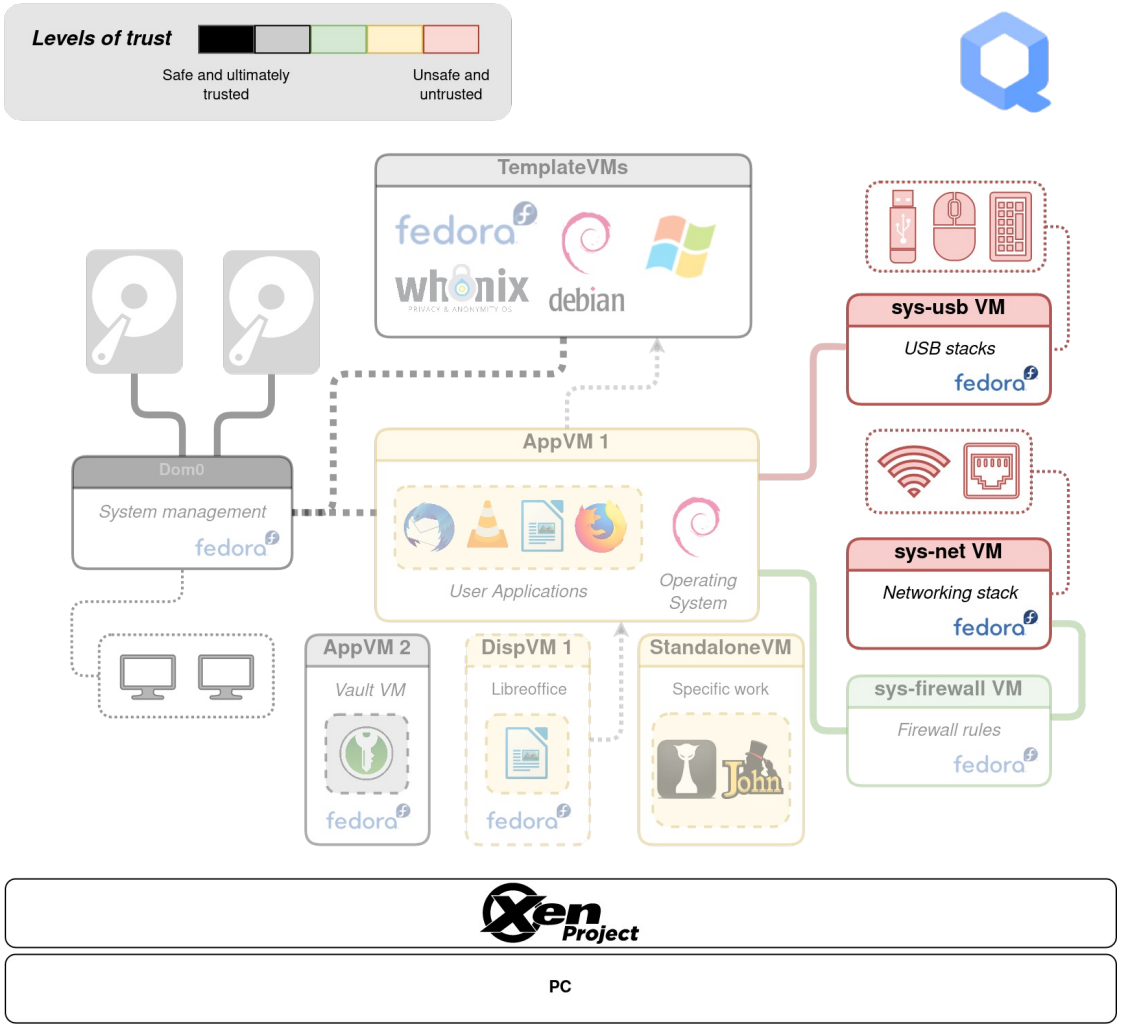
Exploring Qubes OS

SYNACKTIV



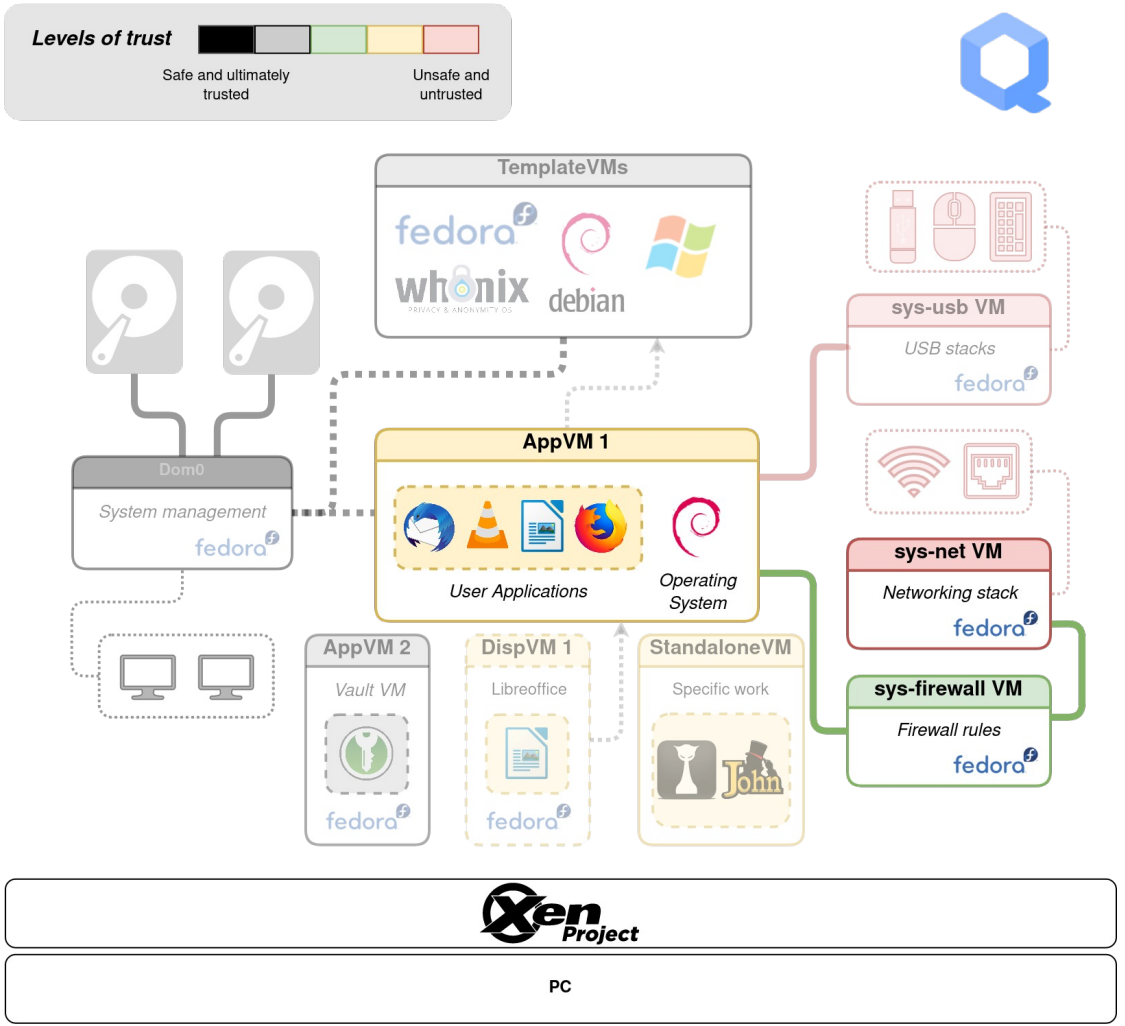
Exploring Qubes OS

SYNACKTIV



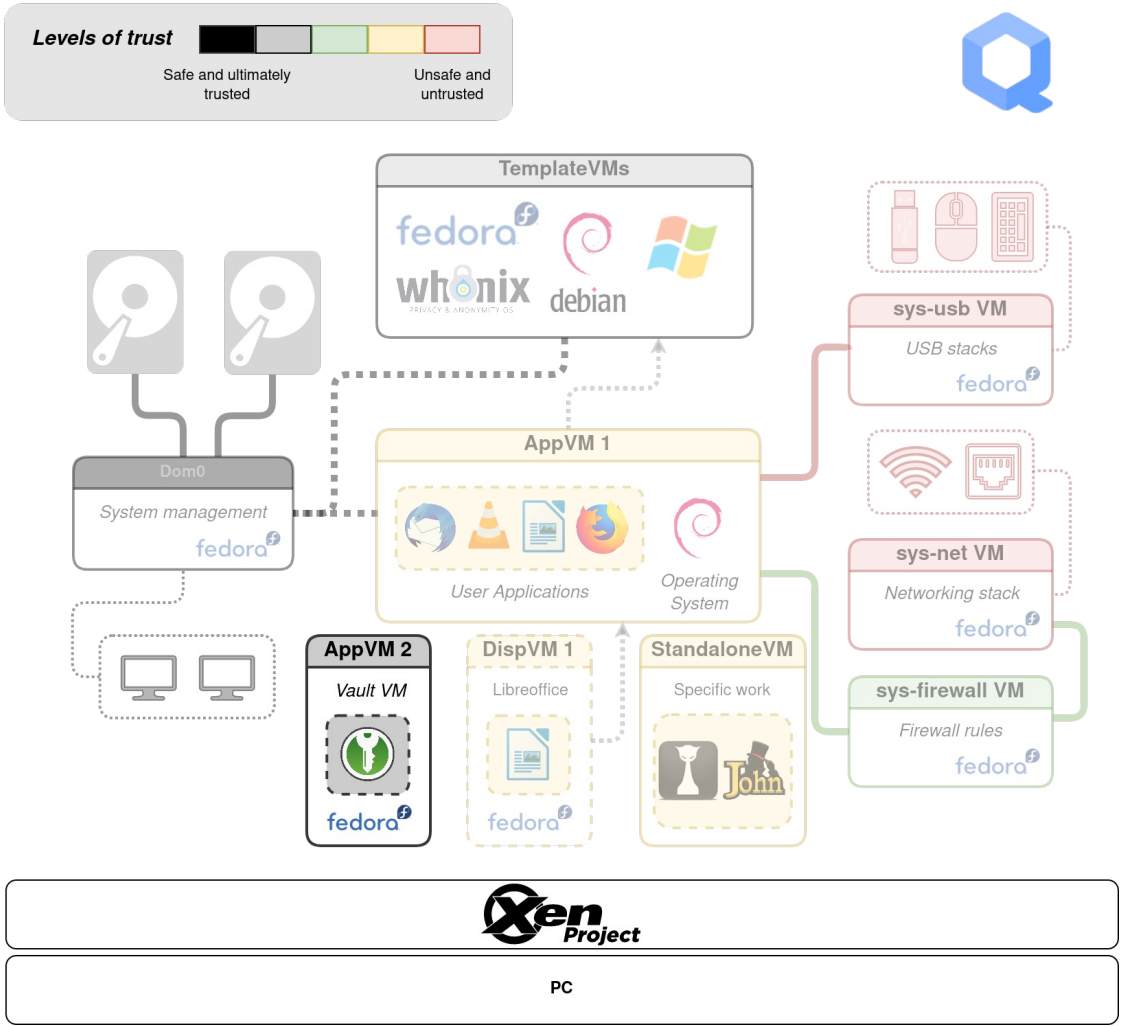
Exploring Qubes OS

SYNACKTIV



Exploring Qubes OS

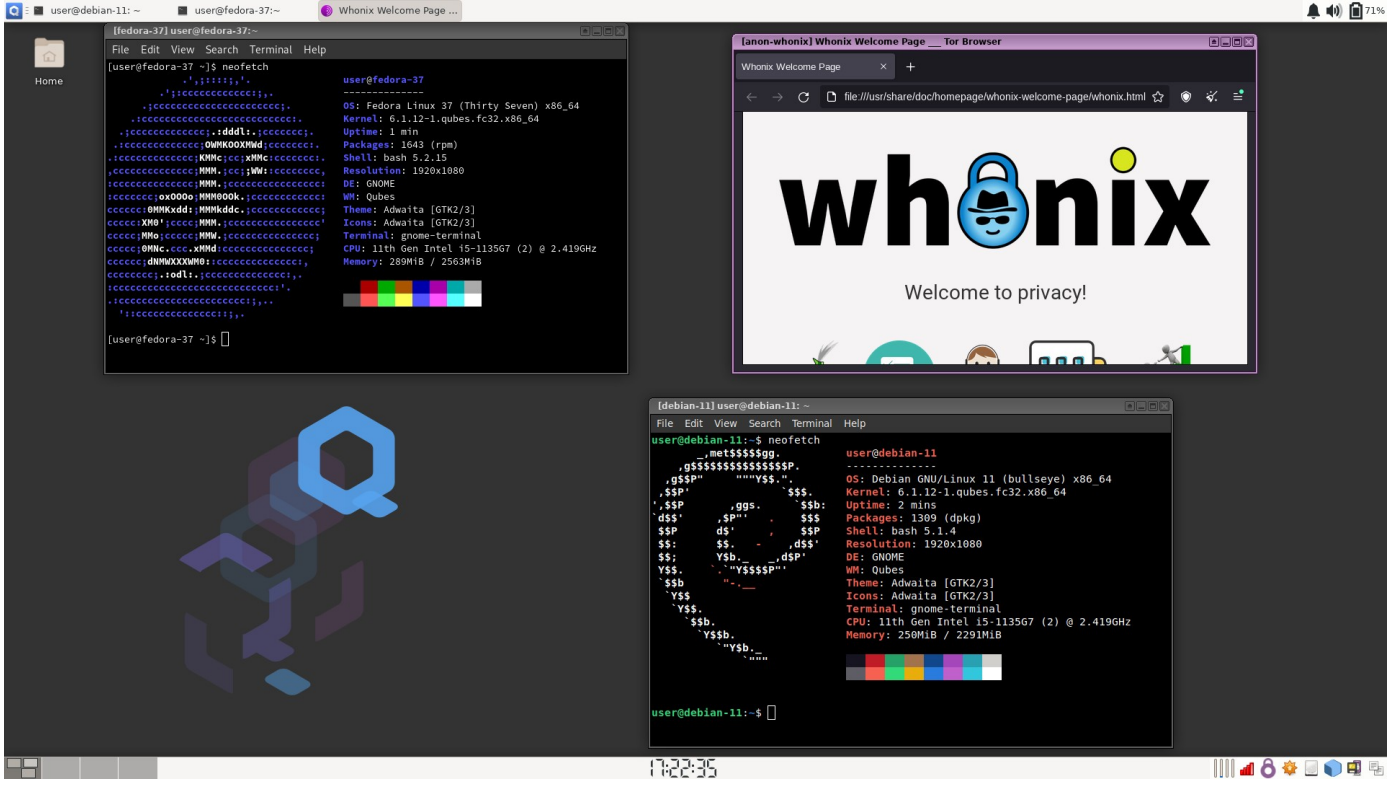
SYNACKTIV



Exploring Qubes OS

SYNACKTIV

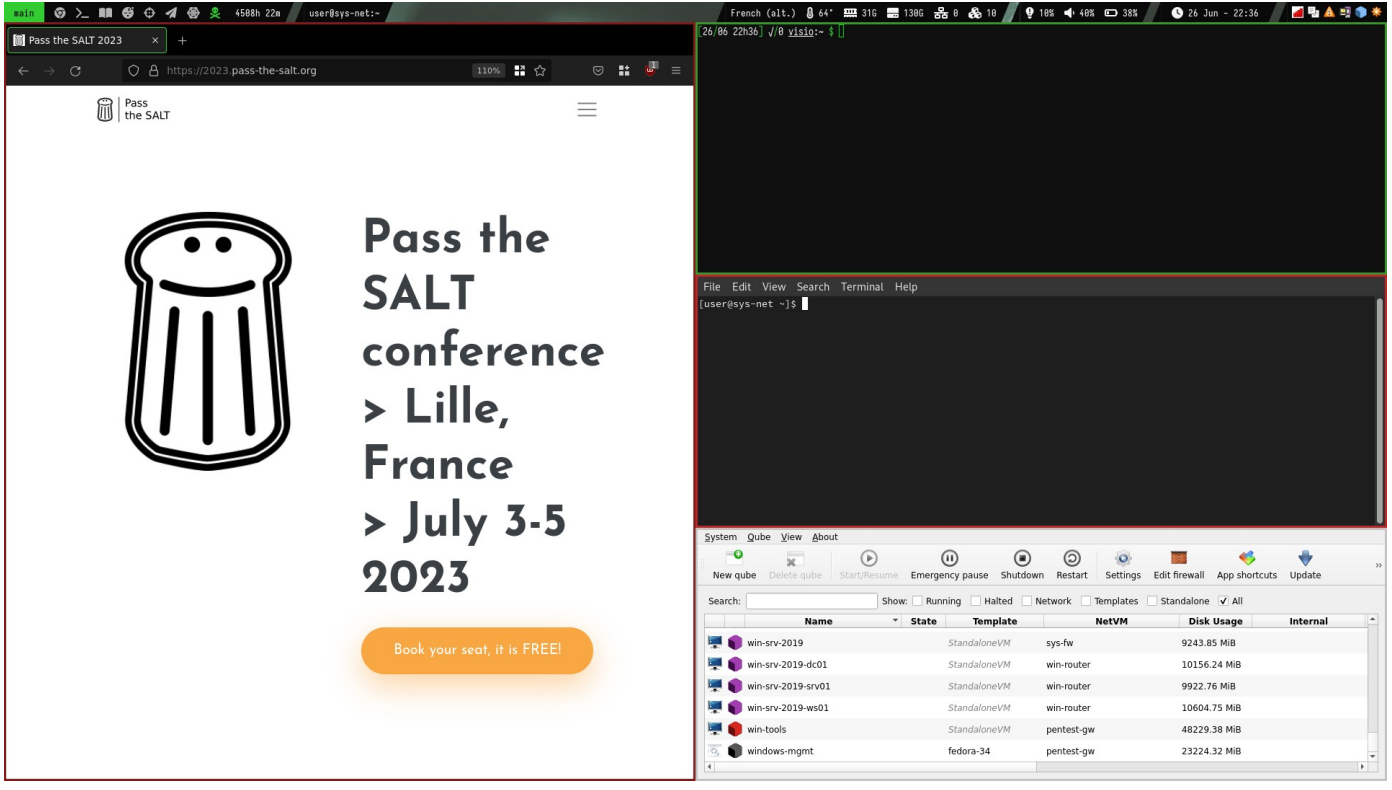
- **Icing on the cake**
  - Seamless integration



Exploring Qubes OS

SYNACKTIV

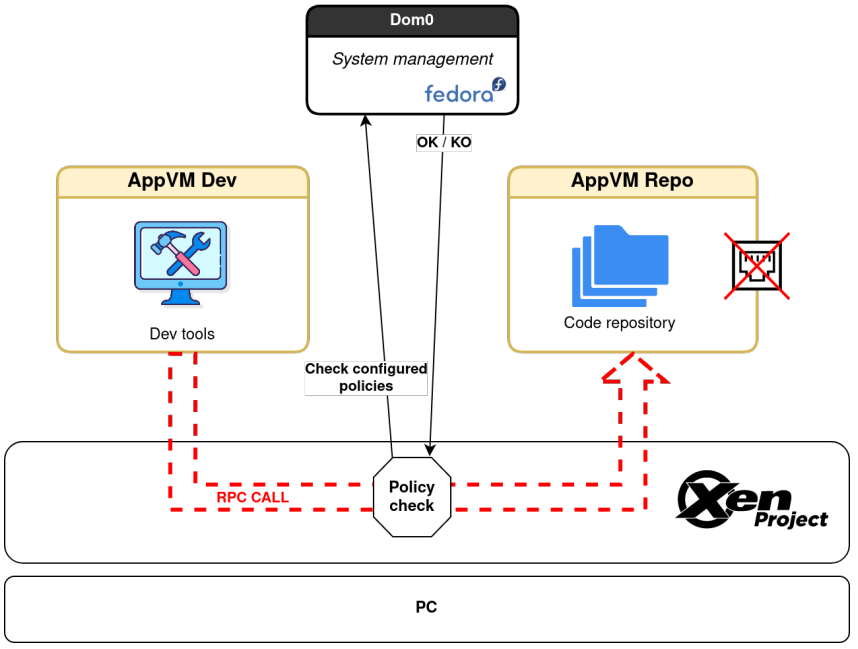
- **Icing on the cake**
  - Seamless integration



Exploring Qubes OS

SYNACKTIV

- **Icing on the cake**
  - RPC mechanism
    - Your handyman
    - Can do pretty much everything
    - Connect stdin/stdout between qubes
      - No need for network connection
    - Security enforced by policies in dom0
      - Allowed or asked
    - Use to expose services from a isolated qube



Exploring Qubes OS

- **Icing on the cake**
  - RPC mechanism
    - Your handyman
    - Can do pretty much everything
    - Connect stdin/stdout between qubes
      - No need for network connection
    - Security enforced by policies in dom0
      - Allowed or asked
    - Use to expose services from a isolated qube
    - Everything and anything
      - Careful not to reduce the overall security

Exploring Qubes OS

SYNACKTIV

- **And much more...**
  - Automation (Saltstack, ansible)
  - Backup system
  - Automatic desktop file distribution
  - Whonix integration
  - Graphical firewall configuration (for nothing too fancy)

Exploring Qubes OS

SYNACKTIV

- **Security benefits**
  - Segmentation is key
    - Rubber ducky
    - Supply chain attacks
    - Browser 0 days
    - Infected documents
    - Malicious POC
    - Stack TCP/IP exploits

Exploring Qubes OS

SYNACKTIV

- **Security benefits**
  - Segmentation is key
    - ~~Rubber ducky~~
      → sys-usb
    - Supply chain attacks
    - Browser 0 days
    - Infected documents
    - Malicious POC
    - Stack TCP/IP exploits

Exploring Qubes OS

SYNACKTIV

- **Security benefits**
  - Segmentation is key
    - ~~Rubber ducky~~
      → sys-usb
    - ~~Supply chain attacks~~
    - ~~Browser 0 days~~
    - ~~Infected documents~~
    - ~~Malicious POC~~
      → dedicated qube / dispVMs
    - Stack TCP/IP exploits

Exploring Qubes OS

SYNACKTIV

- **Security benefits**
  - Segmentation is key
    - ~~Rubber ducky~~
      → sys-usb
    - ~~Supply chain attacks~~
    - ~~Browser 0 days~~
    - ~~Infected documents~~
    - ~~Malicious POC~~
      → dedicated qube / dispVMs
    - ~~Stack TCP/IP exploits~~
      → sys-net / sys-fw

Exploring Qubes OS

SYNACKTIV

- ~~**Security benefits**~~
  - Xen 0 day vulnerabilities

Unveiling the user experience

SYNACKTIV

- **Enough with the commercial talk**
- **My experience**
  - 1 year part-time
    - Played with Qubes OS 4.0
    - Then switched to 4.1 release candidates
  - 1.5 years full-time
    - Started with Qubes OS 4.1-rc4
    - Both personal and professional computers

Unveiling the user experience

SYNACKTIV

- **Some statistics about my usage**
  - 103 qubes
  - 8 qubes started at boot (dom0, networking, USB, email, chat, internal browser, vault)
  - 13 qubes in normal usage (+ pentest, browsing, notes)

- **The computer**
  - Intel i7 (8th gen)
  - 48Go of RAM
  - 1To of SSD storage

  - Intel i7 (12th gen)
  - 32 → 64Go of RAM
  - 1+1To of SSD storage
  - Nvidia GPU

Unveiling the user experience

SYNACKTIV

- **Go over some usages and discuss**
  - Overall utilization
  - Browsing
  - Doing your job
    - Pentesting
    - Developing
    - Reporting
  - Visio conferencing
  - General organization
    - Multiple activities
    - Networking

Unveiling the user experience

SYNACKTIV

- **Overall utilization – the bad**
  - Need a powerful computer
    - The more RAM, the better
      - At the very least 16GB for Qubes OS as a main workstation
      - 32GB to be able to work without really worrying about RAM
      - 48GB to be really comfortable
      - 64GB for people like me who start a million things at once
    - Not so many monitoring tools
      - *Xentop*

Unveiling the user experience

SYNACKTIV

- **Overall utilization – the bad**
  - No hibernation (= S4 sleep) (= Suspend to disk)
    - S3 sleep (suspend to RAM)
      - Your computer has to support it
        → recent Dells do not

Unveiling the user experience

SYNACKTIV

- **Overall utilization – the bad**
  - No hibernation (= S4 sleep) (= Suspend to disk)
    - S3 sleep (suspend to RAM)
      - Your computer has to support it
        → recent Dells do not
    - Get used to power off your system
      - Really annoying at first
      - Forces you to keep your working environment clean
      - Forces you to write scripts to automate your setup

Unveiling the user experience

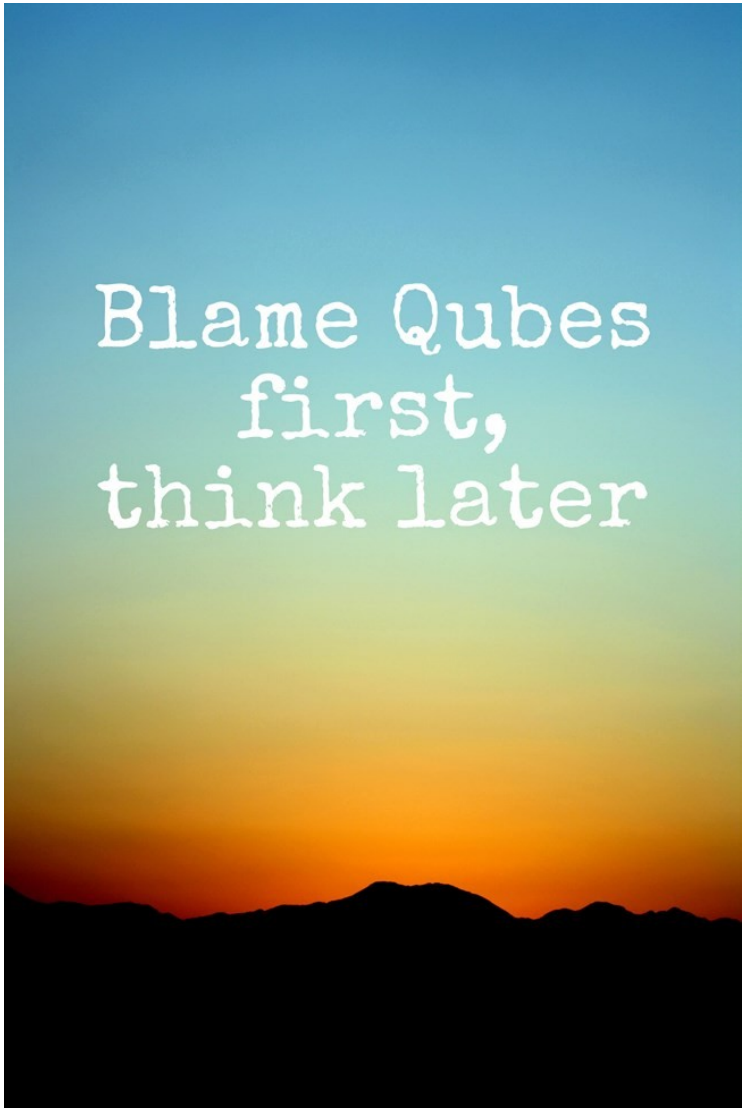
SYNACKTIV

- **Overall utilization – the bad**
  - Bad autonomy
    - Depends on the laptop
      - 1st laptop: 2h30 (vs 4h)
      - 2nd laptop: <2h (vs ?)

Unveiling the user experience

- **Overall utilization – the bad**
  - Bad autonomy
    - Depends on the laptop
      - 1st laptop: 2h30 (vs 4h)
      - 2nd laptop: <2h (vs ?)
  - The Qubes effect

    “Blame Qubes OS first, think later”



Unveiling the user experience

SYNACKTIV

- **Overall utilization – the good**
  - Good for unorganized people
  - Stable system
    - No full reinstall since the switch
      - Swapped disk during laptop change
      - Reinstall regularly some qubes to keep them clean
    - Never booted again on my previous distro since the switch
  - Migration between systems simplified

Unveiling the user experience

SYNACKTIV

- **Browsing**
  - Works just fine
  - Struggles with heavy websites
    - No hardware acceleration
    - No 200+ tabs browsers anymore
  - Just like classical browsing
    - Doing things with Qubes is quite like doing them with a classical distro

Unveiling the user experience

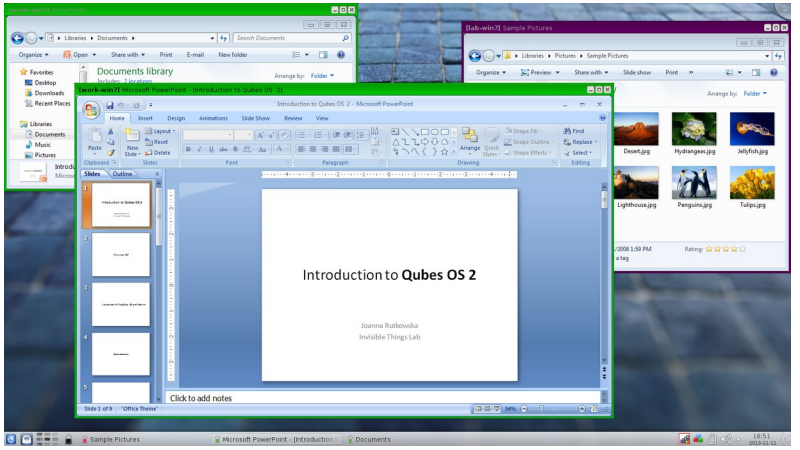
SYNACKTIV

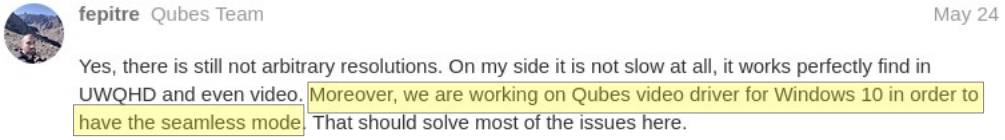
- **Pentesting – the good**
  - Fresh environment
    - Templating
    - Create new environments with ease
  - Simplifies complex network setup
    - Ex: internal pentests, automatic VPN
    - No risks using the wrong IP address
  - Peace of mind
    - Security
    - No mixing different missions

Unveiling the user experience

SYNACKTIV

- **Pentesting – the good**
  - Windows environments
    - Well integrated w/ QWT
      - Copy/paste
      - File exchange
      - RPC system
      - Seamless on Win7, maybe Win10 someday?

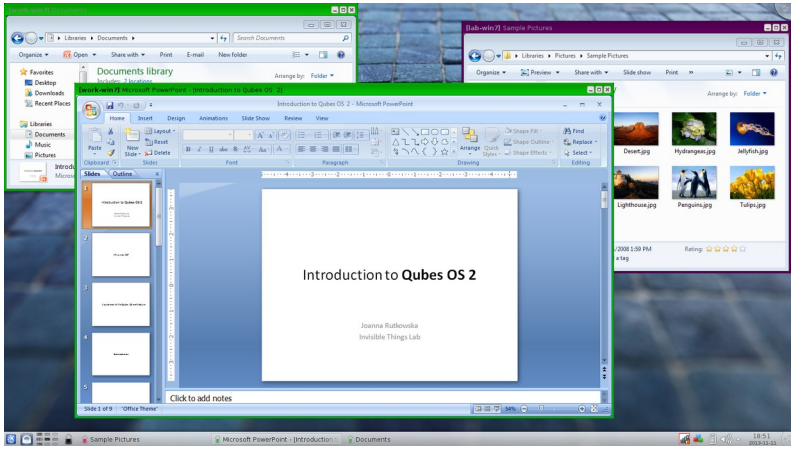




Unveiling the user experience

SYNACKTIV

- **Pentesting – the good**
  - Windows environments
    - Well integrated w/ QWT
      - Copy/paste
      - File exchange
      - RPC system
      - Seamless on Win7, maybe Win10 someday?
    - Templating system too
      - Low size Windows virtual machines



Unveiling the user experience

SYNACKTIV

- **Pentesting**
  - Qubes OS is not a reason to drop hardening
    - Qubes really exposed to vulnerabilities/exploitation
    - No need to automatically give up a qube to attackers

Unveiling the user experience

SYNACKTIV

- **Pentesting – the bad**
  - Templates are annoying with “one-qube” packages
    - Standalones
    - OverlayFS
  - Mobile application audit are painful
    - No nested virtualization
      - At least I did not manage to do it (yet)
    - x86 Android qubes

Unveiling the user experience

SYNACKTIV

- **Developing**
  - Development template
  - One qube per project
  - Synchronization could be cumbersome
    - No shared folder between qubes
    - Custom solution using RPC

Unveiling the user experience

SYNACKTIV

- **Reporting**
  - Disposable VMs to open untrusted documents
  - Copy/Paste only raw data between qubes
    - No image copy-pasting
    - No custom type copy-pasting
    - Custom RPC script: *xclip -target image/png*

Unveiling the user experience

SYNACKTIV

- **Visio conferencing**
  - No builtin functionality to screen share another qube
    - Manual solution: *ffmpeg* + RPC call
  - Lack of performances
  - GPU passthrough

Unveiling the user experience

SYNACKTIV

- **General organization**
  - Own private infrastructure
    - Easy to setup
    - Very powerful
  - Routed network
  - Easy to isolate environments

Closing notes

SYNACKTIV

- **Do not take security for granted**
  - Qubes OS gives good foundations
  - There is still a lot of room for human error
  - Hardening is still relevant

Closing notes

SYNACKTIV

- **Should I switch to Qubes OS?**
  - Still thinking about switching after everything I said?
    It means you probably should
  - Will be usable as is, but…
    - You will spend time matching it to your company standards
      - Especially if you're alone to switch
      - Do not switch before knowing the environment
    - You will spend a crazy amount of time customizing it to be comfortable

Closing notes

SYNACKTIV

- **Should I switch to Qubes OS?**
  - Remember
    - Make sure your hardware is compatible
    - Make sure your company is OK with it
    - Be ready to commit (especially if you are switching solo)
    - Sometimes it will not always work as expected

Closing notes

SYNACKTIV

- **How to switch to Qubes OS?**
  - Install via USB first
    - Do not deploy *sys-usb* during that period!
  - Ensure a proper base
  - Make sure you have nothing too important the next week or so
  - Just do it

Closing notes

SYNACKTIV

- **Did I ever regret switching to Qubes OS?**
  - Sometimes you just want to throw your computer through the window
  - Never looked back
  - Too comfortable compared to “classical” distros

Closing notes

SYNACKTIV

- **Marek (lead dev) was here**

Why?
How?
Details
Status

Improving client systems security with Qubes OS

Marek Marczykowski-Górecki, Invisible Things Lab

4 Jul 2016

https://archives.pass-the-salt.org/RMLL%20Security%20Tracks/2016/slides/RMLL-Sec-2016-07-04-04-Marczykowski-QubesOS.pdf

SYNACKTIV

Questions?

https://www.linkedin.com/company/synacktiv

https://twitter.com/synacktiv

https://synacktiv.com