SECUREDROP

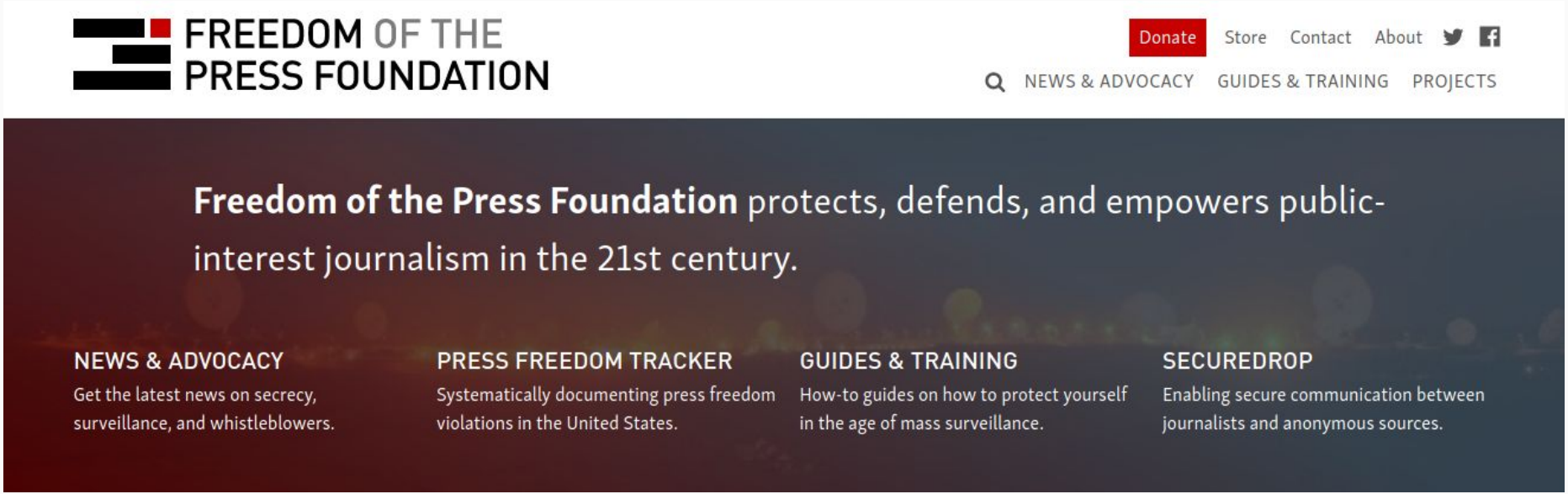
SecureDrop Workstation:

Handling unsafe documents safely

LibrePlanet 2021
Conor Schaefer
Chief Technology Officer, Freedom of the Press Foundation

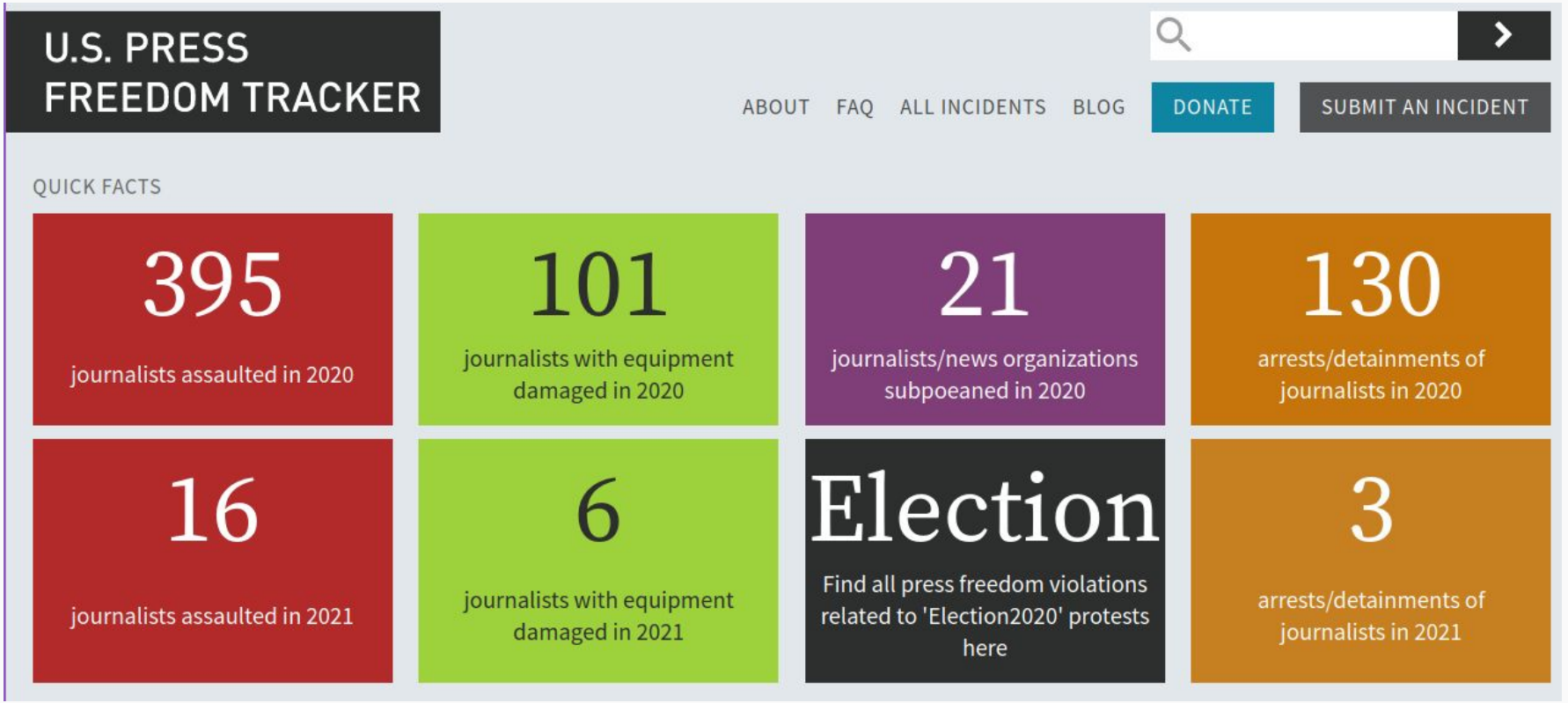
Overview

- Intro, about FPF
- SecureDrop
  - What it is
  - Who uses it
  - Motivations
  - How it works today
- Workstation
  - Qubes OS
  - How isolation works
  - Pilot program
- Security audit
- Next steps


FREEDOM OF THE PRESS FOUNDATION
Donate
Store
Contact
About
NEWS & ADVOCACY
GUIDES & TRAINING
PROJECTS
Freedom of the Press Foundation protects, defends, and empowers public-interest journalism in the 21st century.
NEWS & ADVOCACY
Get the latest news on secrecy, surveillance, and whistleblowers.
PRESS FREEDOM TRACKER
Systematically documenting press freedom violations in the United States.
GUIDES & TRAINING
How-to guides on how to protect yourself in the age of mass surveillance.
SECUREDROP
Enabling secure communication between journalists and anonymous sources.

US Press Freedom Tracker

https://pressfreedomtracker.us



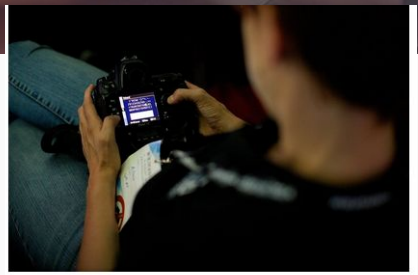
Guides & Training

Our training team delivers digital security trainings to news organizations, freelance and citizen journalists, and other at-risk groups. With education and advocacy, we aim to protect press freedoms through the adoption of the tools and practices included in our trainings.

FROM FPF

What to do if your phone is seized by police

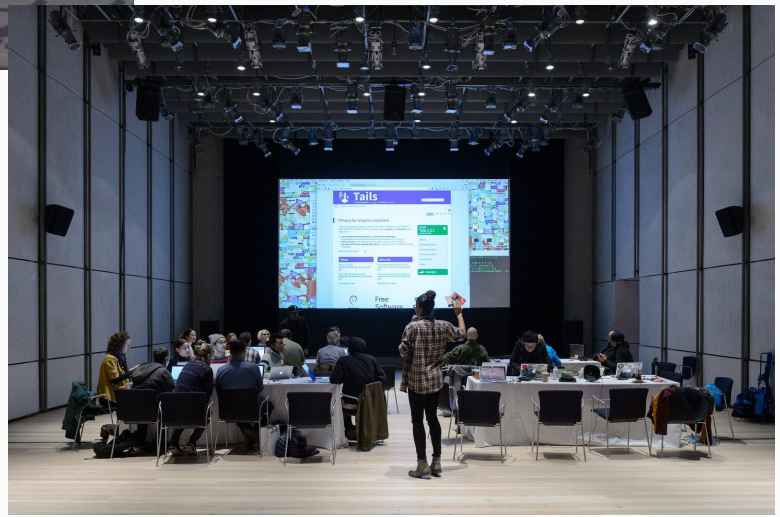
So, you've been arrested at an event. You're taken to the police station and your phone is confiscated. When you're let out, you realize someone has gone through your digital belongings. What now?



FROM FPF

Everything you wanted to know about media metadata, but were afraid to ask

Take a crash course in some of the tools you can use to analyze, manipulate, and scrub media metadata.



SecureDrop is an online whistleblowing platform, hosted on-premise by news organizations. It uses Tor Onion services for anonymity and GPG for encryption. The code is free software, under the AGPL.

Some of the organizations that currently use SecureDrop

SECUREDROP

Why SecureDrop?

Journalists have an inherently risky job

CPJ Committee to Protect Journal

NEWS & ANALYSIS DATA & RESEARCH SERVICES & RESOURCES ADVOCACY & ACTIO

Safety Advisories

CPJ Safety Advisory: Journalist targets of Pegasus spyware

November 6, 2019 11:30 AM ET

The New York Times

TIMES INSIDER

Someone Tried to Hack My Phone. Technology Researchers Accused Saudi Arabia.

From a suspicious text message I received, technology researchers concluded that hackers working for Saudi Arabia had targeted my phone with powerful Israeli software.

By Ben Hubbard

Published Jan. 28, 2020 Updated Jan. 30, 2020

56

Columbia Journalism Review.

The voice of journali

Local News Covering Trump Business of Journalism Innovation

About Donate Membersh

ARCHIVES: BEHIND THE NEWS

The looming threat of newsroom cyber attacks

Recent attacks on the *Albuquerque Journal* and WBOC reveal the importance of digital security

Jeff Bezos hack: Amazon boss's phone 'hacked by Saudi crown prince'

▲ Jeff Bezos, the Saudi crown prince, and the alleged phone-hacking plot – video explainer

The Amazon billionaire Jeff Bezos had his mobile phone "hacked" in 2018 after receiving a WhatsApp message that had apparently been sent from the personal account of the crown prince of Saudi Arabia, sources have told the Guardian.

Whistleblowing is an inherently risky act

Search

Bloomberg

Prognosis

Hospitals Tell Doctors They'll Be Fired If They Speak Out About Lack of Gear

By Olivia Carville, Emma Court, and Kristen V Brown
March 31, 2020, 6:23 AM PDT

'Hero who told the truth': Chinese rage over coronavirus death of whistleblower doctor

The death of a whistleblowing Chinese doctor who was punished for trying to raise the alarm about coronavirus has sparked an explosion of anger, grief and demands for freedom of speech among ordinary Chinese.

BBC News Sport Reel Worklife Travel Future Culture More Search

NEWS

Home Video World US & Canada UK Business Tech Science Stories Entertainment & Arts More

US & Canada

Ex-CIA officer Jeffrey Sterling jailed for leaking

By Tara McKelvey
BBC News, Alexandria, Virginia

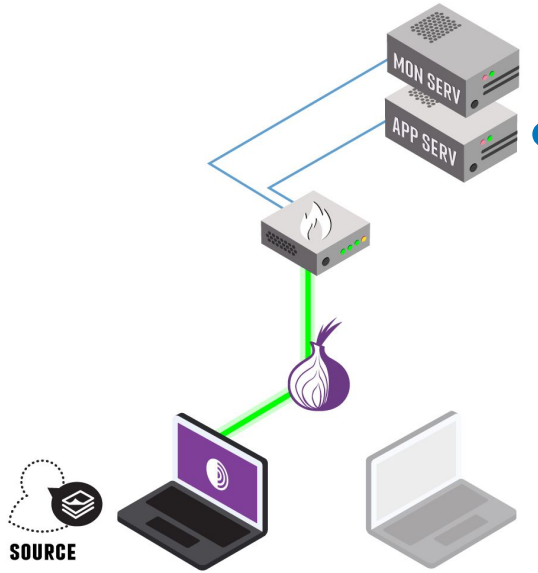
12 May 2015 Share

Jeffrey Sterling, a former CIA officer, will serve out his prison sentence in Missouri

Don’t roll your own implementation

- Security software must be audited, with results public
- Sources need assurances regarding communication
- Free software provides a stable, well-reviewed implementation
- Newsrooms can position themselves downstream from custom development

How it works

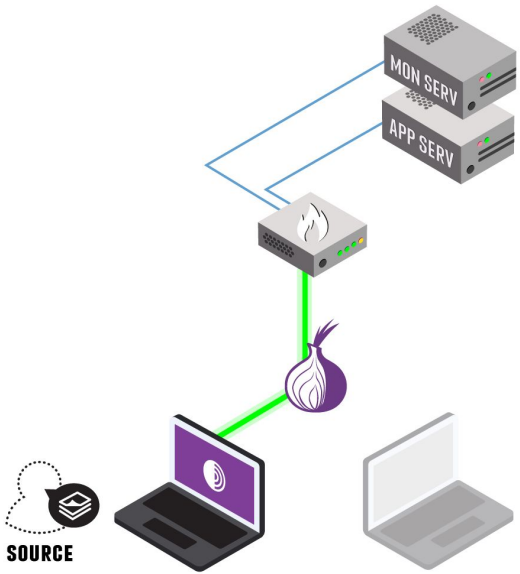


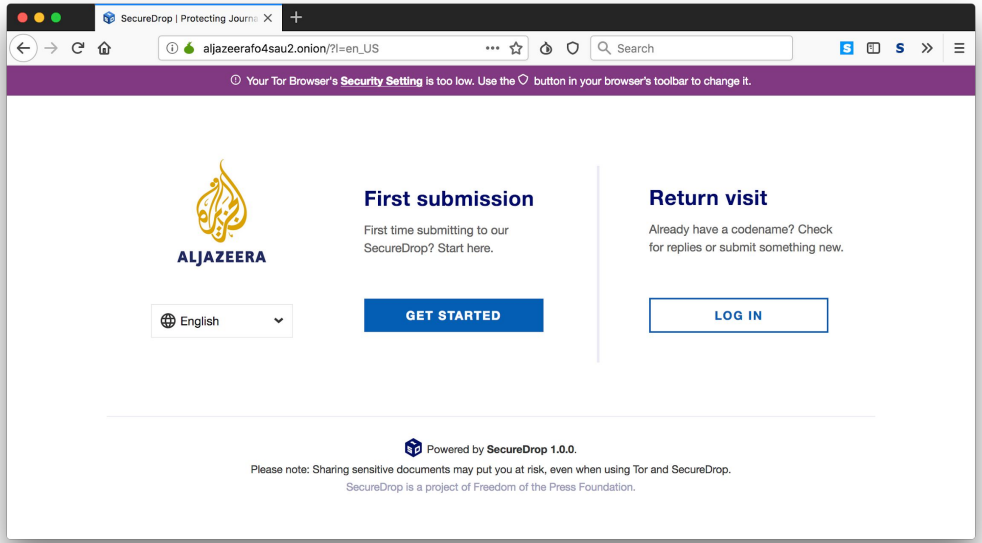
Application server: Runs two Python web applications (one for sources, one for journalists) exposed via Tor Onion Services.

Source Interface: Public v3 Onion URL, accessible by anyone in Tor Browser

Journalist Interface: Authenticated v3 Onion URL. Requires key-based auth to resolve. Only accessible to journalists.

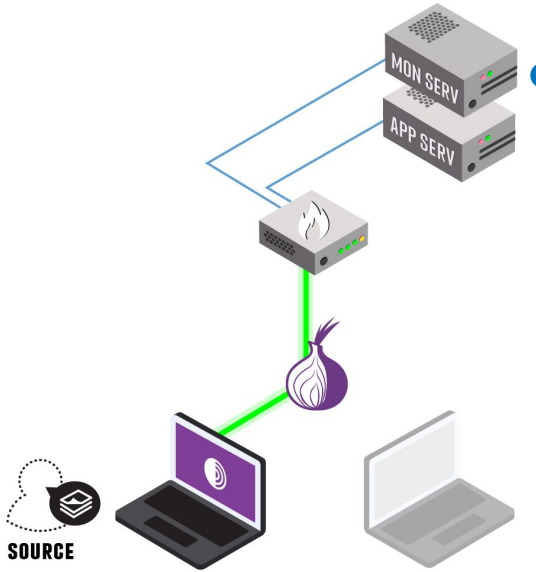
SECUREDROP





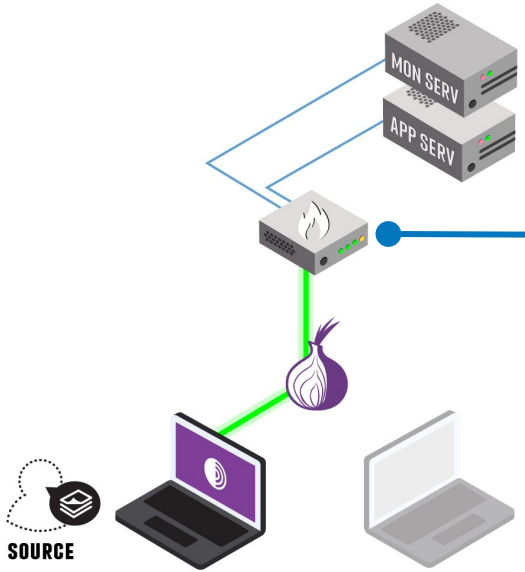
What the source sees

SECUREDROP



Monitoring server: Runs a host-based IDS (OSSEC) to monitor the application server and send alerts to administrators

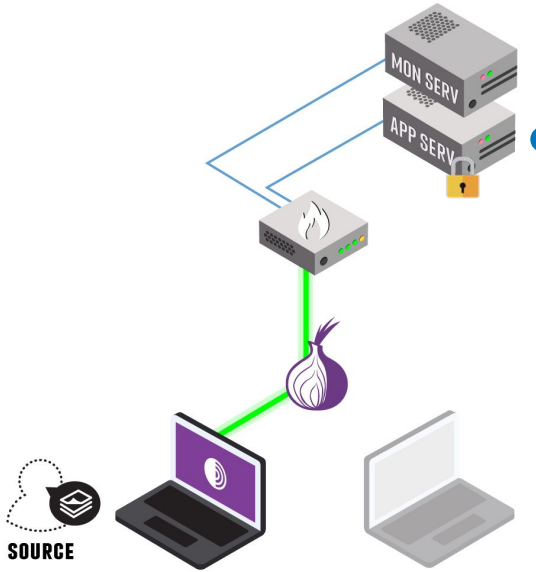
SECUREDROP



Network firewall: pfSense used to isolate the SecureDrop area of the network from the rest of the news organization

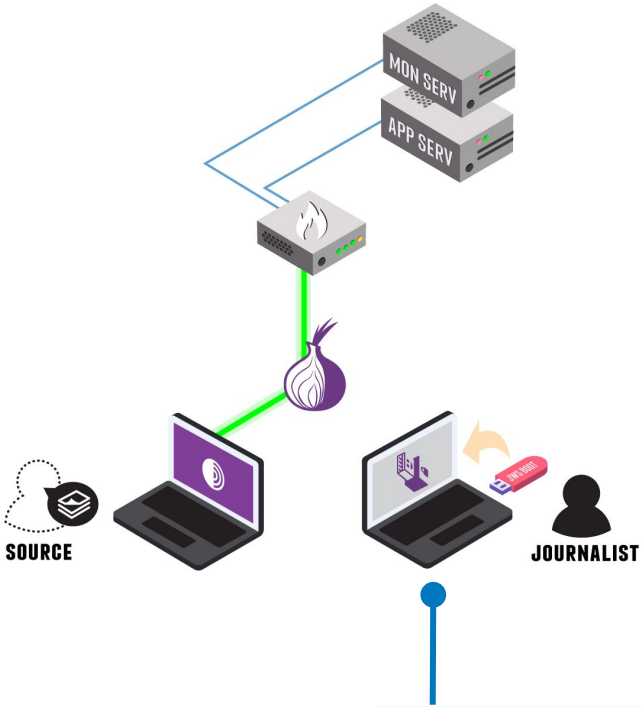
Drops all inbound traffic, except established/related. Tor Onions provide NAT-punching.

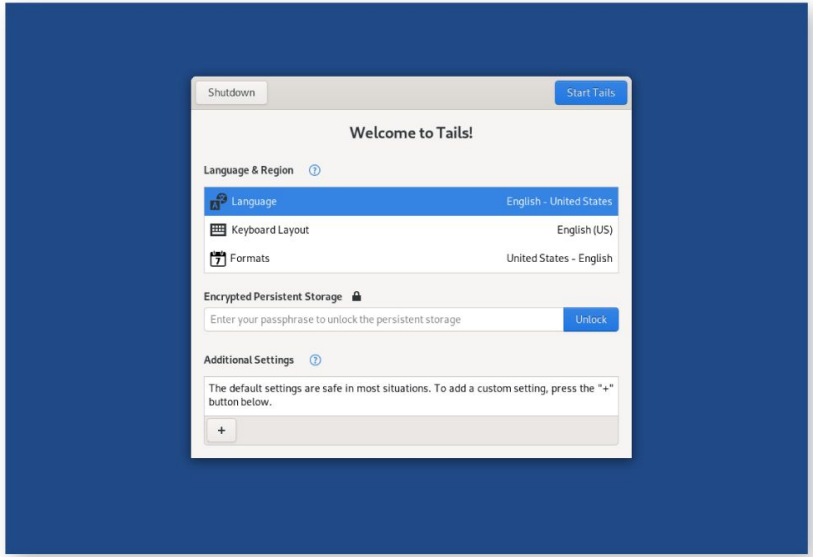
SECUREDROP



Documents stored encrypted to the instance's public key

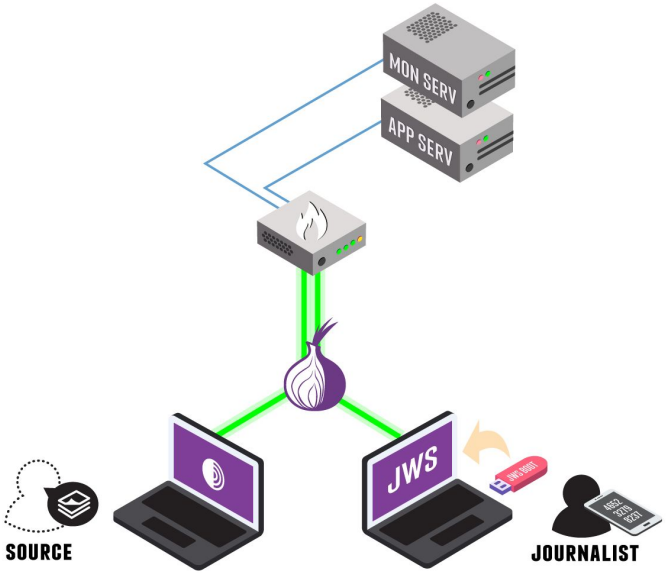
SECUREDROP

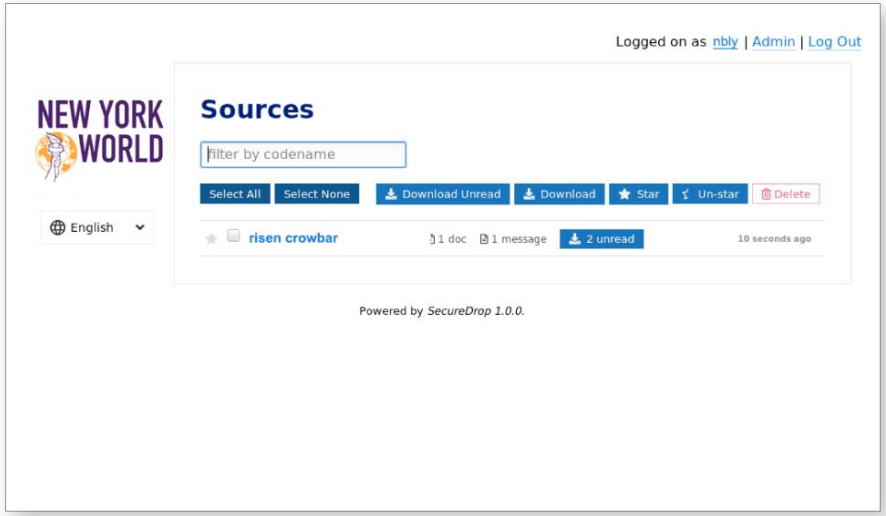




Journalists log in to Tails OS

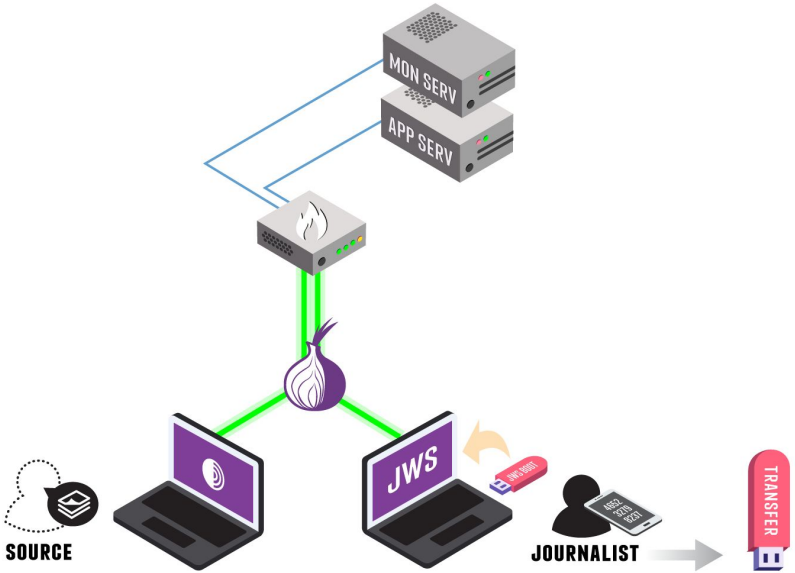
SECUREDROP

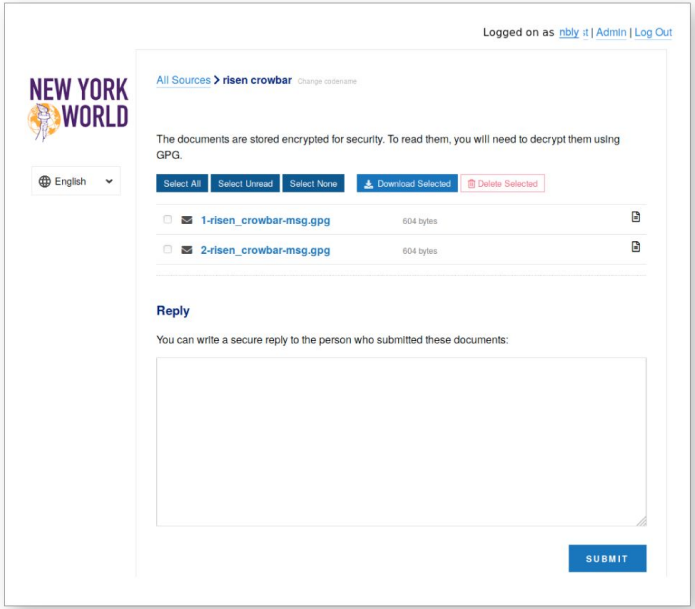




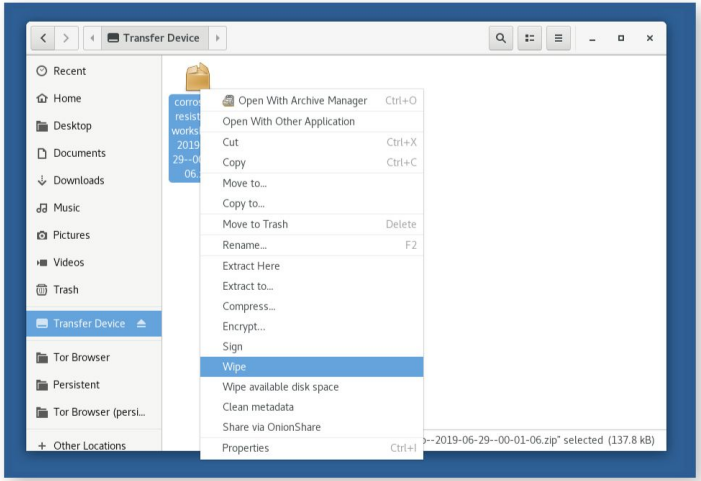
What the journalist sees

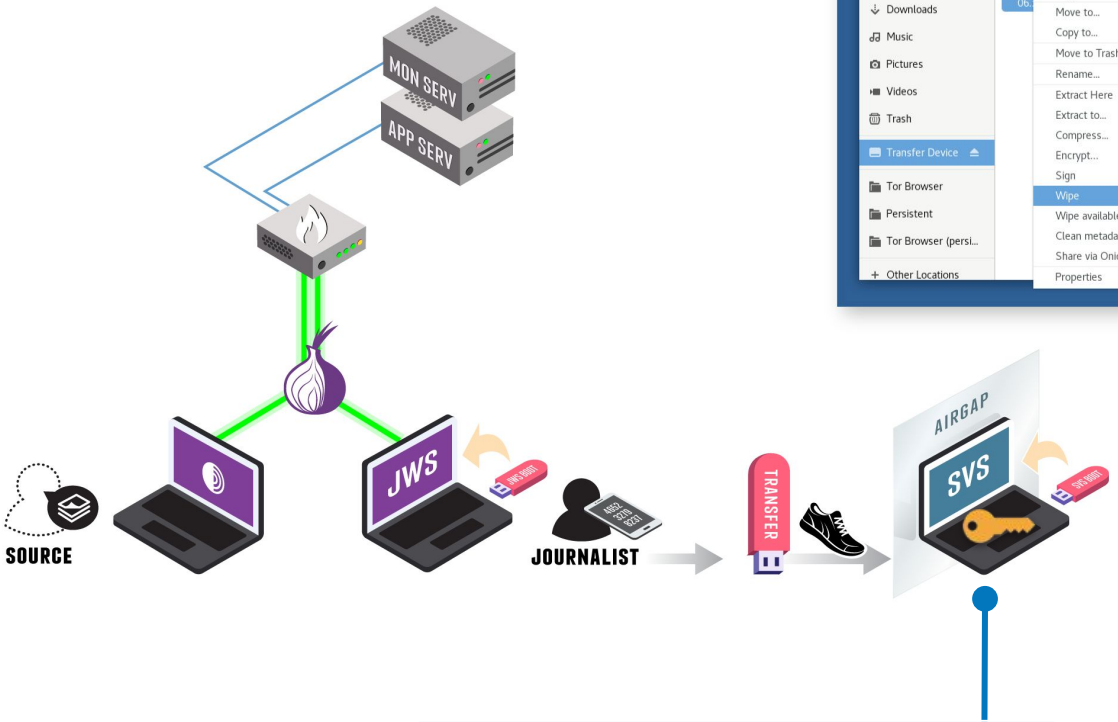
SECUREDROP


MON SERV
APP SERV
JWS
SOURCE
JOURNALIST
TRANSFER


Logged on as nbly it | Admin | Log Out
NEW YORK WORLD
All Sources > risen crowbar Change codename
The documents are stored encrypted for security. To read them, you will need to decrypt them using GPG.
English
Select All
Select Unread
Select None
Download Selected
Delete Selected
1-risen_crowbar-msg.gpg 604 bytes
2-risen_crowbar-msg.gpg 604 bytes
Reply
You can write a secure reply to the person who submitted these documents:
SUBMIT

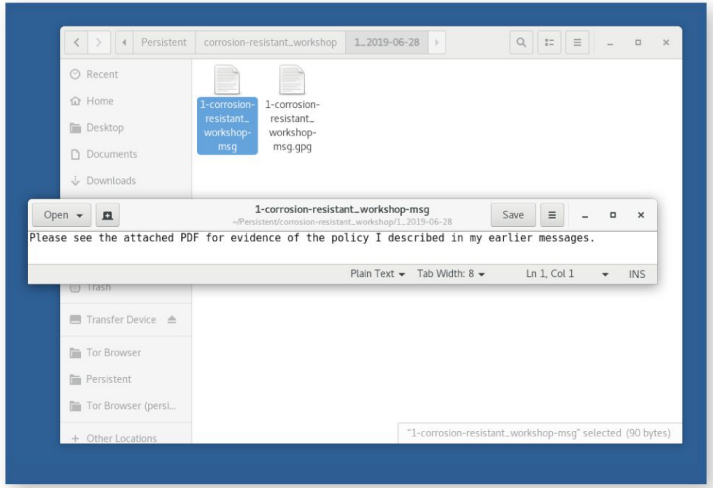
SECUREDROP

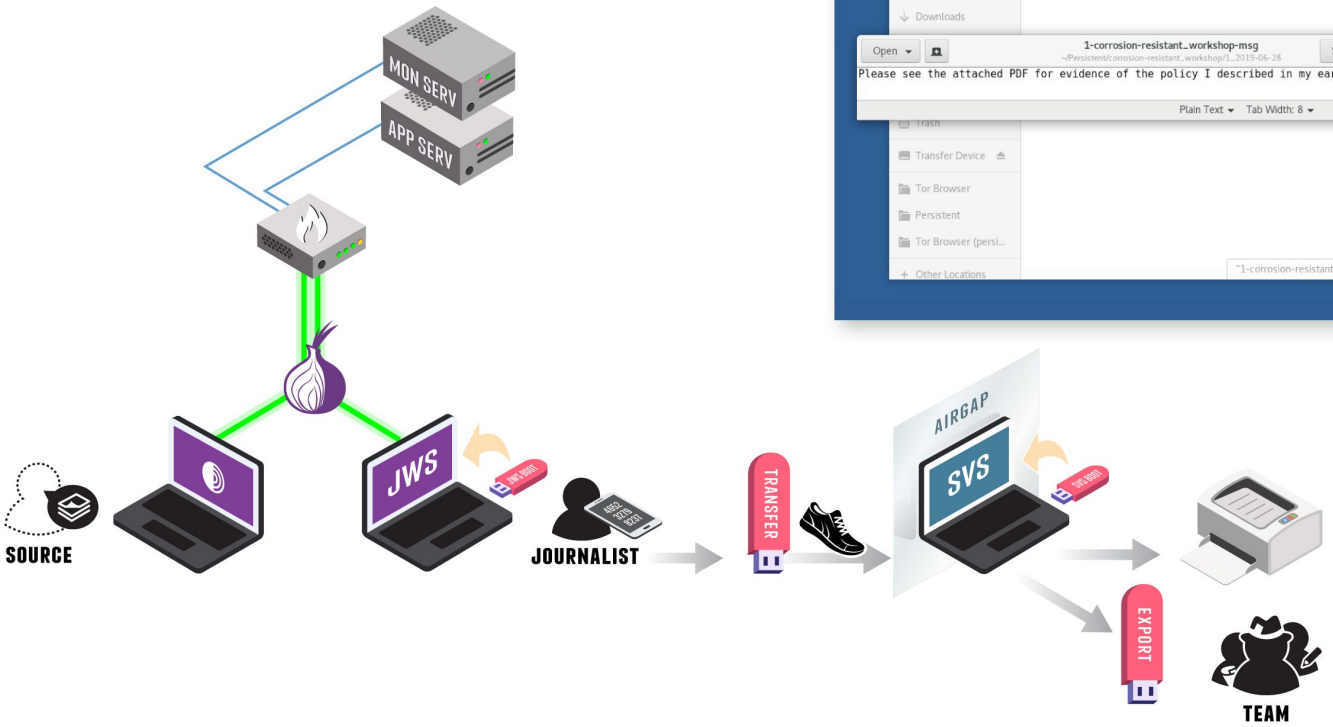




Private key to decrypt documents only in the air-gap environment.

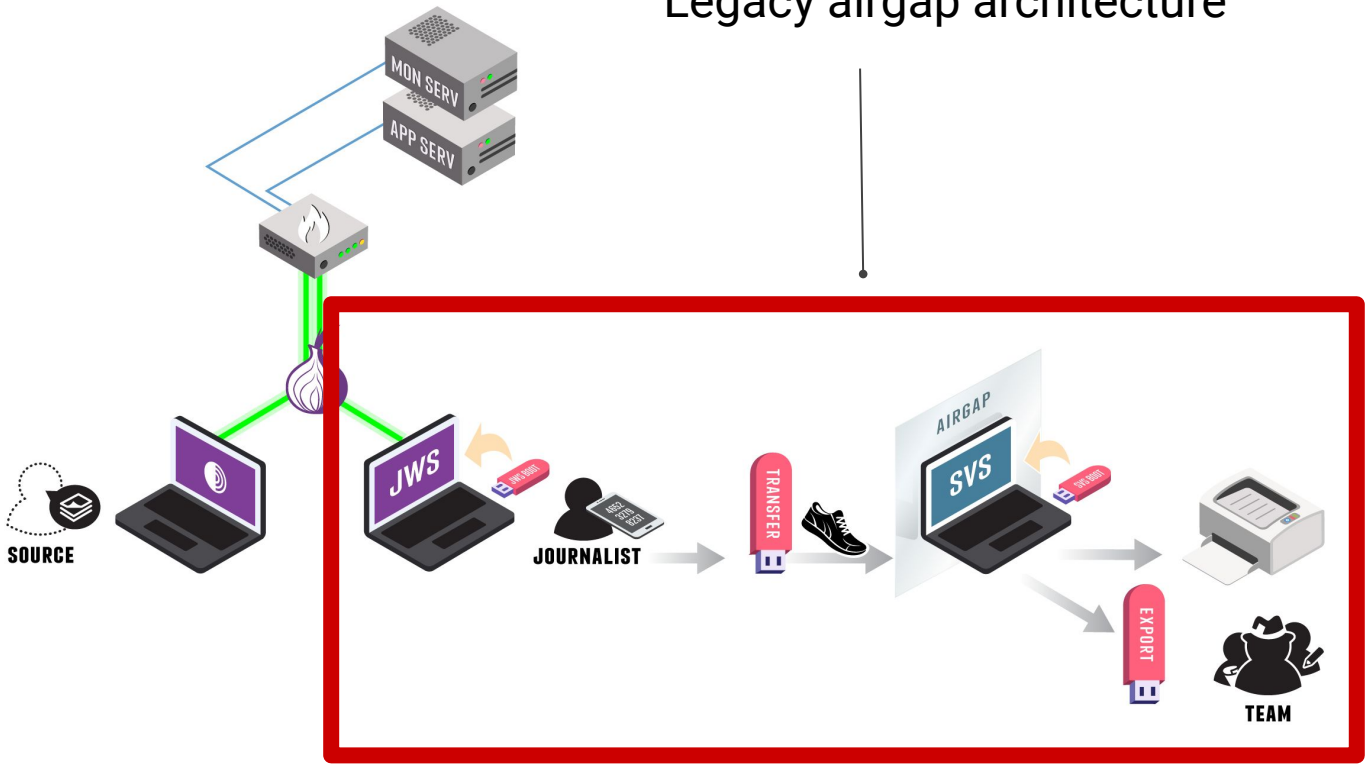
SECUREDROP


Persistent
corrosion-resistant_workshop
1_2019-06-28
Recent
Home
Desktop
Documents
Downloads
1-corrosion-resistant_workshop-msg
1-corrosion-resistant_workshop-msg.gpg
Open
1-corrosion-resistant_workshop-msg
~/Persistent/corrosion-resistant_workshop/1_2019-06-28
Save
Please see the attached PDF for evidence of the policy I described in my earlier messages.
Plain Text
Tab Width: 8
Ln 1, Col 1
INS
Trash
Transfer Device
Tor Browser
Persistent
Tor Browser (persi...
Other Locations
"1-corrosion-resistant_workshop-msg" selected (90 bytes)


MON SERV
APP SERV
JWS
SOURCE
JOURNALIST
TRANSFER
AIRGAP
SVS
EXPORT
TEAM

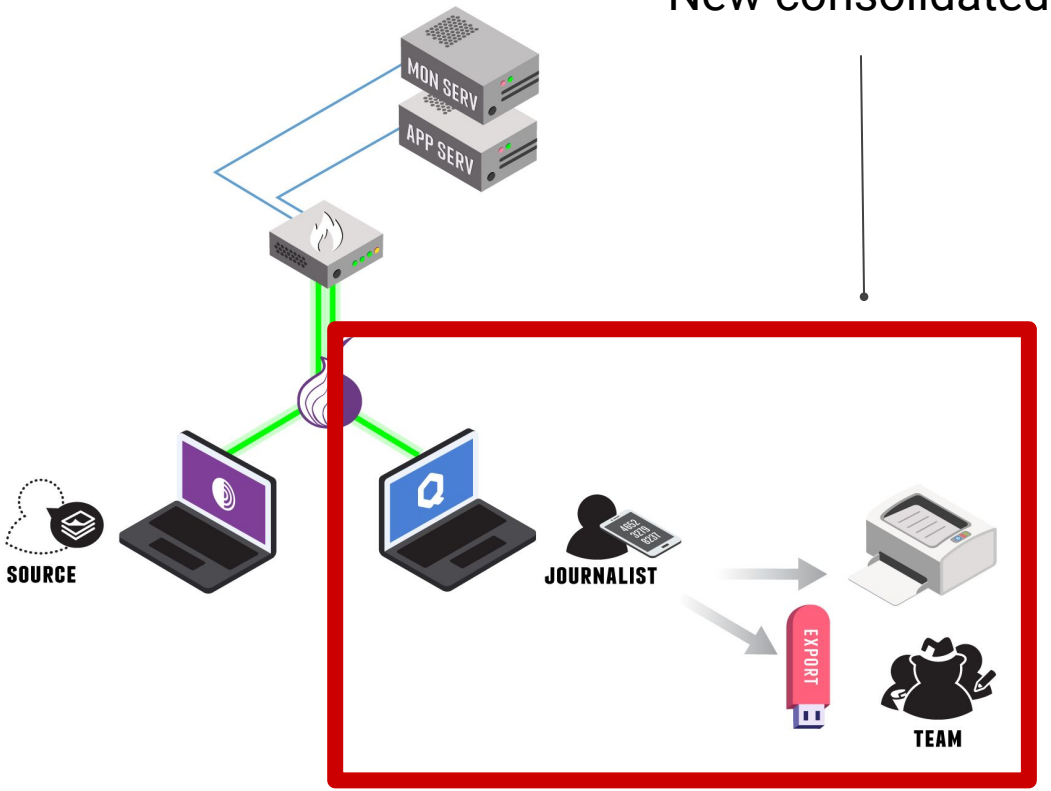
SECUREDROP

Legacy airgap architecture



SECUREDROP

New consolidated architecture



SECUREDROP

SecureDrop Workstation

Motivations for SecureDrop Workstation

- Existing workflows are slow (~1 hour round-trip), and largely one-way
- It's hard to patch an airgapped system
- Airgap is not perfect isolation
- Journalists need more tools than just viewing

Qubes OS

https://qubes-os.org/

- Hypervisor-based isolation, via Xen
- Template & disposable environments to combat malware persistence
- Strict controls for inter-VM communication

How Qubes OS works

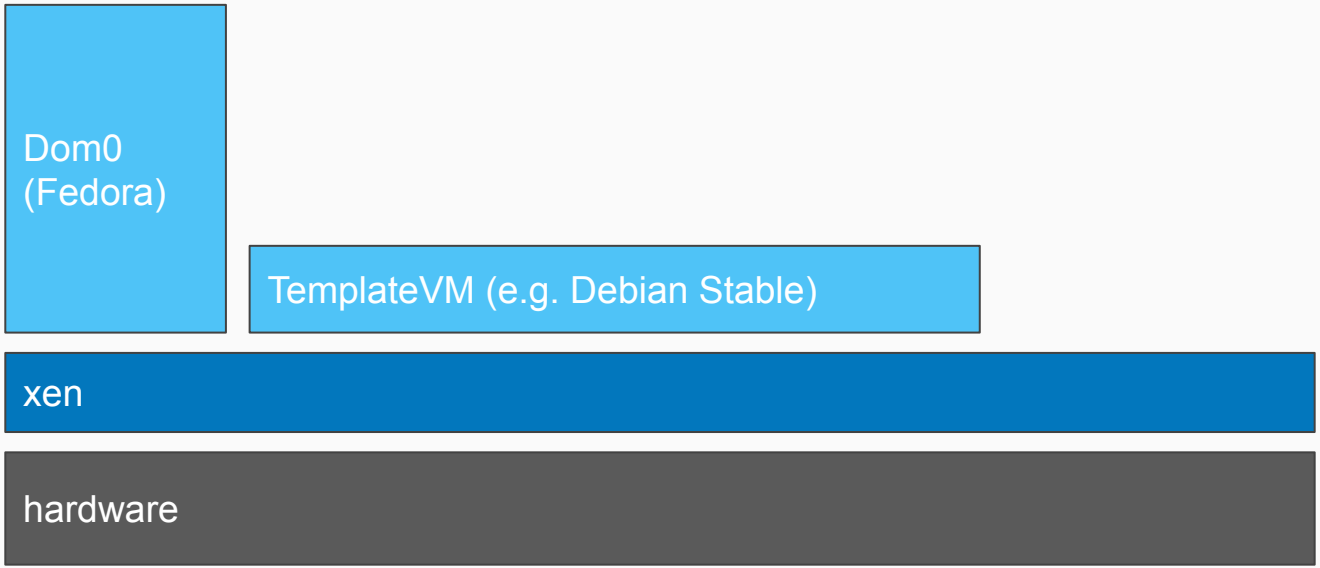
Qubes OS: single-user desktop-based Xen distribution

hardware

Qubes OS: single-user desktop-based Xen distribution

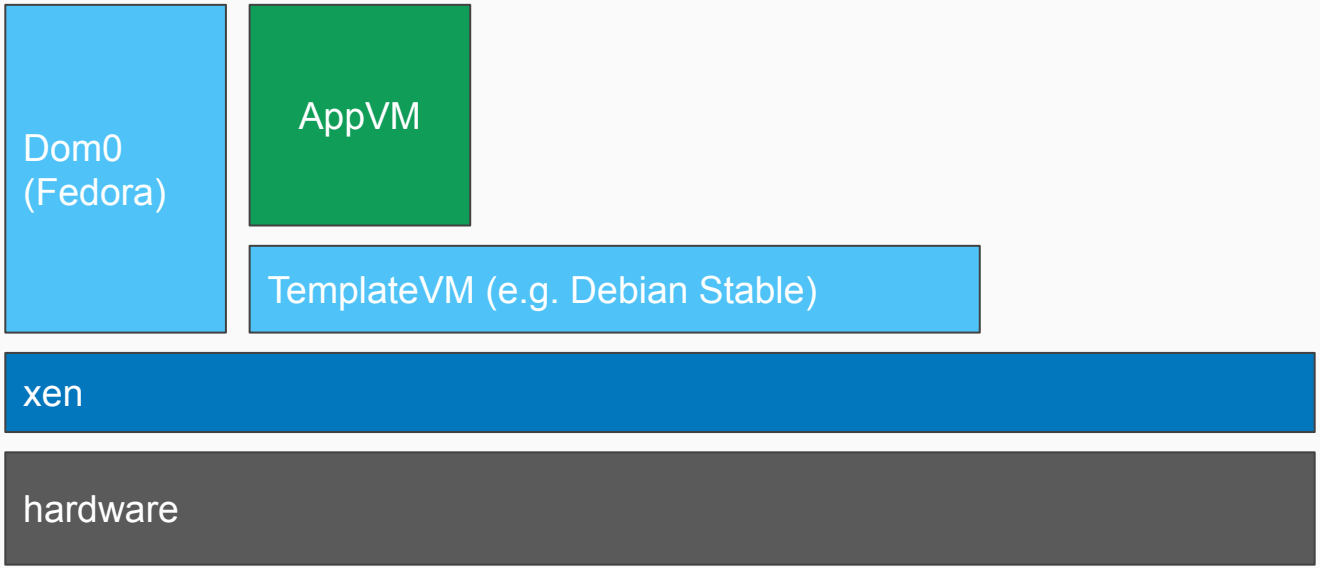
Qubes OS: single-user desktop-based Xen distribution

Qubes OS: single-user desktop-based Xen distribution

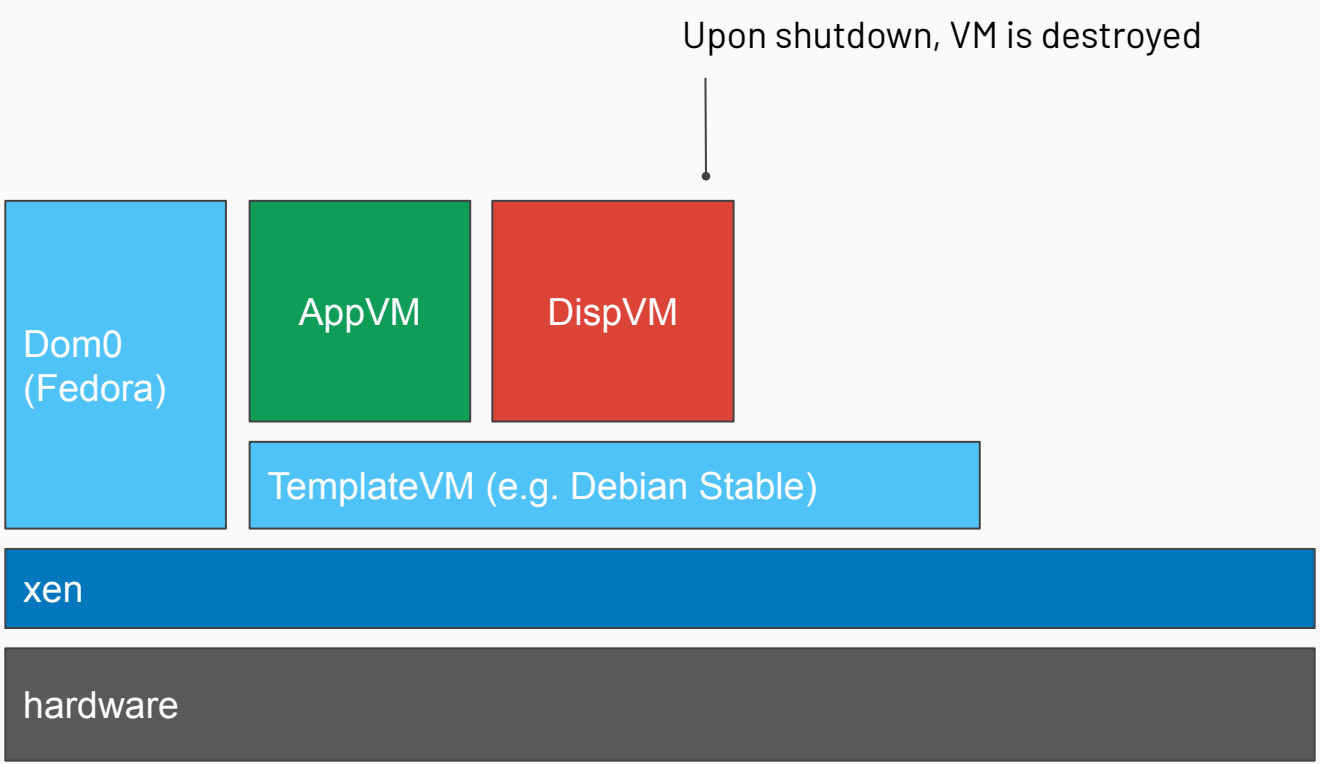


Qubes OS: single-user desktop-based Xen distribution

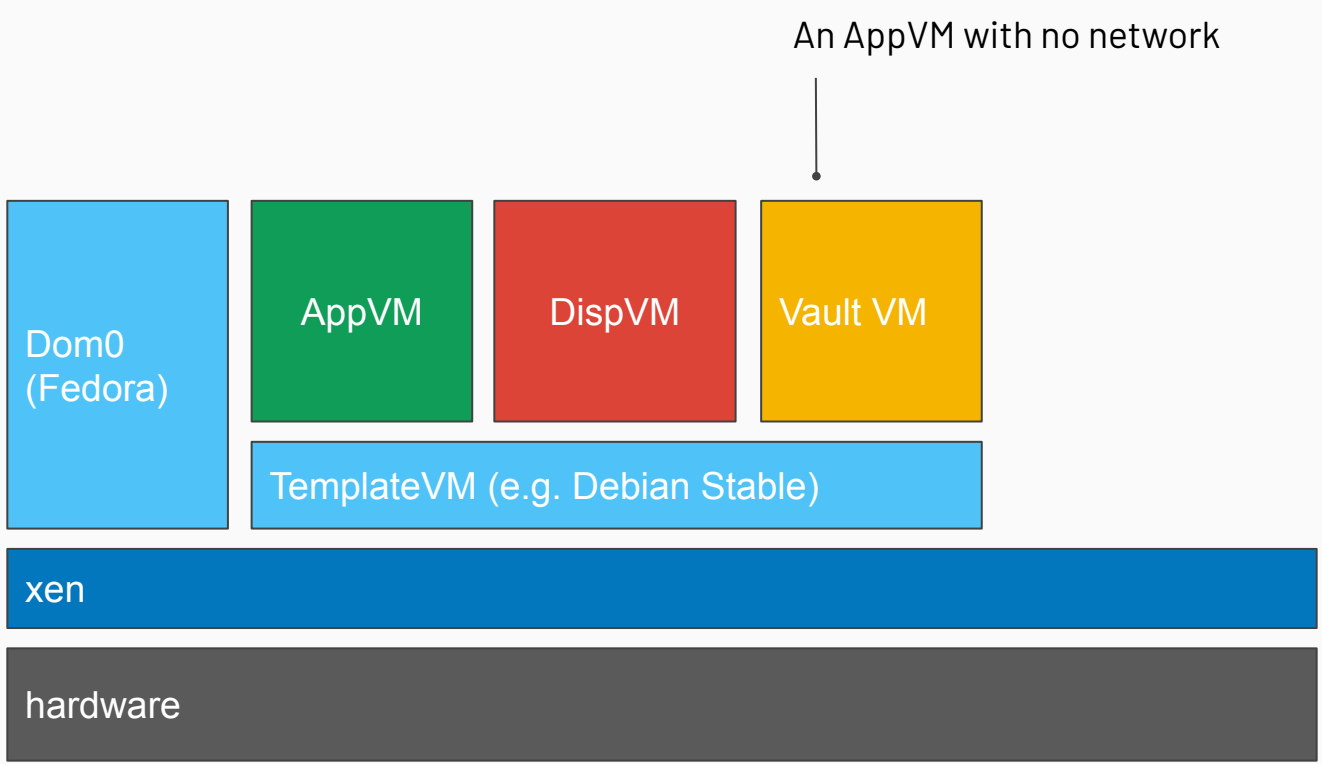
Only `/home`, `/usr/local`, `/rw/config` will persist a reboot, otherwise state is reset to the base TemplateVM



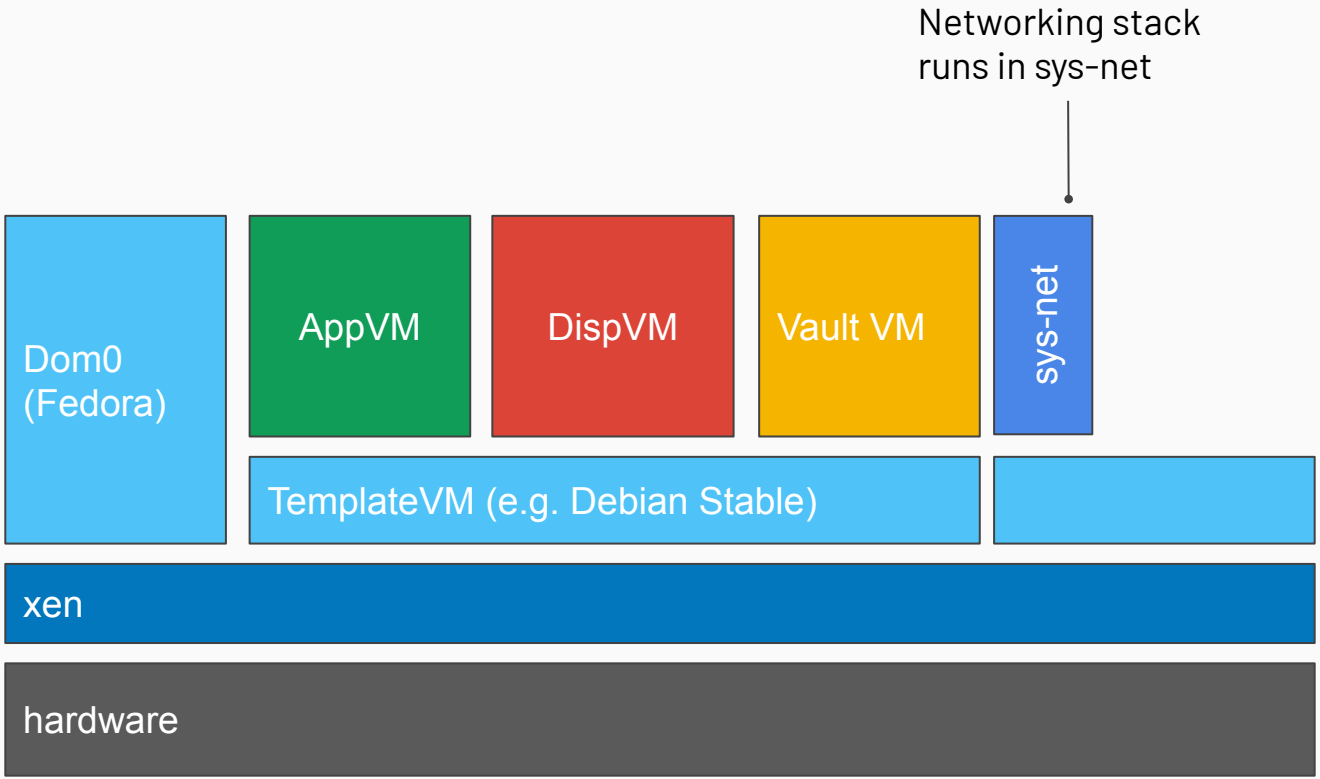
Qubes OS: single-user desktop-based Xen distribution



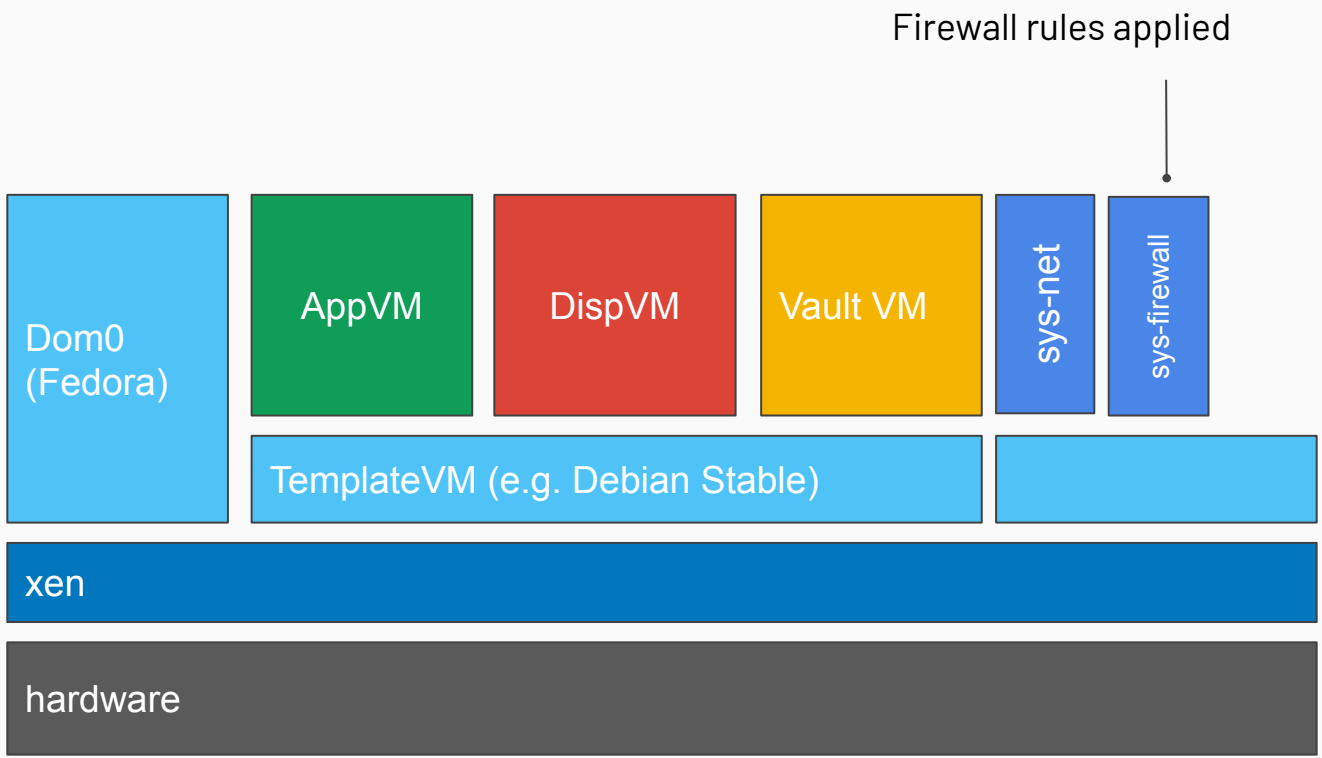
Qubes OS: single-user desktop-based Xen distribution



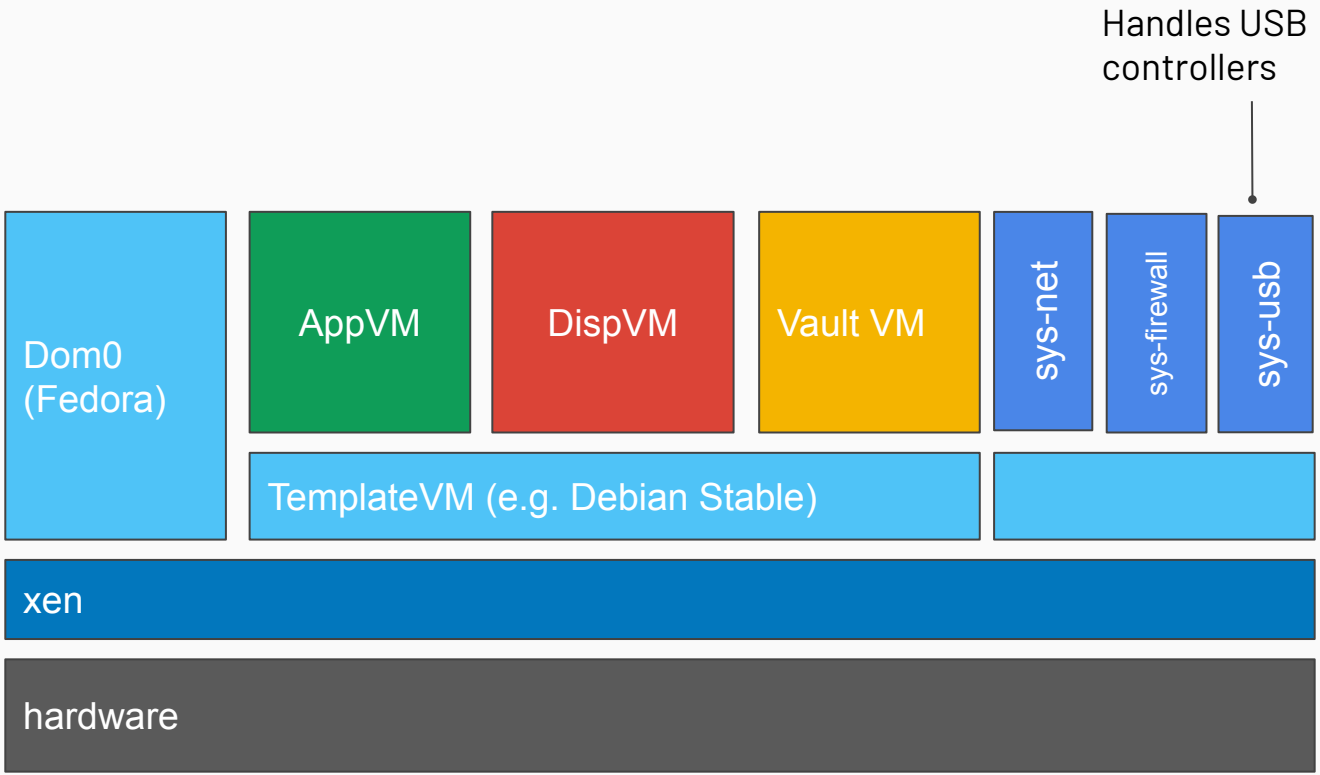
Qubes OS: single-user desktop-based Xen distribution



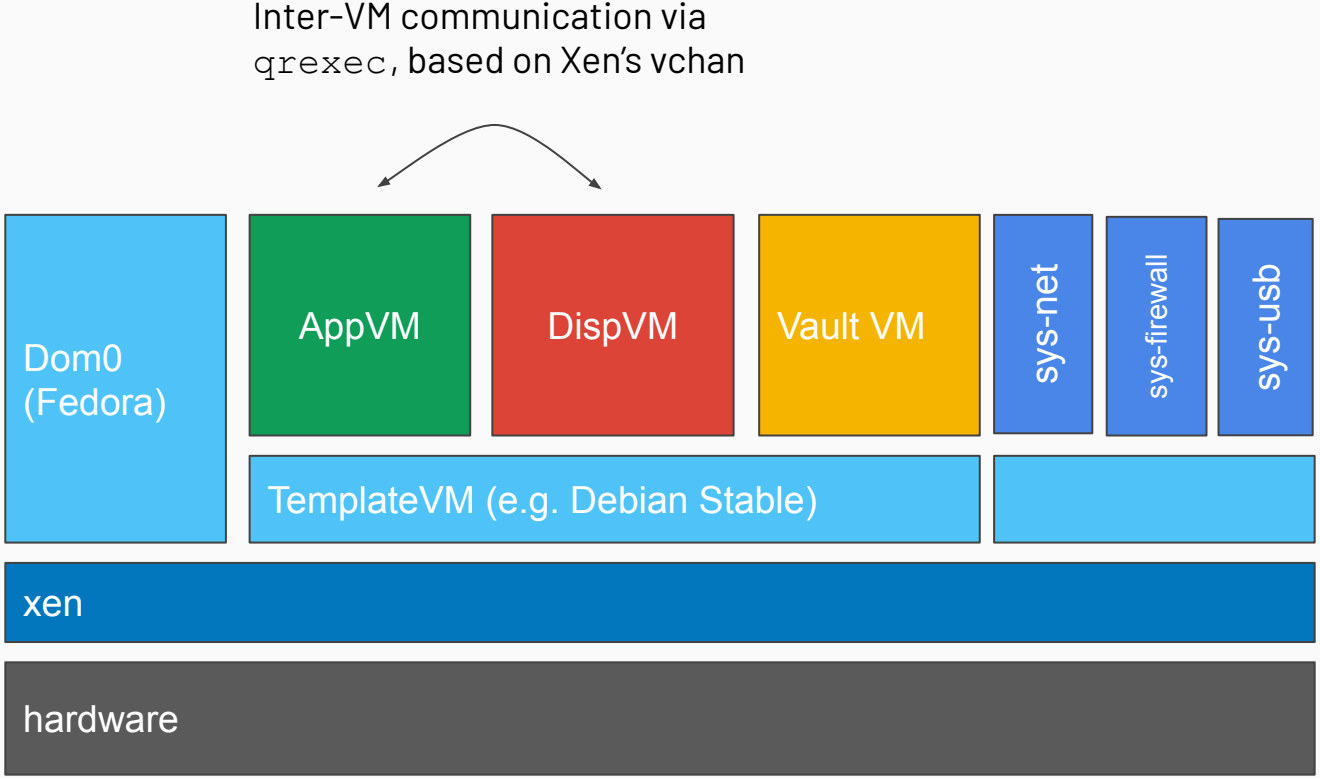
Qubes OS: single-user desktop-based Xen distribution



Qubes OS: single-user desktop-based Xen distribution

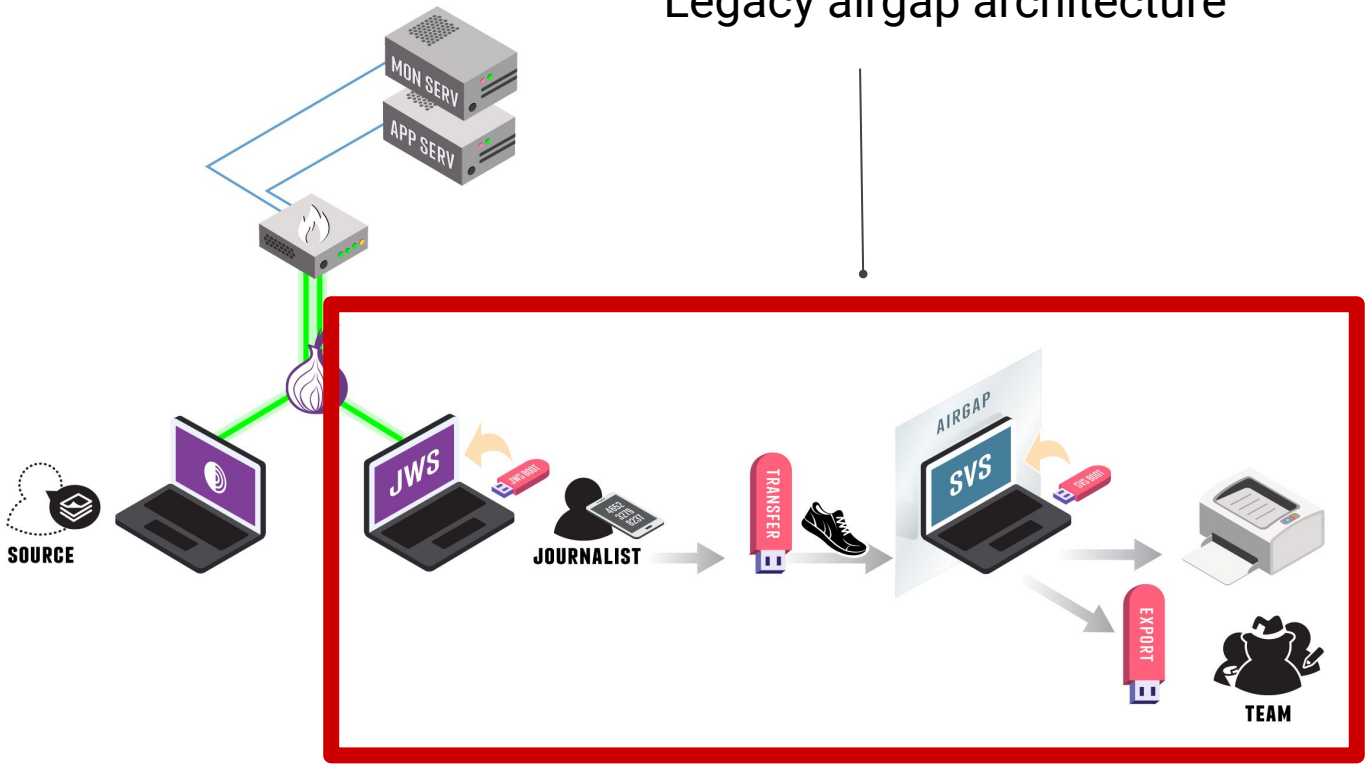


Qubes OS: single-user desktop-based Xen distribution



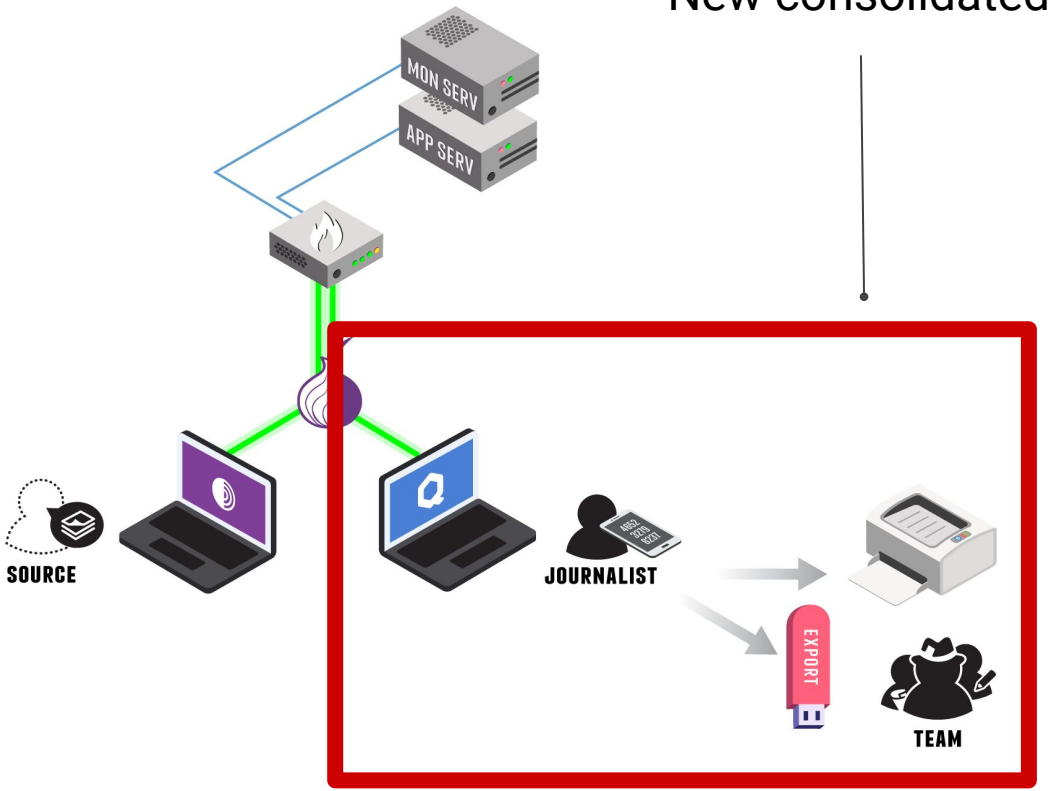
SecureDrop Workstation architecture

Legacy airgap architecture

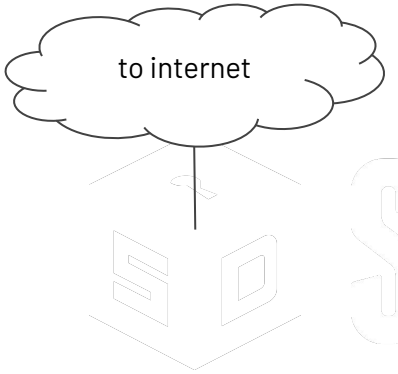


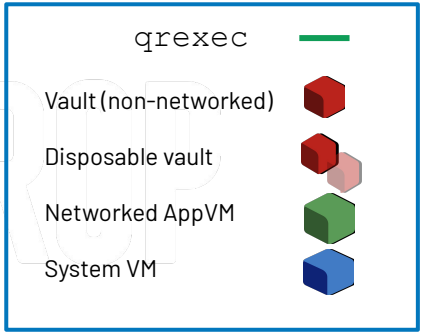
SECUREDROP

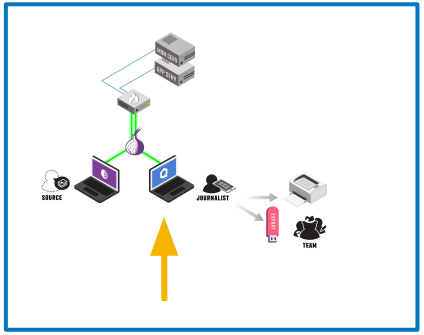
New consolidated architecture

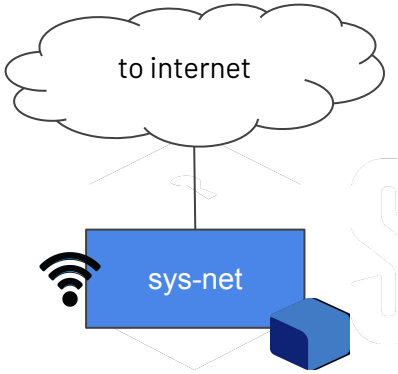


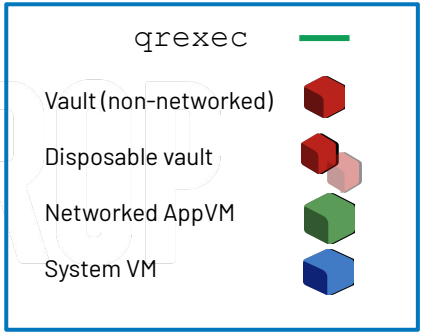
SECUREDROP

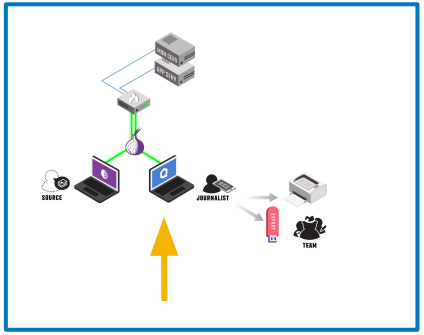

to internet

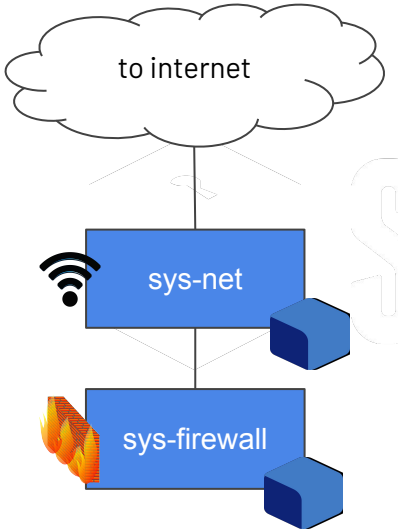

qrexec
Vault (non-networked)
Disposable vault
Networked AppVM
System VM


SOURCE
JOURNALIST
TEAM


to internet
sys-net


qrexec
Vault (non-networked)
Disposable vault
Networked AppVM
System VM


SOURCE
JOURNALIST
TEAM



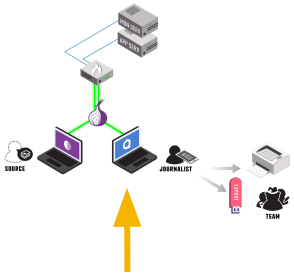
qrexec

Vault (non-networked)

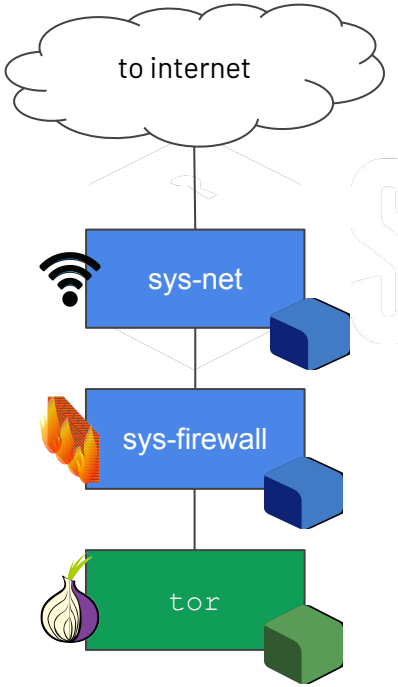
Disposable vault

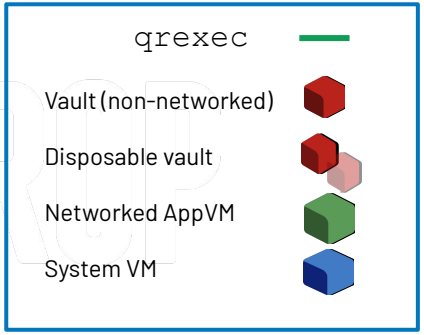
Networked AppVM

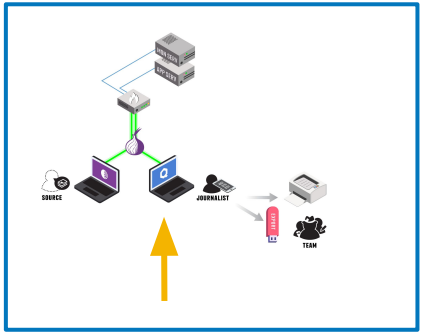
System VM

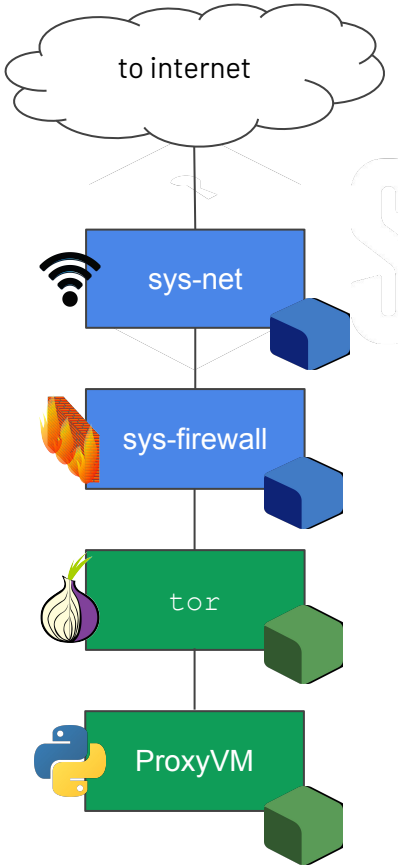


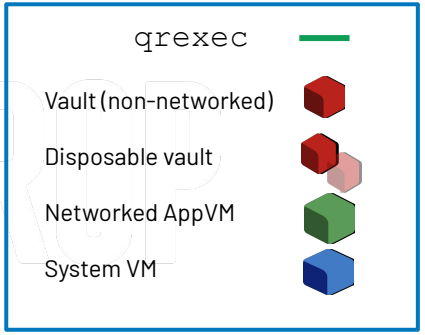
SECUREDROP

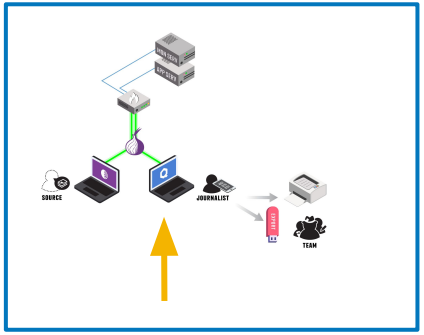

to internet
sys-net
sys-firewall
tor

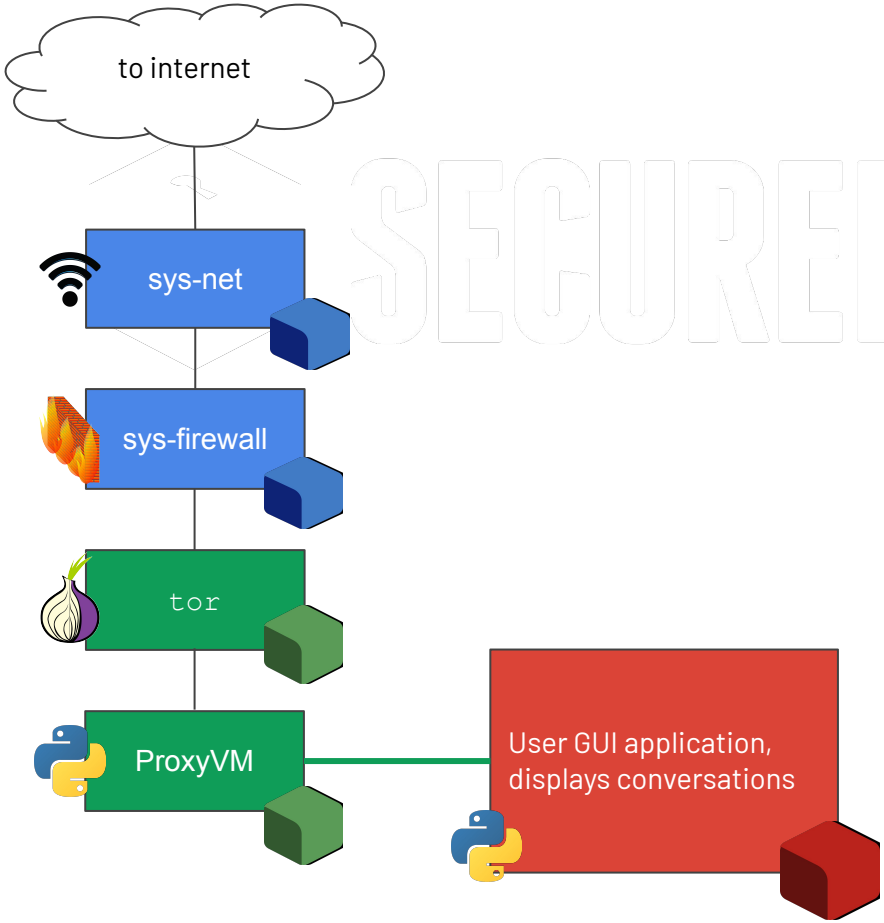

qrexec
Vault (non-networked)
Disposable vault
Networked AppVM
System VM

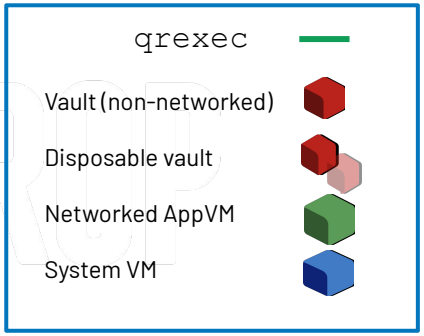

SOURCE
JOURNALIST
TEAM

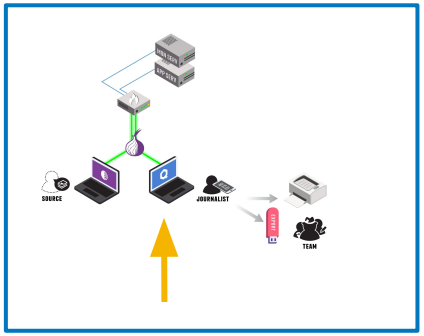

to internet
sys-net
sys-firewall
tor
ProxyVM

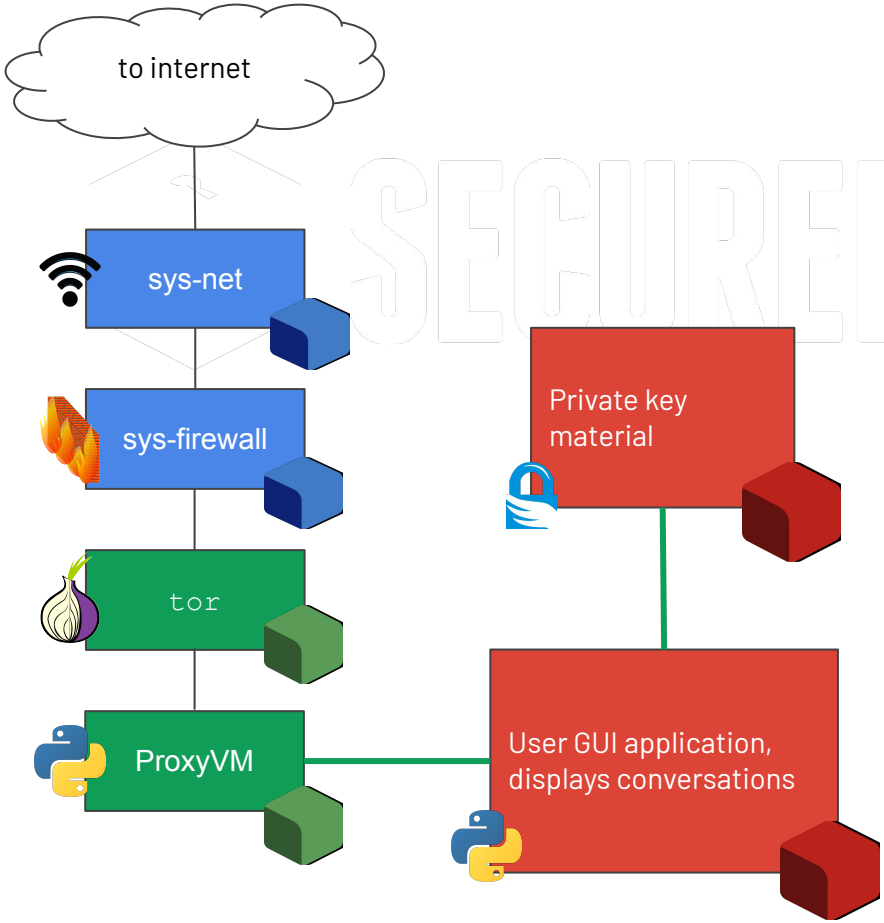

qrexec
Vault (non-networked)
Disposable vault
Networked AppVM
System VM

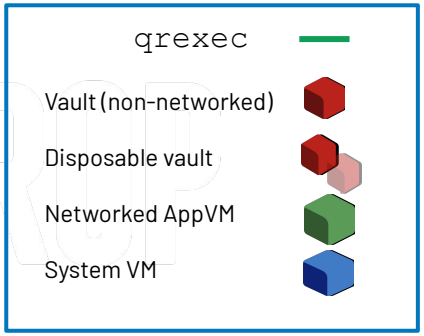

SOURCE
JOURNALIST
TEAM

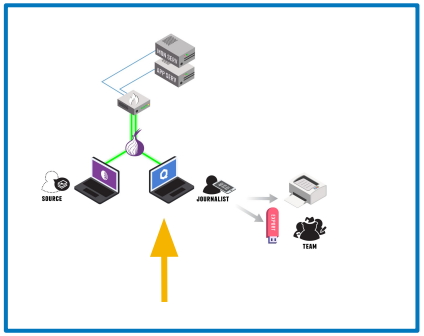

to internet
sys-net
sys-firewall
tor
ProxyVM
User GUI application, displays conversations

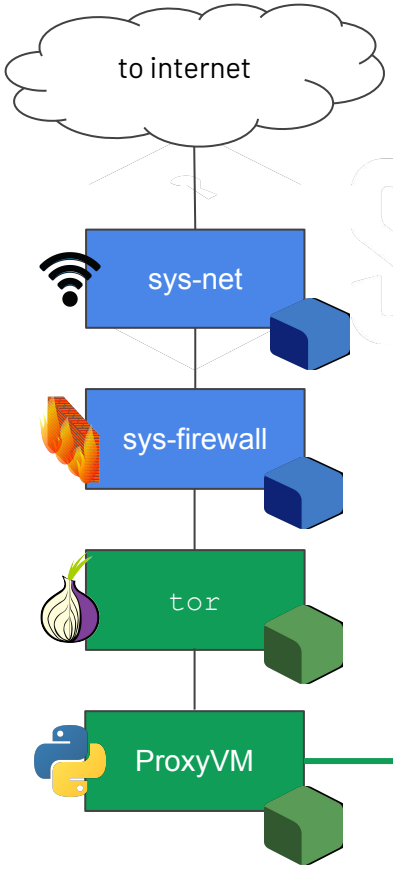

qrexec
Vault (non-networked)
Disposable vault
Networked AppVM
System VM

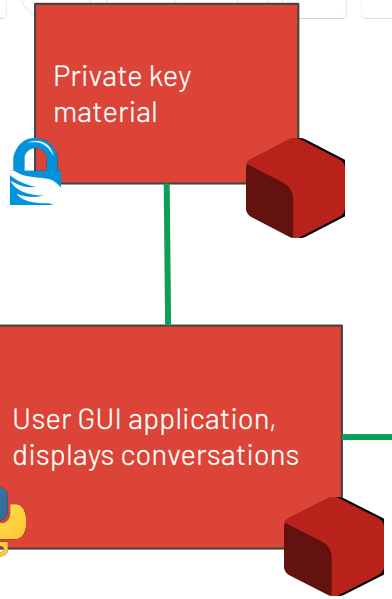

SOURCE
JOURNALIST
TEAM

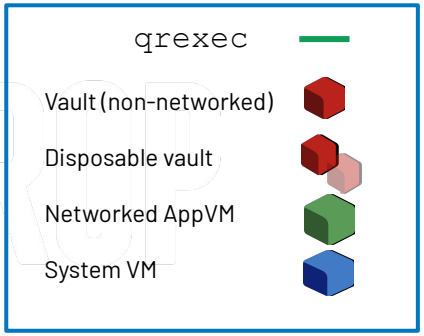

to internet
sys-net
sys-firewall
tor
ProxyVM
Private key material
User GUI application, displays conversations

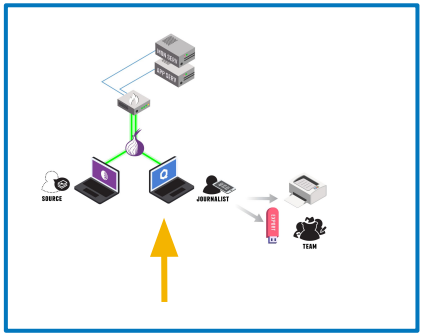

qrexec
Vault (non-networked)
Disposable vault
Networked AppVM
System VM

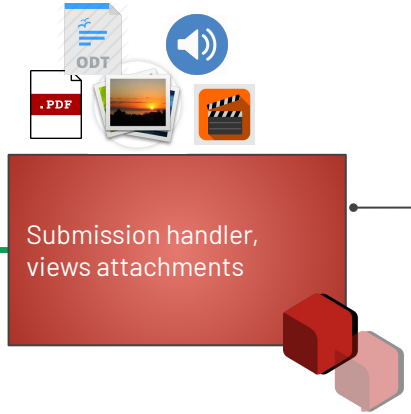

SOURCE
JOURNALIST
TEAM







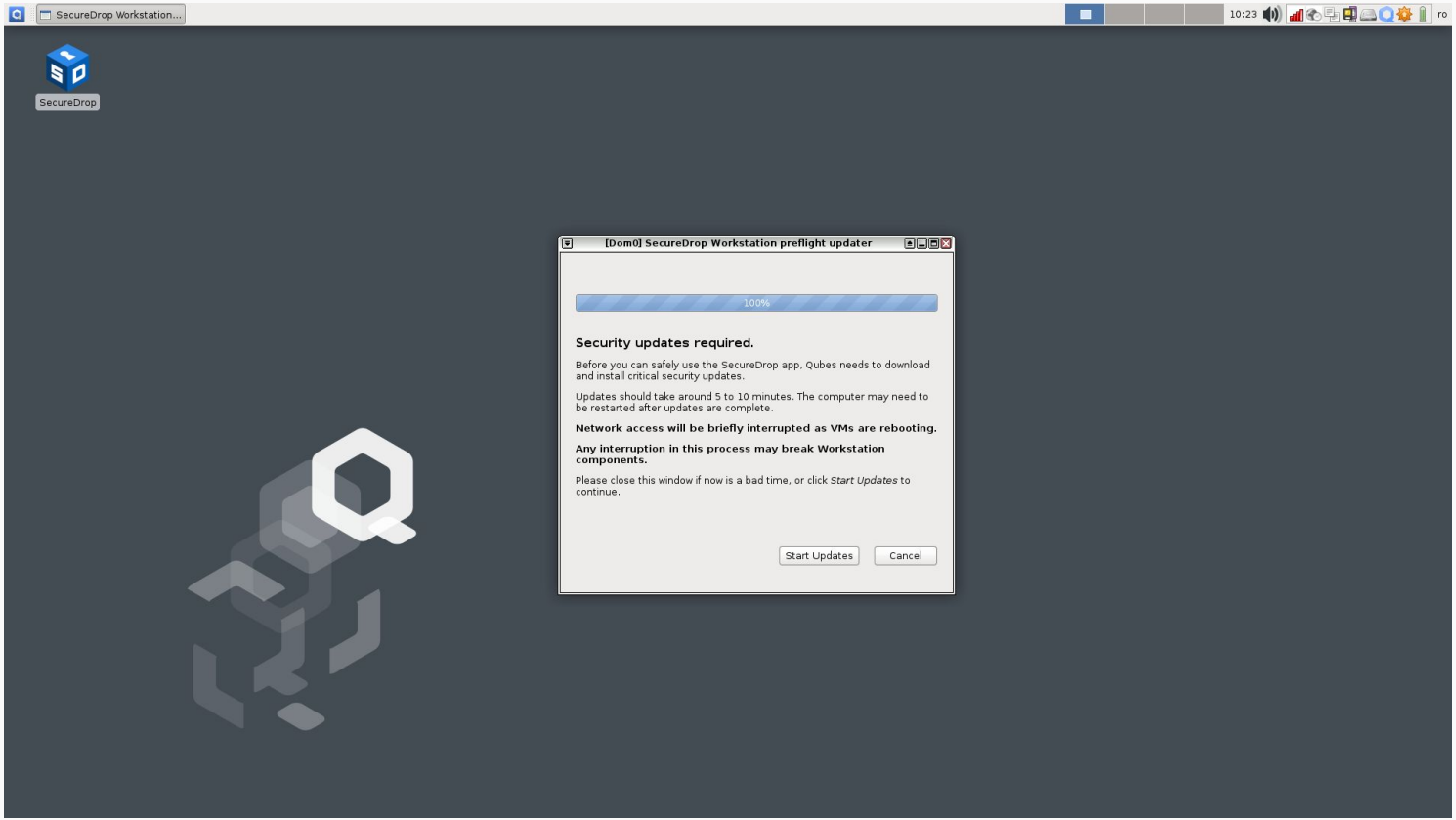




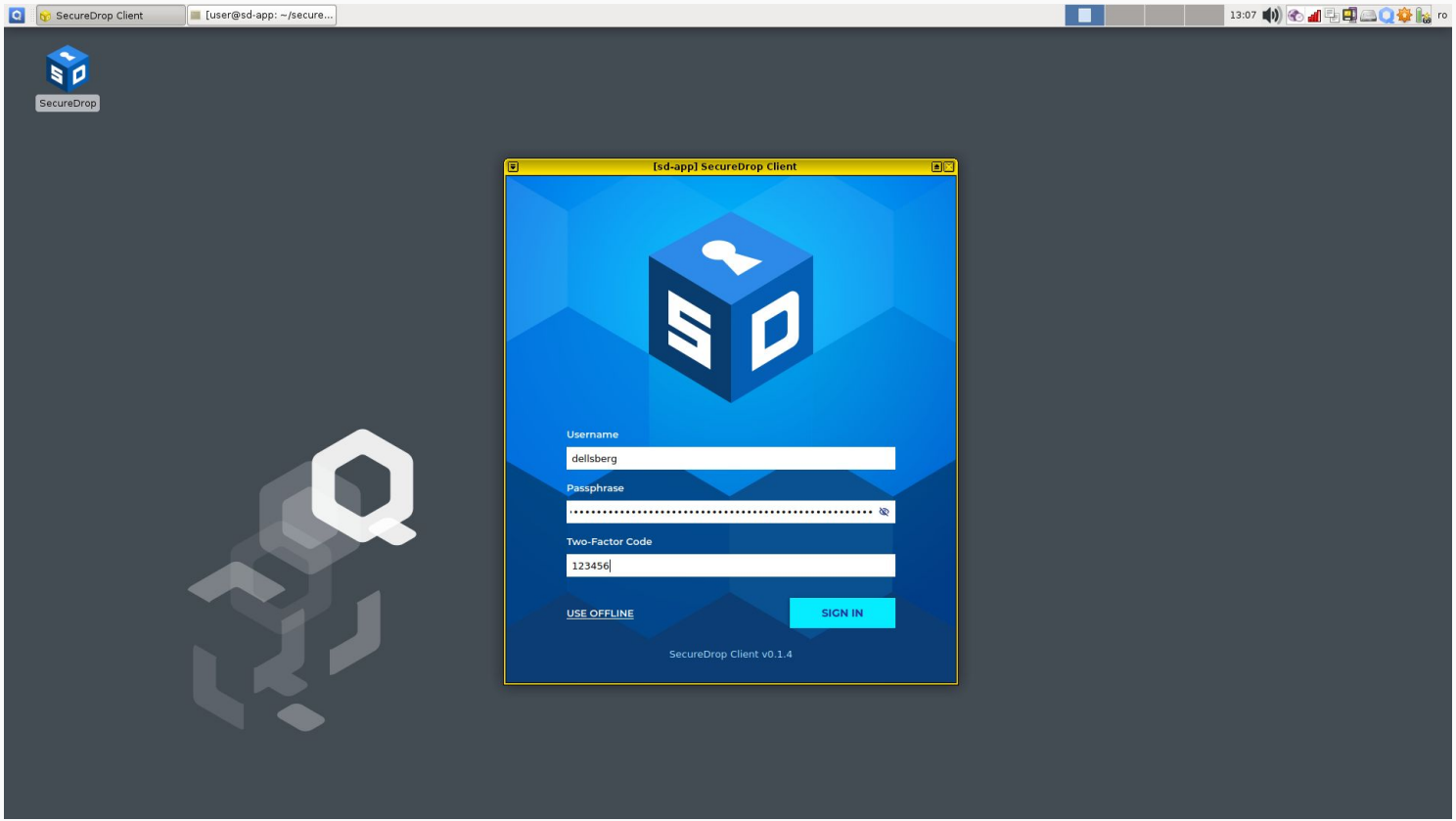
Use a hardened template with grsecurity-patched kernel to provide additional generalized exploit mitigations for memory corruption vulnerabilities

What the journalist sees

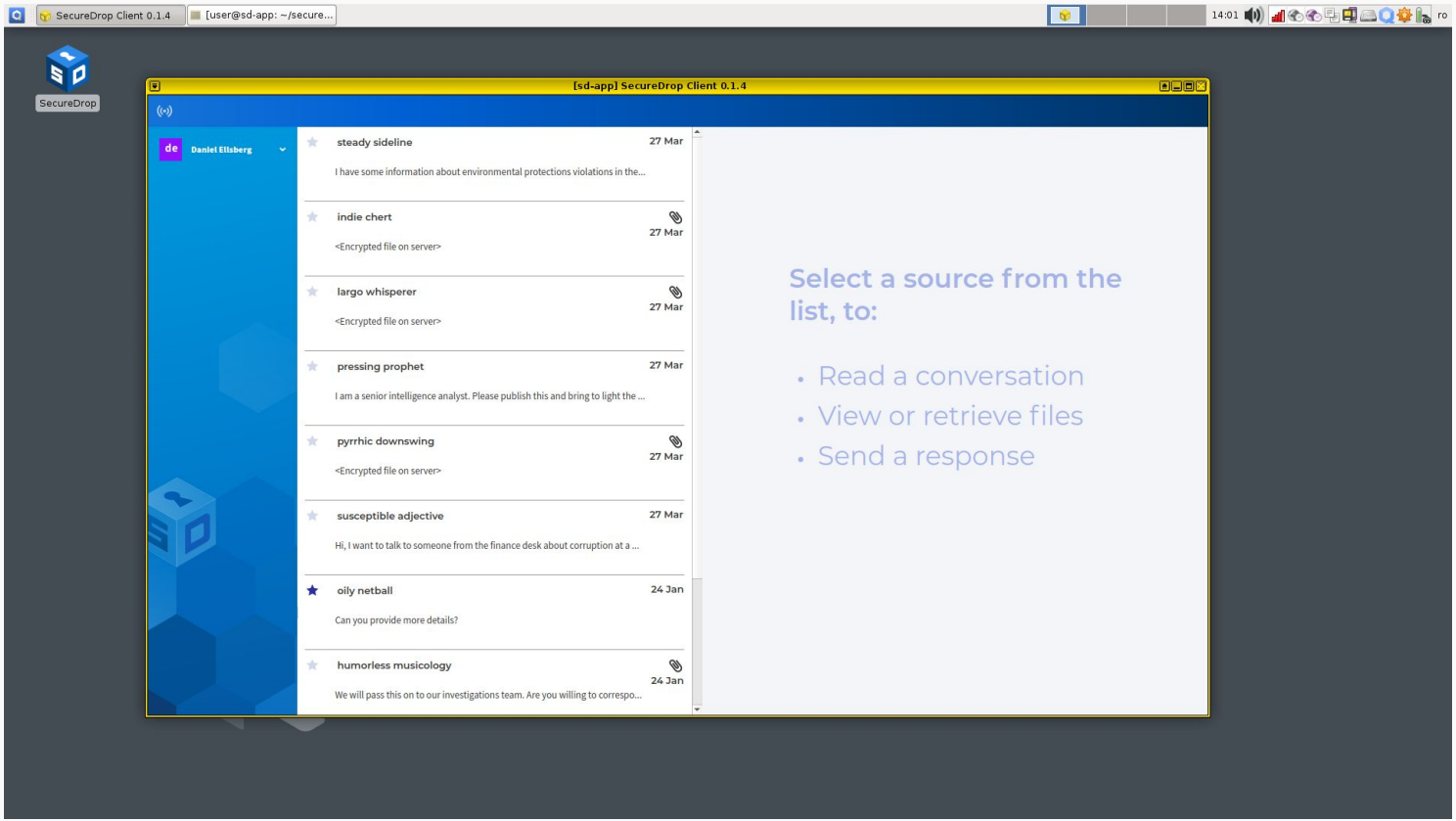
SecureDrop Workstation: Journalist perspective



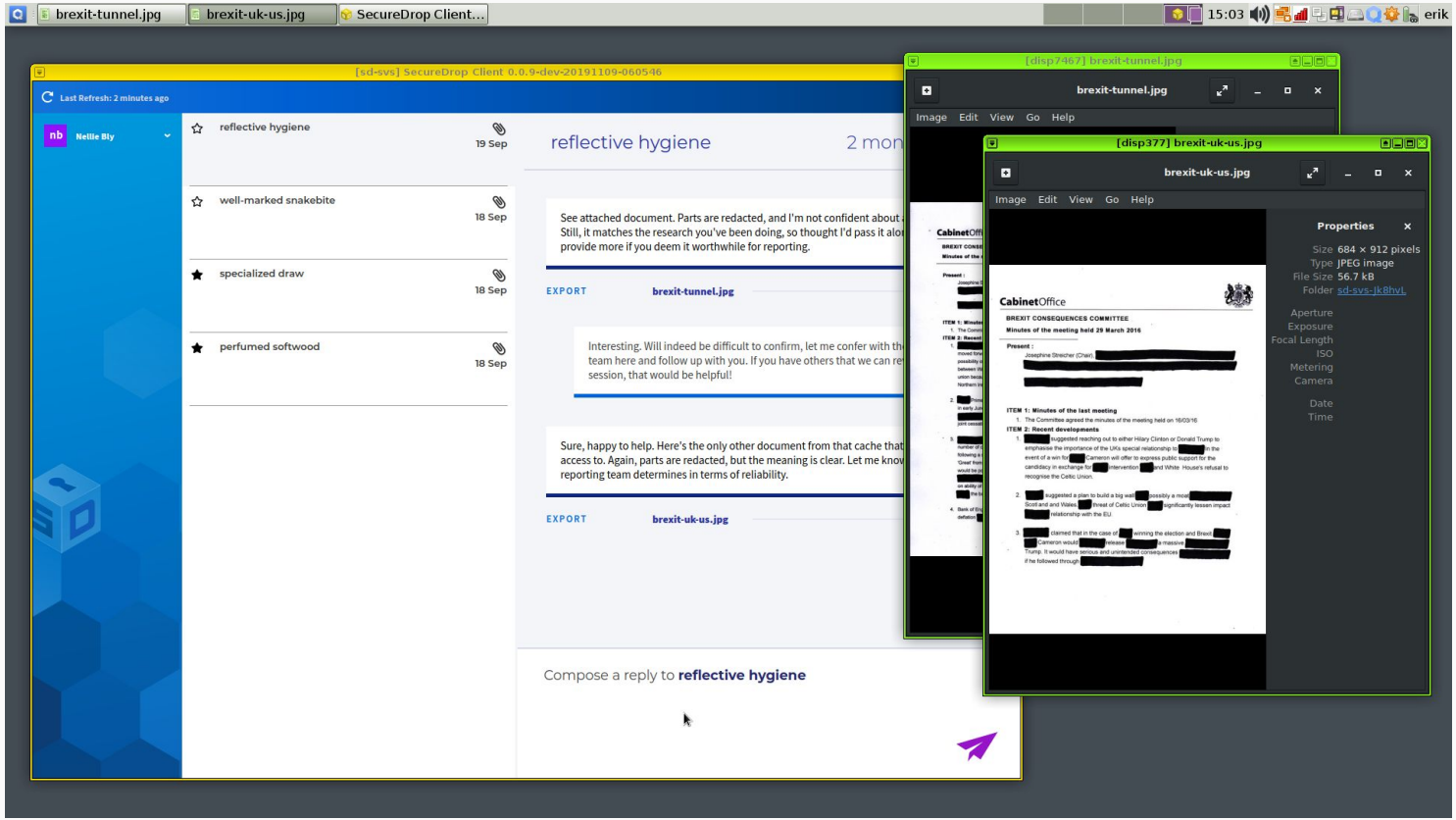
SecureDrop Workstation: Journalist perspective



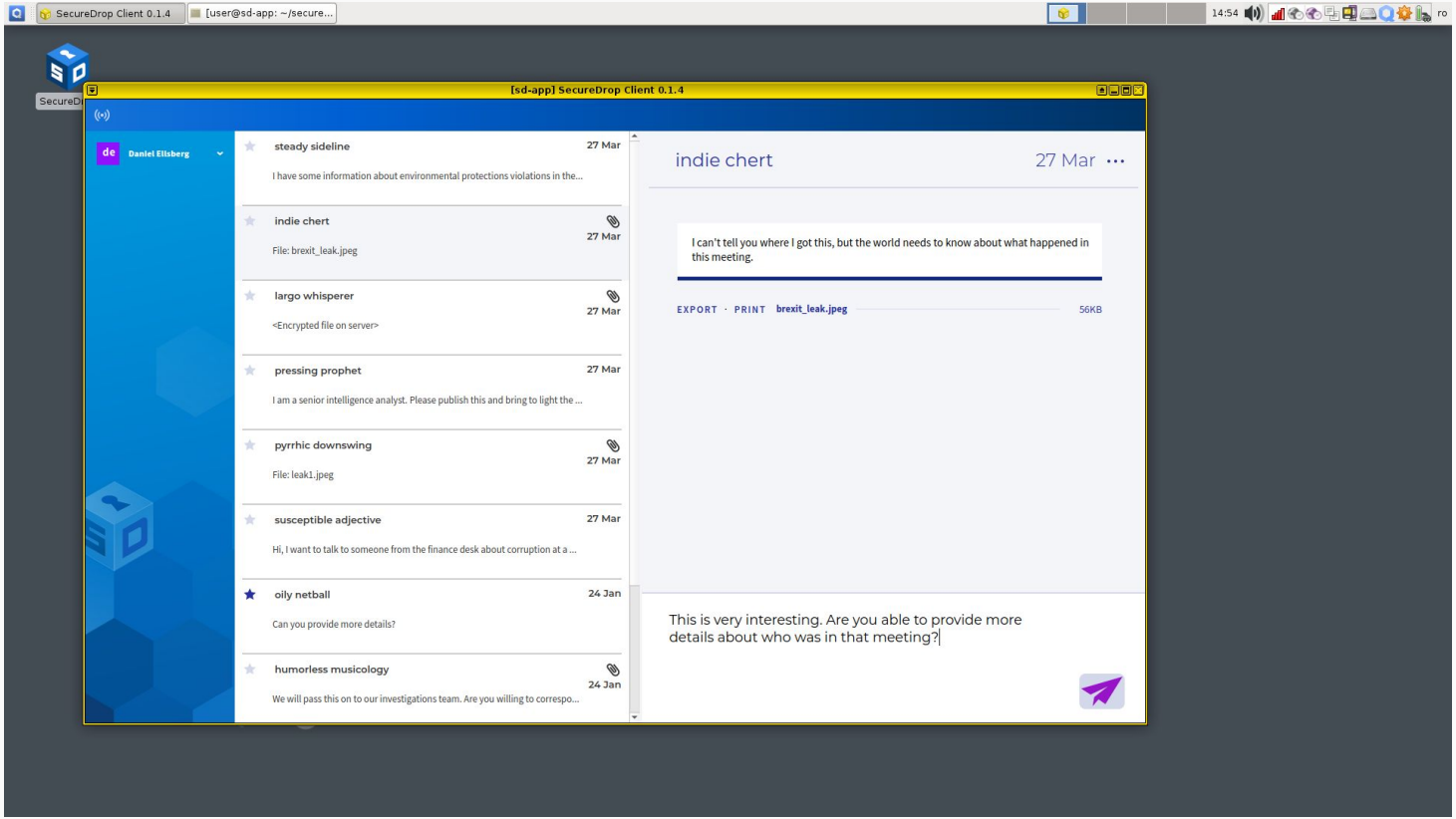
SecureDrop Workstation: Journalist perspective



SecureDrop Workstation: Journalist perspective



SecureDrop Workstation: Journalist perspective



Hardening, beyond VM isolation

- Code execution confined by AppArmor
- VMs use a custom kernel, with the Grsecurity patch set, to guard against memory corruption attacks
- Minimal templates suited to trust model in architecture, with common software excluded when appropriate

"Overall, the SecureDrop Workstation system represents a complex but well researched product that has been thoughtfully designed."

- Trail of Bits, 2020

SECUREDROP

What’s next?

Pilot program, ongoing

- Small set of news organizations running the Workstation
- Gathering user experience to inform design
- Aiming for general availability in the near future

Future work

- Additional export tooling (e.g. Signal, Onionshare)
- Metadata redaction
- Research use
- Malware detection
- Localization

The team

100% of time on SecureDrop


Mickael
Engineering


Kushal
Engineering


Kevin
Support, Engineering


Allie
Engineering


John
Engineering


Rowen
Support

>= 50% of time on SecureDrop


Conor
Engineering


Erik
Project Manager

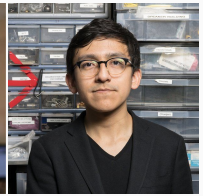

Jen
Engineering


Nina
UX

>= 25% of time on SecureDrop


Harlo
Training


Olivia
Training


David
Training

Takeaways

- Investigative journalism can be dangerous
- Whistleblowers deserve protection
- Technology can reinforce cultural norms about privacy

Questions?

Get involved:

- SecureDrop: https://securedrop.org/contribute/
- Qubes OS: https://qubes-os.org/
- Tor: https://torproject.org/
- Want to donate? https://freedom.press/donate/

Contact:

Conor Schaefer
Chief Technology Officer
conor@freedom.press

SECUREDROP