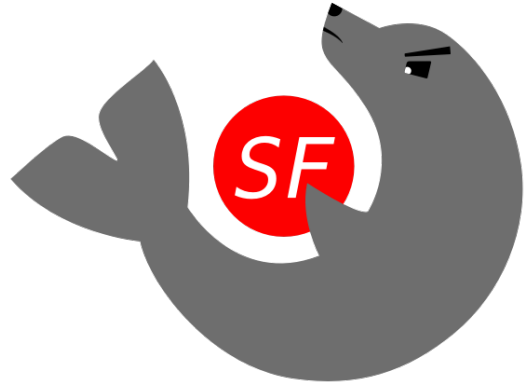
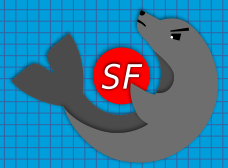
# SEALFAIL




Security Enhanced Alma Linux

For Activism / Insurgency / Liberation

# Table of contents

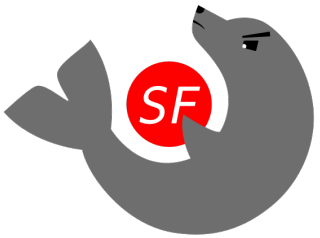


# What SEALFAIL is and is not

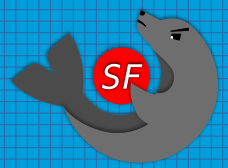
SEALFAIL

Security Enhanced Alma Linux

For Activism / Insurgency / Liberation

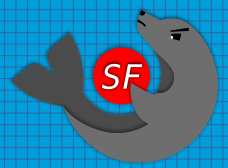


# What SEALFAIL is




- SEALFAIL is a free and open source workstation operating system based on Alma Linux.
- SEALFAIL is hardened/secured out-of-the-box and ready for use immediately after installation.
- SEALFAIL is a tool to help organizations meet higher COMSEC/INFOSEC/OPSEC standards.
- SEALFAIL is built with specific use cases in mind and will only serve those use cases.
- SEALFAIL can and should be customized by your organization to include its own modifications and suit its specific use cases.

# What SEALFAIL is not




- SEALFAIL is not a general-purpose OS like Qubes.
- SEALFAIL is not a "hacktivism" tool designed for offensive action.
- Additional software cannot be installed on top of SEALFAIL.
- SEALFAIL is not a single solution to all security problems. OPSEC doesn't end at operating system selection.

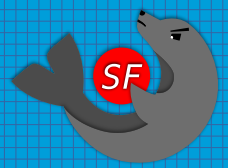
# Target users

SEALFAIL

Security Enhanced Alma Linux

For Activism / Insurgency / Liberation

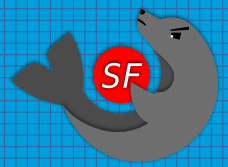
# Target users - 1/3




- **Non Governmental Organizations (NGOs)**

  **Examples:** An NGO field operator investigating the human rights violations taking place within the territory of Yemen in the context of the Yemeni civil war might use SEALFAIL on their device to secure their data in the event of confiscation or interference from states and militias.

# Target users - 2/3



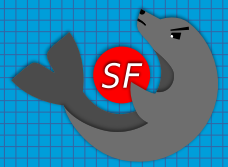

- **Activists and political dissidents**

  **Examples:** Activists might use SEALFAIL to organize between groups spread across the country and help ensure their OPSEC/INFOSEC/COMSEC standards are met.

  SEALFAIL helps put activists on an equal footing against surveillance states and authoritarian regimes.

  SEALFAIL becomes a powerful tool to increase the activist projection capabilities and the scale of their operations.

# Target users - 3/3




- **Militias and underground activists**

  **Examples:** Underground groups in conservative parts of the United States working to provide safe abortions to women that would otherwise be illegal under local jurisdiction.

  Ukrainian partisans engaged in direct action against the Russian invasion.

# Main features

SEALFAIL

Security Enhanced Alma Linux

For Activism / Insurgency / Liberation

# Main features - 1/6

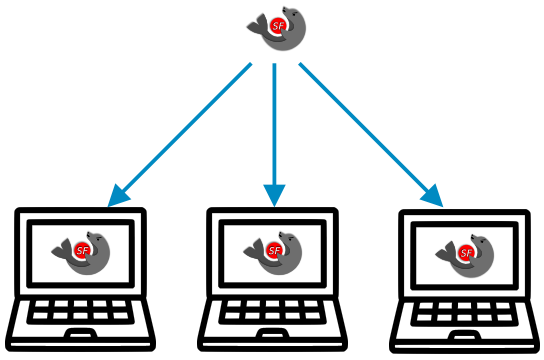
- **Fast mastering process**

  The SEALFAIL installation process is fully automated, only requiring selection of the system's language, keyboard layout, and timezone before proceeding with a zero-click installation process.

**+ Customizable installation process**

**+ Significant time saving**

**+ No technical knowledge required**



# Main features - 2/6

- **Discardable hardware**

  A SEALFAIL installation image will produce the exact same system on all devices it is installed to.

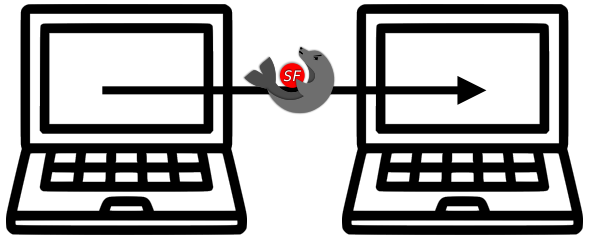
  The system is read-only and fully volatile.

  Permanent storage is delegated to a single LUKS-encrypted qcow2 disk image, the content of which is served by a host-only virtual machine over CIFS, making this file the only difference between two installations of SEALFAIL.

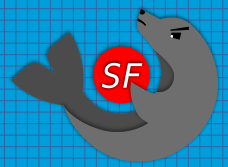
**+ Quickly replace and upgrade user hardware**

**+ Reduce user downtime**

**+ No user re-training required**



# Main features - 3/6




- **Repeatability and hardware abstraction**

  As all systems are strictly identical and volatile, replacing or upgrading devices is a matter of minutes that requires no re-training of the end user and ensures a common user experience on all devices.

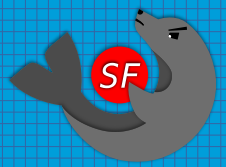
  This saves on cost and time, both of which target users often cannot afford.

**+ Shutting down the machine brings it back to its factory state**

**+ Shared experience between users**

**+ Hardware interoperability**

# Main features - 4/6




- **Prepackaged software**

  SEALFAIL comes with a plethora of pre-packaged software, all pre-configured and containerized to ensure security standards.

  The pre-packaged software collection includes common cryptographic tools, communication utilities and the LibreOffice suite among many other.

**+ No time wasted mastering software**

**+ No time wasted securing software**

**+ More time spent using quality software**

GNURadio
THE FREE & OPEN SOFTWARE RADIO ECOSYSTEM

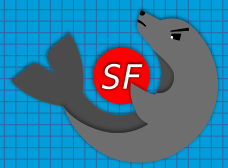
LibreOffice
The Document Foundation

OPENVPN

Tor

GnuPG

# Main features - 5/6




- **Deep hardening**

  All of the software that comes pre-packaged with SEALFAIL runs in its own LXC container.

  State-of-the-art security tools are used to ensure the system is secured to US DoD STIG compliance.

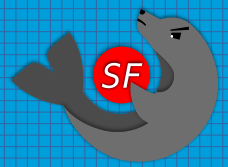
  SEALFAIL leverages the full power of hardware cryptography and modern access-control techniques to ensure security on all levels of execution.

**+ Volatile containers ensure system integrity**

**+ Scheduled checks ensure the device has not been compromised**

**+ Hardware cryptography ensures a chain of trust from startup**

# Main features - 6/6




- **Kill switch**

  SEALFAIL comes with a built-in kill switch to destroy the permanent storage in case of a security incident.

  The kill switch can only be triggered manually by the user.

**+ Prevent secret leaks**

**+ The kill switch cannot be remotely triggered**

**+ The permanent data is physically erased from the device**

# Technical outlook

SEALFAIL

Security Enhanced Alma Linux

For Activism / Insurgency / Liberation

# Technical outlook - 1/6

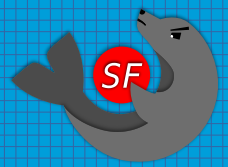
- **Based on Alma Linux**

  SEALFAIL is based on Alma Linux, a community owned, forever-free version of Red Hat Enterprise Linux (RHEL).

  Entirely compatible with the Enterprise Linux (EL) ecosystem, SEALFAIL is based on tried and trusted technologies that have been industry standards for years.

AlmaLinux

# Technical outlook - 2/6



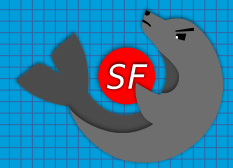

- **Kickstarts & built-in RPM repositories**

  SEALFAIL is automatically installed using a kickstart file bundled with the installation image.

  The kickstart file can be customized to deploy customized SEALFAIL installations.

  The installation image also contains a bundled RPM repository with all the extra packages required by SEALFAIL.

# Technical outlook - 3/6




- **OpenSCAP & AIDE**

  OpenSCAP is used to harden the system to US DoD DISA STIG GUI compliance.

  AIDE is used to check the system's integrity and detect changes that would result from an intrusion into the system.

  Scheduled OpenSCAP compliance checks and AIDE integrity checks are performed at regular intervals using systemd timers.

DISA

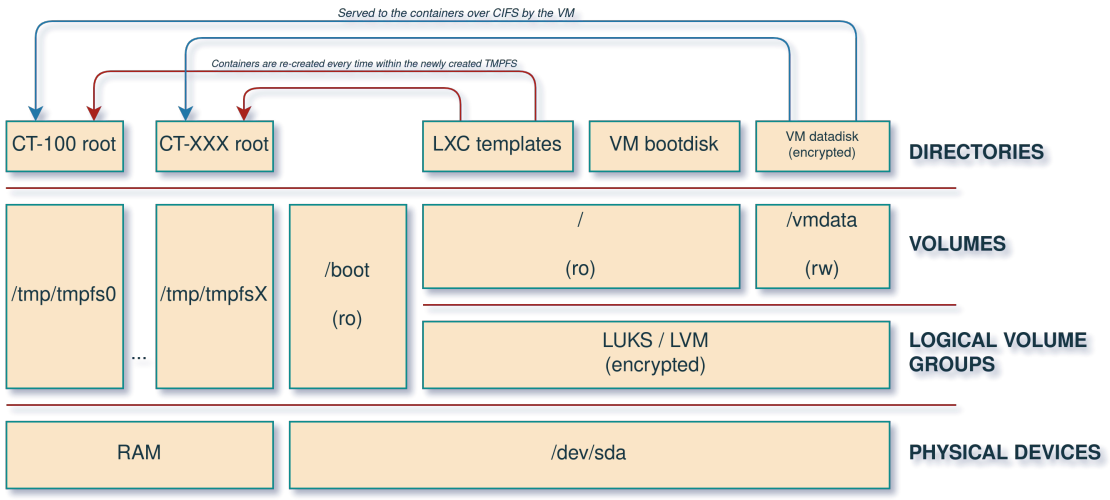
OpenSCAP

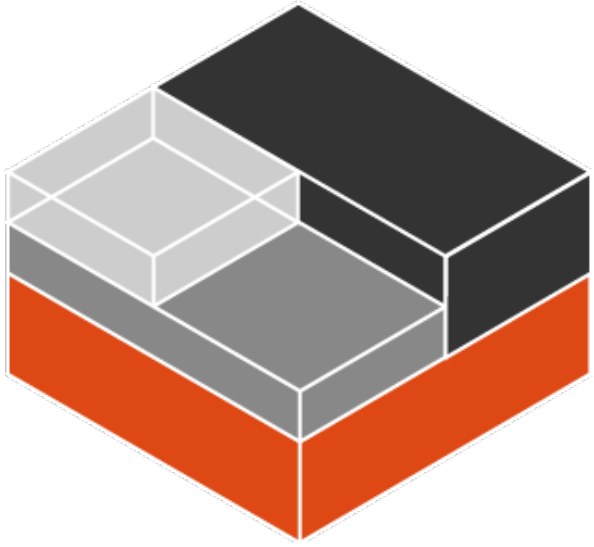
# Technical outlook - 4/6

- **All software runs under LXC**

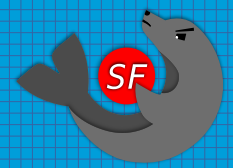
  The bundled software cannot be launched directly. It is instead spawned in Linux containers (LXC) running from TMPFS to ensure volatility.

  Each software instance is completely isolated from the others.



# Technical outlook - 5/6




- **Virtualized permanent storage**

  Permanent storage is delegated to CIFS shares.

  The shares are served to the device from a qemu VM.

  The VM has a read-only bootdisk, and a write-enabled datadisk located on its own host partition. The datadisk is used for the CIFS shares.

  The datadisk is encrypted and requires a user secret to be decrypted.

  The shares are served to the LXC containers with strict access control.

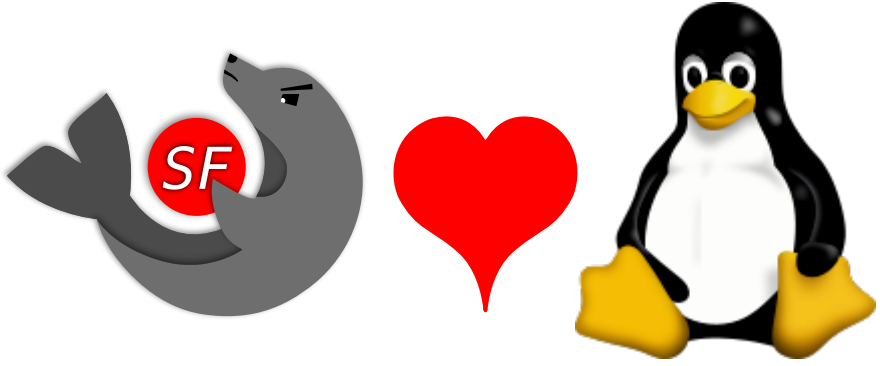
QEMU

# Technical outlook - 6/6

- **Custom kernel**

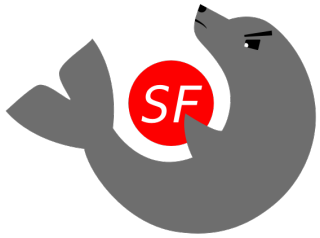
  Run-time module loading is disabled.

  The kernel is built with only the required modules, drastically decreasing its attack surface.



https://sealfail.org
contact@sealfail.org

# SEALFAIL




Security Enhanced Alma Linux

For Activism / Insurgency / Liberation