Personal Desktop Security with Linux

Why, What and How to Use It

My Own Linux Journey (2015 - Now)

Ubuntu → Linux Mint → Manjaro → Arch → Fedora → ??? → Profit

But I’ve Settled Down… I Swear… And With Good Reason!

01 Security is a must… Else why am I here?

02 I wanted a system that offered minimal to no compromises on functionality from a traditional Windows system.

03 Well documented, with good community / commercial support.

The Answer for **Me**;

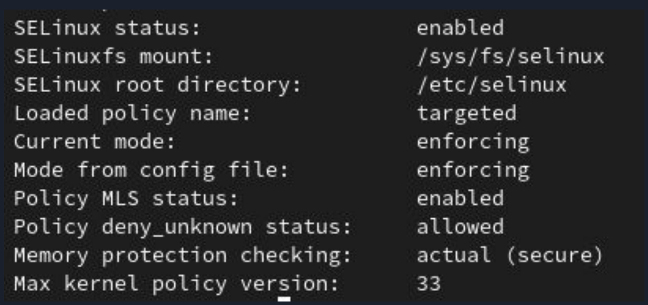
Some Security Highlights and Features

- SELinux Support Out of the Box(OotB)
- BTRFS with snapshots and LUKS Full-Disk Encryption
- GNOME Device Security Dashboard
- Automatic firmware updates (subject to vendor)
- Logs as standard
- Brilliant support for sandboxed applications

Slaps Roof of Desktop This bad boy can fit so many features in it

Why You Want SELinux

- Mandatory and Fine-Grained Access Control which results in…
  - Improved System Security
  - Reduced Attack Surface
- Compatible with other security solutions
  - Firewalls
  - Intrusion Detection Systems
- Customisable security policies



```
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      33
```

For more information see;
https://www.redhat.com/en/topics/linux/what-is-selinux

Sounds Great, but Windows has...

I’ll stop you right there!

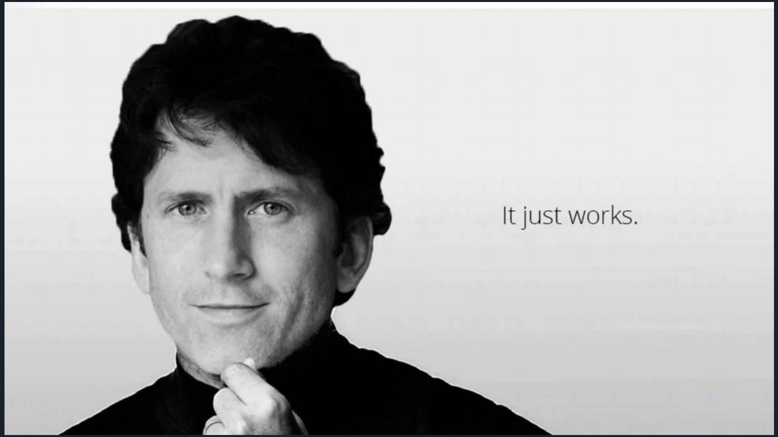
1. SELinux provides more Fine-grained access control compared to Windows ACLs.
2. SELinux gives you mandatory access control, whereas Windows ACL uses discretionary access control.
3. SELinux is policy based, meaning you can set non-user specific rules for access to system resources, Windows is user specific which can be hard to maintain at scale.

How to Use It

It Just Works©

Joking aside the default configuration out of the box on Fedora Workstation edition and other SELinux enabled distributions (RHEL, CentOS) will suit most people and shouldn't require any manual intervention and can be set to "permissive" mode if you don't want to get your hands dirty (that's less secure though, mileage may vary).

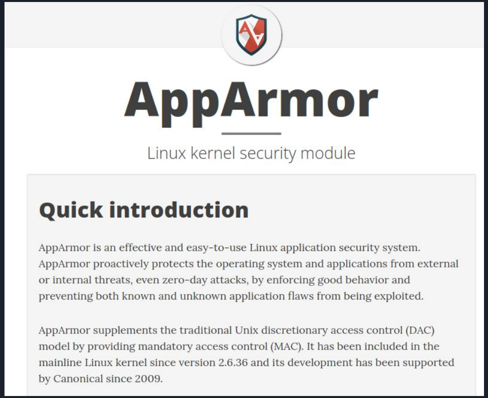
Manual Setup Guides:
[Arch]
[Debian]
[Ubuntu (See next slide as to why this has diminishing returns)]



Quick Comments on an Alternative

AppArmor

- Found primarily in Ubuntu based distributions.
- Easier to set up from scratch.
- Can be loaded and unloaded dynamically, unlike SELinux.
- Less fine-grained control compared to SELinux.
- Still great though :)



AppArmor

Linux kernel security module

Quick introduction

AppArmor is an effective and easy-to-use Linux application security system. AppArmor proactively protects the operating system and applications from external or internal threats, even zero-day attacks, by enforcing good behavior and preventing both known and unknown application flaws from being exploited.

AppArmor supplements the traditional Unix discretionary access control (DAC) model by providing mandatory access control (MAC). It has been included in the mainline Linux kernel since version 2.6.36 and its development has been supported by Canonical since 2009.

BTRFS and LUKS; What is it?

B-Tree File System (BTRFS) is a modern file system designed for Linux operating systems, set as a replacement for Ext4. It’s used on Fedora Workstation by default and has the following native features;

- Data and metadata checksumming
- Snapshots and rollbacks
- Compression
- Software RAID support

It can be used optionally in conjunction with Linux Unified Key Setup(LUKS), a widely-used disk encryption specification for Linux, to enable full-disk encryption. This is easy to enable in the installer for Fedora Workstation.

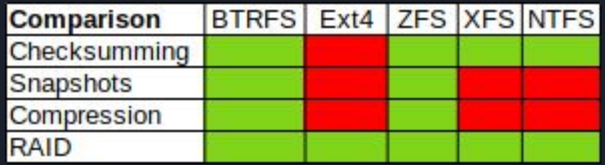
Comparing to the Competition...

Ext4: Default file system for many Linux distributions but lacks features such as snapshots, checksumming and on-the-fly compression.

ZFS: Supports features such as snapshots, checksumming, and RAID configurations. However, ZFS is more complex to configure and manage than BTRFS, and may require more system resources. Can be enabled easily in the advanced features of Ubuntu.

XFS: Better for large files and high-speed data transfer, however, XFS lacks snapshots and compression.

NTFS: Default on Windows, lacks snapshots and checksumming. Proprietary.



Comparison	BTRFS	Ext4	ZFS	XFS	NTFS
Checksumming	🟩	🟥	🟩	🟩	🟩
Snapshots	🟩	🟥	🟩	🟥	🟥
Compression	🟩	🟥	🟩	🟥	🟥
RAID	🟩	🟩	🟩	🟩	🟩

How Do I Use It?

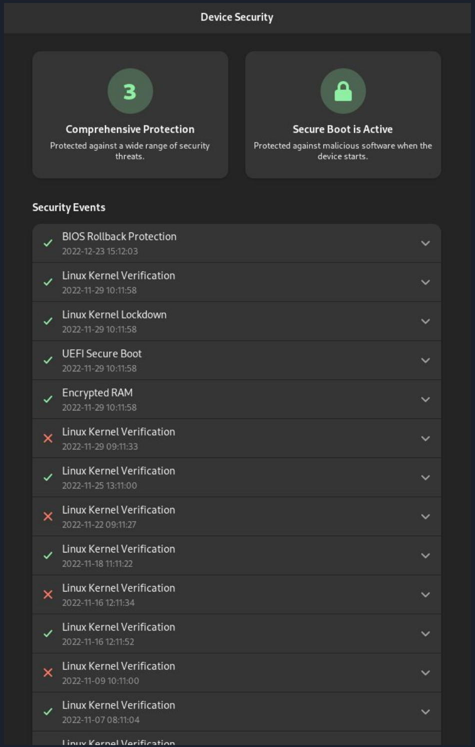
- **RAID**
  - Runs by default at RAID0 if you select multiple drives to install to in the Fedora Workstation installer.
  - Otherwise politely RTFM; https://btrfs.readthedocs.io/en/latest/Volume-management.html

- **Compression**
  - Runs out of the box on a fresh Fedora Workstation install.
  - Otherwise politely RTFM; https://btrfs.readthedocs.io/en/latest/Compression.html

- **Snapshots**
  - **GUI:** Timeshift (Note: Needs Ubuntu-type subvolume layout)
  - **CLI:** RTFM & Fedora Magazine Article

- **Checksumming**
  - Issues logged by default on BTRFS; RTFM

GNOME Device Security Dashboard; If You Want to be Crazy About It



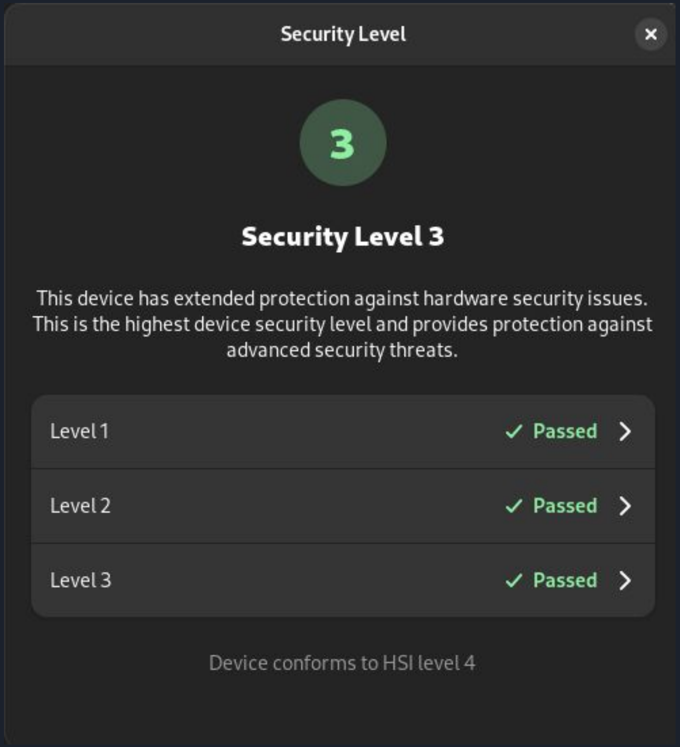
Device Security

3
Comprehensive Protection
Protected against a wide range of security threats.

Secure Boot is Active
Protected against malicious software when the device starts.

Security Events

- ✓ BIOS Rollback Protection 2022-12-23 15:12:03
- ✓ Linux Kernel Verification 2022-11-29 10:11:58
- ✓ Linux Kernel Lockdown 2022-11-29 10:11:58
- ✓ UEFI Secure Boot 2022-11-29 10:11:58
- ✓ Encrypted RAM 2022-11-29 10:11:58
- ✗ Linux Kernel Verification 2022-11-29 09:11:33
- ✓ Linux Kernel Verification 2022-11-25 13:11:00
- ✗ Linux Kernel Verification 2022-11-22 09:11:27
- ✓ Linux Kernel Verification 2022-11-18 11:11:22
- ✗ Linux Kernel Verification 2022-11-16 12:11:34
- ✓ Linux Kernel Verification 2022-11-16 12:11:52
- ✗ Linux Kernel Verification 2022-11-09 10:11:00
- ✓ Linux Kernel Verification 2022-11-07 08:11:04
- Linux Kernel Verification



Security Level

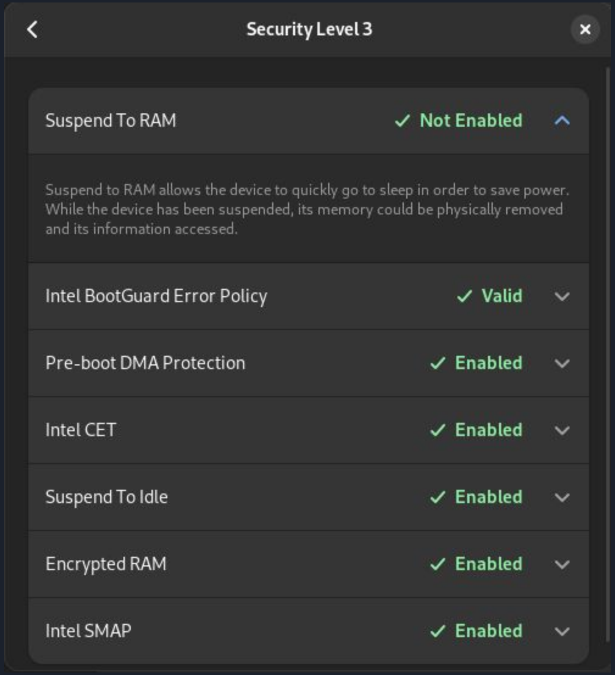
3

Security Level 3

This device has extended protection against hardware security issues. This is the highest device security level and provides protection against advanced security threats.

Level 1	✓ Passed	›
Level 2	✓ Passed	›
Level 3	✓ Passed	›

Device conforms to HSI level 4



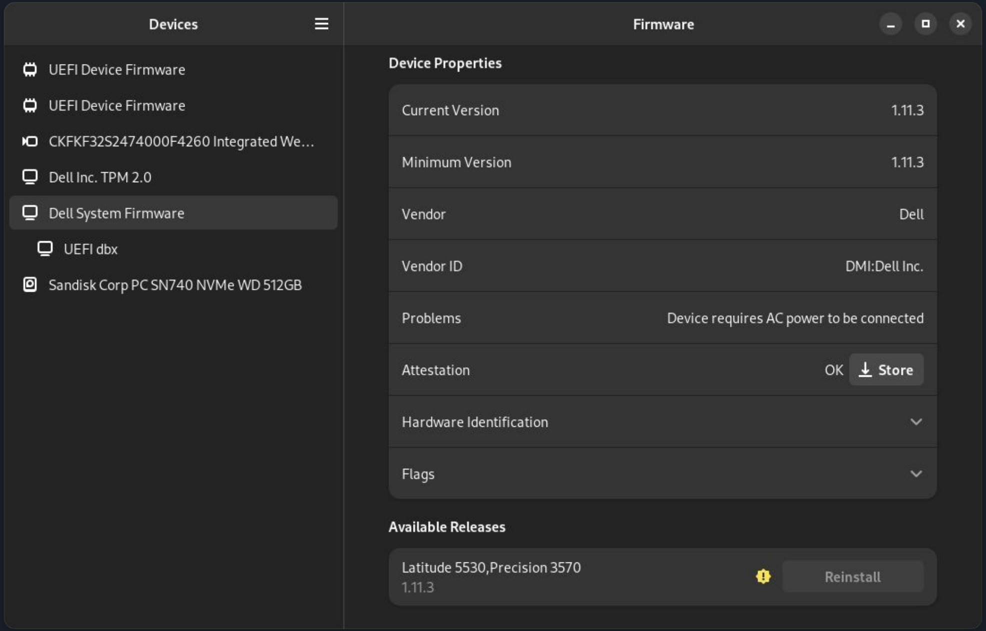
Security Level 3

Suspend To RAM	✓ Not Enabled

Suspend to RAM allows the device to quickly go to sleep in order to save power. While the device has been suspended, its memory could be physically removed and its information accessed.

Intel BootGuard Error Policy	✓ Valid
Pre-boot DMA Protection	✓ Enabled
Intel CET	✓ Enabled
Suspend To Idle	✓ Enabled
Encrypted RAM	✓ Enabled
Intel SMAP	✓ Enabled

Firmware Updating and Device Management



- UEFI Device Firmware
- UEFI Device Firmware
- CKFKF32S2474000F4260 Integrated We…
- Dell Inc. TPM 2.0
- Dell System Firmware
  - UEFI dbx
- Sandisk Corp PC SN740 NVMe WD 512GB

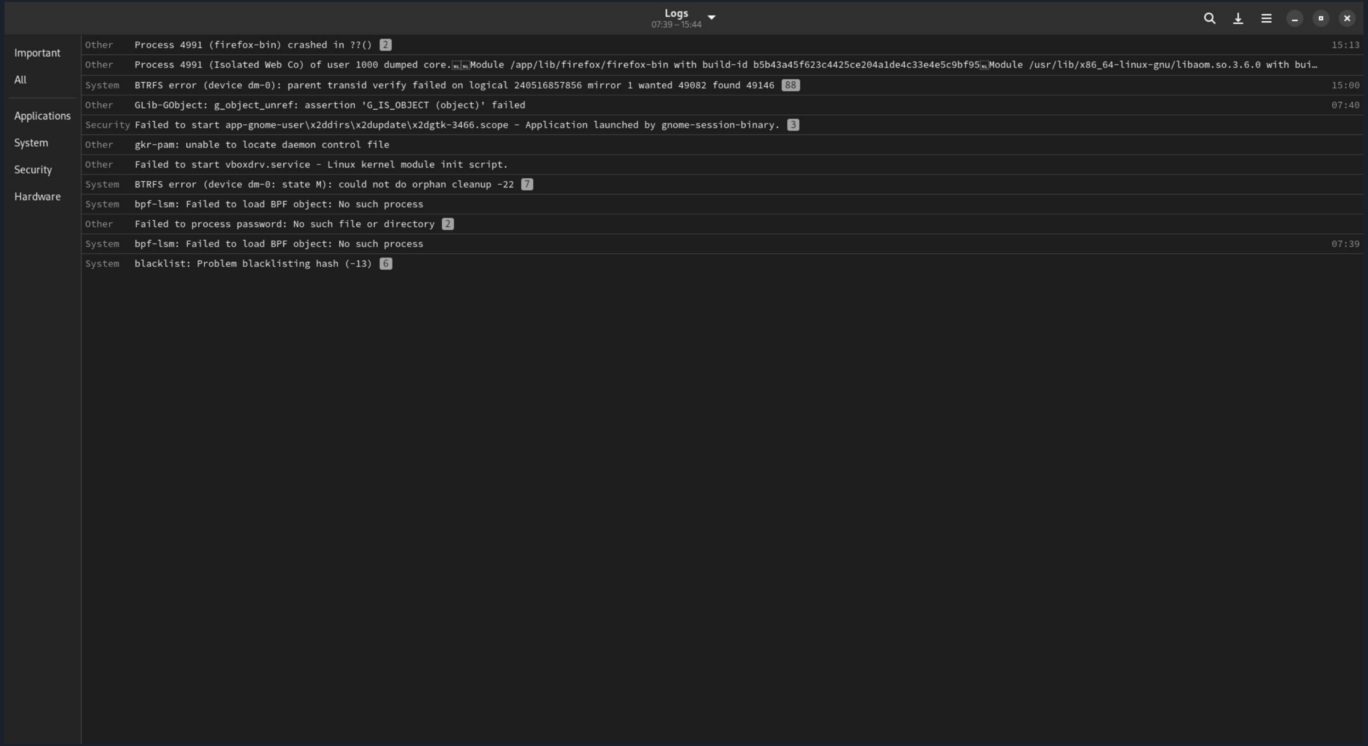
Device Properties

Current Version	1.11.3
Minimum Version	1.11.3
Vendor	Dell
Vendor ID	DMI:Dell Inc.
Problems	Device requires AC power to be connected
Attestation	OK Store
Hardware Identification	
Flags	

Available Releases

Latitude 5530,Precision 3570
1.11.3

Logs, logs and more logs



```
Other    Process 4991 (firefox-bin) crashed in ??() 2                                                     15:13
Other    Process 4991 (Isolated Web Co) of user 1000 dumped core.␤␤Module /app/lib/firefox/firefox-bin with build-id b5b43a45f623c4425ce204a1de4c33e4e5c9bf95␤Module /usr/lib/x86_64-linux-gnu/libaom.so.3.6.0 with bui…
System   BTRFS error (device dm-0): parent transid verify failed on logical 240516857856 mirror 1 wanted 49082 found 49146 88    15:00
Other    GLib-GObject: g_object_unref: assertion 'G_IS_OBJECT (object)' failed                           07:40
Security Failed to start app-gnome-user\x2ddirs\x2dupdate\x2dgtk-3466.scope - Application launched by gnome-session-binary. 3
Other    gkr-pam: unable to locate daemon control file
Other    Failed to start vboxdrv.service - Linux kernel module init script.
System   BTRFS error (device dm-0: state M): could not do orphan cleanup -22 7
System   bpf-lsm: Failed to load BPF object: No such process
Other    Failed to process password: No such file or directory 2
System   bpf-lsm: Failed to load BPF object: No such process                                             07:39
System   blacklist: Problem blacklisting hash (-13) 6
```

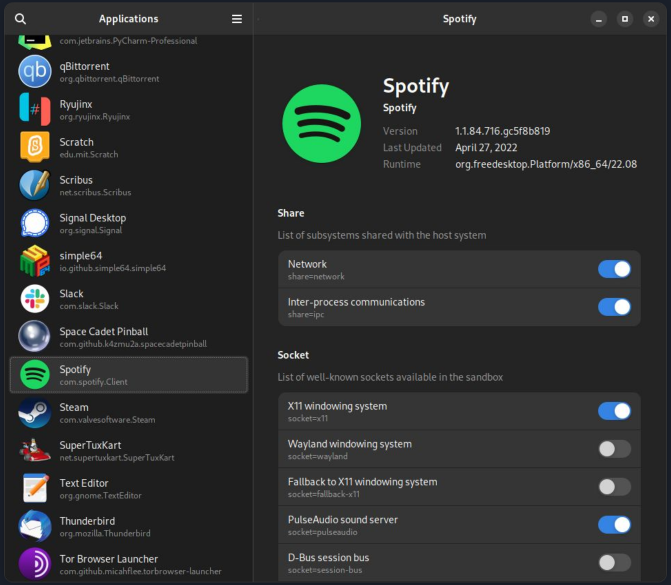
Sandboxed Applications

Flatpak

snapcraft

Firejail

security sandbox



com.jetbrains.PyCharm-Professional

qBittorrent
org.qbittorrent.qBittorrent

Ryujinx
org.ryujinx.Ryujinx

Scratch
edu.mit.Scratch

Scribus
net.scribus.Scribus

Signal Desktop
org.signal.Signal

simple64
io.github.simple64.simple64

Slack
com.slack.Slack

Space Cadet Pinball
com.github.k4zmu2a.spacecadetpinball

Spotify
com.spotify.Client

Steam
com.valvesoftware.Steam

SuperTuxKart
net.supertuxkart.SuperTuxKart

Text Editor
org.gnome.TextEditor

Thunderbird
org.mozilla.Thunderbird

Tor Browser Launcher
com.github.micahflee.torbrowser-launcher

Spotify
Spotify

Version	1.1.84.716.gc5f8b819
Last Updated	April 27, 2022
Runtime	org.freedesktop.Platform/x86_64/22.08

Share

List of subsystems shared with the host system

- Network (share=network) ☑
- Inter-process communications (share=ipc) ☑

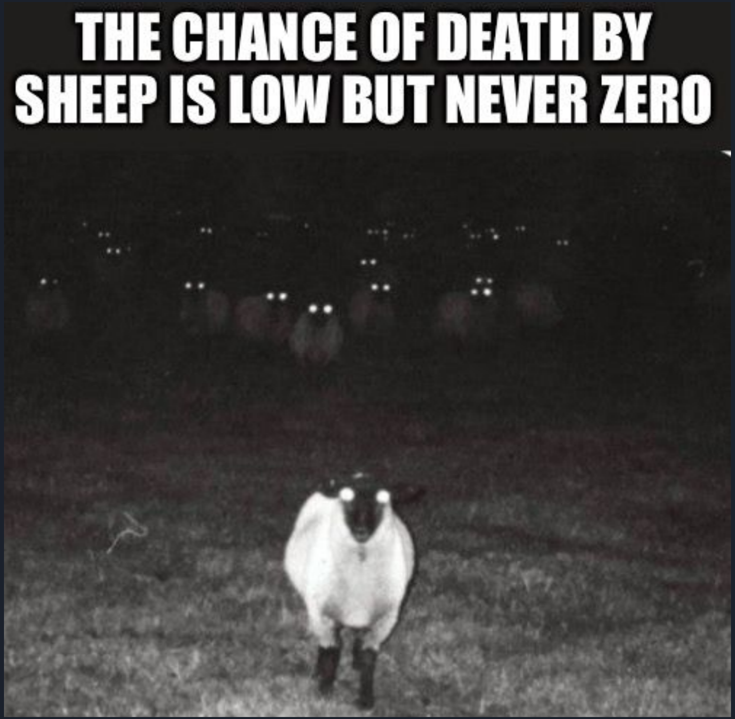
Socket

List of well-known sockets available in the sandbox

- X11 windowing system (socket=x11) ☑
- Wayland windowing system (socket=wayland) ☐
- Fallback to X11 windowing system (socket=fallback-x11) ☐
- PulseAudio sound server (socket=pulseaudio) ☑
- D-Bus session bus (socket=session-bus) ☐

Quickfire Security Round and Disclaimer

- Malware targeting desktop systems rarely target Linux based systems.
- Software from trusted and vetted repositories.
  - On that note, default software center gives a security breakdown on applications from official repos, RPM fusion (more on that in caveats) and Snaps in the Snap store.
- Immutability is the planned future of the Fedora project, but can be used today under the name of Silverblue.
- Typical security solutions are easily available, firewalld comes as standard for Fedora Workstation.
- Like the sheep on the right, you're minimising your personal attack surface, but still employ common sense and critical thinking to keep yourself safe.



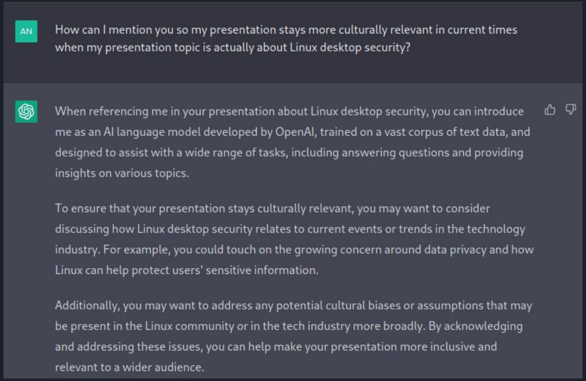
Surely With All These Benefits, Sacrifices Had to be Made?

With some caveats (see closing comments later), I was able to move from daily driving Linux to Windows pretty smoothly (and that was back in 2015, things were much worse then). Issues do occur but they’re less frequent or annoying than what I experienced on Windows.

So in terms of functionality, some areas are the same, some areas you lose out on and some areas you make gains. With security being one of the areas where you’ll garner significant gains. It’s all highly subjective.

And What About Documentation, Support & Project Funding?

- Documentation can be found here; https://docs.fedoraproject.org/en-US/docs/
- Forums are here; https://discussion.fedoraproject.org/
- The project is sponsored by RedHat and Fedora itself operates as the upstream for RHEL. For more information see here; https://www.redhat.com/en/topics/linux/fedora-vs-red-hat-enterprise-linux
- Push come to shove you can always trust the holy trinity of Google, Stack Overflow and ChatGPT.



How can I mention you so my presentation stays more culturally relevant in current times when my presentation topic is actually about Linux desktop security?

When referencing me in your presentation about Linux desktop security, you can introduce me as an AI language model developed by OpenAI, trained on a vast corpus of text data, and designed to assist with a wide range of tasks, including answering questions and providing insights on various topics.

To ensure that your presentation stays culturally relevant, you may want to consider discussing how Linux desktop security relates to current events or trends in the technology industry. For example, you could touch on the growing concern around data privacy and how Linux can help protect users' sensitive information.

Additionally, you may want to address any potential cultural biases or assumptions that may be present in the Linux community or in the tech industry more broadly. By acknowledging and addressing these issues, you can help make your presentation more inclusive and relevant to a wider audience.

That’s All Well and Good, Where to Start?

- Installation instructions can be found here; https://docs.fedoraproject.org/en-US/fedora/latest/getting-started/

Some Caveats, Tips and Advice

- There's a learning curve, don't expect to be a master from day one and be ready to learn.
- Software compatibility is something that needs to be checked before making the plunge, for general application compatibility and alternatives check https://alternativeto.net/.
  - In a similar vein, gaming gets better by the day, but not quite as good as Windows (yet ;)), here's some resources for that;
    - Reports for game compatibility with Valve's Proton layer; https://www.protondb.com/
    - A third party launcher for non-steam games; https://lutris.net/
  - Fedora by default omits proprietary applications, to have the best software availability enable the following repositories post-install. I've ordered them by my own personal recommendation for search order. Note; Nvidia drivers, broadcom drivers, pycharm and other bits and bobs can be enabled instantly after install for compatibility sake);
    - RPM Fusion;
      - Setup; https://rpmfusion.org/Configuration
      - Codecs; https://rpmfusion.org/Howto/Multimedia
    - Flatpak; https://www.flatpak.org/setup/Fedora
    - Snap; https://snapcraft.io/docs/installing-snap-on-fedora
    - AppImage (Not a repo, just a resource); https://appimage.github.io/apps/
    - Copr; https://copr.fedorainfracloud.org/
- Try it on a VM first, then a spare machine if you have one, before installing on your daily driver, dual booting is also an option.

That’s All Folks!

Any Questions? :)

For any follow up or if you need help getting started feel free to get in touch;

andrew.kenneally1@mycit.ie