Red Hat Summit

Connect

Invisible Security Technologies That Keeps Your Business Safe

Lukas Vrabec
Principal Software Engineer &
Security Product Owner

Red Hat

Lukas Vrabec

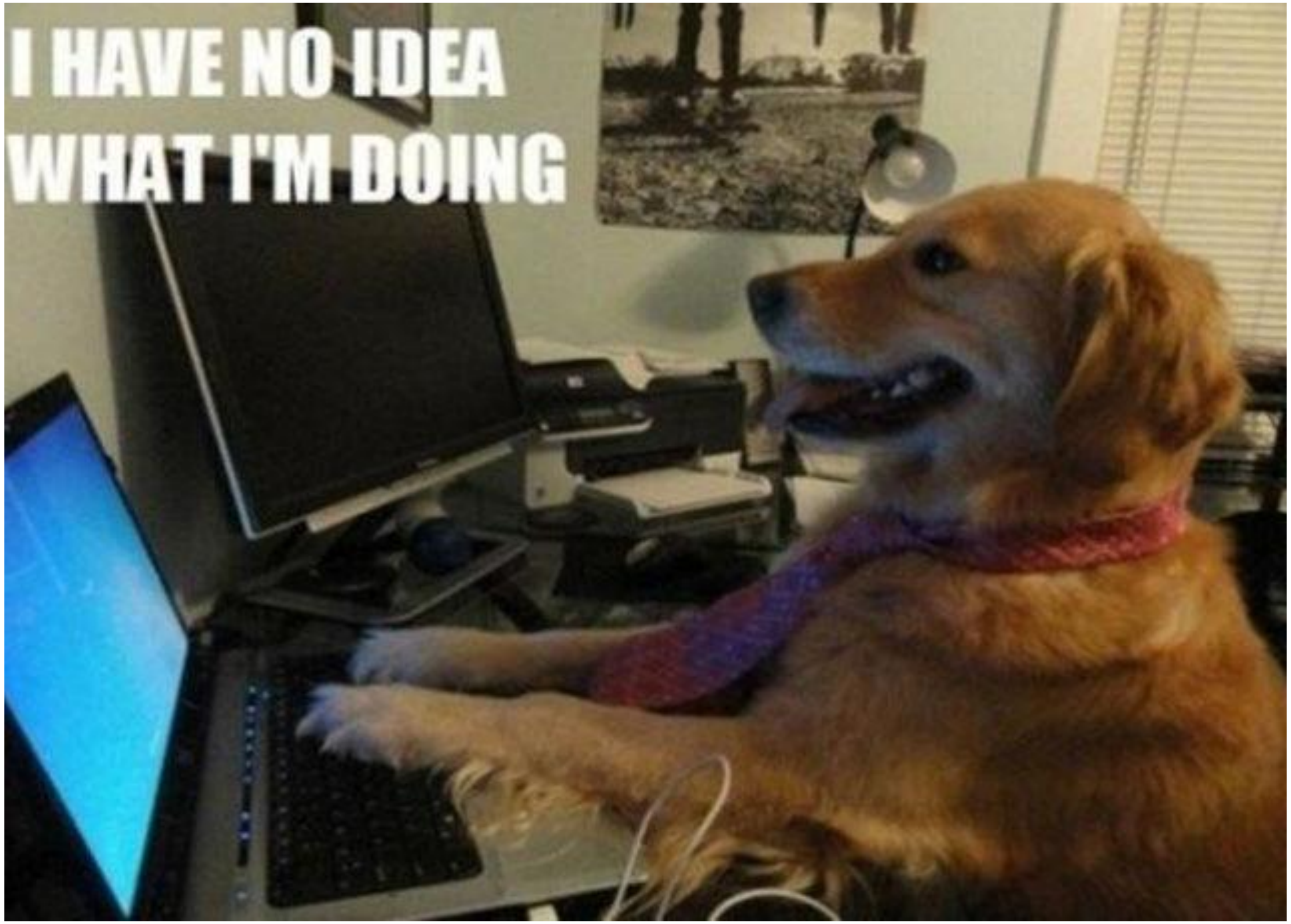
- Team Lead of 2 standalone security engineering teams
- Security Special Projects & SELinux Product Owner
- RHEL & Fedora Contributor
- https://github.com/wrabcak

When do people care about security?

Red Hat

This Hack Will
Destroy Your Phone!

Where do security issues come from?


I HAVE NO IDEA
WHAT I'M DOING

Proactive Security & Technologies

A Move Towards Zero Trust

Traditional Security Models

Assumed Trust

Perimeter based security model which assumed trust. Higher level of trust once inside the perimeter

Zero Trust Security Model

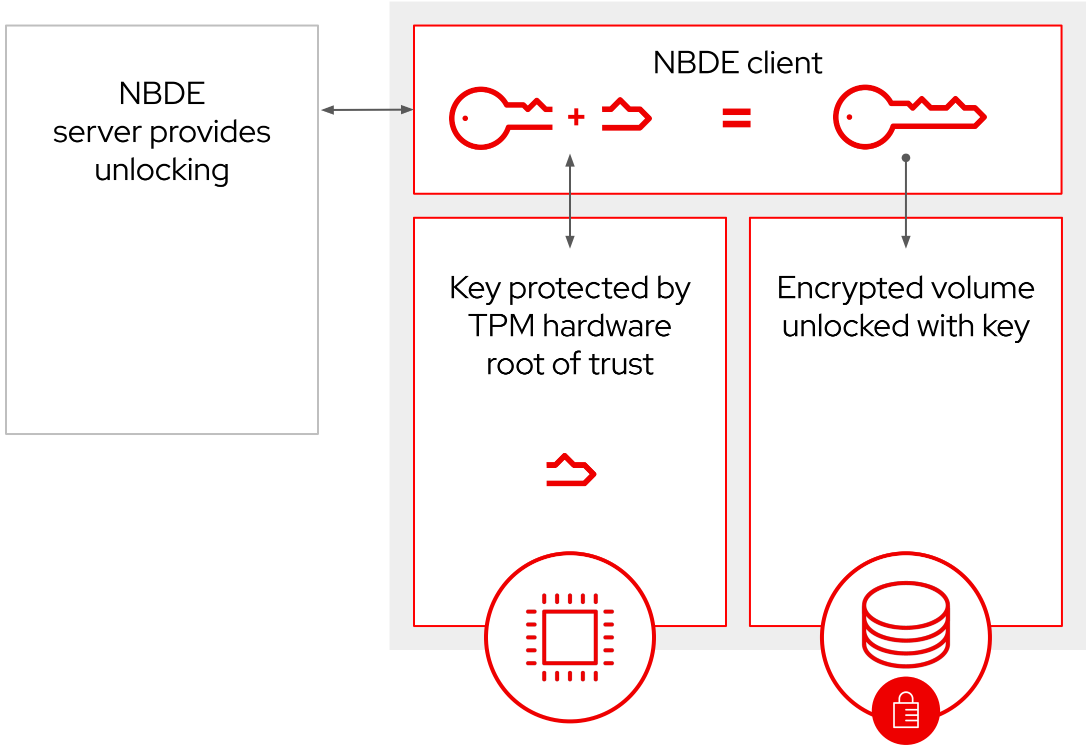
Deny all, Verify all

No implicit trust. Authentication and authorization required between all parties. Identity, Integrity, Isolation

Proactive Security

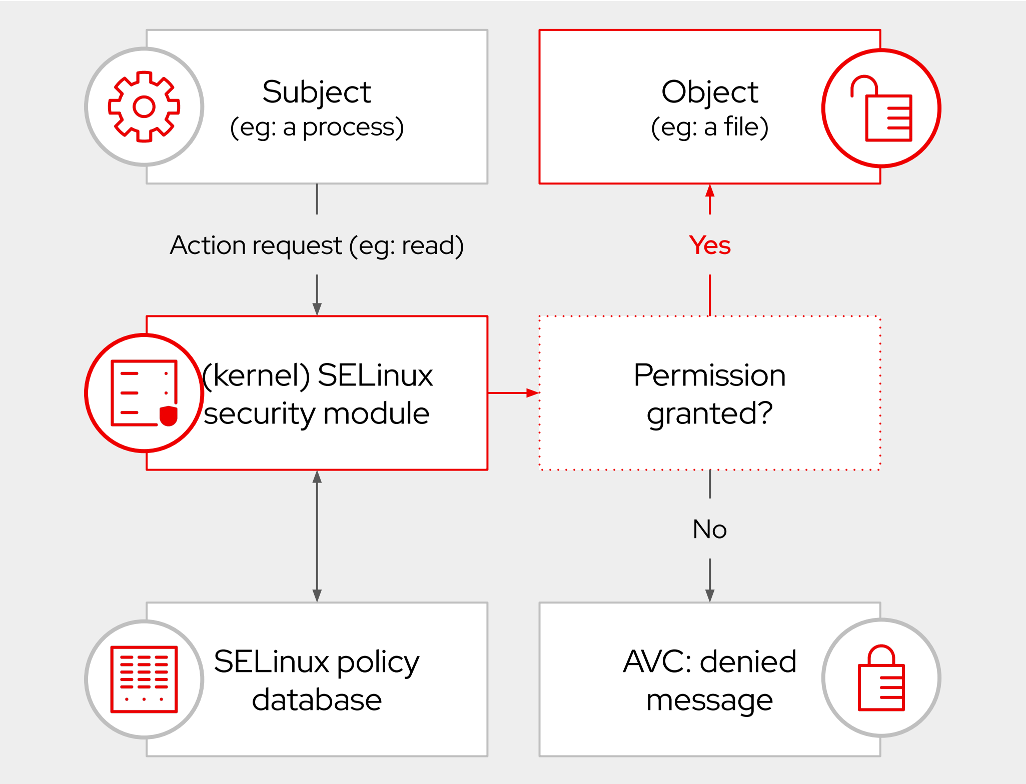
- RHEL OS “built-in Security Technologies” – It’s free!
  - NBDE/luks
  - SELinux
  - Fapolicyd
  - System-wide crypto policies
  - Keylime
  - Aide
  - USBGuard
- Compliance

Easy data protection using network bound disk encryption (NBDE)


NBDE server provides unlocking
NBDE client
+
=
Key protected by TPM hardware root of trust
Encrypted volume unlocked with key

- Consistent, hands-off unlocking of encrypted volumes on-premise or in the hybrid cloud
- Allows binding encrypted volumes to a special network server
- No need to manually manage encryption keys
- Does not require complex PKI solution
- Can leverage TPM to ensure system integrity before unlocking encrypted volumes

SELinux mandatory access controls provides an OS layer of security

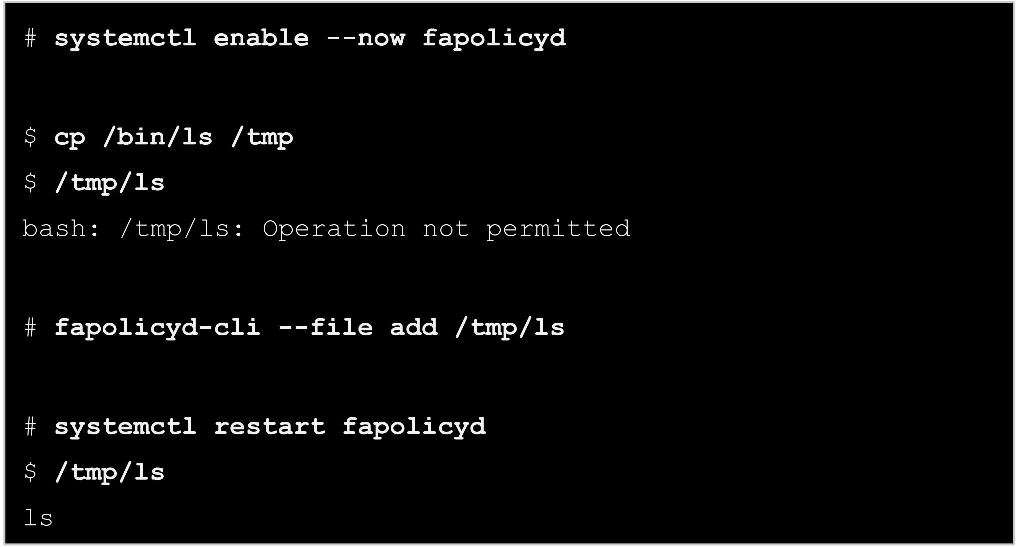


Live demo

- Apply fine-grained level of control over files, processes, users and apps via SELinux policy
- By default denied -> needs to exists allow rules
- Customizable per application or container
- Process isolation to mitigate attacks via privilege escalations
- Provides container separation and protection
- Prevent several CVEs: Runcescape, Shellshock!

Red Hat

Application allowlisting (fapolicyd) prevents unauthorized access



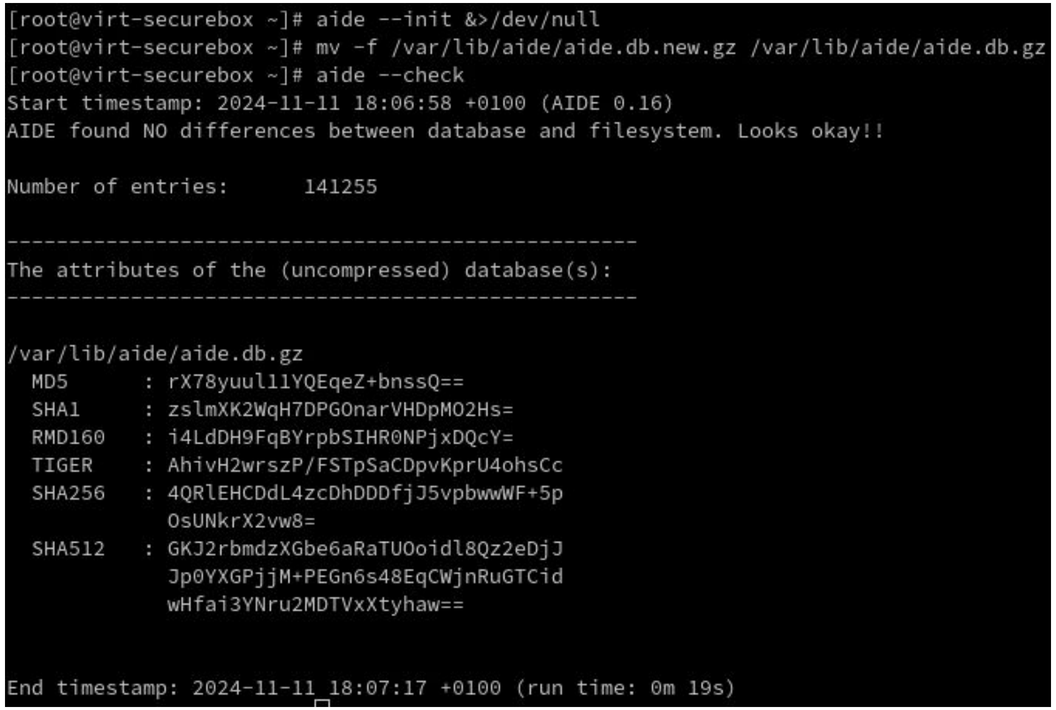
```
# systemctl enable --now fapolicyd

$ cp /bin/ls /tmp
$ /tmp/ls
bash: /tmp/ls: Operation not permitted

# fapolicyd-cli --file add /tmp/ls

# systemctl restart fapolicyd
$ /tmp/ls
ls
```

Control execution based on file path, hash, or integrity

Here fapolicyd prevents the ls command from executing when it's not in the expected location, but one simple command can enable this, if needed.

- Predetermine trusted programs authorized to run on a machine
- Detect or prevent modified apps from running
- Leverage predefined policy for most use cases(rpm database)
- Place more control in the hands of admins

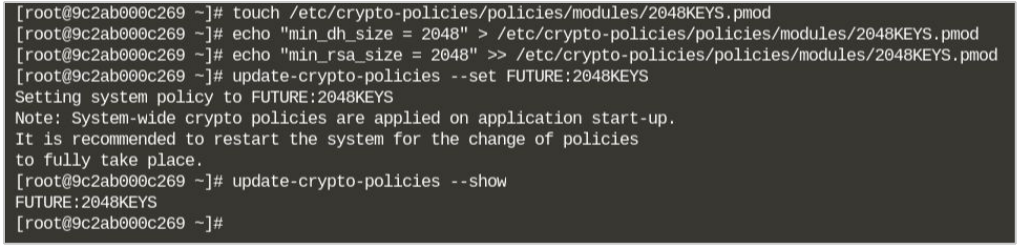
File system integrity checking with AIDE



```
[root@virt-securebox ~]# aide --init &>/dev/null
[root@virt-securebox ~]# mv -f /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz
[root@virt-securebox ~]# aide --check
Start timestamp: 2024-11-11 18:06:58 +0100 (AIDE 0.16)
AIDE found NO differences between database and filesystem. Looks okay!!

Number of entries:      141255

---------------------------------------------------
The attributes of the (uncompressed) database(s):
---------------------------------------------------

/var/lib/aide/aide.db.gz
  MD5      : rX78yuul11YQEqeZ+bnssQ==
  SHA1     : zslmXK2WqH7DPGOnarVHDpMO2Hs=
  RMD160   : i4LdDH9FqBYrpbSIHR0NPjxDQcY=
  TIGER    : AhivH2wrszP/FSTpSaCDpvKprU4ohsCc
  SHA256   : 4QRlEHCDdL4zcDhDDDfjJ5vpbwwWF+5p
             OsUNkrX2vw8=
  SHA512   : GKJ2rbmdzXGbe6aRaTUOoidl8Qz2eDjJ
             Jp0YXGPjjM+PEGn6s48EqCWjnRuGTCid
             wHfai3YNru2MDTVxXtyhaw==


End timestamp: 2024-11-11 18:07:17 +0100 (run time: 0m 19s)
```

- AIDE is a tool that monitors file integrity to detect unauthorized changes.
- Regularly compares current files to a baseline for unexpected modifications.
- Flags anomalies, providing logs for quick incident response.
- Mainly suited for configuration and other data types

System-wide cryptography policies for the modern enterprise



```
[root@9c2ab000c269 ~]# touch /etc/crypto-policies/policies/modules/2048KEYS.pmod
[root@9c2ab000c269 ~]# echo "min_dh_size = 2048" > /etc/crypto-policies/policies/modules/2048KEYS.pmod
[root@9c2ab000c269 ~]# echo "min_rsa_size = 2048" >> /etc/crypto-policies/policies/modules/2048KEYS.pmod
[root@9c2ab000c269 ~]# update-crypto-policies --set FUTURE:2048KEYS
Setting system policy to FUTURE:2048KEYS
Note: System-wide crypto policies are applied on application start-up.
It is recommended to restart the system for the change of policies
to fully take place.
[root@9c2ab000c269 ~]# update-crypto-policies --show
FUTURE:2048KEYS
[root@9c2ab000c269 ~]#
```

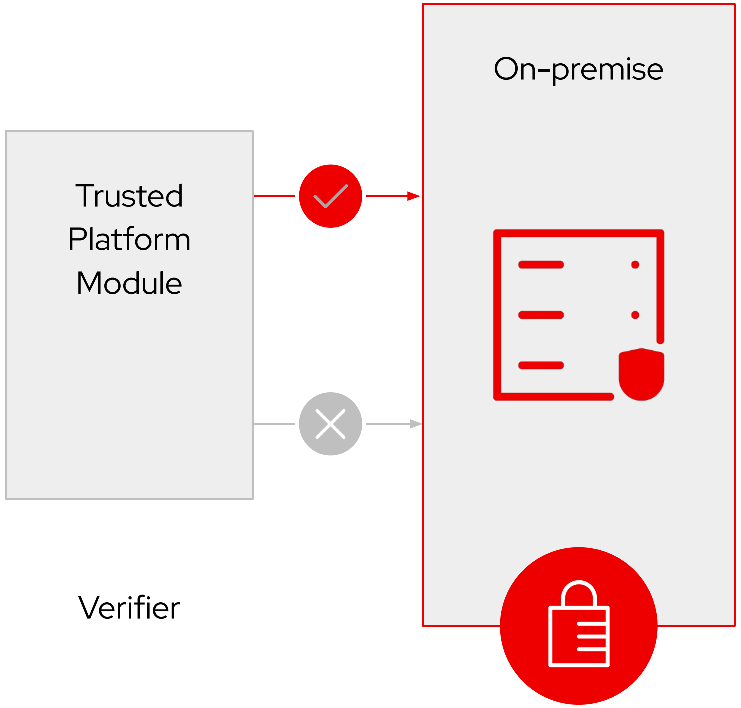
One command to create, manage, load policies

DH and RSA key lengths are increased to 2048 bits by default. Applies to all applications and all built-in cryptography.

- Ensure system wide, consistent settings for addressing compliance
- Manage crypto policy baselines at scale
- Use one-command method of managing the security of cryptography across all footprints
- Easily customize to meet your site-specific policy requirements

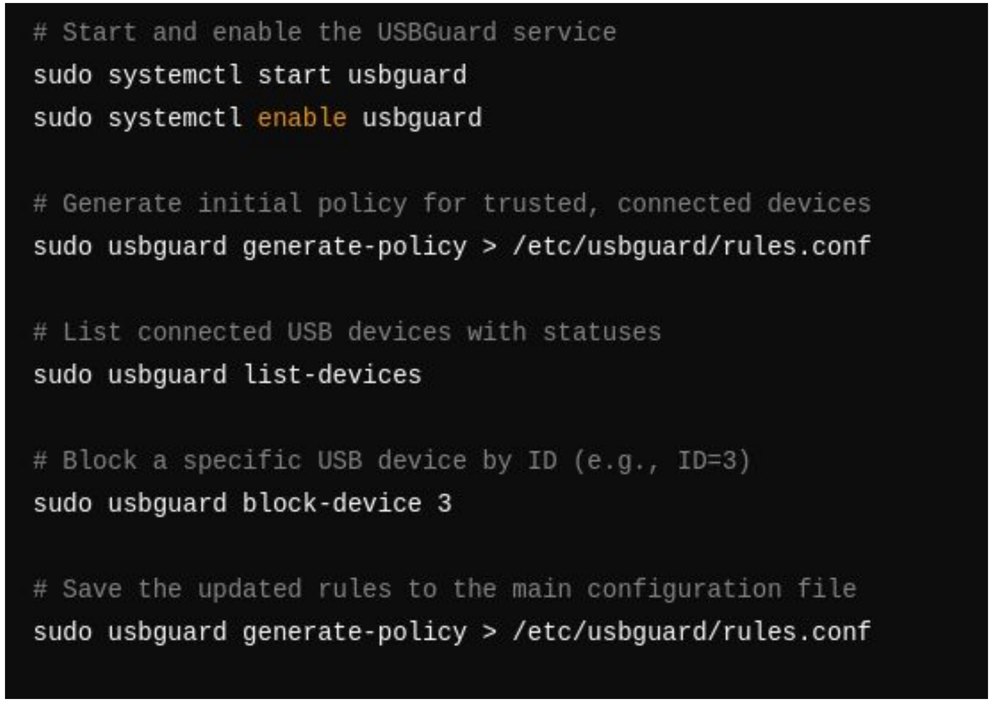
Live demo 1 and Live demo 2

Remote attestation and measured boot (keylime)



- During secure boot, kernel, loadable modules and boot environment are cryptographically measured
- Measure also runtime binaries before execution
- Measurement compute using tamper-resistant hardware Trusted Platform Module (TPM)
- Attestation agent collects measurements and sends to attestation verifier
- The verifier maintains list of known good measurements and compares incoming measurements
- If the system was compromised, the verifier will detect this and remediation can then take place
- A remediation framework exist for customers to create their own actions based upon verification failure

Allow-Listing of USB devices via USBGuard



```
# Start and enable the USBGuard service
sudo systemctl start usbguard
sudo systemctl enable usbguard

# Generate initial policy for trusted, connected devices
sudo usbguard generate-policy > /etc/usbguard/rules.conf

# List connected USB devices with statuses
sudo usbguard list-devices

# Block a specific USB device by ID (e.g., ID=3)
sudo usbguard block-device 3

# Save the updated rules to the main configuration file
sudo usbguard generate-policy > /etc/usbguard/rules.conf
```

- USBGuard controls which USB devices can connect to the system.
- Enables detailed policies to allow only trusted devices, blocking unknown ones by default.
- Restricts USB access to authorized devices, reducing risks of data theft and malware.

Ansible provides a comprehensive automation platform

For securing and hardening RHEL at scale

Red Hat Enterprise Linux + **Red Hat** Ansible Automation Platform

- Automate security configuration and maintain consistency across all your environments over time via Ansible
- Ensure security and compliance at scale and with less resources than ever before
- Use automation to meet governance and compliance requirements

Security roles: SELinux, NBDE client & server, Keylime, Sudo, fapolicyd, Crypto Policies, Identity and many more!

Live demo

Compliance

Compliance goals

Configuration of OS as part of regulatory requirements

Our goals are:

- To help orient, simplify and make cheaper
  - Guide how to get closer to the requirements while following best practices
  - Automated configuration adjustments (hardening/remediation)
  - Scanning of the systems to find divergence to standards
- We don’t guarantee certifications, we help to get closer.

Compliance goals

Examples of standards in RHEL

- PCI-DSS (Payment Card Industry - Data Security Standard)
- HIPAA (The Health Insurance Portability and Accountability Act)
- CIS (Center for Internet Security)

Compliance of the product

Certifications on our side

RHEL undergoes several certifications

- FIPS (Federal Information Processing Standards)
  - RHEL crypto able to switch to FIPS mode
- Common Criteria (under NIAP - US version)
  - Ability of the OS to become secure

Do we have a profile for you?

- Most of the profiles are industry specific, so you'd know you need to follow them
- Writing profiles from scratch is not trivial
  - We have a hands-on lab for that, though!
- Very good (and flexible) general purpose profile is CIS
  - Backed by independent security non-profit

Red Hat Summit

Connect

Thank you

linkedin.com/company/red-hat

facebook.com/redhatinc

youtube.com/user/RedHatVideos

twitter.com/RedHat

Red Hat