Red Hat
Enterprise Linux

Security hardening in RHEL

Innovate Together
Prague 2026

Lukas Vrabec

Security Product Owner

Red Hat

About me

- Lukas Vrabec - lvrabec@redhat.com
- Team Lead of 2 standalone security teams
- Security Special Projects & SELinux Product Owner
- RHEL & Fedora Contributor
- Red Hat blogs
- Github



Agenda

- Zero Trust
- RHEL Hardening
- Post Quantum Cryptography

Red Hat

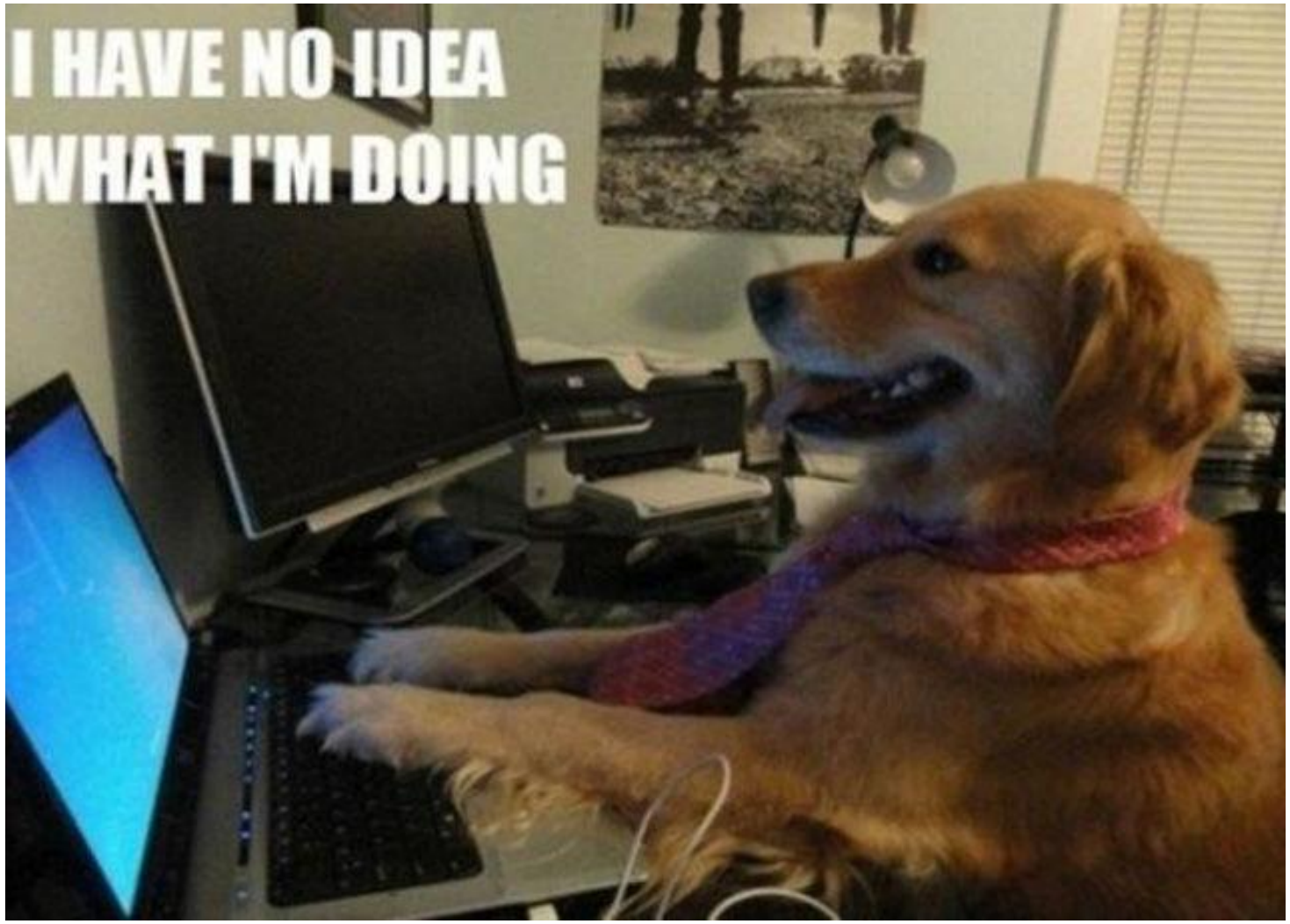
When do people care about security?

Red Hat


This Hack Will
Destroy Your Phone!

Where do security issues come from?

Red Hat


I HAVE NO IDEA
WHAT I'M DOING


I HAVE NO IDEA
WHAT I'M DOING

Zero Trust & 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



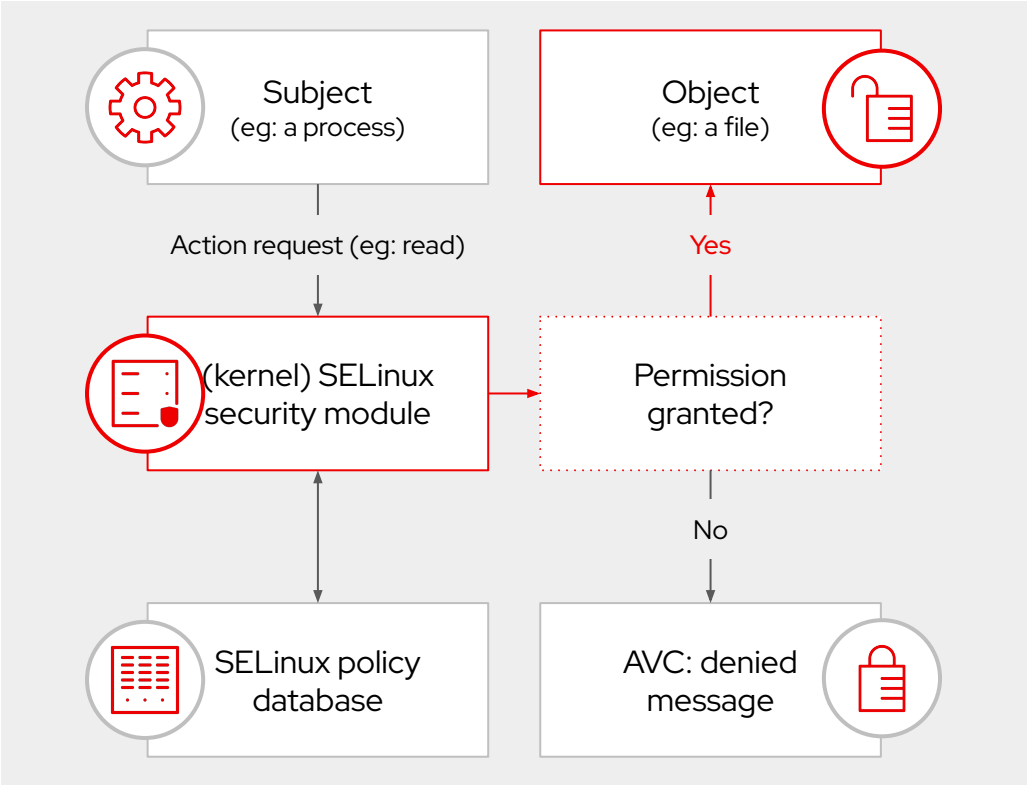
Zero Trust Security Model

Deny all, Verify all

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



SELinux mandatory access controls provides an OS layer of security



Live demo

- Process isolation to mitigate attacks via privilege escalations
- 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
- Provides container separation and protection

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
```

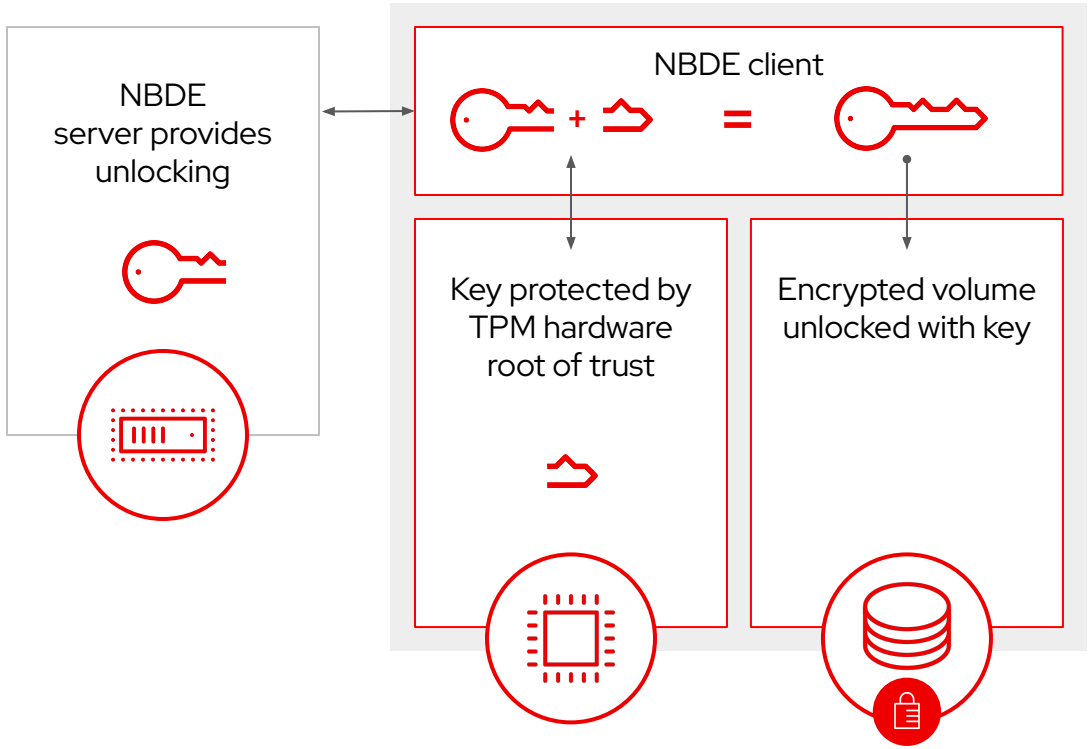
Control execution based on file path, hash, or integrity

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

Red Hat

Easy data protection using network bound disk encryption (NBDE)



- 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
- Can leverage TPM to ensure system integrity before unlocking encrypted volumes
- PKCS#11 support - Smart cards since RHEL-10.1

Red Hat

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)
```

- Advanced Intrusion Detection Environment
- 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

Red Hat

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.

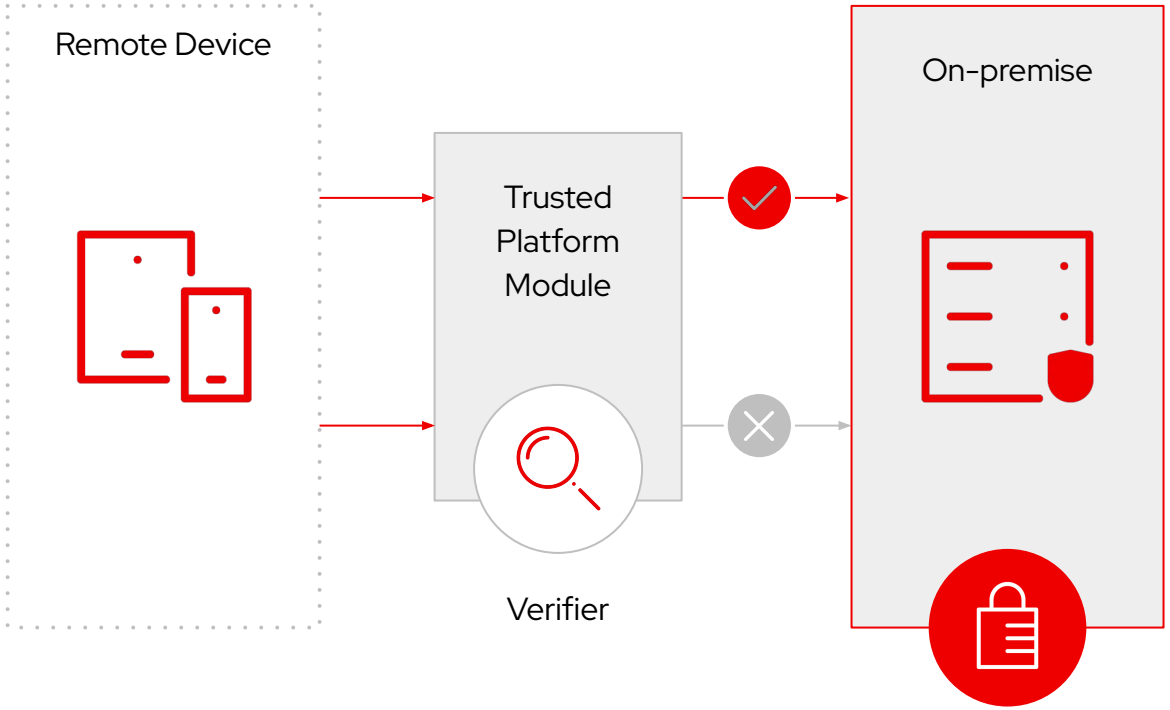
Applies to all applications and all built-in cryptography.

- 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

Red Hat

Remote attestation and measured boot (keylime)

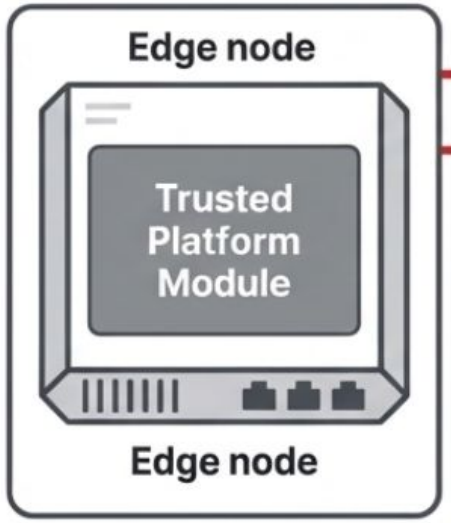


- During secure boot, kernel, loadable modules and boot environment are cryptographically measured
- Measure also runtime binaries before execution
- Measurement compute using tamper-resistant hardware Trusted Platform Module (TPM)
- Attestation agent collects measurements and sends to attestation verifier
- 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

Red Hat

Remote Device

On-Premise Control Plane



Tamper-resistant hardware provides the root of trust.

1. Measure: During secure boot, the kernel, loadable modules, and runtime binaries are cryptographically measured.

2. Collect & Send: The remote attestation agent collects these measurements using the TPM and transmits them securely.

3. Verify: The on-premise Verifier cross-references incoming data against a strict list of known-good measurements.



4. Remediate: If the system state deviates, the Verifier detects the compromise and triggers automated remediation actions.

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.

Red Hat

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

Post Quantum Cryptography

Post-Quantum Cryptography

Start to prepare now to protect against attacks

and fulfill future regulatory requirements

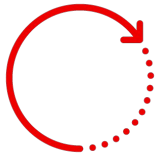


- RHEL 10 is the **first Linux distribution to be post-quantum capable** with new quantum-resistant algorithms (and more to come) so you can prepare now, for future compliance mandates
  - OpenSSL
  - ML-KEM (FIPS 203)
  - ML-DSA (FIPS 204)

Link to blog on PQC

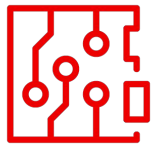
Post Quantum Cryptography (PQC) simplified

POST



After...

QUANTUM



Refers to quantum computers which will be able to crack[1] today's security algorithms

CRYPTOGRAPHY



Refers to the process of protecting content and communications, keeping material authentic for intended users

***Therefore**, PQC simply refers to the ability to protect information after quantum computers become available.*

Cryptography

One-way hash algorithms

Digest algorithms that are used for fingerprinting and compressing data into a short ID.



Symmetric key cryptography

Ciphers that use a secret key to both encrypt and decrypt data.



Asymmetric key cryptography

Pair of keys is used: one private key and one public key



Cryptography at risk

Safe

(with large enough keys)

One-way hash algorithms

Digest algorithms that are used for fingerprinting and compressing data into a short ID.



Safe

(with large enough keys)

Symmetric key cryptography

Ciphers that use a secret key to both encrypt and decrypt data.



At risk

Asymmetric key cryptography

Pair of keys is used: one secret key and one public key



It’s like Y2K, except… we don’t know the exact date

Clock is ticking

Gartner: By 2029, advances in quantum computing will make classic asymmetric cryptography unsafe and breakable by 2034.[1]



Risk is real

Time to break RSA-2048 prime number factor encryption:

2020s computer: 300T years

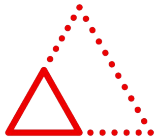
Quantum computer: 10 sec.[2]



Demand is growing

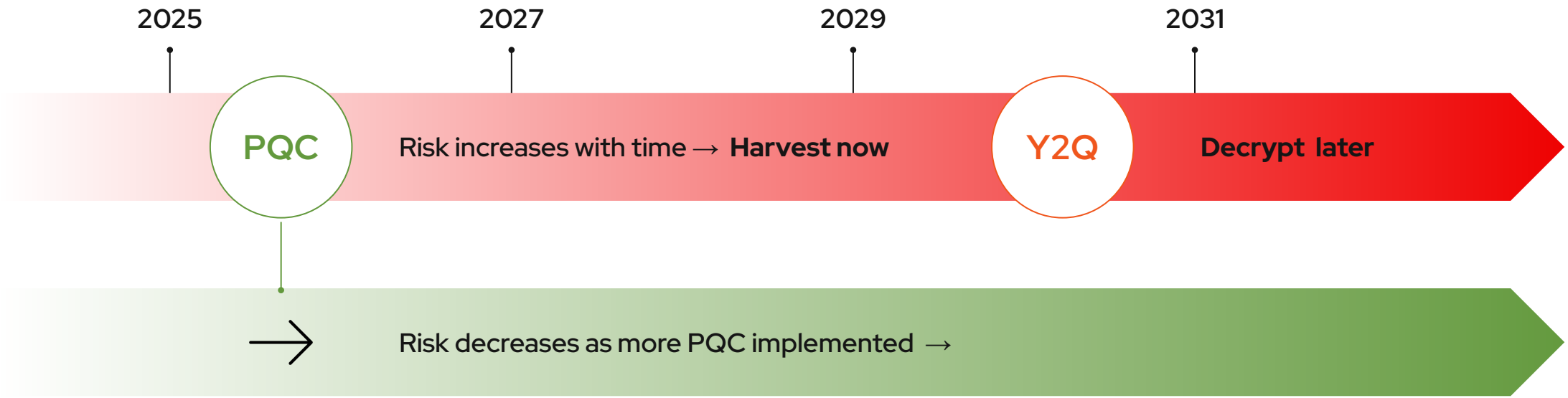
The PQC market is estimated to grow from:

- 2024, 302.5 million USD
- 2029, 1.88 billion USD



1: https://www.gartner.com/en/articles/post-quantum-cryptography
2: https://www.forbes.com/councils/forbesbusinesscouncil/2025/01/14/how-businesses-can-prepare-for-quantum-threats-with-post-quantum-cryptography/

The threat is already here



Organizations adopting PQC today are protecting their data now **and in the future**

Red Hat

Red Hat Implementation Strategy



Classical

Red Hat products and services use classical cryptography algorithms

PQ-Capable

Red Hat products or services include classical cryptography by default

PQC functions are configurable

Classical and PQC available and both are supported (as available)

RHEL 10 includes the first installment of QRAs:

- ML-KEM [FIPS 203]
- ML-DSA [FIPS 204]

PQ-Ready

Red Hat products or services include PQC functions by default

Classical cryptography is configurable

Deprecation and Removal

Classical cryptography algorithms are marked as deprecated

Classical cryptography algorithms are removed

https://www.redhat.com/en/blog/red-hats-path-post-quantum-cryptography

Wrap up

- Quantum computers can potentially break cryptography, this is a current problem.
- Red Hat is integrating NIST-approved PQC algorithms into its core products and and modernizing its own operations
- The transition is complex, we need to start now

Confidential Computing

"Confidential Computing is the protection of **data in use** by performing computation in a hardware-based, attested Trusted Execution Environment."



Source: https://confidentialcomputing.io/about/

What is Confidential Computing ?

Processing Without Peeking

In Motion

- Encrypt data that is flowing between untrusted public or private networks
- TLS, IPSec, VPNs, etc



At Rest

- Encrypt inactive data when stored in blob storage, database, etc.
- LUKS, Data encryption, etc



In Use

- **Protect data during computation - in memory or CPU**
- Prevents memory-based, side-channel attacks



Security benefits to confidential computing

Protection of data in use



Reduce Attack Surface

- Even if an attacker gains access to the OS, hypervisor, or cloud infrastructure, they cannot read or alter data inside a secure enclave.
- Protects against malicious insiders, compromised administrators, and privileged attacks.



Mitigate Cloud Security Risks

- Enables secure computing on untrusted environments, including public clouds.
- Prevents cloud providers or third parties from accessing sensitive workloads running in hyperscalers



Enhance Compliance & Data Privacy

- Helps meet regulatory compliance by ensuring data remains encrypted even when processed.
- Supports sovereign cloud solutions, allowing countries to enforce strict data privacy regulations.

Confidential Computing



Encrypted workloads /
trusted environment execution

\+



Remote attestation

=



Confidential computing

Red Hat

Confidential Computing Footprints

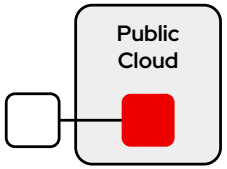
- **RHEL Confidential VM (guest)** - RHEL as a confidential guest on public cloud/hypervisor.
- **Host for Confidential VMs** - OpenShift Virtualization with Confidential Computing enabled, i.e. its VMs can be Confidential VMs
- **Confidential Containers** - OpenShift sandboxed containers where the Kata pod is a confidential VM (an implementation detail hidden from the end user, who would choose the Confidential Containers runtime of OSC)
- **Confidential Clusters** - an OpenShift Cluster of which the nodes are Confidential VMs, e.g. OpenShift cluster installed on Azure CVM nodes

Categorization of use cases



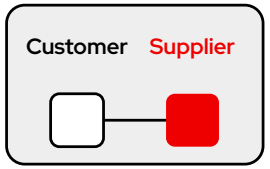
Partner Interaction

2 protected datasets interacting in confidential container in the same cluster



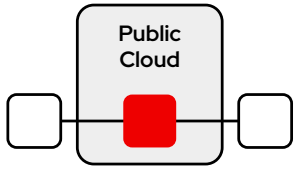
Secure Cloudburst

Using the public cloud to for peak workload or shared resources



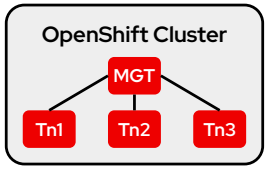
IP Protection/Integrity

Protection of supplier data and business logic in customer environments



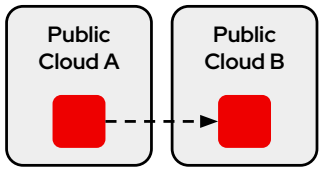
Edge Use Case

Protecting Edge device data in the public cloud for aggregation



Single Tenant Isolation

Isolating OpenShift Clusters



Digital Sovereignty

Encapsulating and moving workload from one provider to the next

Key takeaways

- Confidential Computing helps to enable a zero trust architecture
- Red Had Confidential Computing solutions add another layer of protection to Red Hat's existing defense in depth capabilities
- Confidential Computing with attestation expands the options for using public cloud with confidence
- Confidential Computing is particularly important for protecting proprietary data in AI-enabled applications

Red Hat

Red Hat Enterprise Linux provides a secure foundation

For traditional and cloud-native platforms

Securable by Design Operating System

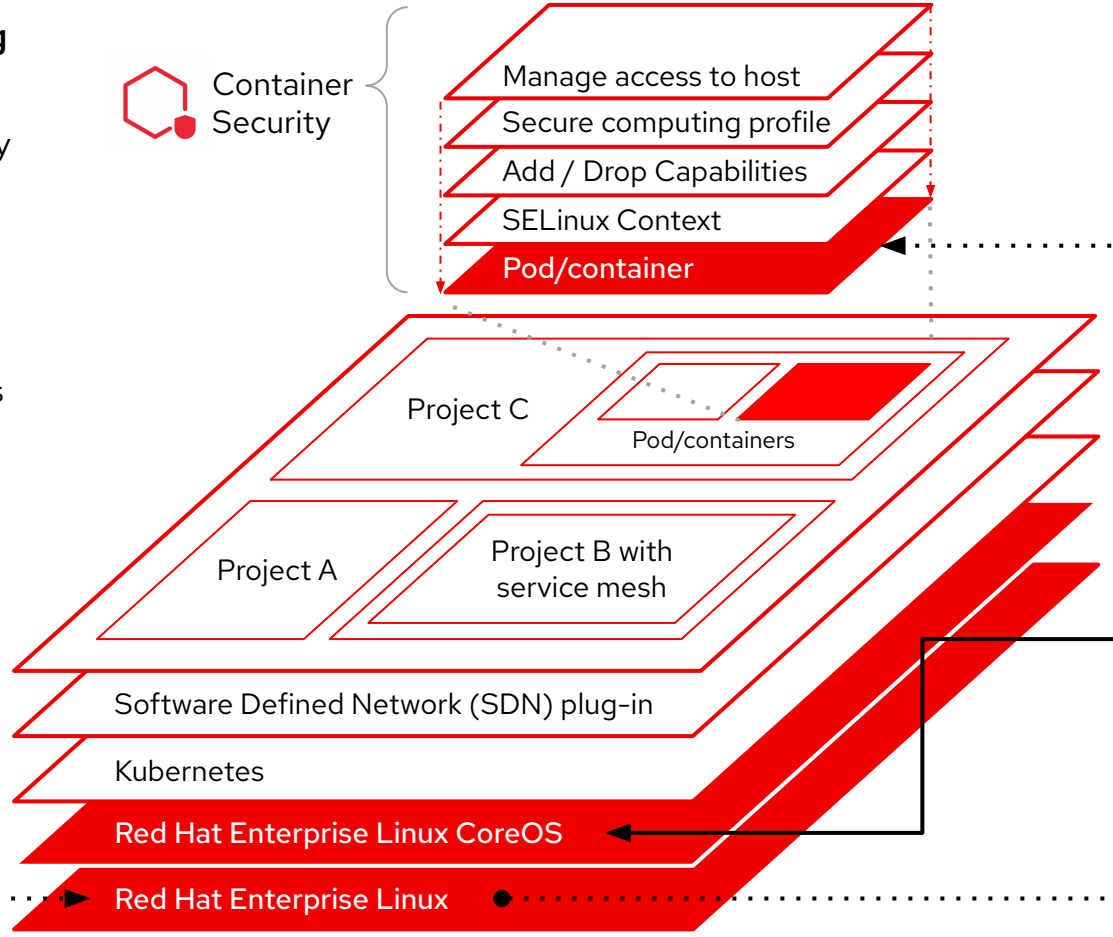
Secure boot enhanced with integrity measurement and remote attestation

Mandatory access control and multi-level security with SELinux

System-wide cryptographic policies and FIPS validated cryptographic libraries

Encrypting data at rest and in motion

Automated security and compliance configuration



Red Hat Universal Base Image containers can leverage RHEL trusted and maintained content

Hardened/Optimized Operating System

Reduced attack surface

Controlled immutability

Read-only user space

Transactional Updates

Secure Boot

Network Bound Disk Encryption

Red Hat

Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.


linkedin.com/company/red-hat


youtube.com/user/RedHatVideos


facebook.com/redhatinc


twitter.com/RedHat

Red Hat