Red Hat Summit

Connect

Top security features

you should be using in RHEL 10

Sam Wachira

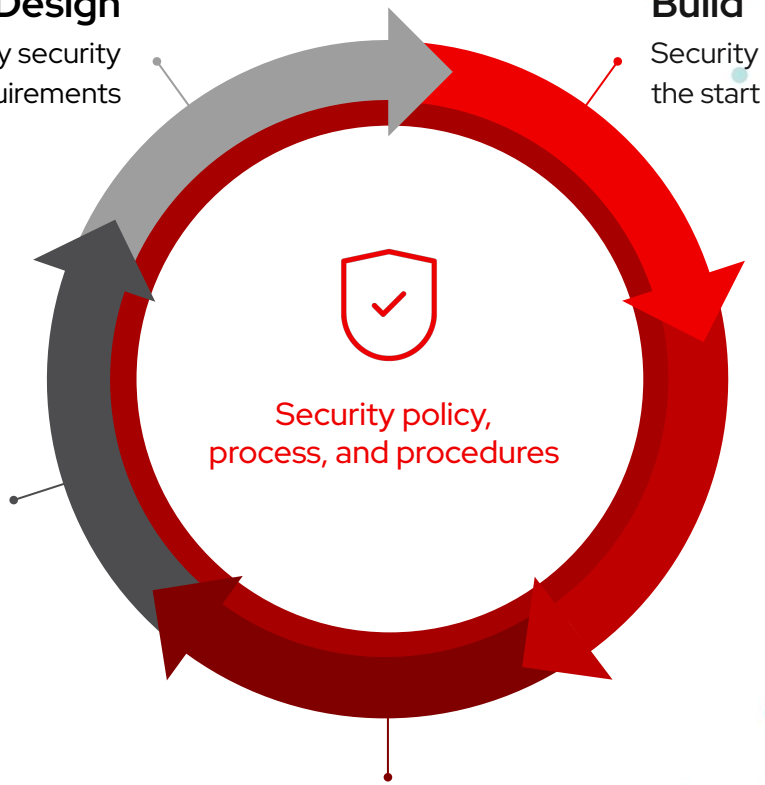
Principal Technical Account Manager

samthetam@redhat.com

Red Hat Enterprise Linux

Security and compliance built in, from the start

National Cyber Security Centre · NIST National Institute of Standards and Technology U.S. Department of Commerce · PCI Security Standards Council · FedRAMP · CIS Center for Internet Security · HIPAA



Standardizing and innovating with containers

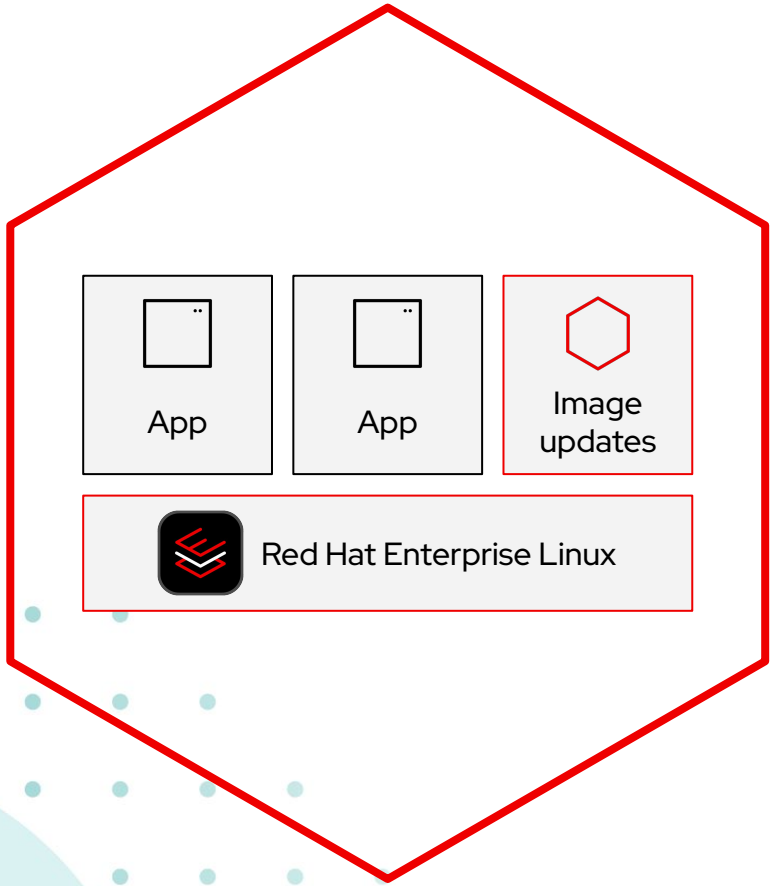
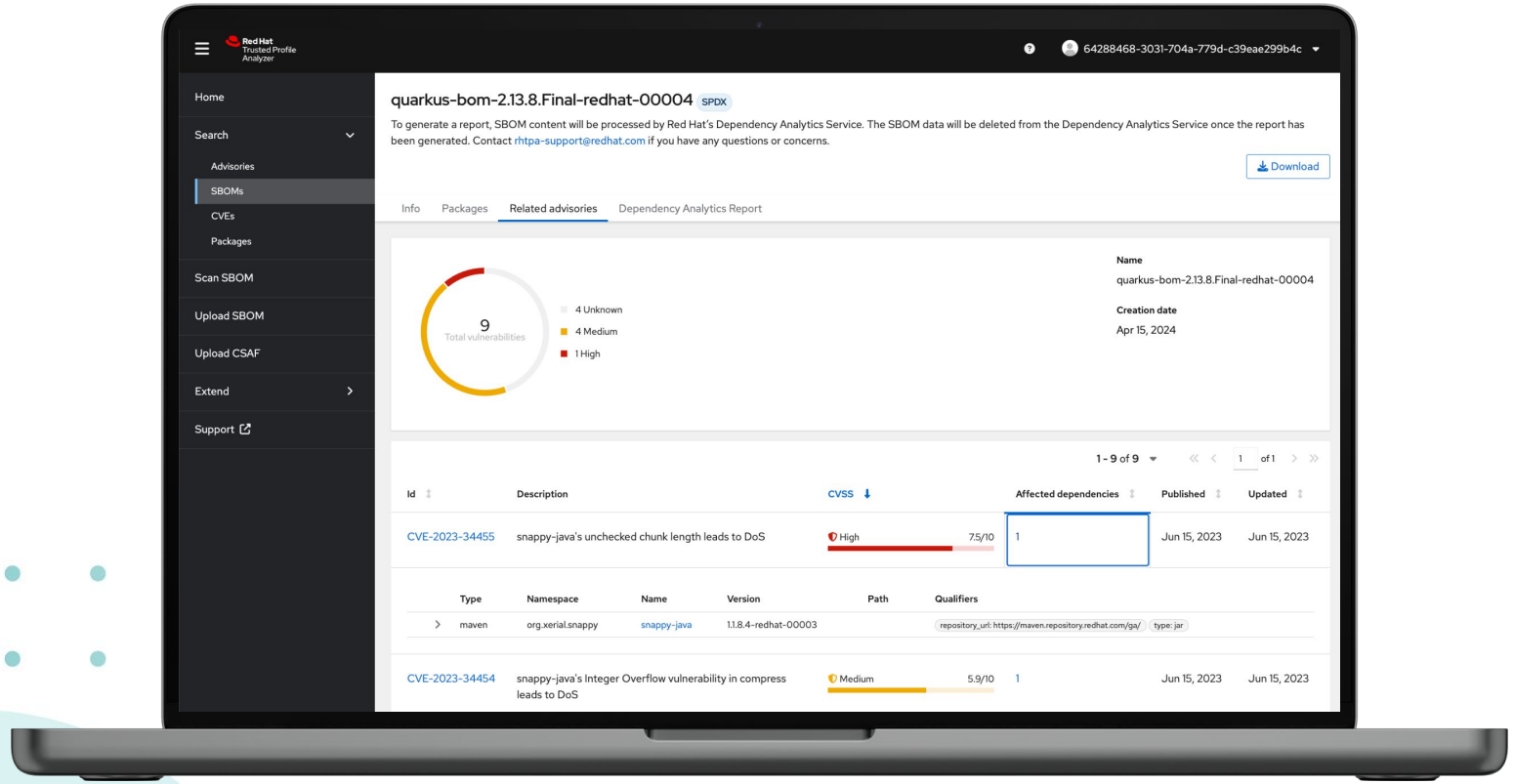


Image mode for Red Hat Enterprise Linux is a simple, consistent approach to build, deploy and manage the operating system using container technologies.

Now you can manage the operating system with the same tools and workflows as applications, promoting a common experience and language across teams.

Hybrid Cloud Console

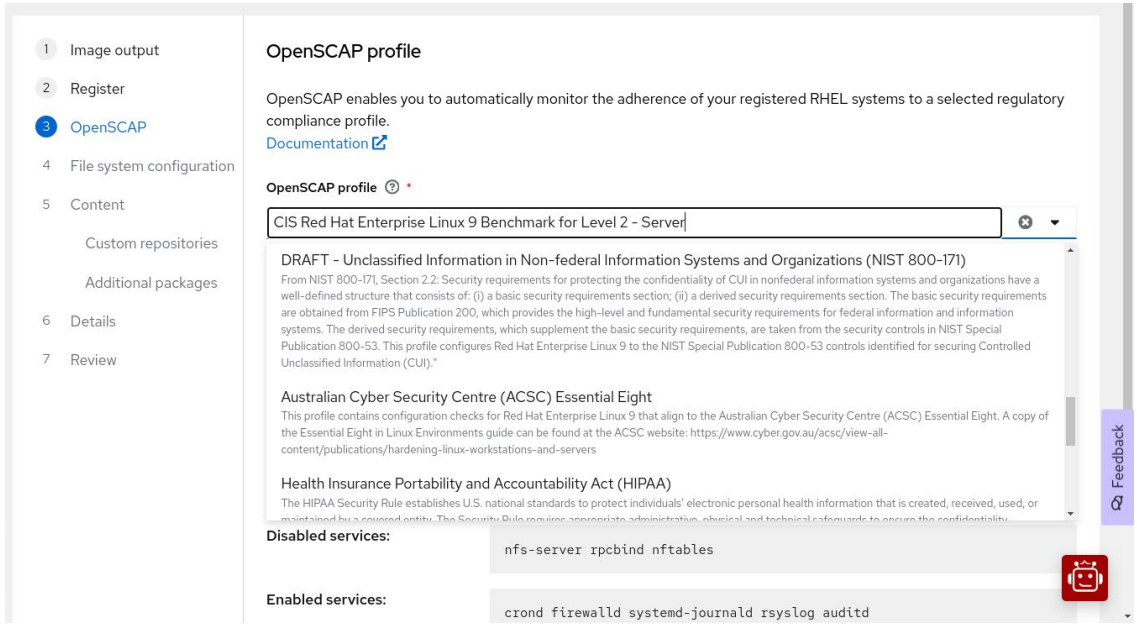
Analysis of software for vulnerabilities, on demand, at code-time, or over lifetime



- Build compliant RHEL images, detect malware, Trusted Profile Analyzer and more...
- Centralized management of SBOMs, VEX, and CVE data.
- Identify, analyze dependencies to map, evaluate impact
- Curate content that's verified, trusted to prevent malicious code
- Act on recommendations directly from the IDE, as code is written

Shift Left Security

Enhance the security architecture, promote immutability, and reduce the attack surface



Pre-hardened images

Deploy images already configured against known security compliance standards

Domain join

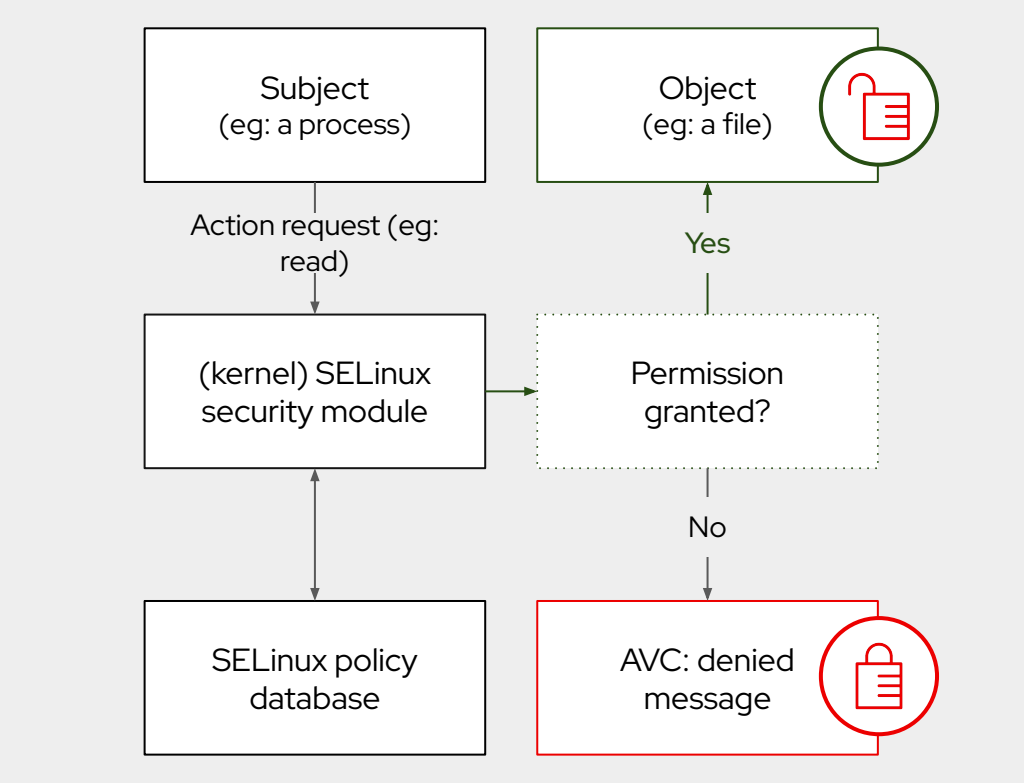
Auto-enroll newly created machines into an existing identity and access management (IAM) system

Guardrails at build time

Helps users to remain secure and compliant

SELinux

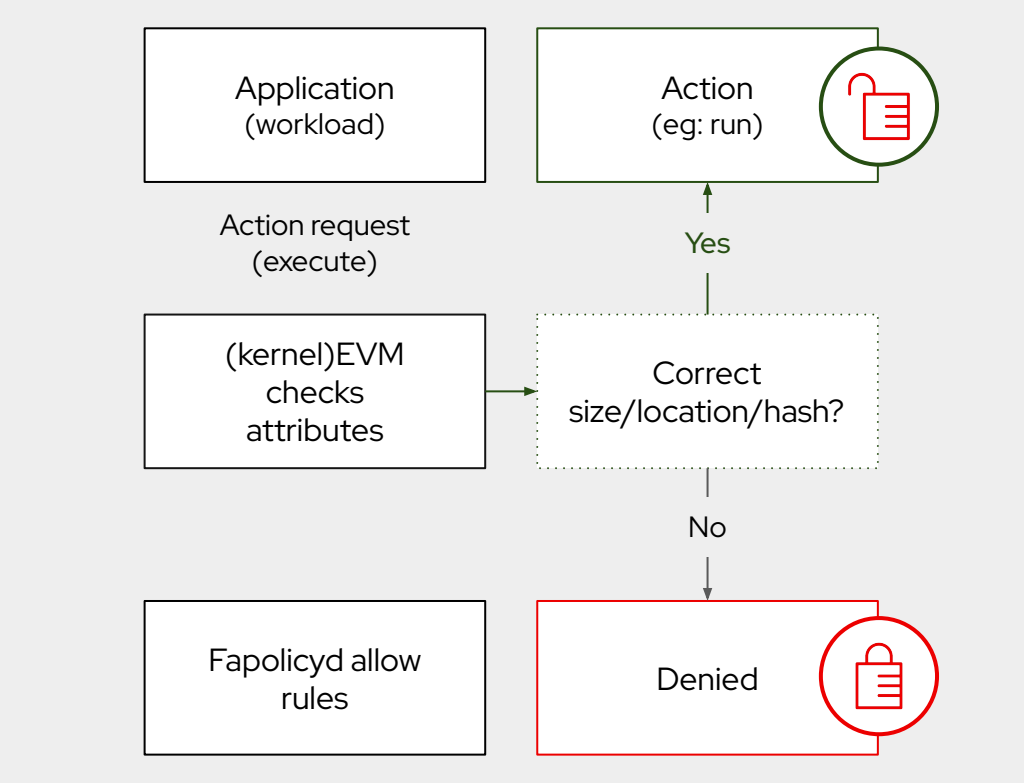
Security architecture providing more controls



- Process isolation to mitigate attacks via privilege escalations. All is Denied by default
- CVEs are often mitigated from Critical and Important to Moderate or Low when SELinux is in enforcing mode!
- Start with Permissive Mode and see what policy needs to be created or changed
- Target problematic applications to use permissive mode, while rest of OS is enforcing, to prevent opening up wider attack surface

fapolicyd

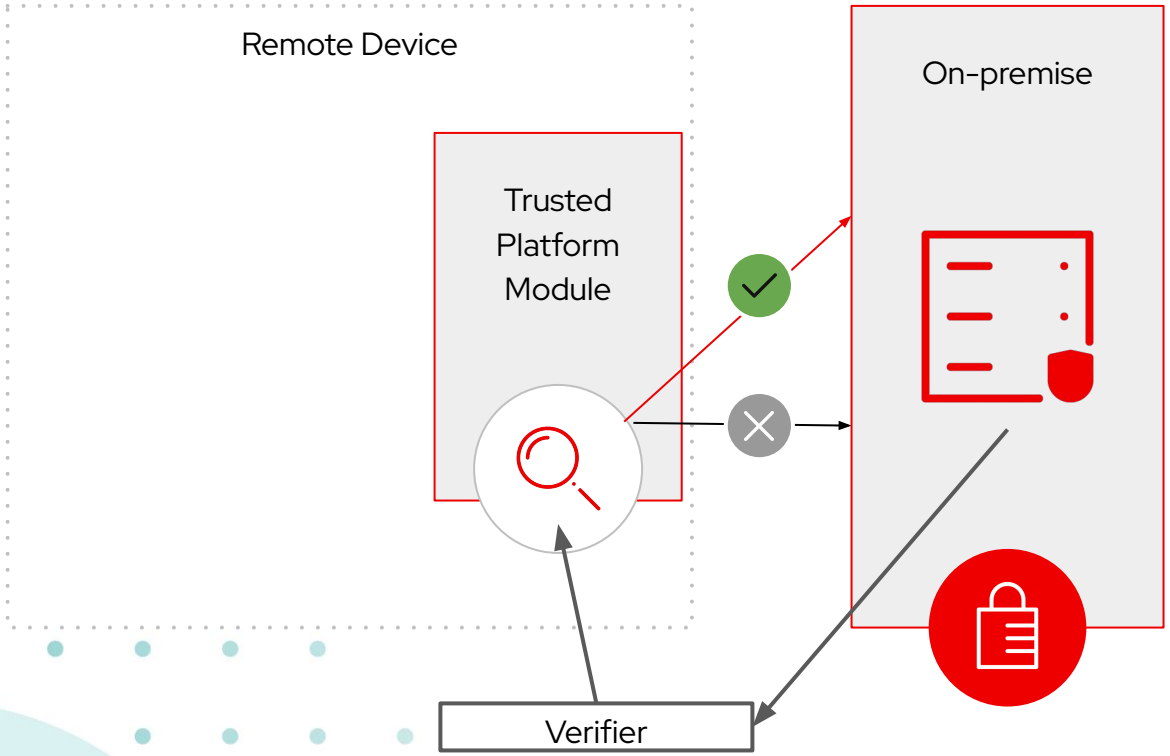
Adds layered access controls for application and integrity security



- 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)
- Control execution based on file path, hash, or integrity
- Allows open/exec for binaries
- Place more control in the hands of admins

Keylime: Remote Attestation

Verify integrity of system in an untrusted environment via a trusted source

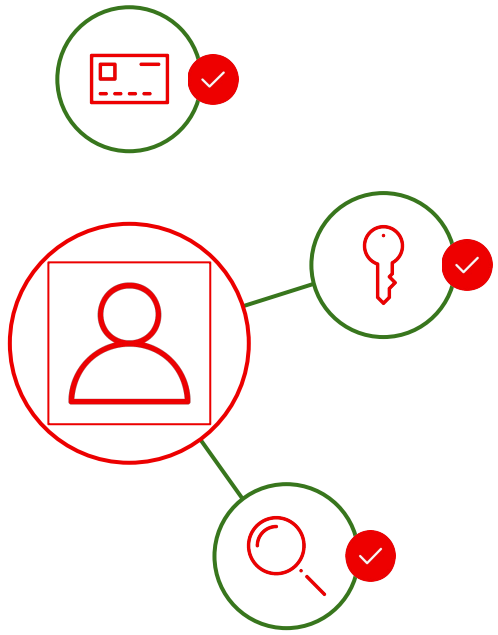


- Kernel, loadable modules and boot environment are cryptographically measured
- Trusted Platform Module (TPM) verifies integrity and authenticity of a system's boot process and running state
- Runtime binaries measured before execution
- Attestation agent collects measurements
- Verifier reviews measurements to detect if system was compromised
- Remediation plans can be executed (and can be customized)

Identity Management

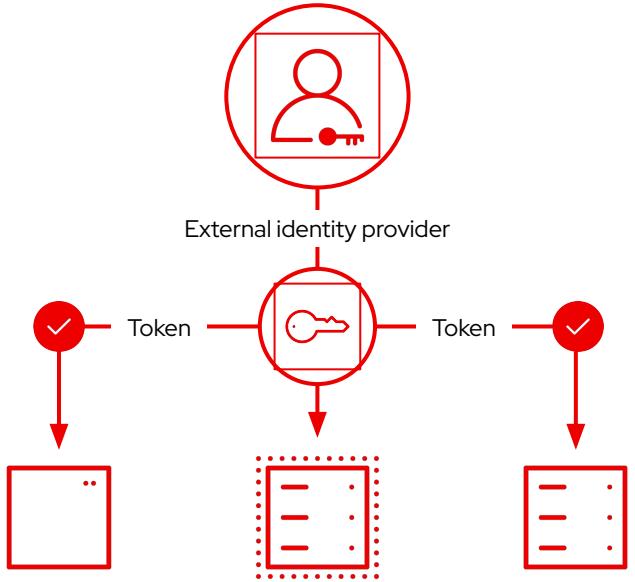
Included as part of Red Hat Enterprise Linux

Use Multifactor Authentication as an extra layer of security



Configure password, radius, password OTP, PKINIT, OAuth 2, hardened password, or Passkey support using FIDO2 protocol

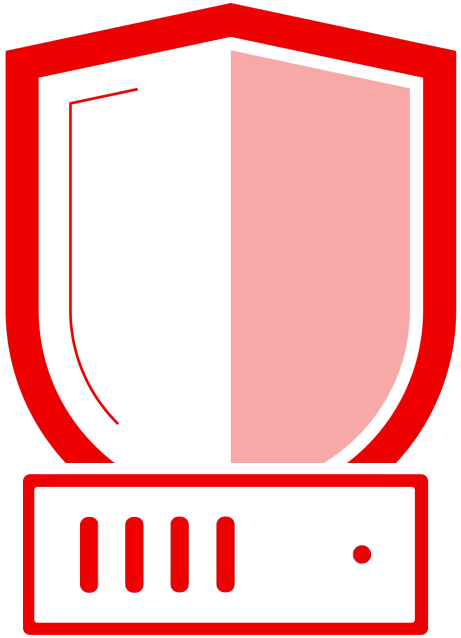
Authentication using external identity providers



Can be integrated with Red Hat Build of Keycloak (RHBK), Entra ID (Azure AD), Github, and others

Encrypted DNS (Tech Preview)

When all traffic must be authenticated, authorized and encrypted



- Encrypted DNS Support to fulfill Zero Trust Mandate from US OMB M-22-09
- RHEL will be able to create and send requests to DNS Servers using encryption over TLS and HTTP protocols
- Identity Management in RHEL has the ability to act as an eDNS server

Crypto Policies

Built-in Policies, Data Protection using LUKS, Confidential Computing

```
[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, and load policies

DH and RSA key lengths are decreased to 2048 bits by default.

Applies to all applications and all built-in cryptography.

- Red Hat certifies and validates cryptography within RHEL to provide a secure baseline for our users
- 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 environments
- Easily customize to meet your site-specific policy requirements

Post quantum cryptography

- Data we encrypt today might not be secure in five years
- Red Hat Enterprise Linux 10 is the first enterprise Linux distribution to be post-quantum capable with new quantum-resistant algorithms (more to come) so you can prepare now for future compliance mandates
- ML-KEM (FIPS 203) and ML-DSA (FIPS 204) algorithms

Source:
https://newsroom.ibm.com/download/quantum-computers-and-accelerated-discovery_40645906341_o.jpg
https://quantum.ibm.com/services/resources?limit=50&view=table
https://security.stackexchange.com/q/87345
https://crypto.stackexchange.com/q/436

PQC will be part of compliance mandates

Currently no one global cryptographic authority exists. Most countries and compliance bodies are waiting on the National Institute of Standards and Technology (NIST - creators of the Cyber Security Framework) to publish final standards. In the meantime, here is their current guidance:

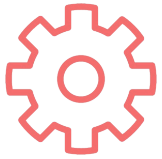
- NIST - encouraging transitioning asap
- ANSSI - encouraging transitioning
- ETSI - now require trust service providers to begin migration
- CNSA[4] - multiple dates for specific cryptographic capabilities, 2025- 2033
- PCI-DSS 4.0 - will be mandatory for some organizations on March 31, 2025
- ENISA - encouraging organizations to start transitioning
- CSA - encouraging now and expected to release firm guidelines in 2025

4: These are the timelines that Red Hat is working towards as it is the most comprehensive, particularly consider delays in implementation

Red Hat's transition phases

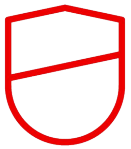
We anticipate having to support a long, hybrid transition period

RHEL 10, 9.7



Classical

Traditional Cryptography; no quantum resistant algorithms (QRAs) available



PQ-Capable

Includes available QRAs and PQC functions. Not available for all applications. Still classical by default with configurable use of available QRAs

PQ-Ready

QRAs and PQC functions by default where available, configurable classical where needed.

Deprecation & Removal

Classical Algorithms and functions will be marked as deprecated with eventual removal. Capabilities and solutions to be resistant to downgrade attacks.

Summary

1. Image Mode
2. SBOMs
3. Shift Left Security
4. SELinux
5. fapolicyd
6. Keylime: Remote Attestation
7. Identity Management
8. Encrypted DNS (Tech Preview)
9. Crypto Policies
10. Post-Quantum Cryptography

Red Hat Summit

Connect

Thank you


linkedin.com/company/red-hat


facebook.com/redhatinc


youtube.com/user/RedHatVideos


twitter.com/RedHat