



Connect

Are you drowning in CVEs?

Use AI to look after your RHEL estate and stay compliant





Alessandro Rossi

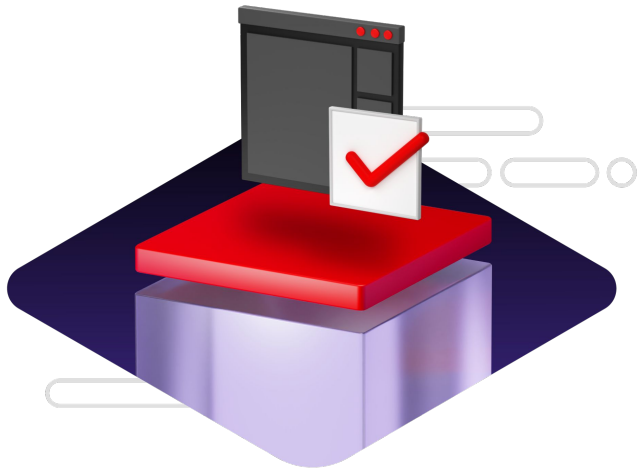
RHEL Advocate
Red Hat



Juan van der Breggen

RHEL Advocate
Red Hat





The Challenges

Discovery is exponential. Remediation is linear.



-7 days

Days to exploitation

Attackers exploit before
most CVEs are patched ¹



\$4.8M

Data breach cost

Cost of a data breach
in 2025 ²



\$60B

Attack cost in 2025

Projected \$138 billion
by 2031 ³

Your attack surface is expanding overnight

AI discovery pours gasoline on the fire with increased volume of CVEs

AI models like Anthropic's Mythos are uncovering vulnerabilities at a scale humans can't match

2,000+

In just 7 weeks, Mythos found over 2,000 unknown zero-days, and many thousands more since. The discovery bottleneck has been obliterated.



Source: [Mythos Unleashed](#) | Lyrie Research

Self-support security is a significant undertaking

When running a self-supported open source Linux distribution, the following falls to you

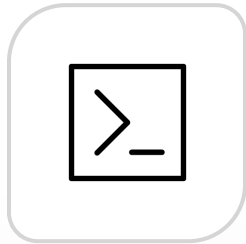
Self-support requires



Triage **100s of new CVEs** per day



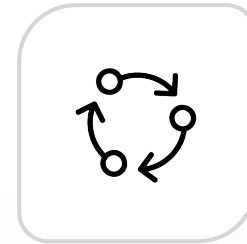
Hunt online for **upstream patches**



Backport the fix for their version



Quality assurance and testing



Deploy and watch for any issues



In case of fire, **ask the community**



How Red Hat helps with the CVE flood

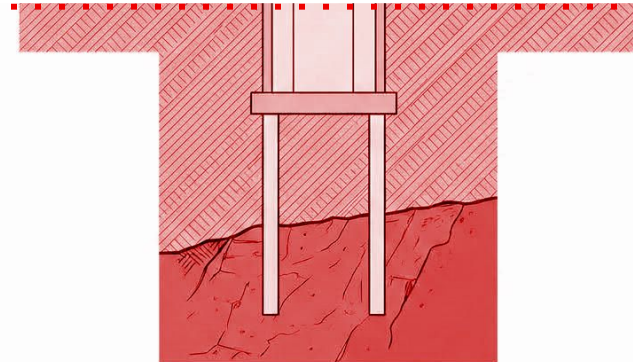
A hardened platform for applications to **run on**

FOUNDATION LAYER



Red Hat
Enterprise Linux

Red Hat Product Security helps secure the platform
applications **run on.**



FOUNDATION



How Red Hat helps with the CVE flood

Help to secure open source libraries applications are **built with**

APPLICATION LAYER



For customer Apps built on maven / PyPI / npm

Helps secure the open source libraries and dependencies that applications are **built with**.

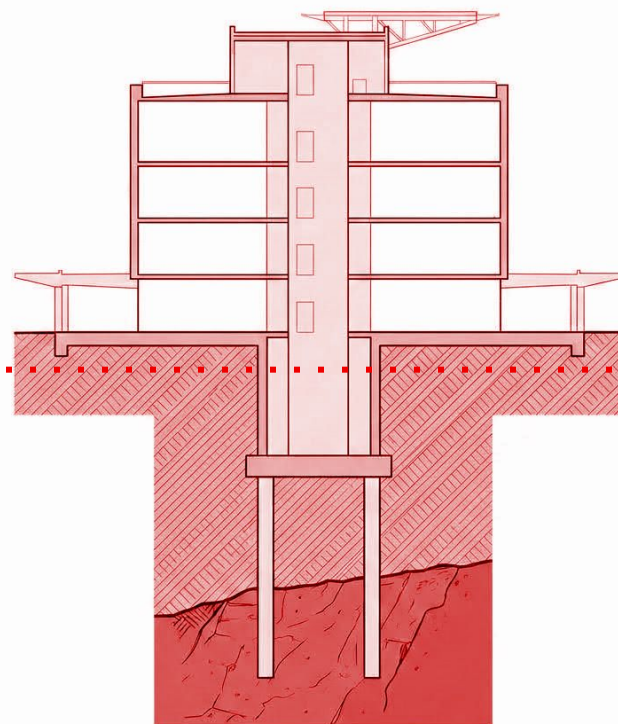


FOUNDATION LAYER



Red Hat Product Security helps secure the platform applications **run on**.

APPLICATIONS

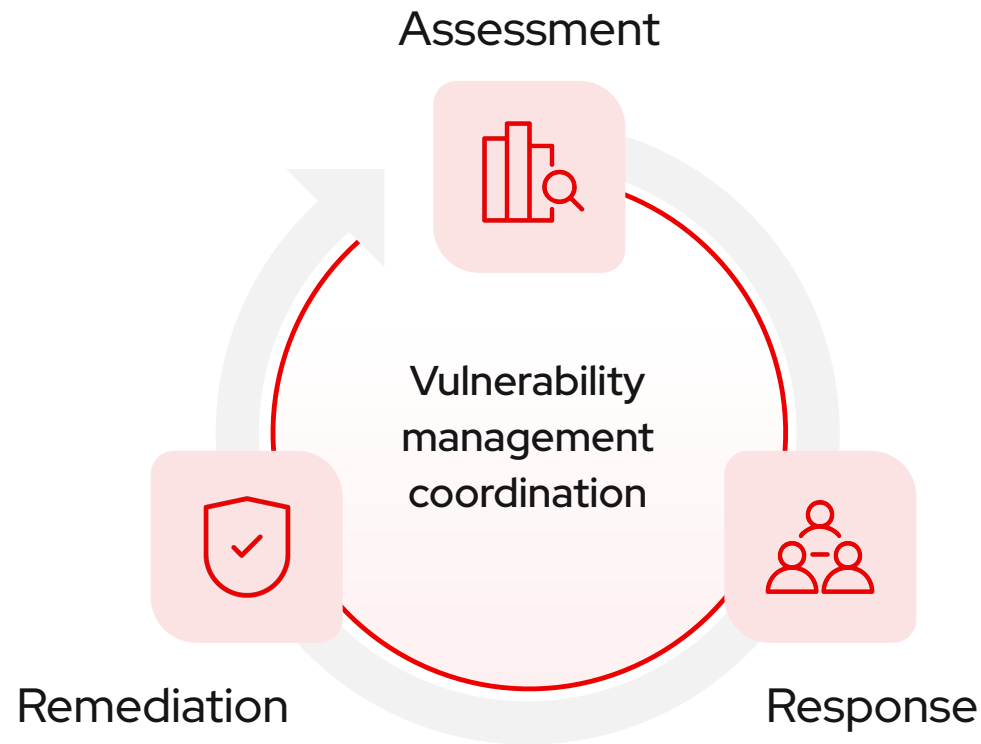


FOUNDATION



Red Hat security response at AI scale

Same trusted process, rebuilt for speed and volume



Find earlier

- ▶ AI-augmented scanning in CI/CD helps catch issues earlier in production
- ▶ Over 455M lines of code scanned (Spring 2026)



Triage smarter

- ▶ Expert validation cuts through AI noise
- ▶ ~9% signal-to-noise on high-impact findings



Fix and release faster

- ▶ Tested, signed advisories at scale
- ▶ 2,671 RHEL advisories, only 0.4% were critical (2025)¹



With a Red hat subscription, we take care of these

Offload a massive, non-core technical burden to Red Hat's team of security experts



Red Hat
Enterprise Linux



Monitor for new
vulnerabilities



Perform risk
assessment



Compliance,
standards and testing



Remediation and
automation



Red Hat Support
in case of fire



Proactive remediation, at any scale

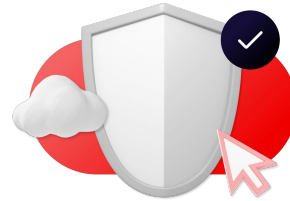


See it

Identifies vulnerabilities in your actual environment, contextualized to your workloads.



Red Hat
Lightspeed



Stage it

Loads the patch in content views and promotes it through "dev-test-prod" lifecycle gates.



Red Hat
Satellite



Ship it

Applies remediation fleet-wide with a full, policy-driven audit trail.



Red Hat
Ansible Automation
Platform



Red Hat
Enterprise Linux

Start on a hardened foundation with built-in security capabilities



Start on a hardened foundation

Minimize risk, maximize uptime, and simplify compliance



Continuous compliance
and minimized CVEs



Zero-trust
architecture



Platform integrity
and hardening

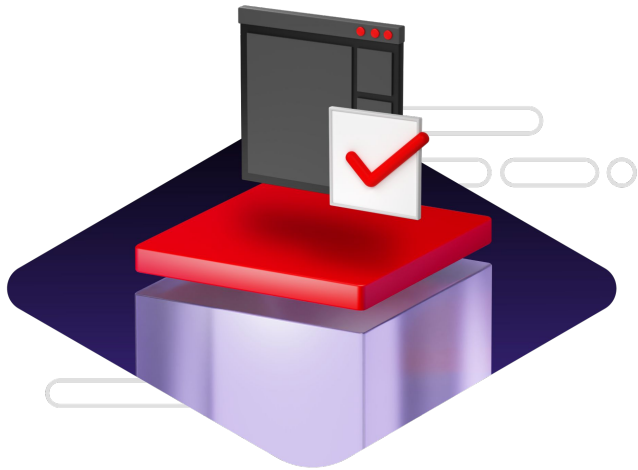


Trusted software
supply chain



Red Hat
Enterprise Linux

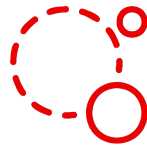




MCP server for RHEL (Developer Preview)

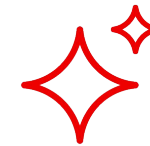
What is MCP?

Model Context Protocol



Open standard

Introduced by Anthropic in November 2024, and later donated to the Agentic AI Foundation



Unlocks new LLM use cases

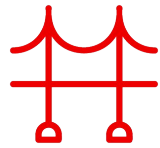
MCP enables LLMs to interact with outside tools and data sources

For more info, see:

<https://modelcontextprotocol.io/docs/getting-started/intro>

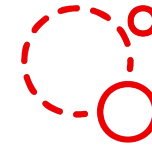
We need MCP to bridge the “context” gap

Without MCP, LLMs are powerful, but disconnected from your infrastructure



Bridge between LLM and RHEL infrastructure

Enables LLM to have real-time access to your RHEL system’s actual state (logs, CPU usage, disk space, etc.)



Standardized interoperability

Because MCP is an open standard, it can plug-and-play with a variety of AI clients and tools

Example of life without MCP

Without MCP, the LLM is unable to interact with outside tools and data sources

```
brian@rhel10:~$ c "How much memory is on this system?"  
~.+ Asking RHEL Lightspeed...
```

To check the amount of memory on your Red Hat Enterprise Linux system, you can use the `free` command with the `-h` option for human-readable output.

```
— bash snippet  
free -h
```

This command will display information about total, used, and free physical and swap memory in a user-friendly format.

Always review AI-generated content prior to use.



Example of life with MCP

With MCP, the LLM can use an MCP server to get real-time memory information from the system

```
Context: ○○○○○○○○ 0% (0/128000 tokens)
( 0)> How much memory is on this system?

— get_memory_information | mcp-server-for-rhel —————

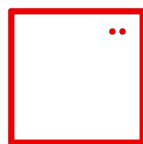
◇ Goose would like to call the above tool, do you allow?
| Allow
|
The system has 8GB of RAM, with 5.49GB available. There is also 2GB of swap space, all of which is free.

⌚ Elapsed time: 16.02s
Always review AI-generated content prior to use.
```



Prerequisites to get started

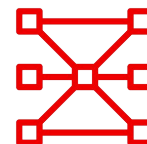
MCP server for RHEL (Developer Preview) is included as part of the value of a RHEL subscription



MCP client

This is the application where you interact with the LLM model.

Use goose-redhat or goose from the RHEL Extensions repository, or use the client of your choice which supports the MCP standard.



LLM

Use goose-redhat from the RHEL Extensions repository that connects to the Red Hat hosted command line assistant backend infrastructure, or use the LLM of your choice, which can be a hosted model, or a local open source model.

Managing RHEL with MCP



Red Hat Lightspeed

[Available as a Developer Preview](#)

Initial use cases:

- Image builder
- Inventory
- Advisor
- Vulnerabilities



Satellite

Launched as a Technology Preview
in Satellite 6.18

[Documentation](#)

Initial use case:

- Reporting, for example, determine lists of hosts that need to be patched
- Patching hosts
- Promote content views



RHEL

[Available as a Developer Preview](#)

Initial use cases include:

- Log analysis
- Performance monitoring
- Troubleshooting



Tools provided by MCP server for RHEL

Pre-vetted read-only tools



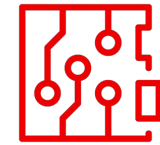
System information

- OS / Kernel
- CPU load
- Memory / RAM
- Disk space
- Hardware



Troubleshooting

- List running processes
- Process details
- List services
- Service status
- System logs
- Service logs
- Specific log file



Network, file, and storage

- Network interface info
- Open ports
- Network connections
- Disk partitions
- List directory info
- List files

For more info, see upstream documentation

<https://rhel-lightspeed.github.io/linux-mcp-server/>

Example use case: checking health of systems

I have 5 systems named rhel10-server[123].example.com and rhel9-server[12].example.com. Check the health of these systems and generate 2 tables of info: 1 table should have an overview of the systems, and the other table should have a list of high priority potential issues on the systems that should be further investigated.

I'll check the health of all 5 RHEL systems by gathering comprehensive system information. Let me start by collecting data from each system.

— Get System Information host: rhel10-server1.example.com >

— Get System Information host: rhel10-server2.example.com >

— Get System Information host: rhel10-server3.example.com >

— Get System Information host: rhel9-server1.example.com >

— Get System Information host: rhel9-server2.example.com >

— Get Cpu Information host: rhel10-server1.example.com >

— Get Cpu Information host: rhel10-server2.example.com >

— Get Cpu Information host: rhel10-server3.example.com >



Example use case: checking health of systems

Table 1: System Overview

System	OS	Kernel	Uptime	CPU Cores	RAM (Total/Used/Available)	Root Disk (Total/Used/Use%)	Network IP	Services Running	Failed Services
rhel10-server1	RHEL 10.1 (Coughlan)	6.12.0-124.28.1.el10_1	9h 6m	1 phys / 8 threads	7.5GB / 1GB (13.2%) / 6.5GB	17GB / 17GB / 96%	192.168.122.34	35	mcelog
rhel10-server2	RHEL 10.1 (Coughlan)	6.12.0-124.28.1.el10_1	1h 33m	1 phys / 1 thread	15.4GB / 989MB (6.3%) / 14.4GB	35GB / 5.1GB / 15%	192.168.122.21	35	mcelog
rhel10-server3	RHEL 10.1 (Coughlan)	6.12.0-124.28.1.el10_1	9h 6m	1 phys / 2 threads	3.6GB / 851MB (23.3%) / 2.7GB	26GB / 4.7GB / 18%	192.168.122.219	35	httpd, mcelog
rhel9-server1	RHEL 9.7 (Plow)	5.14.0-611.24.1.el9_7	6h 50m	1 phys / 10 threads	3.6GB / 748MB (20.5%) / 2.8GB	22GB / 5.2GB / 24%	192.168.122.144	33	mcelog
rhel9-server2	RHEL 9.7 (Plow)	5.14.0-611.24.1.el9_7	6h 50m	1 phys / 2 threads	7.5GB / 812MB (10.6%) / 6.7GB	26GB / 5.5GB / 21%	192.168.122.84	34	mcelog

Table 2: High Priority Potential Issues

Priority	System	Issue	Severity	Description
CRITICAL	rhel10-server1	Root filesystem 96% full	Critical	Only 792MB available on 17GB root filesystem. Immediate action required.
CRITICAL	rhel10-server3	Apache HTTP service failed	Critical	httpd.service is in 'failed' state. May need to restart or diagnose.
HIGH	rhel10-server2	Extremely high CPU usage	High	91.7% user CPU, 8.3% system, 0% idle. System appears overloaded.
HIGH	rhel10-server2	MariaDB environment warnings	High	Unset environment variables: MYSQLD_OPTS, _WSREP_NEW_CLUSTER.
MEDIUM	rhel10-server1	Network packet drops	Medium	16,390 RX packets dropped. May indicate network congestion or interface issues.

Next, we'll look into a few of the potential issues identified here



Example use case: report on the security posture

I need a report to share with my security operations team to assess the current security posture of our installed servers. Can you provide all the relevant information of my install base (security advisories, vulnerabilities, compliance data, and malware) with the available data from the Lightspeed, Satellite, and RHEL tools?

****SECURITY METRICS SUMMARY****

Metric	Status	Count
Total Systems	✔ Managed	76 systems
Critical CVEs	● Active	207 vulnerabilities
Security Errata	● Pending	1 system with outstanding security updates
Compliance Status	⚠ Conflicts	Potential policy conflicts detected
Malware Status	✔ Clean	No malware detected
Known Exploits	✔ None	No active exploit campaigns

****RECOMMENDED REMEDIATION STRATEGY****

- **Emergency Patch Window****: Schedule immediate maintenance for OpenSSL vulnerability
- **Satellite Health Check****: Investigate and resolve error states on 4 hosts
- **Container Security Audit****: Review container runtime configurations across affected systems
- **Upgrade Path Validation****: Begin planning for RHEL 9→10 transitions
- **Continuous Monitoring****: Enhance vulnerability scanning frequency given high CVE density



Example use case: high level overview of CVEs

Give me a count of all CVEs that affect my environment AND list the top 5 most important to fix based on the criticality of the vulnerability.

```
## **CVE Summary for Your Environment**

**Total CVEs Affecting Your Infrastructure: 207 unique vulnerabilities**

### **TOP 5 MOST CRITICAL CVEs TO FIX IMMEDIATELY:**

## **🔴 CRITICAL PRIORITY**

### **1. CVE-2025-15467**
- **CVSS Score:** 9.8 (Critical)
- **Affected Systems:** 71 systems (100% of your environment)
- **Impact:** OpenSSL stack buffer overflow - potential remote code execution
- **Description:** Remote attackers can exploit a stack buffer overflow vulnerability by supplying crafted CMS messages with oversized IV when parsing AuthEnvelopedData structures using AEAD ciphers like AES-GCM
- **Red Hat Advisory:** https://access.redhat.com/security/cve/CVE-2025-15467

### **2. CVE-2026-3497**
- **CVSS Score:** 8.2 (High)
- **Affected Systems:** 69 systems (97% of your environment)
- **Impact:** OpenSSH GSSAPI information disclosure and denial of service
- **Description:** Remote attackers can exploit unexpected GSSAPI message types during key exchange, leading to uninitialized connection variables and undefined behavior
- **Red Hat Advisory:** https://access.redhat.com/security/cve/CVE-2026-3497

### **3. CVE-2025-68121**
- **CVSS Score:** 7.4 (Moderate)
- **Affected Systems:** 71 systems (100% of your environment)
- **Impact:** TLS certificate validation bypass - authentication bypass
- **Description:** Attackers can bypass certificate validation during TLS session resumption when CA settings are mo
```



Example use case: CVE remediation in Satellite

Use ONLY the Satellite MCP AND the RHEL MCP servers to help me create a plan to address important and critical CVEs for rhel-backend host group.

****SECURITY VULNERABILITY MANAGEMENT PLAN****

Based on the Satellite MCP and RHEL MCP server data, I've identified critical security issues requiring immediate attention.

****EXECUTIVE SUMMARY****

Both systems are ****RHEL 10.1**** hosts in ****ERROR status**** with pending security errata. They share identical vulnerability profiles and require urgent remediation.

****CRITICAL SECURITY FINDINGS****

****System Status Summary****

- ****Total Systems:**** 2 hosts
- ****Operating System:**** Red Hat Enterprise Linux 10.1
- ****Kernel Version:**** 6.12.0-124.8.1.el10_1.x86_64
- ****Management Platform:**** Red Hat Satellite
- ****Assessment Date:**** April 9, 2026

****Vulnerability Overview****

Both systems have ****7 pending errata**** requiring attention:

- ****Security Errata:**** 1 critical
- ****Bugfix Errata:**** 6 important
- ****Applicable Packages:**** 24 packages need updates
- ****Upgradable Packages:**** 24 packages ready for update

****PRIORITY 1: IMMEDIATE ACTIONS (Next 24 hours)****

****Critical Security Updates****

Both systems have ****1 critical security errata**** that must be applied immediately:



****SECURITY VULNERABILITY MANAGEMENT PLAN****

Based on the Satellite MCP and RHEL MCP server data, I've identified critical security issues requiring immediate attention.

****EXECUTIVE SUMMARY****

Both systems are ****RHEL 10.1**** hosts in ****ERROR status**** with pending security errata. They share identical vulnerability profiles and require urgent remediation.

****CRITICAL SECURITY FINDINGS****### ****System Status Summary****

- ****Total Systems:**** 2 hosts
- ****Operating System:**** Red Hat Enterprise Linux 10.1
- ****Kernel Version:**** 6.12.0-124.8.1.el10_1.x86_64
- ****Management Platform:**** Red Hat Satellite
- ****Assessment Date:**** April 9, 2026

****Vulnerability Overview****

Both systems have ****7 pending errata**** requiring attention:

- ****Security Errata:**** 1 critical
- ****Bugfix Errata:**** 6 important
- ****Applicable Packages:**** 24 packages need updates
- ****Upgradable Packages:**** 24 packages ready for update

****PRIORITY 1: IMMEDIATE ACTIONS (Next 24 hours)****### ****Critical Security Updates****

Both systems have ****1 critical security errata**** that must be applied immediately:

```bash

# For both rhel-3-5x8jn and rhel-4-5x8jn:  
subscription-manager refresh  
dnf update --security  
```

****PRIORITY 2: PACKAGE SECURITY UPDATES (Next 48 hours)****

Example use case: CIS hardening

Help me figure out how to enable CIS Level 1 Server compliance for the rhel-backend host group.
Specifically I'd like to use Red Hat Satellite to scan for compliance.

```
## **SATELLITE CIS COMPLIANCE IMPLEMENTATION**

### **Phase 1: Upload CIS Level 1 SCAP Content**

**Option A: Download CIS RHEL 10 Level 1 Benchmark**

```bash
Download from Red Hat Customer Portal or CIS website
curl -o "cis-rhel10-level1.xml" "https://www.redhat.com/security/data/oval/com.redhat.rhsa-RHEL10.xml"

Or from CIS website directly
wget "https://workbench.cisecurity.org/files/4323/download" -O cis-rhel10-level1.xml
```

**Option B: Use Satellite's Bulk Upload**

```bash
Upload SCAP content via Satellite API
curl -X POST "https://satellite.[redacted]/api/compliance/scap_content_k_upload" \
 -H "Content-Type: application/json" \
 -d '{
 "type": "files",
 "files": ["/path/to/cis-rhel10-level1.xml"]
 }'
```

### **Phase 2: Create CIS Level 1 Compliance Policy**
```



Example use case: older systems needing attention

Provide a simple summary of the versions of RHEL 9 and older in use and compare to the newest versions, highlighting the number of systems that are approaching end of life. The output should be a simple to read table. Do NOT list hostnames, just a count of systems. Do NOT report on RHEL 10 versions. Use the Lightspeed planning service to get this information.

```
# RHEL Version Summary: 9 and Older
# Fleet Version Distribution
```

| RHEL Version | Systems Count | Status | End of Life Date | Days Remaining |
|---------------------|---------------|---|------------------|--------------------|
| **RHEL 9.7** | **17** |  **CRITICAL** | May 15, 2026 | **36 days** |
| RHEL 9.8+ | 0 | Available | Active | - |
| RHEL 8.x and older | 0 | Retired | Various | Expired |

```
## Systems Approaching End of Life Summary
```

| Risk Category | System Count | Percentage of Fleet |
|--|-----------------------|-------------------------------|
| **CRITICAL - RHEL 9.7 (36 days)** | **17 systems** | **24% of total fleet** |
| **LOW RISK - RHEL 9.8+** | 0 systems | 0% |
| **NO RISK - RHEL 8.x and older** | 0 systems | 0% |

```
## Version Comparison to Newest
```

| Current vs. Newest | Gap | Impact |
|--|-----------------------|---|
| **RHEL 9.7 → 9.8** | 0.1 version | **Migration required immediately** |
| **Total systems needing upgrade** | **17 systems** | **All must migrate before May 15, 2026** |

```
## Key Takeaway
```

- **17 systems**** are approaching end of life in ****36 days****
- **0 systems**** are running outdated RHEL 8 x or older versions



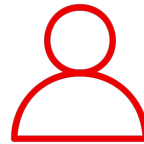
Guarded command execution multi-layered defenses

Defense in depth guardrails designed to help mitigate the risks of dynamic script execution



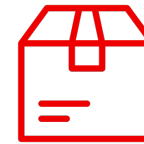
Gatekeeper model

A gatekeeper model helps mitigate risk by evaluating proposed scripts for policy adherence, clarity and safety before they are allowed to execute



Human in the loop

For compatible LLM clients, an MCP Apps approval UI prompts the user to confirm changes that will modify the system



Sandboxing

When possible, uses systemd-run to help limit the permissions of the script when executed



New Agent Skills for RHEL

Bringing Red Hat Knowledge into your AI Tools



Translator skill for RHEL

When AI tools encounter Linux questions, they sometimes respond with answers written for other distributions. The translator skill acts as a bridge, helping AI assistants to recognize those non-RHEL concepts and commands and to seamlessly map them to RHEL-native equivalents.



Best practices skill for RHEL

When troubleshooting complex systems, administrators need solutions that align with RHEL best practices, rather than generic or outdated advice found on public forums. The best practices skill empowers AI tools with Red Hat's recommended frameworks for diagnostics, health monitoring, and proactive maintenance.

Unlock local RHEL management with Red Hat Satellite

Your toolkit for managing RHEL environments locally

The Satellite subscription is essential for comprehensive local management of RHEL environments, and provides the following capabilities:

- ▶ Satellite itself
- ▶ Offline Knowledge Portal
- ▶ Offline RHEL command line assistant (Developer Preview)





Connect

Thank you



linkedin.com/company/red-hat



facebook.com/redhatinc



youtube.com/user/RedHatVideos



x.com/RedHat

