

Der “Mythos-Moment”:
Warum Enterprise Open Source Software
im Agentic AI Zeitalter für die IT-Security
entscheidend ist.

Walther Zimmerli, Red Hat

Track 3, IONOS Summit 2026

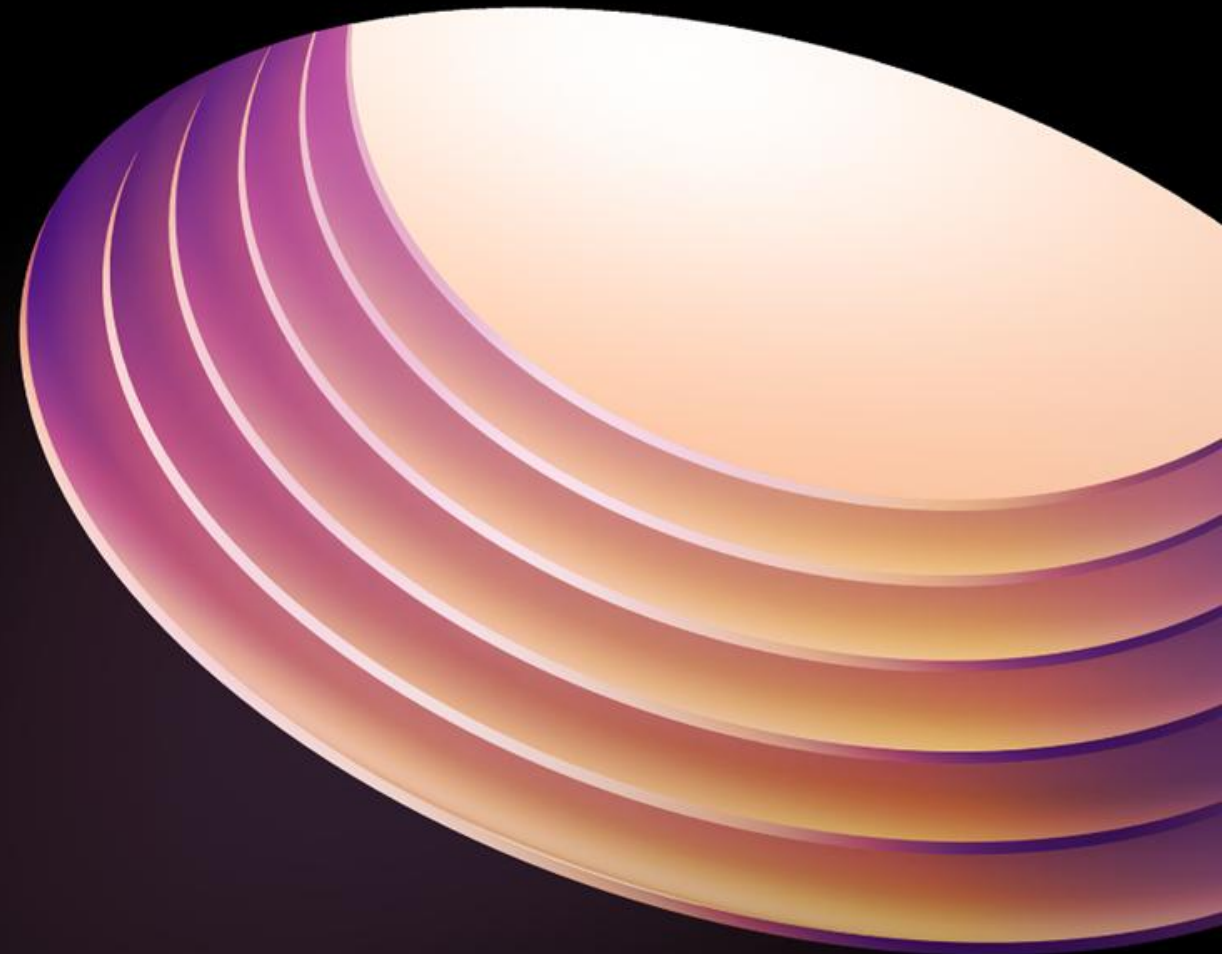


Der “Mythos-Moment”:

Warum Enterprise Open Source
Software im Agentic AI Zeitalter für die
IT-Security entscheidend ist

Walther Zimmerli

Partner Account Manager - Cloud Ecosystem Germany



The Mythos Moment

When discovery outpaces defense



AI discovers vulnerabilities at machine speed

Frontier models find critical zero-day vulnerabilities autonomously — including bugs hidden for 27 years — at under \$50 each.



Vulnerability discovery now exceeds remediation capacity

Discovery is exponential. Remediation is linear.

Less than 1% of AI-discovered vulnerabilities have been patched.



Discovery is no longer the bottleneck. Response is.

4.8M Unfilled cyber roles. Growing 19% year over year.

The National Vulnerability Database is shifting to selective enrichment.



Shift from vulnerability management to exposure management.

The number of published CVEs has grown more than 520% since 2016.

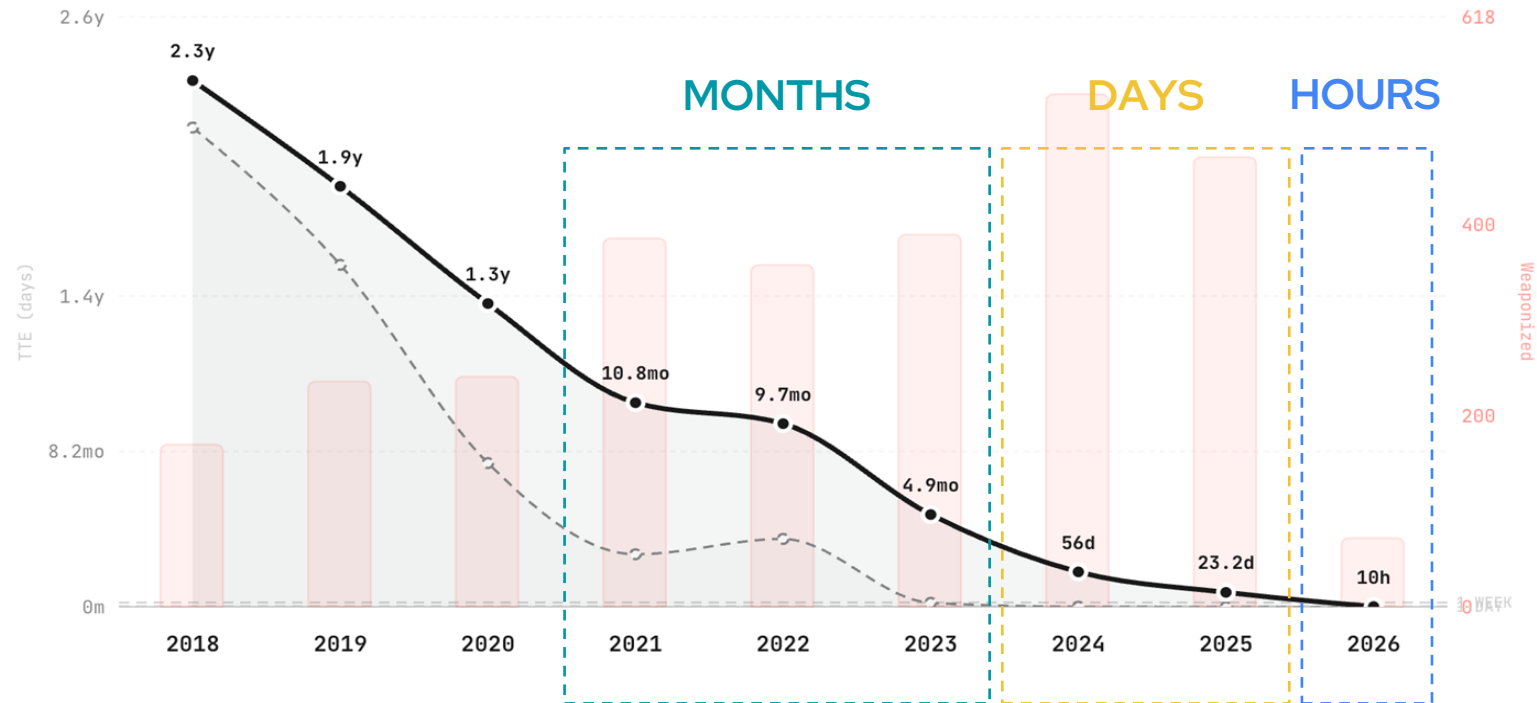
Cost of attacks in 2025 was ~\$60B. That's projected to grow to \$138B by 2031.

AI is Accelerating the Security Vulnerability Landscape

From Vulnerability to Exploitation

TTE (Time-to-Exploit) measures the gap between CVE disclosure and confirmed exploitation

— Mean TTE (10% trimmed, days) - - - Median TTE (days) ■ Weaponized Exploits (count)



Based on 3,532 CVE-exploit pairs from trusted sources (CISA KEV, VulnCheck KEV & XDB)

• zerodayclock.com

Mythos Threats to Customers

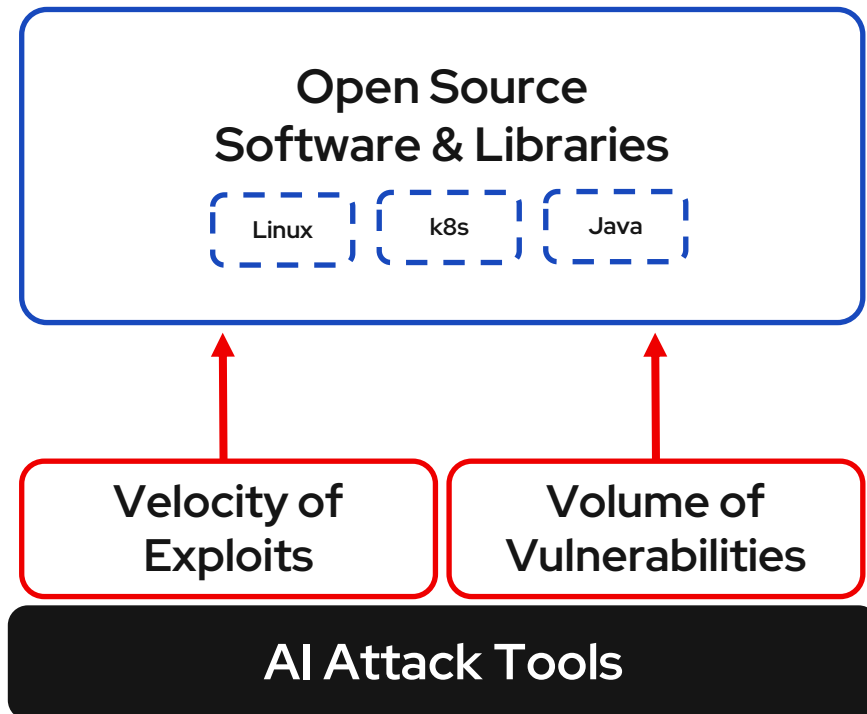
- Automate Exploitations
- Chaining Vulnerabilities
- Expose Critical Infrastructure
- Increase Threat Volume
- Increase Threat Velocity
- Lower Barrier to Entry

The Mythos Moment

Accelerating Two Parallel Challenges - "The Vulnerability Gap"

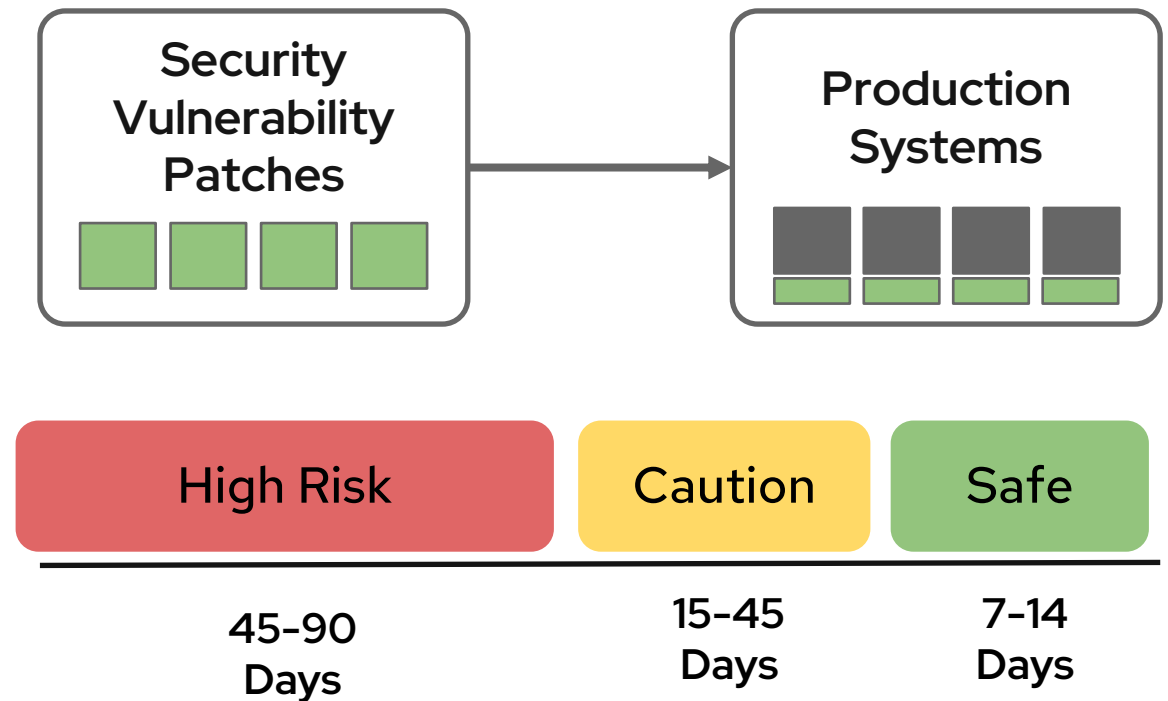
Massive CVE Growth

Problem: Time to Exploitation Dropping



Avg. Days Patch to Production: **40+**

Problem: Re-Build and Deployment Velocity

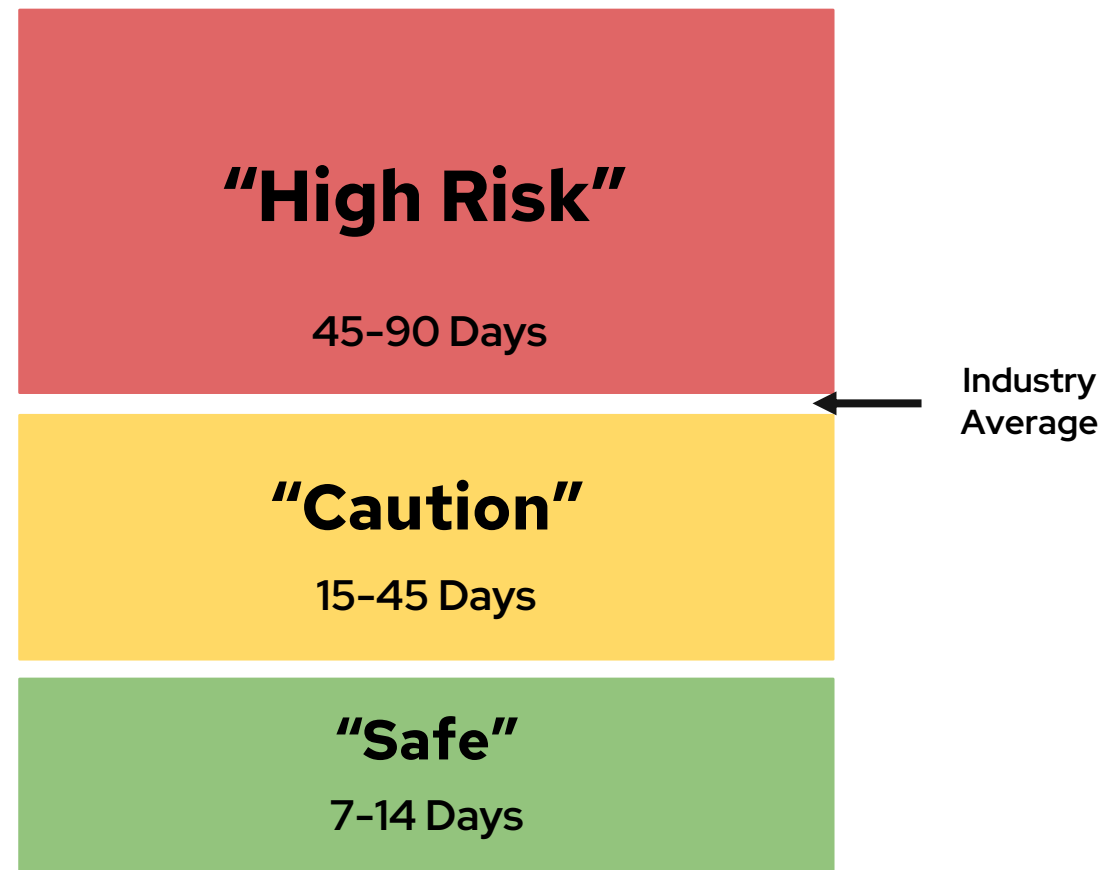


From Patch to Production?

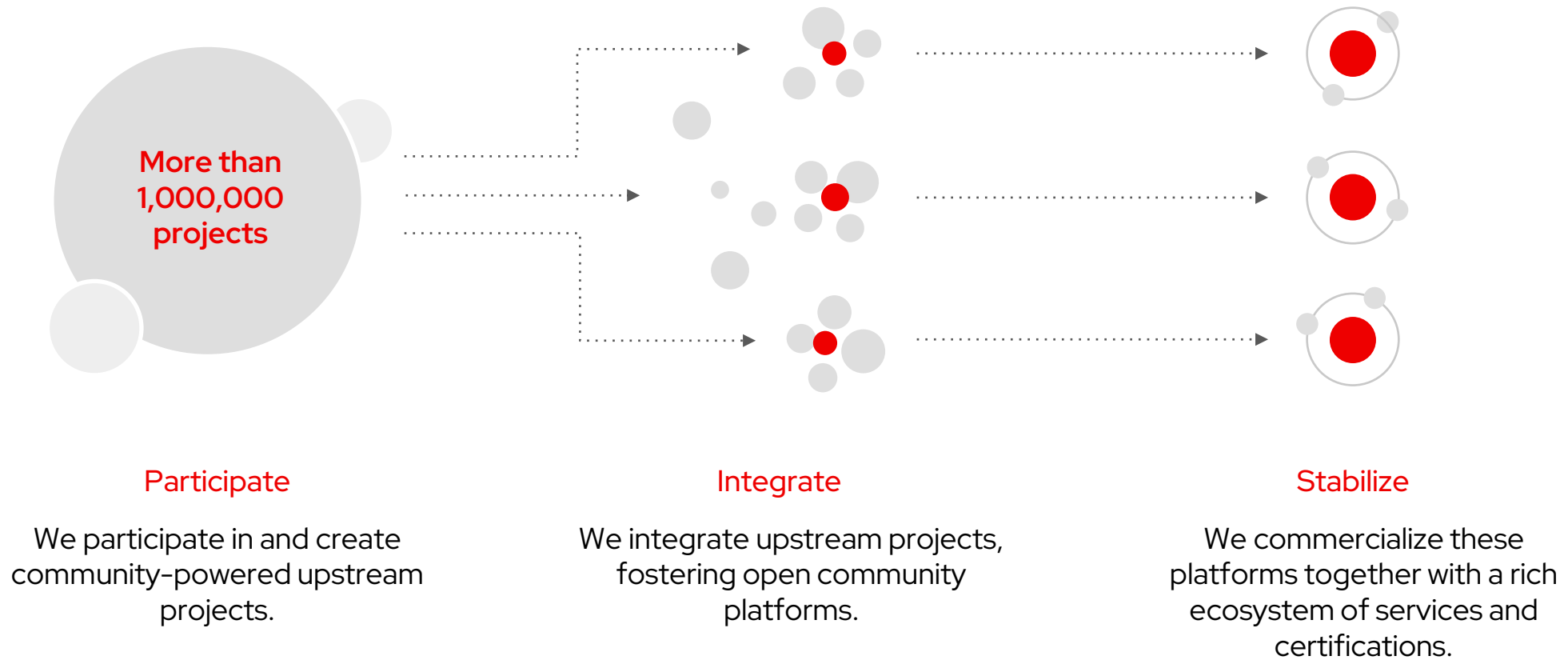
Security Remediation is only part of the challenge

How long does it take to
get from patch to
production*?

(* not just Sev 1s)



How do community projects become enterprise products?



Community Open Source vs. Enterprise Open Source

Community Open Source (DIY)

Enterprise Open Source (Red Hat)

Development Model

"Release early, release often." Focus is on rapid feature innovation.

Stabilized & Hardened. Focus is on production reliability and security certifications.

Security

Fragmented. Users must track, test, and apply their own patches from various repositories.

Trusted Supply Chain. Proactive CVE monitoring, signed packages, and backported fixes for older versions.

Lifecycle

Fast-moving. Older versions are often abandoned quickly as the community moves to the next "new" thing.

Predictable & Long-term. Up to 10–13 years of supported lifecycle for major releases (e.g., RHEL, OpenShift).

Support

Best-effort. Rely on forums, IRC, and documentation. You troubleshoot and fix issues alone.

24x7 Enterprise SLAs. Unlimited technical support with a committed partner until the issue is resolved.

Ecosystem

Use at your own risk. No guarantee that software will work with specific hardware or cloud providers.

Certified Interoperability. Thousands of certified integrations with ISV and hardware partners like SAP, Oracle, and AWS.

Ownership

High DIY Burden. Your team acts as the software vendor—integrating, testing, and maintaining the stack.

Strategic Partnership. Red Hat handles the maintenance burden, allowing your team to focus on high-value innovation.



Enterprises choose Red Hat because the alternative is costly

When running a self-supported Open Source Linux distribution, the following tasks fall on you:



Triage 100s new
CVEs per day



Hunt online for
upstream patch



Backport the fix
for their version



Quality Assurance
& Testing



Deploy & watch
for any issues



In case of fire, ask
the community

“Free” still ends up costing you in other ways

Enterprises choose Red Hat because the alternative is costly

With a Red hat subscription, we take care of these:



Red Hat
Enterprise Linux



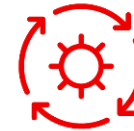
Monitor for new
vulnerabilities



Perform risk
assessment



Compliance,
Standards & testing



Remediation &
automation



In case of fire, call
Red Hat Support

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

Unlocking the business value of security and management



CURRENT REALITIES

- AI models like **Anthropic's Mythos** are uncovering vulnerabilities at an unprecedented pace, at a scale humans can't match.
- **Continued struggles to find and retain Linux expertise** are leading to operational instability, increased downtime, and dependencies on hero engineers to "keep the lights on."
- **Configuring and maintaining compliance** with local and industry standards.



RED HAT VALUE ADD

- **Increase productivity** by streamlining infrastructure management and security at scale across on-prem, cloud, and edge.
- **Reduce risk** with built-in security capabilities to protect your systems from the start and troubleshoot faster.
- **Maintain compliance** by leveraging out-of-the-box tools to easily deploy security baselines and monitor at scale from day one.



BUSINESS IMPACT¹

32%

More efficient IT infrastructure teams

\$21.91 M

Potential benefits over 5 years

52%

Faster security updates

72%

Less unplanned downtime

Red Hat Enterprise Linux
is the security foundation
leveraged across the Red
Hat portfolio

Available on **IONOS**
CLOUD



Red Hat Enterprise Linux includes built-in security that minimizes risk, maximizes uptime, and simplifies compliance.



Red Hat Enterprise Linux Continuous Compliance & Minimize CVEs



How Red Hat helps your team by:

- **Treating security and compliance as a continuous cycle**, not just an event to react to after the fact
- **Streamlining compliance validation processes** (i.e.: OpenSCAP profiles for BSI IT-Grundschutz allow auditing & remediation)
- Providing **assistance tools to remove burdens** that your team normally undertakes:
 - **proactive analytics and automation** to identify affected servers,
 - **Prioritize risks** with deep threat intelligence
 - Deliver an **actionable remediation plan**

"Every week we have to do security scans...list vulnerabilities in packages that are on the operating systems. Any time that occurs, we can immediately go to the Red Hat site, and get full explanations of the vulnerabilities, which help determine if we're affected. Nobody else does that for other Linux distributions."

Ryan Kimbrell,
Senior Cloud
Operations Engineer,
Zoom

Red Hat Enterprise Linux Zero Trust Architecture



How Red Hat helps your team with Zero Trust:

- **Ensures user access is granted based on who you are**, not just which network you are plugged into
- **Take steps to protect sensitive information**, digital "sandboxes" (SELinux) used to lock applications down
- **Block unauthorized tools** by only allowing software that is on your approved list
- **Help identify file tampering or suspicious activity** with continuous monitoring of the OS

- Identity
- Data
- Devices/Networks
- Apps/Workloads

*Red Hat helps in each key
pillars of the Zero Trust
Maturity Model 2.0*

Red Hat Enterprise Linux Platform Integrity and Hardening

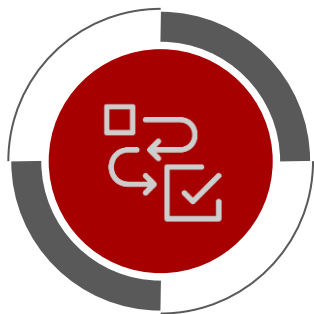


How Red Hat helps your team apply security, easily:

- **Automate and enforce security configurations** *at scale* with Automation playbooks, powered by Ansible
- **Achieve consistency** in automating security tasks (certificates, crypto policies, compliance profiles) across thousands of systems
- **Meet compliance standards** with continuous scanning and remediation

- Security architecture
- Consistency
- Reduce risk

Red Hat Enterprise Linux Trusted Software Supply Chain



Some of the elements Red Hat applies to their trusted software supply chain:

- Secure development life cycle (**SDLC**) framework
- Supply-chain Levels for Software Artifacts (**SLSA**)
Level 3: Extra resistance to specific threats¹
- Product Pipeline Partnership Security Program²
- Complete Software Bill of Materials³
- Multiple cybersecurity validations and certificates⁴

- Transparency
- Integrity
- Security Automation



National Cyber
Security Centre



1. SLSA 3 description ([source](#))

2. Product Pipeline Partnership Security Program ([Red Hat Customer Portal](#))

3. Published index of SBOMs ([link](#))

4. Red Hat ProdSec Compliances ([link](#))

Why Red Hat on IONOS



IONOS Cloud

Data Sovereignty

Scalability

High Availability

+

Red Hat Enterprise Linux

Red Hat OpenShift

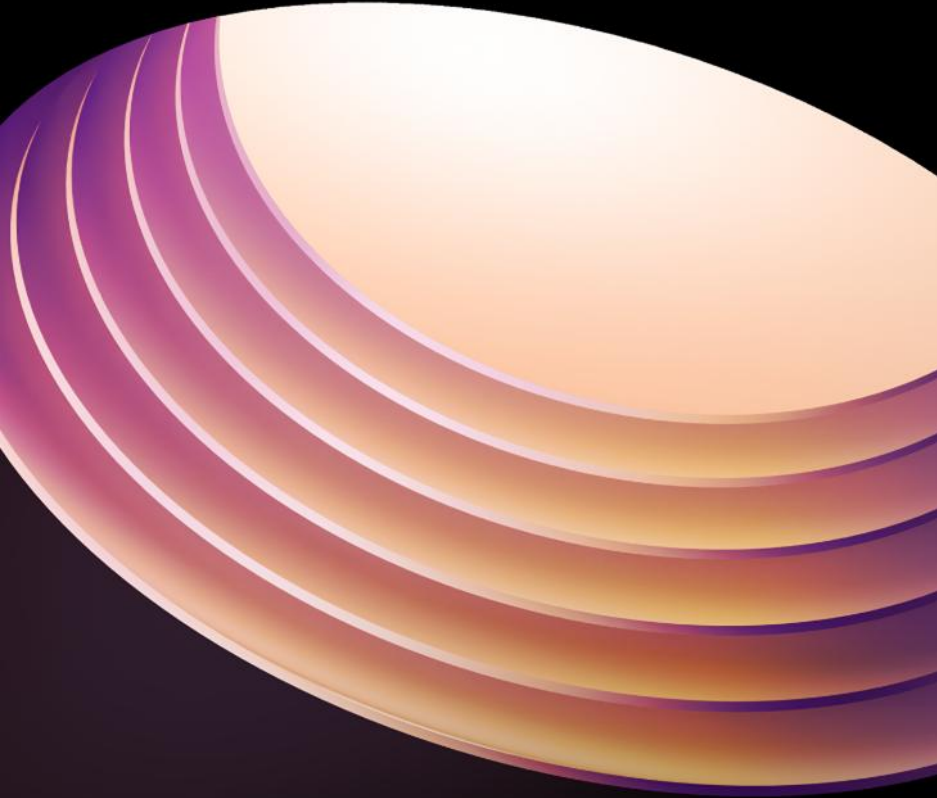
=

**SECURE
SOVEREIGN CLOUD**

High Reliability and Security

Enterprise grade Support

Enterprise Open Source



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](https://www.linkedin.com/company/red-hat)

 [facebook.com/redhatinc](https://www.facebook.com/redhatinc)

 [youtube.com/user/RedHatVideos](https://www.youtube.com/user/RedHatVideos)

 twitter.com/RedHat

