Red Hat

Improve security and compliance

Reduce risk with an open source Linux platform

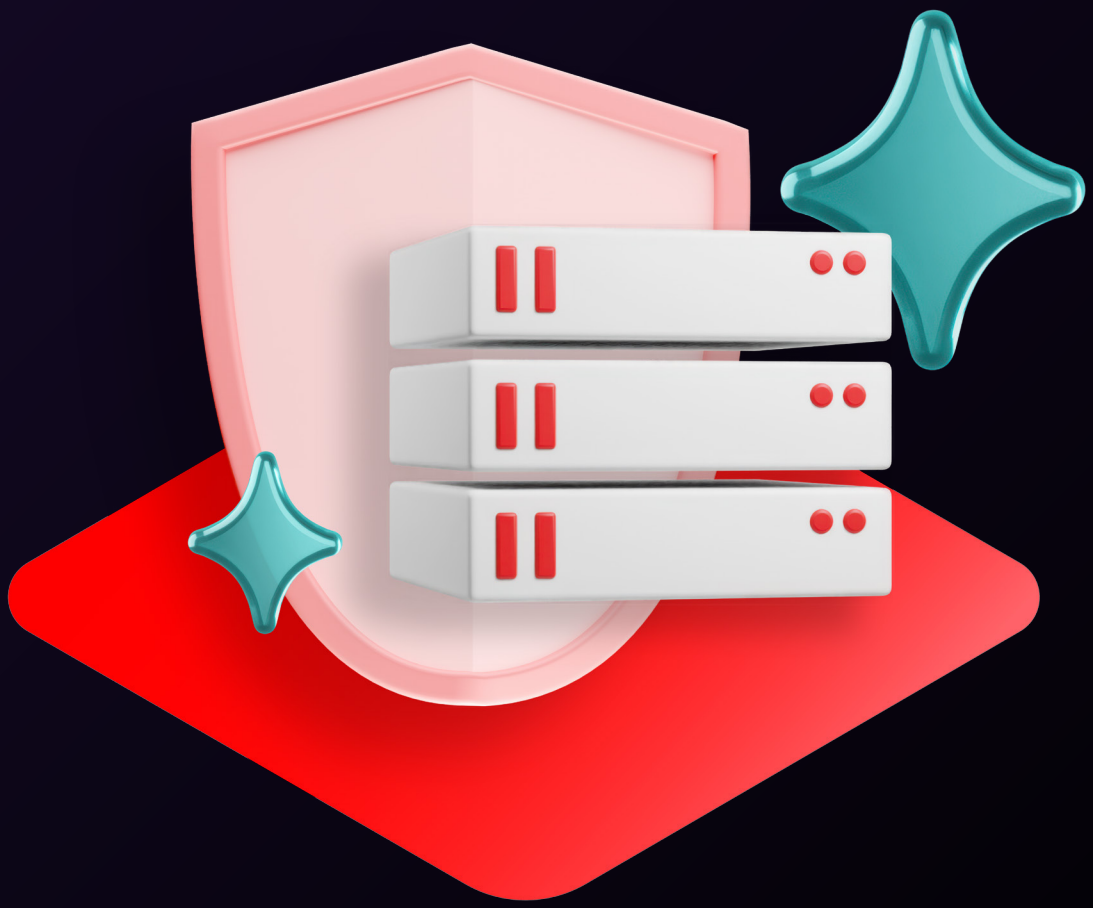

Table of contents

3 Chapter 1:
Linux is the foundation for the future

4 Chapter 2:
Adopt an effective security and compliance approach

5 Chapter 3:
Vulnerability identification and remediation in Linux environments

6 Chapter 4:
Compliance management in Linux environments

7 Chapter 5:
Best practices and tool recommendations

8 Chapter 6:
Boost security and compliance with Red Hat

9 Chapter 7:
Take advantage of integrated tools

10 Chapter 8:
Zoom establishes a solid enterprise system with Red Hat

11 Get more from your data

Recent benchmarks illustrate the typical consequences of ineffective security incidents:[1]

- **US$4.4M** average total cost of a data breach in 2025 .
- **241 days** the mean average time to identify and contain a data breach in 2025.
- **97%** of organizations that reported an AI-related security incident lacked proper AI access controls.

Chapter 1

Linux is the foundation for the future

As one of the most popular operating systems (OSes), Linux® provides an ideal platform for modern IT landscapes. It is the standard for highly available, reliable, and critical workloads in datacenters and cloud computing environments, supporting a variety of use cases, target systems, and devices. Many major public cloud providers offer multiple Linux distributions within their marketplaces.

Even so, the specific Linux distribution and management tools an organization chooses can greatly affect the efficiency, security, and interoperability of its IT environment. This e-book provides effective security management approaches, key integrated tool features and recommendations, and guidance on managing security vulnerabilities and compliance risks within Linux environments.

AI brings new concerns

Managing IT security and compliance is an ongoing challenge for many organizations. "Globally, 1 in 5 organizations has experienced a significant cyber incident within the past 2 years. These events are costly with the global average cost of a data breach being US$4.44 million."[1] The rise of AI has introduced new threats and added complexities to the security landscape. Specifically, the use of unsanctioned AI tools used by employees outside of IT oversight, known as "shadow AI", introduced a new major threat. "Breaches involving shadow AI added an average of US$670,000 to the [total] bill—a 15% increase [over standard breach costs]."[1]

Avoid the consequence of ineffective security

Speed is essential in reducing the risk and impact of breaches. The faster an organization can identify a potential threat, the lower the financial and operational fallout. Recent benchmarks illustrate the typical consequences of ineffective security incidents:[1]

- **US$4.4M** average total cost of a data breach in 2025 .
- **241 days** the mean average time to identify and contain a data breach in 2025.
- **97%** of organizations that reported an AI-related security incident lacked proper AI access controls.

3 common security challenges

Several factors complicate modern security vulnerability and compliance management:[1]

Changing security and compliance landscapes

Teams are no longer just managing devices; they're struggling to govern sanctioned AI models while simultaneously defending against shadow AI tools.

- **20%** of breaches are caused by security incidents involving shadow AI.

When data is stored across multiple environments, it becomes significantly harder to protect. This complexity makes it more difficult for security teams to identify and contain a breach compared to data stored in a single environment.

- **30%** of breaches now involve data stored across multiple environments.

1 *IBM Security. "Cost of a Data Breach Report 2025." 2025.*

The complexity premium

Large infrastructures often incorporate multiple security and compliance tools, which can complicate risk management operations.

- Data breaches involving multiple environments are now the most common and the most expensive, costing an average of **US$5.05 million** per incident—slightly higher than breaches occurring solely on premise.

Staffing challenges

Most organizations lack the staff headcount required to manage security and compliance tasks manually. Additionally, the rise of remote work has increased the burden of safeguarding devices and access points to an organization's digital assets.

- **63%** of organizations lack the governance policies necessary to manage AI, largely because they don't have the staff to create and enforce them.

Chapter 2

Adopt an effective security and compliance management approach

Security and compliance management is a continuous, risk-based discipline. It helps organizations strengthen their security posture while meeting regulatory and business requirements across increasingly complex environments. A modern approach helps teams establish consistent, repeatable, and auditable practices across their entire IT estate—on premise, cloud, and hybrid infrastructures—so they can:

Assess

Continuously identify noncompliant or vulnerable systems. Evaluate the security state of the organization's entire environment, from infrastructure to workload, to determine which security advisories actually apply to specific systems.

Prioritize

Prioritize remediation efforts based on risk, impact, and operational effort, with support of verified automation and AI-driven tools. Use risk management techniques to understand the business impact of each issue and plan remediation efforts accordingly. For example, a vulnerability on a development system may pose minimal risk, while the same issue on a production workload requires immediate attention.

Remediate

Patch and reconfigure systems quickly. Automating remediation processes ensures consistency across systems and reduces the risk of human error. When applied effectively, automated tools speed up remediation to protect the business and its data.

Report

Continuously validate that changes were applied and automate reporting to streamline audits. Clear, role-appropriate reporting delivers the right level of insight for executives, auditors, and technical teams

Square Enix simplifies management of online gaming infrastructure

"Since switching to Red Hat Enterprise Linux, we can more quickly discover and investigate bugs and vulnerabilities than in the Linux distribution we were previously using."

Yuki Miyamoto
IT Infrastructure/Business Online Infrastructure System, Information Technology Division, Square Enix Co., Ltd.

Note: The information contained in this content was current at the time of the interview.

to understand current security posture and risk exposure over time. By combining continuous validation with automated, auditable reporting, organizations can move beyond reactive security practices to support modern operating models such as DevSecOps, where speed, consistency, and governance must coexist.

Chapter 3

Vulnerability identification and remediation in Linux environments

Vulnerability identification and remediation is the process of evaluating infrastructure to find and fix systems that are susceptible to attack. These vulnerabilities can be caused by emerging threats, outdated or missing patches, or system misconfigurations. Remediation usually includes patching, updating, and reconfiguring systems to resolve the underlying risk.

Why is vulnerability identification important?

Security vulnerabilities can lead to costly breaches that can damage customer trust, company reputation, and revenue. In fact, "attackers targeted customer personally identifiable information (PII) over other types of data by a wide margin. At 53%, it was the most stolen or compromised data type."[1] This remains the most targeted data type because of its high value for identity theft and fraud.

Challenges to effective vulnerability identification and remediation

Most organizations lack a consistent security strategy for operations at scale, a gap further widened by the rapid, unmanaged adoption of AI tools and workloads. Key obstacles include:

- Skills and resource gaps: As AI environments expand, limited staff are overwhelmed and may lack the skills required to develop and execute a comprehensive security strategy.
- Alert fatigue: Generic security scanning tools generate massive lists of potential vulnerabilities. Because many are not applicable to a specific environment, staff must spend more time investigating relevant risks.
- Manual bottlenecks: Manual identification, remediation, and tracking processes slow down operations, leaving known vulnerabilities unpatched for extended periods.
- Inconsistent remediation: Ad hoc remediation methods lead to inconsistent application of patches and the risk of increased security breaches across the entire infrastructure.

Key security management tool features

To be effective, organizations must be able to rapidly identify and resolve system vulnerabilities before they result in a breach. When evaluating unified security management tools, look for these key features:

- **Systems analysis** to identify risks at both the OS and workload levels in systems and instances across any environment.
- **Automated remediation** to identify risks with increased speed, accuracy, and efficiency for IT and security teams.
- **Incorporate vendor expertise** to provide remediation guidance for their products to ensure fixes are verified.

- **Regularly access the latest data** about known vulnerabilities and security risks from the organization's OS and application providers.
- **Generate audit-ready reports** with appropriate levels of detail for executives, auditors, and technical teams.

Read this PeerSpot report[2] to discover how even the best IT departments can benefit from using Red Hat® Satellite solutions for improving infrastructure management and security.

Chapter 4

Compliance management in Linux environments

Compliance management is the process of ensuring systems are compliant with corporate policies, industry standards, and applicable regulations over time. It involves infrastructure assessment to identify systems that are noncompliant due to regulatory and policy changes, misconfiguration, or other internal standards.

Why is compliance management important?

Beyond increasing the risk of security breaches, noncompliance with applicable regulations can lead to significant fines, damage to business reputation, and the loss of necessary certifications. Regulatory compliance failures add to the average cost of a data breach by US$173,692.[1]

Challenges to effective compliance management

Many organizations rely on manual operations and custom scripts—methods that are slow and limited in scale for fast-paced technology development and business operations. However:

- A multitude of generic standards and baselines makes it difficult to determine which requirements are relevant to a specific environment.
- Manual processes slow compliance monitoring, remediation, and auditing operations, which leads to inefficient use of staff time, inconsistent policy application, and further risk of compliance issues.
- Separate tools for security and compliance management can result in lower operational efficiency, making it laborious to set up consistent and custom policies.

Key compliance management tool features

To be effective, organizations need to define and apply contextual policies to maintain system integrity and generate audit-ready reports in less time. When evaluating unified compliance management tools, look for tools that:

- **Use analytic features** to consistently identify compliance risks in a time-efficient manner.
- **Remediate** noncompliant systems automatically.
- **Provide a complete view** of current compliance posture across multiple environments.

2 *PeerSpot report. "7 Ways Red Hat Satellite Can Improve Security and Infrastructure Management Efficiency." 24 April 2024.*

Zoom establishes a solid enterprise system with Red Hat

"Every week we have to do security scans against every system in the environment. And those scanners 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. It would quickly become a nightmare trying to run a production government environment without it because we would have to do all that research every month ourselves."

Ryan Kimbrell
Senior Cloud Operations Engineer,
Zoom

- **Generate automated compliance reports** according to auditing requirements and audience needs.
- **Deliver expert advice** and contextual guidance for remediating noncompliant systems across multiple environments.

The next chapter explores best practices for managing security and compliance risk more effectively in dynamic enterprise environments.

Chapter 5
Best practices and tool recommendations

Analyze systems regularly

Daily monitoring helps organizations identify vulnerability and compliance risks before they interrupt business operations or result in a breach. Use the latest security data from the OS and application vendors to improve analysis accuracy, and establish custom security policies tailored to a specific environment.

- For vulnerabilities listed in the CISA Known Exploited Vulnerability (KEV) catalog, the median time for an attacker to begin mass exploitation is only **5 days**.[3]

Patch often and test thoroughly

Keeping systems up to date improves security, reliability, performance, and compliance. While general patches should be applied regularly, critical bugs and defects require immediate attention. Test patched systems for acceptance before returning them back into production.

Deploy automation and approved AI tools

As the organization's infrastructure grows, it becomes harder to manage manually. Use automation and AI-driven tools to streamline monitoring, speed remediation, and ensure consistent reporting.

- Security teams using AI and automation extensively shortened their breach times by 80 days and lowered their average breach costs by **US$1.9 million** compared to organizations that didn't use these solutions.[1]

Connect tools and align processes

Integrate disparate platform management tools via application programming interfaces (APIs) to maintain visibility across distributed environments. Reducing the number of interfaces simplifies operations and ensures a more consistent, reliable security posture.

- Security system complexity adds an average of **US$207,914** to the cost of a breach.[1]

Adopt a consistent, continuous security strategy

Effective security demands a holistic approach that aligns people, processes, and technology. A defense-in-depth strategy maximizes protection by applying security controls across all layers, including

3 *Verizon Business. "2025 Data Breach Investigations Report." 2025.*

OSes, container platforms, automation and AI tools, software-as-a-service (SaaS) solutions, and cloud services.

- **63% of organizations** lack a formal AI governance policy, which directly contributes to higher breach costs.[1]

Understanding the needs of an organization's security and compliance posture at any moment is the first step to improvement. Ideal security and compliance tools will include several key features and capabilities:

- **Proactive analysis:** Tools that provide proactive, automated analysis can ensure systems are monitored at regular intervals, providing alerts to issues without requiring constant manual oversight.
- **Prioritized response:** Tools should provide prescriptive remediation steps and prioritize actions based on potential impact, allowing teams to make the most of limited patching windows.
- **Customizable results:** To reduce false positives, look for tools that allow organizational IT leaders to define business context, ensuring checks only apply to relevant systems and workloads. Some vulnerability and compliance checks may not apply to certain systems due to their use, configuration, or workload.
- **Intuitive reporting:** Tools that generate clear, intuitive reports for multiple audiences regarding patch status and policy compliance improve auditability and stakeholder alignment.
- **Unified interface:** Tools that manage multiple layers of the IT environment can simplify security operations and provide a better understanding of the current security and compliance posture. Unified tools can also provide increased context for scans and remediation guidance.
- **Actionable insight:** Tools that provide information tailored to the IT environment can help quickly identify affected systems, and the potential impact of a vulnerability, helping organizations prioritize and plan remediation actions.

Chapter 6

Boost security and compliance with Red Hat

Red Hat takes a holistic, proactive approach to security and compliance risk management, improving speed, scalability, and stability across the entire IT environment, from bare-metal and virtualized servers to private, public, hybrid cloud, and edge deployments. By aligning people, processes, and technology, Red Hat® platforms help organizations achieve operational efficiency, boost innovation, and improve employee satisfaction.

At the core of this strategy is Red Hat Enterprise Linux, a consistent, intelligent operating foundation for modern IT. This consistency across infrastructure allows IT teams to deploy applications, workloads, and services using the same tools, regardless of location.

Security is a key part of the Red Hat Enterprise Linux architecture and lifecycle. Multilayered breach defenses use automated, repeatable security controls to mitigate exposure to vulnerabilities while critical security upgrades and live patches—included as part of a Red Hat Enterprise Linux subscription—helps keep the IT environment protected without downtime.

How Zoom meets FedRAMP and DoD requirements

"Compliance is nothing but discipline. And Red Hat has the discipline that we need..."

John Keese
Head of Technology Compliance,
Zoom

"Since switching to Red Hat Enterprise Linux, we can more quickly discover and investigate bugs and vulnerabilities than in the Linux distribution we were previously using."[4]

Yuki Miyamoto
IT Infrastructure/Business Online Infrastructure System,
Information Technology Division,
Square Enix Co., Ltd.

Red Hat Enterprise Linux is enhanced by integrated management tools and AI-powered insights that provide a holistic view for managing security and compliance across hybrid environments. Organizations can benefit from:

- **Reduced alert fatigue:** Reduce false positives with configurable tools and baselines to provide an accurate view of IT current infrastructure status.
- **Proactive remediation:** Improve configuration and patching accuracy with automation and reduce human errors, without needing to contact support.
- **Comprehensive visibility:** Use vulnerability and malware detection capabilities to scan systems for Common Vulnerabilities and Exposures (CVEs) and malware signatures while customizable views deliver the right data to the right audience at the right time and speed.
- **Streamlined integration:** Take advantage of on-site and Software-as-a-Service (SaaS) deployment options, along with APIs, to help ensure Red Hat Enterprise Linux connects smoothly with existing security, compliance, and management tools and interfaces. This streamlined integration is supported by an extensive library of resources providing detailed, targeted information 24x7.
- **Resource optimization capabilities:** Help organizational IT teams select the appropriate size of its public cloud deployments using compute, memory, and performance metrics.
- **Prepared defense:** Prepare for threats from future quantum computers with National Institute of Standards and Technology (NIST)-approved, quantum-resistant algorithms and confidential computing[5] to protect sensitive data even while in use.

Read What is confidential computing?

Chapter 7

Take advantage of integrated tools

Red Hat management tools are built on decades of Linux development and support experience. These Red Hat tools work together to streamline IT administration, saving IT teams valuable time while ensuring the environment remains security-focused, optimized, and reliable.

Analyze, observe, and manage Red Hat systems

Red Hat provides the trusted Linux platform alongside the integrated management tools and services needed for security-focused operations and innovation.

4 *Red Hat case study. "Square Enix simplifies management of online gaming infrastructure." 17 May 2023.*

5 *Red Hat overview. "What is confidential computing?" 22 Oct. 2025.*

- **Red Hat Lightspeed:** Included with the subscription and delivered as a service, Red Hat Lightspeed (formerly Red Hat Insights) continuously analyzes platforms and applications to predict risk, recommend actions, and track costs. It allows organizations to monitor IT efficiency, stability, and performance while managing security and compliance risk across hybrid cloud environments.

Learn more about Red Hat Lightspeed

Streamline and automate system management

Adopting effective automated management approaches and tools is essential for protecting an organization.

- **Red Hat Satellite:** The platform provides digitally sovereign and agentic Red Hat Enterprise Linux management. The management tool provision can be configured to Red Hat Enterprise Linux systems in minutes, extending Red Hat's security-focused supply chain through content and patch management in air-gapped environments, and consistently monitored for compliance. Integrated analytics help IT security teams preemptively identify issues and receive remediation recommendations, with the option to automate fixes at scale.

Learn more about Red Hat Satellite

Chapter 8

Zoom establishes a solid enterprise system with Red Hat [6]

Zoom Video Communications, Inc. (Zoom) is a global communications technology company, innovating since 2011. Beginning as a video communication solution, it has grown to offer much more, such as Zoom for Government. To comply with the rigorous security mandates of the Federal Risk and Authorization Management Program (FedRAMP) and the Department of Defense (DoD), Zoom operates its platform using Red Hat Enterprise Linux. The company also relies on Red Hat Ansible® Automation Platform and Red Hat Satellite for infrastructure automation, ensuring compliance functions, and managing deployments.

Zoom for Government relies on Red Hat Enterprise Linux and other Red Hat tools to ensure the regular adjudication process runs smoothly, with Red Hat involved in almost every step of the process. Zak Peirce, Head of Data Center Operations at Zoom, had no doubt about using Red Hat solutions. "I've always been a Red Hat guy," said Peirce. "I'd choose Red Hat as my enterprise platform of choice to run a solid enterprise system."

Peirce went on to share why he finds the entire ecosystem useful. "I know that when I update IdM, it's going to work with my Red Hat systems. I know that when I update the System Security Services Daemon (SSSD) agent, it's going to work. And then the ability to use Red Hat Satellite to host those packages, keep my systems up to date, and manage the exact packages that go onto my systems helps me test my systems and make sure that the development stage and production are the same. All the pieces help us to run our operation."

The resources on the Red Hat website, including the Common Vulnerabilities and Exposures (CVE) database and the Red Hat security advisory (RHSA), are invaluable when working with the U.S. Government.

---

6 *Red Hat case study. "Zoom for Government enhances security with a Red Hat platform." 10 March 2023.*

"Every week we have to do security scans against every system in the environment. And those scanners 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. It would quickly become a nightmare trying to run a production government environment without it because we would have to do all that research every month ourselves."

Ryan Kimbrell,
Senior Cloud Operations Engineer, Zoom

Get more from your data

Businesses rely on the stability and reliability of its IT infrastructure and applications. Adopting a pro-active approach to security vulnerability and compliance risk management is the most effective way to protect your organization's assets.

Red Hat provides a trusted Linux platform and integrated management tools and services needed for security-focused, high-scale operations.

Analyze organizational risk with Red Hat Lightspeed

- Learn more about Red Hat Lightspeed
- Read this Red Hat overview [7] to learn about how Red Hat Lightspeed can help simplify compliance and vulnerability management

Manage at scale with Red Hat Satellite

Discover more about Red Hat Satellite

Learn more about the Business Value of Red Hat Satellite[8]

7 *Red Hat overview. "Simplify Linux management with Red Hat Lightspeed." 2 May 2025.*

8 *IDC Business Value White Paper, sponsored by Red Hat. "The Business Value of Red Hat Satellite." July 2024.*

About Red Hat

Red Hat is the world's leading provider of enterprise open source software solutions, using a community-powered approach to deliver reliable and high-performing Linux, hybrid cloud, container, and Kubernetes technologies. Red Hat helps customers develop cloud-native applications, integrate existing and new IT applications, and automate and manage complex environments. A trusted adviser to the Fortune 500, Red Hat provides award-winning support, training, and consulting services that bring the benefits of open innovation to any industry. Red Hat is a connective hub in a global network of enterprises, partners, and communities, helping organizations grow, transform, and prepare for the digital future.

North America	Europe, Middle East, and Africa	Asia Pacific	Latin America
1 888 REDHAT1 www.redhat.com	00800 7334 2835 europe@redhat.com	+65 6490 4200 apac@redhat.com	+54 11 4329 7300 info-latam@redhat.com

facebook.com/redhat
x.com/RedHat
linkedin.com/company/red-hat

redhat.com
#US52390824_0426