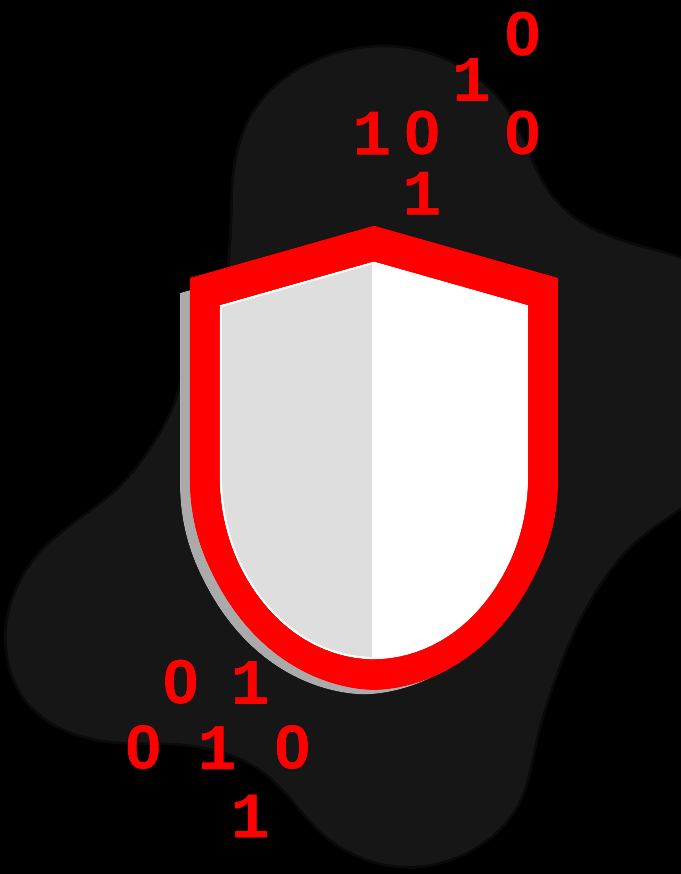
Red Hat

Improve security and compliance

Reduce risk with a robust open source Linux platform

Contents



Linux is the foundation for the future

As one of the world's most popular operating systems, Linux® provides an ideal platform for modern, innovative IT. It is commonly used for highly available, reliable, and critical workloads in datacenters and cloud computing environments and supports a variety of use cases, target systems, and devices. Every major public cloud provider offers multiple distributions of Linux in their marketplaces.

Even so, the Linux distribution and management tools you choose can greatly affect the efficiency, security, and interoperability of your IT environment. This e-book reviews key considerations and guidance around security vulnerability and compliance risk for Linux environments.

Security and compliance are top concerns

Managing IT security and compliance risk is an ongoing concern for all organizations. In fact, 23% of organizations experienced a major cybersecurity attack in the last 2 years.[1] And security breaches can be costly. The average cost of a data breach is US$4.45 million.[2]

Industry and government regulations are also changing. Keeping up can be challenging and compliance failures increase the cost of a data breach by around 5% on average.[2]

Avoid the impacts of ineffective security

Speed is essential in reducing the risk and impact of breaches.

$4.45M
average total cost of a data breach in 2023 (USD).[2]

277 days
average time to identify and contain a data breach in 2023.[2]

$1.02M
average savings in costs if a breach can be identified and contained in 200 days or less.[2]

[1] Nash Squared. "2023 Nash Squared Digital Leadership Report," November 2023.
[2] IBM Security. "Cost of a Data Breach Report 2023," 2023.

Common security and compliance challenges

Several factors make security vulnerability and compliance management challenging.

Changing security and compliance landscapes

Security threats change quickly, requiring rapid response to new threats and evolving regulations.

23%
of organizations of all sizes experienced a major cybersecurity attack in the last 2 years.[3]

82%
of breaches in 2023 involved data stored in cloud environments or across multiple environments.[4]

Distributed cloud environments

Geographically and logically distributed hybrid and multicloud environments can prevent you from gaining a complete view into your IT infrastructure, making it harder to maintain consistent configurations across all systems.

Large and complex IT environments

Large infrastructures often incorporate multiple security and compliance tools, complicating risk management operations.

Security system complexity increases data breach cost by

$240,889.[4]

Remote workforces increase the average cost of a data breach by

$173,074

compared to breaches where remote work was not a factor.[4]

Limited staff and remote work directives

Most organizations lack the staff headcount needed to manage security and compliance tasks manually, and remote work can add to the burden of safeguarding devices and access points to an organization's digital assets.

[3] Nash Squared. "2023 Nash Squared Digital Leadership Report," November 2023.
[4] IBM Security. "Cost of a Data Breach Report 2023," 2023.

Adopt an effective security and compliance management approach

Security vulnerability and compliance management involves monitoring and assessing systems to ensure they comply with security and regulatory policies. An ideal security vulnerability and compliance management approach will let you develop consistent, repeatable processes across your entire environment to:

Assess

Identify systems that are noncompliant or vulnerable. Assess the actual security state of your environment from infrastructure to workload. Understand which of the multitude of security advisories are really applicable to your systems and environment.

Prioritize

Organize remediation actions by effort, impact, and issue severity. Apply risk management techniques to determine the actual business risk of each issue and plan remediation efforts accordingly. Risk encompasses the likelihood of an issue resulting in a breach, the potential severity of a breach, and the implications of fixing the issue. It may not make sense to fix a certain issue on development and test systems, but that same issue may be a high priority for production systems.

Remediate

Patch and reconfigure systems that require action with speed. Automate configuration and patching processes to speed remediation, ensure consistency across systems, and reduce the risk of human error. Applied effectively, automated tools can help you remediate issues rapidly to improve the security of your environment and business.

Report

Validate that changes were applied and automate reporting to streamline audits. Effective reporting helps you deliver information at the right level of detail for C-suite roles, auditors, and technical teams to understand current security risks and exposures.

This approach also helps to prepare your organization for modern, fast-moving development and management techniques like DevSecOps. The following sections discuss key considerations and actions to more effectively manage your security and compliance risk.

Vulnerability identification and remediation in Linux environments

Vulnerability identification and remediation is the process of evaluating infrastructure to find and fix systems that are vulnerable to attack. These vulnerabilities can be caused by emerging threats, outdated or missing patches, or system misconfiguration. Remediation actions often include patching, updating, and reconfiguring systems to resolve the vulnerability.

Why is it important?

Security vulnerabilities can lead to costly breaches that may also result in reduced customer trust, company reputation, and revenue. In fact, lost business accounts for 29.2% of the average cost of a data breach.[5]

Challenges to effective vulnerability identification and remediation

Most organizations lack a consistent security strategy for operations at scale.

- Limited staff are overwhelmed and may not have the skills needed to develop and execute a complete security strategy.
- Generic security scanning tools generate massive lists of potential vulnerabilities, but not all will be applicable to your environment, requiring staff to spend large amounts of time investigating vulnerabilities and remediation actions.
- Manual identification, remediation, and tracking processes slow operations, and known vulnerabilities often go unpatched.
- Ad hoc remediation methods result in inconsistent application of patches and increased potential security risks.

[5] *IBM Security. "Cost of a Data Breach Report 2023," 2023.*

Key security management tool features

To be effective, you must be able to rapidly identify and remediate system vulnerabilities before they result in a breach. Look for unified security management tools that:

Analyze systems to identify risks—at both the operating system and workload levels—in systems and instances across your environment.

Automate remediation for identified risks to improve speed, accuracy, and efficiency for IT and security teams.

Incorporate vendor expertise to provide remediation guidance for their products—there may be simple actions you can take to reduce your risk.

Regularly access the latest data about known vulnerabilities and security risks from your operating system and application vendors.

Generate reports regarding potential risks, remediation actions, and auditing at the appropriate level of detail for different audiences.

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 uses infrastructure assessment to identify systems that are noncompliant due to regulatory, policy, or standards changes, misconfiguration, or other reasons.

Why is it important?

Noncompliance can result in fines, damage to your business, and loss of certification, in addition to security breaches. Compliance failures result in greater data breach costs on average.[6]

Challenges to effective compliance management

Many organizations manage compliance using manual operations and custom scripts—processes that are too slow and limited in scale for modern, fast-moving development and operations.

- A multitude of generic standards and baselines make it difficult to understand the relevance and impact on your environment.
- Manual processes slow compliance monitoring, remediation, and auditing operations, leading to inefficient use of staff time, inconsistent policy application, and increased risk of compliance issues.
- Many organizations use separate tools for security and compliance management, resulting in lower operational efficiency and making it difficult to set up consistent and custom policies.

Key compliance management tool features

To be effective, you need to define and apply contextual policies, keep systems in compliance, and rapidly create and manage reports for audits. Look for unified compliance management tools that:

Use analytics to consistently identify compliance risks in a time-efficient manner.

Automatically remediate noncompliant systems.

Provide a complete view of your compliance posture across your environment.

Automatically generate compliance reports according to your auditing requirements and audience needs.

Deliver expert advice and contextual guidance for remediating noncompliant systems across your environment.

[6] IBM Security. "Cost of a Data Breach Report 2023," 2023.

Best practices and tool recommendations

Analyze systems regularly

Daily monitoring can help you identify vulnerability and compliance risks before they interrupt business operations or result in a breach. Ensure you use the latest security data from your operating system and application vendors to improve analysis accuracy. And set up custom security policies tailored to your environment and operations to generate more accurate compliance results.

Finding and stopping a breach in

200 days

or less can significantly reduce its resulting cost.[7]

Patch often and test your patches

Keeping systems up to date can boost security, reliability, performance, and compliance. Apply patches regularly to keep pace with important issues in general. Apply patches for critical bugs and defects as soon as possible. Test patched systems for acceptance before placing them back into production.

An effective management tool can speed system patching.

Deploy automation

As the size and complexity of your infrastructure grows, it becomes harder to manage manually. Use automation to streamline monitoring, speed remediation, improve consistency, and ensure regular reporting.

Security automation and artificial intelligence (AI) can reduce data breach cost by

39.3%.[7]

[7] *IBM Security. "Cost of a Data Breach Report 2023." 2023.*

Connect your tools and align your processes

Distributed environments often contain different management tools for each platform. Integrate these tools via application programming interfaces (APIs) and use your preferred interfaces to perform tasks in other tools. Use a smaller number of interfaces to streamline operations and improve visibility into the security and compliance status of all systems in your environment. And align your processes across environments for increased consistency and reliability.

High levels of security system complexity can increase the average cost of a data breach by

31.6%.[9]

Adopt a consistent, continuous security strategy

Effective security requires a holistic approach that incorporates people, processes, and technology. A continuous security strategy relies on feedback and adaptation to support modern development techniques, DevSecOps, and digital business needs. Adopt a layered, defense-in-depth security approach to make the most of the capabilities of each layer in your environment, including operating systems, container platforms, automation tools, Software-as-a-Service (SaaS) assets, and cloud services.

Adopting DevSecOps approaches can reduce the average cost of a data breach by

38.4%.[9]

[9] IBM Security. "Cost of a Data Breach Report 2023," 2023.

Ideal security and compliance tools will include several key features and capabilities.

Proactive analysis

Understanding your security and compliance posture is the first step to improving it. Tools that provide automated analysis can ensure systems are monitored at regular intervals and alert you to issues without expending much staff time and effort.

Prioritized response

Tools that provide prescriptive remediation steps eliminate the need to research actions yourself, saving time and reducing the risk of mistakes. Prioritization of actions based on potential impact and systems affected helps you make the most of limited patching windows.

Customizable results

Some vulnerability and compliance checks may not apply to certain systems due to their use, configuration, or workload. Ideal tools will let you define business context to reduce false positives, manage risk, and provide a realistic view of your security and compliance status.

Intuitive reporting

Tools that generate clear, intuitive reports about which systems are patched, which need patching, and which are noncompliant with security policies increase auditability and help you gain a better understanding of the status of your environment.

Unified interface

Tools that go beyond managing a single component or layer of your environment can simplify security operations and gain a better understanding of your security and compliance posture. Unified tools can also provide increased context for scans and remediation guidance.

Actionable insight

Tools that provide information that is tailored to your environment can help you more quickly identify which potential security vulnerabilities and compliance issues are present, which systems are affected, and what potential impacts you can expect. These tools can also help you prioritize and plan remediation actions.

Boost security and compliance with Red Hat

Red Hat takes a holistic approach to security and compliance risk management that improves speed, scalability, and stability across your entire IT environment, from bare-metal and virtualized servers to private, public, and hybrid cloud infrastructure to edge deployments. By incorporating people, processes, and technology, Red Hat® platforms help you 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 and enterprise hybrid cloud deployments, Red Hat Enterprise Linux delivers optimal benefits for your organization. Consistency across infrastructure allows you 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 life cycle. Multilayer breach defenses use automated, repeatable security controls to mitigate your risk of exposure to vulnerabilities. Critical security upgrades and live patches—provided as part of your Red Hat Enterprise Linux subscription—help you keep your environment up to date and more secure.

> 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.[10]
>
> **Yuki Miyamoto**
> IT Infrastructure/Business Online Infrastructure System, Information Technology Division, Square Enix Co., Ltd.

[10] *Red Hat case study. "**Square Enix simplifies management of online gaming infrastructure**," May 2023.*

Red Hat management tools integrate with Red Hat Enterprise Linux to provide the capabilities you need to effectively manage security vulnerability risk and compliance.

Configurable tools and baselines reduce false positives and give you an accurate view of your infrastructure status.

Automation capabilities improve configuration and patching accuracy and reduce human errors.

Customizable views deliver the right information for the right audience at the right time, fast.

Automated and proactive remediation help you fix issues faster, without needing to contact support.

An extensive library of resources provides detailed, targeted information 24x7.

On-site and Software-as-a-Service (SaaS) options let you deploy tools according to your preference.

APIs connect with your existing and preferred security, compliance, and management tools and interfaces.

Vulnerability and malware detection capabilities scan systems for Common Vulnerabilities and Exposures (CVEs) and malware signatures.

Resource optimization capabilities help you right-size your public cloud deployments using compute, memory, and performance metrics.

Take advantage of integrated tools

Red Hat management tools are based on years of Linux development and support experience. They work together to streamline IT administration, saving your team time and effort and making your environment more security-focused, optimized, and reliable.

Analyze, observe, and manage Red Hat systems

Included with Red Hat Enterprise Linux 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 to help you better manage hybrid cloud environments. With Red Hat Lightspeed, you can monitor IT efficiency, stability, and performance; manage security and compliance risk; and track and optimize spending across clouds.

Learn more about Red Hat Lightspeed

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

Streamline and automate system management

Red Hat Satellite is an infrastructure management solution designed to provision and maintain Red Hat Enterprise Linux systems, wherever they reside—physical, virtual, cloud, or edge environments. Satellite streamlines provisioning, patching, and other repetitive system management tasks—at scale—to increase operational efficiency while maintaining system security, availability, and compliance with policies.

Learn more about Satellite

Adopting effective security vulnerability and compliance risk management approaches & tools can help you protect your organization.

See success in action

The Met Office

The Meteorological Office, the U.K.'s national weather service, provides weather- and climate-related services daily to people around the world. Seeking to establish a comprehensive approach to server management, the Met Office adopted Red Hat Lightspeed to complement its use of Red Hat Satellite. With the support of a Red Hat Technical Account Manager, the Met Office has now significantly improved visibility into its server environment.

The Met Office first started by testing Red Hat Lightspeed on several of their machines with known issues. The issues were surfaced immediately, and the IT team decided to move forward with wider deployment. The team used Satellite—in accordance with internal change management processes—to simplify installation of Red Hat Lightspeed across their entire estate.

Red Hat Lightspeed has made it more simple for the team to prioritize tasks, see if there are issues, and understand which systems are affected and how severity of the issue. It has also helped the Met Office bring their server estate to the desired standard by identifying and remediating configuration issues.

The Met Office plans to continue to use Red Hat Lightspeed and Satellite to manage their overall environment and improve their security posture in a more proactive manner.

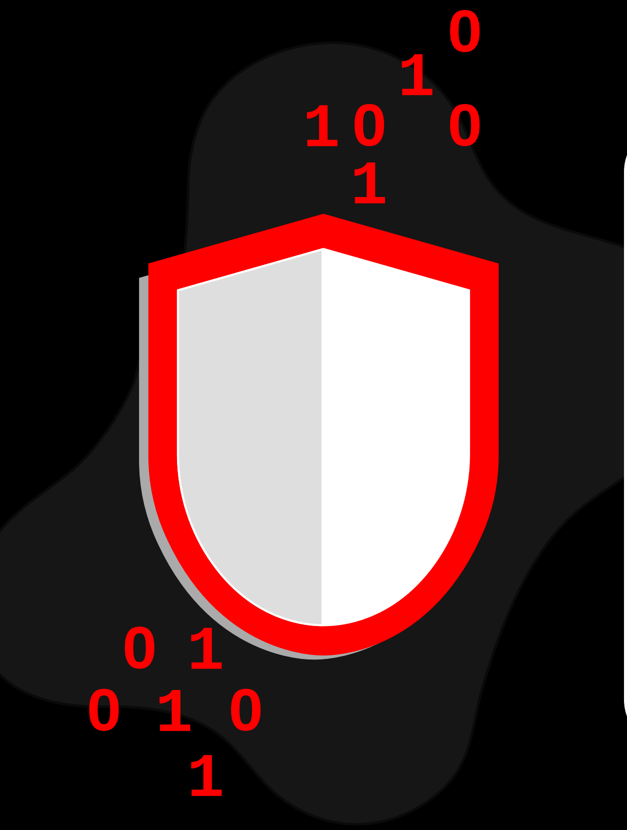
> I saw that Red Hat Lightspeed could help to provide a top-down overview and allow us to adopt a **more holistic approach to our estate management**. Red Hat Satellite does a great job at surfacing issues on individual machines, whereas Red Hat Lightspeed ties in common issues across the estate rather than treating it on a machine-by-machine basis.
>
> Senior Systems Engineer,
> The Meteorological Office, U.K.

Read the success story

Ready to get started?

Your business relies on your IT infrastructure and applications. Adopting effective security vulnerability and compliance risk management approaches and tools can help you protect your organization.

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



Analyze your risk with Red Hat Lightspeed

- **Learn** about Red Hat Lightspeed
- **See what analysts are saying** about Red Hat Lightspeed

Manage at scale with Red Hat Satellite

- **Learn** about Red Hat Satellite
- **See what analysts are saying** about Red Hat Satellite

Red Hat