Improve security and compliance

Reduce risk with a robust, open source Linux platform

Red Hat

See what's inside

Linux is the foundation for the future

Linux® is one of the world's most dominant operating systems, with widespread adoption across industries and emerging technologies.[1] 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 impact 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 key IT concerns

Managing IT security and compliance risk is an ongoing concern for all organizations. In fact, 33% of CEOs consider cyber attacks to be a top threat to their organization's growth prospects.[2] And security breaches can be costly. The average cost of a data breach is US$3.86 million.[3]

Industry and government regulations are also changing. Keeping up can be challenging and compliance failures increase the cost of a data breach by around 6% on average.[3]

Common security and compliance challenges

Several factors make security vulnerability and compliance management challenging.

Impacts of ineffective security

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

US$3.86 million
average cost of a data breach in 2020[3]

280 days
average time to identify and contain a data breach in 2020[3]

US$1.12 million
savings in costs if a breach can be identified and contained in 200 days or less[3]

Changing security and compliance landscapes

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

Distributed hybrid and multicloud environments

Geographically and logically distributed environments can prevent you from gaining a complete view into your IT.

Large and complex environments

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

Limited staff and remote work directives

Most organizations lack the staff headcount needed to manage security and compliance tasks manually.

1 *The Linux Foundation.* "**Linux is the most successful open source project in history**," *Accessed 24 September 2020.*

2 *PWC.* "**23rd Annual Global CEO Survey: Navigating the rising tide of uncertainty**," *2020.*

3 *IBM Security.* "**Cost of a Data Breach Report 2020**," *2020.*

Adopt an effective security and compliance risk 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. Easily 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
Quickly and easily patch and reconfigure all systems that require action. 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 get to a state where you can remediate issues rapidly, improving the security of your environment and business.

Report
Validate that changes were applied and automate remediation reporting to streamline auditing efforts. 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**. In fact, 38% of organizations consider vulnerability assessment to be the most critical security element in their DevOps workflow.[4]

The following sections discuss key considerations and actions to more effectively manage your security and compliance risk.

4 451 Research, part of S&P Global Market Intelligence – Voice of the Enterprise, DevOps H2 2019.

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 39.4% 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.

Key security management tool features

To be most 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.

5 *IBM Security. "Cost of a Data Breach Report 2020," 2020.*

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 application of policies, 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 most effective, you must be able to define and apply contextual policies, keep systems in compliance with those policies, and rapidly generate and manage compliance 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 2020," 2020.*

Best practices

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 patch management tool can help you patch systems up to **88.9% faster**.[8]

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 can reduce the average cost of a breach by **93%**.[7]

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.

52% of organizations are optimizing their IT infrastructure and processes to improve security.[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 a DevSecOps approach can reduce the average cost of a data breach by **5%**.[7]

7 IBM Security. "Cost of a Data Breach Report 2020," 2020.

8 Principled Technologies, sponsored by Red Hat. "Save administrator time and effort by activating Red Hat Insights to automate monitoring," September 2020.

9 Qualtrics and Red Hat. IT optimization study, February 2020.

Tool recommendations

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

Proactive analysis

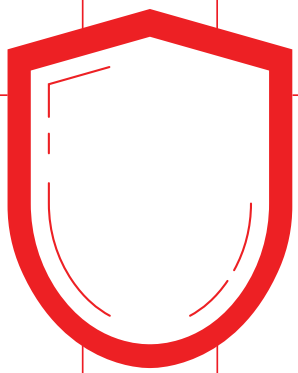
Understanding your security and compliance posture is the first step to improving it. Tools that provide automated analysis can ensure systems are monitored at regular intervals and alert you to issues without expending much staff time and effort.

Prioritized remediation

Tools that provide prescriptive remediation instructions 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 help you make the most of limited patching windows.

Customizable results

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



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 help you 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. 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. Multi-layer 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.

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 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.

"Building servers that are tuned, ready-to-go and more secure from day one is a key need for our IT organization. Red Hat Enterprise Linux with Red Hat Insights gives us this capacity, enabling us to deploy servers that are immediately usable and meet our specific needs as they go live."[10]

Steve Short
Platforms Manager, Unix, Kingfisher PLC

10 *Red Hat press release. "**Red Hat Delivers Force Multiplier for Enterprise IT with Enhanced Intelligent Monitoring, Unveils Latest Version of Red Hat Enterprise Linux 8**," 21 April 2020.*

Take advantage of integrated management 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 secure, optimized, and reliable.

Red Hat Insights

Predictive IT risk analytics

Included with all active Red Hat Enterprise Linux subscriptions, **Red Hat Insights** helps IT teams proactively identify and remediate a variety of threats to avoid outages, unplanned downtime, and risks to security and compliance.

- Deeply analyze systems to proactively detect security vulnerabilities, compliance issues, and policy violations.
- Prescribe and prioritize remediation actions and generate Red Hat Ansible® Automation Platform Playbooks to help.
- Compare systems to baselines, histories, and other systems.
- Easily deploy across on-site and cloud environments.

96% faster detection of app-specific issues.[11]

91% faster security vulnerability identification.[11]

89% faster detection of configuration drift.[11]

Learn more

Red Hat Smart Management

Actionable management and remediation

Red Hat Smart Management combines the powerful infrastructure capabilities of Red Hat Satellite with the simplicity of management from the cloud to enhance and complement the capabilities of Red Hat Insights.

- Patch, provision, and control your Red Hat Enterprise Linux hosts and generate detailed reports using Red Hat Satellite.
- Identify and remediate issues via cloud.redhat.com in conjunction with Red Hat Insights.
- Remediate issues identified by Red Hat Insights with the push of a button through Cloud Connector.

56% more efficient system patching.[12]

14% more efficient IT security teams.[12]

23% more productive compliance teams.[12]

Learn more

11 *Principled Technologies, sponsored by Red Hat. "**Save administrator time and effort by activating Red Hat Insights to automate monitoring**," September 2020.*

12 *IDC White Paper, sponsored by Red Hat. "**Red Hat Satellite Helps Enterprise Organizations Optimize Infrastructure with Automation Tools**," March 2020. Document #US46109220.*

Customer success highlight

Metalloinvest

Ensure critical system performance using data insights and predictive risk analytics

Challenge

Metalloinvest is a leading global producer and supplier of hot-briquetted iron (HBI) and iron ore products, and a regional producer of high quality steel. After decades of operations, Metalloinvest faced a new challenge: Industry 4.0, the manufacturing industry's shift toward automated, data-centric operations. By automating and digitizing production, the company aims to operate and use resources more efficiently. Its goal is to become not only the biggest mining company in the world, but also the most productive. To create a foundation for Industry 4.0, the company sought to integrate and optimize its complex SAP® environment.

Solution

With help from its managed services provider, JSA-Group, Metalloinvest adopted Red Hat Enterprise Linux for SAP Solutions to create a robust, enterprise foundation for its SAP S/4HANA® environment. Co-engineered by **Red Hat and SAP**, Red Hat Enterprise Linux for SAP Solutions includes Red Hat Insights for predictive data analytics and Red Hat Smart Management to simplify management of Red Hat Enterprise Linux environments through Red Hat Satellite and cloud management services. This single subscription combines the reliability, scalability, and high performance capabilities of Linux with technology that meets the specific requirements of SAP applications.

Metalloinvest now runs its entire SAP S/4HANA production environment on Red Hat Enterprise Linux for SAP Solutions. The company can take advantage of comprehensive data insight and predictive risk analytics to ensure reliable, stable performance across its critical systems as it prepares to digitize its production environment.

"With Red Hat we have the tools to make our people and our operations more productive."

Konstantin Zelenkov
Chief Technology Officer, JSA Group

Improved reliability and performance for critical operational systems

Gained comprehensive data insight with better SAP integration

Reduced risk with security management and comprehensive support

Read the success story

Ready to boost your security and compliance?

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 Linux platform and integrated management tools needed for security-focused operations and innovation.

Get your team started with Red Hat Insights:

redhat.com/insights

See how you can speed IT workflows with Red Hat Insights:

red.ht/insights_savetime

Read the Manage security risks with Red Hat Insights brief:

red.ht/insights-security-brief

Watch the Red Hat Insights risk management demo:

red.ht/insights-security-demo

F26049_1120_KVM

Red Hat