



# Renforcer le niveau de sécurité et de conformité

Réduisez les risques grâce à une plateforme Linux  
Open Source et robuste

# Sommaire

**1** Linux, une base solide pour l'avenir

**2** Adopter une approche efficace en matière de sécurité et de conformité

**2.1** Identification et correction des vulnérabilités dans les environnements Linux

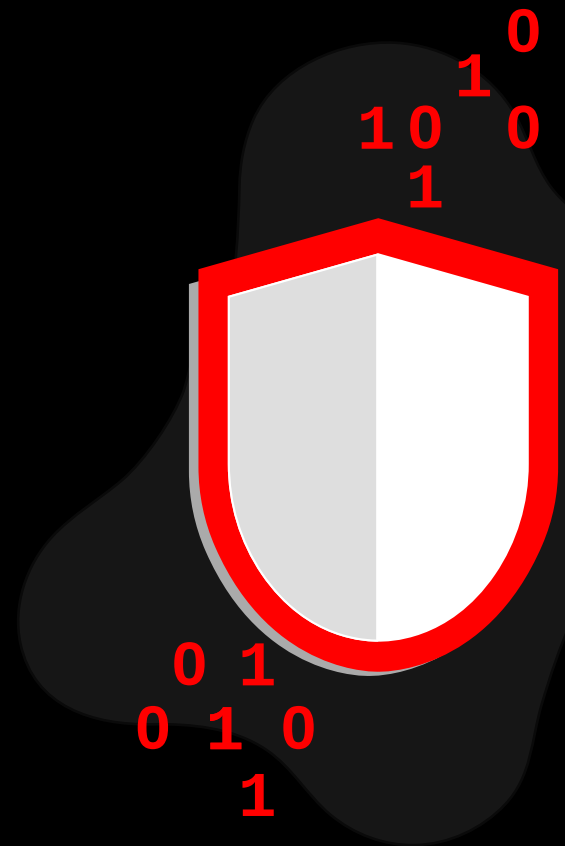
**2.2** Gestion de la conformité dans les environnements Linux

**3** Meilleures pratiques et recommandations d'outils

**4** Davantage de sécurité et de conformité avec les solutions Red Hat

**5** Réussites de clients : Met Office

**6** Vous souhaitez vous lancer ?



# Linux, une base solide pour l'avenir



Linux® est l'un des systèmes d'exploitation les plus répandus au monde, ce qui en fait une plateforme idéale pour l'informatique moderne et innovante. Couramment utilisé pour les charges de travail essentielles, fiables et à haute disponibilité, dans les datacenters et environnements de cloud computing, il prend en charge divers cas d'utilisation, systèmes cibles et appareils. Tous les principaux fournisseurs de cloud public incluent plusieurs distributions Linux dans leur offre.

Cependant, la distribution Linux et les outils de gestion que vous choisissez peuvent avoir une influence considérable sur l'efficacité, la sécurité et l'interopérabilité de votre environnement informatique. Ce livre numérique passe en revue les éléments à prendre en compte et fournit des conseils utiles pour réduire la vulnérabilité des environnements Linux et les risques liés à la conformité.

## Sécurité et conformité : deux préoccupations majeures

Les entreprises sont constamment préoccupées par la gestion des risques liés à la sécurité informatique et à la conformité. En effet, 23 % d'entre elles ont été victimes d'une cyberattaque majeure au cours des deux dernières années<sup>1</sup>. Or, les failles de sécurité peuvent se révéler coûteuses : environ 4,45 millions de dollars en moyenne pour une fuite de données<sup>2</sup>.

Les réglementations sectorielles et gouvernementales sont également en pleine évolution. Il est parfois difficile de suivre le rythme de ces changements, et le non-respect des règles de conformité augmente le coût d'une fuite de données de 5 % en moyenne<sup>2</sup>.

### Se prémunir contre les conséquences d'une stratégie de sécurité inefficace

Pour réduire les risques et les effets des vulnérabilités, il est essentiel d'agir rapidement.

## 4,45 millions \$

Coût total moyen (en USD) d'une fuite de données en 2023<sup>2</sup>

## 277 jours

Temps moyen nécessaire pour identifier et maîtriser une fuite de données en 2023<sup>2</sup>

## 1,02 million \$

Montant moyen économisé si la faille peut être identifiée et corrigée en 200 jours ou moins<sup>2</sup>

<sup>1</sup> Nash Squared, « 2023 Nash Squared Digital Leadership Report », novembre 2023

<sup>2</sup> IBM Security, « Rapport 2023 sur le coût d'une violation de données », 2023

## Défis courants liés à la sécurité et à la conformité

Différents facteurs compliquent la gestion des vulnérabilités et de la conformité.

### Évolution des exigences en matière de sécurité et de conformité

Les menaces évoluent rapidement, ce qui nécessite une adaptation rapide pour suivre le rythme des nouvelles menaces et réglementations.

**23 %**

des entreprises, toutes tailles confondues, ont été victimes d'une cyberattaque majeure au cours des deux dernières années<sup>3</sup>.

**82 %**

des fuites en 2023 concernaient des données stockées dans des environnements cloud ou dans plusieurs environnements<sup>4</sup>.

### Environnements cloud distribués

Les environnements de cloud hybride et multicloud distribués géographiquement et logiquement peuvent vous empêcher d'avoir une vue complète de votre infrastructure informatique, ce qui complique la gestion de configurations cohérentes sur l'ensemble des systèmes.

### Environnements vastes et complexes

Les infrastructures vastes intègrent souvent de multiples outils de sécurité et de conformité, ce qui complique la gestion des risques.

La complexité des systèmes de sécurité augmente le coût des fuites de données de

**240 889 dollars<sup>4</sup>**.

Le recours au télétravail augmente le coût moyen d'une fuite de données de

**173 074 dollars**

par rapport à une fuite dans un environnement sans télétravail<sup>4</sup>.

### Personnel limité et travail à distance

La plupart des entreprises ne disposent pas du personnel nécessaire pour gérer manuellement les tâches liées à la sécurité et à la conformité. Le télétravail peut également accroître la charge de travail liée à la protection des appareils et des points d'accès aux ressources numériques d'une entreprise.

<sup>3</sup> Nash Squared, « 2023 Nash Squared Digital Leadership Report », novembre 2023

<sup>4</sup> IBM Security, « Rapport 2023 sur le coût d'une violation de données », 2023

# Adopter une approche efficace en matière de gestion de la sécurité et de la conformité

La gestion des vulnérabilités et de la conformité consiste à surveiller et évaluer les systèmes pour s'assurer qu'ils restent conformes aux politiques de sécurité et de réglementation. Avec une approche adaptée, vous pourrez développer des processus cohérents et reproductibles dans l'ensemble de votre environnement pour effectuer les tâches suivantes :



## Évaluer

Identifiez les systèmes non conformes ou vulnérables. Évaluez l'état réel de la sécurité de votre environnement, de l'infrastructure aux charges de travail. Identifiez les avis de sécurité réellement applicables à vos systèmes et à votre environnement.



## Établir les priorités

Organisez les mesures de correction en fonction des efforts à fournir, des effets et de la sévérité du problème. Appliquez des techniques de gestion des risques pour déterminer le risque métier réel de chaque problème et planifier les corrections en conséquence. Les risques englobent la probabilité qu'un problème entraîne une fuite, la gravité potentielle d'une fuite et les conséquences de la résolution du problème. Si la correction d'un problème donné peut sembler inutile sur les systèmes de développement et de test, elle peut en revanche être une priorité sur les systèmes de production.



## Corriger

Appliquez les correctifs et reconfigurez rapidement les systèmes non conformes. Automatisez les processus de configuration et d'application des correctifs pour accélérer la correction, assurer la cohérence entre les systèmes et réduire le risque d'erreur humaine. Bien utilisés, les outils automatisés peuvent accélérer la résolution des problèmes, et ainsi renforcer la sécurité de votre environnement et de votre entreprise.



## Générer des rapports

Confirmez la bonne application des changements et automatisez les rapports afin de rationaliser les audits. Avec un système de rapport efficace, les dirigeants, auditeurs et équipes techniques obtiennent des informations suffisamment détaillées pour comprendre les risques et vulnérabilités actuels.

Cette approche permet également à l'entreprise de se préparer à l'adoption de techniques de développement et de gestion modernes et rapides telles que le **DevSecOps**. Dans les sections suivantes, nous verrons les principales considérations à prendre en compte et les actions nécessaires pour gérer plus efficacement les risques liés à la sécurité et à la conformité.

# Identification et correction des vulnérabilités dans les environnements Linux

L'identification et la correction des vulnérabilités correspondent au processus d'évaluation des infrastructures qui permet de détecter et réparer les systèmes vulnérables aux attaques. Ces vulnérabilités peuvent être causées par des menaces émergentes, des correctifs obsolètes ou manquants, ou une mauvaise configuration du système. Les mesures de correction comprennent souvent l'application de correctifs ainsi que la mise à jour et la reconfiguration des systèmes.

## Pourquoi est-ce important ?

Les vulnérabilités peuvent entraîner des fuites qui coûtent cher à l'entreprise, et qui risquent d'ébranler la confiance de ses clients, de nuire à sa réputation et de réduire son chiffre d'affaires. En effet, la perte d'activité représente 29,2 % du coût moyen d'une fuite de données<sup>5</sup>.

## Les problèmes liés à l'identification et à la correction efficaces des vulnérabilités

La plupart des entreprises n'ont pas de stratégie de sécurité cohérente pour leur exploitation à grande échelle.

- ▶ Souvent, les effectifs sont insuffisants et le personnel, déjà débordé, n'est pas qualifié pour élaborer et exécuter une stratégie de sécurité complète.
- ▶ Les outils génériques d'analyse de sécurité produisent de longues listes de vulnérabilités potentielles qui ne sont pas toutes applicables à votre environnement. Le personnel est alors obligé de passer beaucoup de temps à enquêter sur ces vulnérabilités et à prendre les mesures de correction qui s'imposent.
- ▶ Les processus manuels d'identification, de correction et de suivi ralentissent l'exploitation et souvent, les vulnérabilités connues ne sont pas corrigées.
- ▶ Les méthodes de correction ad hoc entraînent une application incohérente des correctifs et une augmentation des risques pour la sécurité.

## Les principales fonctions des outils de gestion de la sécurité

Pour assurer l'efficacité, vous devez identifier et corriger rapidement les vulnérabilités du système avant qu'elles n'entraînent une fuite. Pour ce faire, optez pour des outils de gestion unifiée de la sécurité qui incluent les fonctions suivantes :



**Analyse des systèmes**, pour identifier les risques (tant au niveau du système d'exploitation que des charges de travail) dans les systèmes et instances de votre environnement



**Automatisation de la correction** des risques identifiés, afin d'améliorer la rapidité, la précision et l'efficacité des équipes informatiques et de sécurité



**Expertise des fournisseurs** et conseils sur les mesures de correction à appliquer aux produits ; il existe peut-être des mesures simples pour réduire les risques



**Accès régulier aux données les plus récentes** que vos fournisseurs de système d'exploitation et d'applications publient sur les vulnérabilités et risques de sécurité connus



**Production de rapports** sur les risques potentiels, les mesures de correction et les audits, adaptés à différents profils de lecteurs

## Gestion de la conformité dans les environnements Linux

La gestion de la conformité consiste à s'assurer que les systèmes restent toujours conformes aux politiques de l'entreprise, aux normes du secteur et aux réglementations applicables. Les infrastructures doivent également être contrôlées afin d'identifier les systèmes non conformes suite aux changements apportés aux réglementations, politiques ou normes, à une erreur de configuration ou pour d'autres raisons.

## Pourquoi est-ce important ?

Le non-respect des règles de conformité peut nuire à votre entreprise et entraîner des amendes, la perte d'une certification ainsi que des failles du système de sécurité. En moyenne, le coût d'une fuite de données est plus élevé en cas de défaut de conformité<sup>6</sup>.

## Les problèmes liés à la gestion efficace de la conformité

De nombreuses entreprises gèrent la conformité à l'aide d'opérations manuelles et de scripts personnalisés. Ces processus sont toutefois trop lents et trop limités pour un développement et une exploitation modernes et rapides.

- ▶ Il est difficile de comprendre la pertinence et les effets de la gestion sur l'environnement en raison du nombre élevé de normes génériques et de références.
- ▶ Les processus manuels ralentissent les opérations de contrôle de la conformité, de correction et d'audit, ce qui entraîne une utilisation inefficace du personnel, une application incohérente des politiques et un risque accru de problèmes de conformité.
- ▶ Beaucoup d'entreprises utilisent des outils différents pour la gestion de la sécurité et de la conformité, ce qui réduit l'efficacité opérationnelle et complique la mise en place de politiques cohérentes et personnalisées.

## Les principales fonctions des outils de gestion de la conformité

Pour être efficace, vous devez définir et appliquer des politiques contextuelles, assurer la conformité des systèmes ainsi que générer et gérer rapidement des rapports pour les audits. Pour ce faire, optez pour des outils de gestion unifiée de la conformité qui incluent les fonctions suivantes :



**Analyses** pour identifier de manière cohérente et rapide les risques de non-conformité



**Correction automatique** des systèmes non conformes



**Vue complète** du niveau de conformité dans tout l'environnement



**Création automatique de rapports de conformité** en fonction de vos exigences en matière d'audit et des besoins des lecteurs



**Avis de spécialistes** et conseils contextuels pour corriger les systèmes non conformes de votre environnement

# Meilleures pratiques et recommandations d'outils

## Analysez régulièrement vos systèmes

Une surveillance quotidienne peut vous aider à identifier les risques de vulnérabilité et de conformité avant qu'un problème n'interrompe l'exploitation ou n'entraîne une fuite. Assurez-vous d'utiliser les données de sécurité les plus récentes publiées par vos fournisseurs de système d'exploitation et d'applications pour améliorer la précision des analyses. Enfin, mettez en place des politiques de sécurité personnalisées et adaptées à votre environnement et à votre exploitation pour optimiser la conformité.

Il est possible de réduire considérablement le coût d'une faille si elle est identifiée et corrigée en

**200 jours**

ou moins<sup>7</sup>.

## Appliquez et testez régulièrement vos correctifs

La mise à jour régulière des systèmes renforce la sécurité, la fiabilité, les performances et la conformité. Appliquez régulièrement les correctifs disponibles pour éliminer immédiatement les problèmes importants. Appliquez dès que possible les correctifs pour traiter les bogues et failles critiques. Testez les systèmes après l'installation des correctifs pour vérifier leur état de fonctionnement avant de les remettre en production.

Un outil de gestion efficace peut accélérer l'application des correctifs aux systèmes jusqu'à

**56 %**<sup>8</sup>.

## Déployez l'automatisation

Plus la taille et la complexité de votre infrastructure augmentent, plus il est difficile de la gérer manuellement. Tirez parti de l'automatisation pour rationaliser la surveillance, accélérer l'application des mesures de correction, améliorer la cohérence et assurer la régularité des rapports.

L'automatisation de la sécurité et l'intelligence artificielle (IA) peuvent réduire le coût des fuites de données de

**39,3 %**<sup>7</sup>.

<sup>7</sup> IBM Security, « [Rapport 2023 sur le coût d'une violation de données](#) », 2023

<sup>8</sup> Livre blanc d'IDC commissionné par Red Hat, « [Red Hat Satellite Helps Enterprise Organizations Optimize Infrastructure with Automation Tools](#) », document n° US46109220 août 2021

## Connectez vos outils et harmonisez vos processus

En général, les environnements distribués incluent des outils de gestion différents pour chaque plateforme. Intégrez ces outils via des API et utilisez vos interfaces favorites pour effectuer des tâches dans d'autres outils. Réduisez le nombre d'interfaces pour rationaliser l'exploitation et bénéficier d'une meilleure visibilité sur la sécurité et l'état de conformité de tous les systèmes de votre environnement. Harmonisez aussi les processus de vos différents environnements pour renforcer la cohérence et la fiabilité.

La grande complexité des systèmes de sécurité peut augmenter le coût moyen d'une fuite de données de

**31,6 %<sup>9</sup>**.

## Adoptez une stratégie de sécurité cohérente et continue

Un dispositif de sécurité efficace nécessite une démarche globale qui implique à la fois les individus, les processus et les technologies. Pour assurer la sécurité en continu, il faut s'appuyer sur les retours d'expérience et sans cesse adapter les systèmes afin de prendre en compte les techniques de développement modernes, les pratiques DevSecOps et les besoins des entreprises numériques. Adoptez une approche de défense en profondeur qui utilise les capacités de chaque couche de votre environnement, y compris les systèmes d'exploitation, les plateformes de conteneurs, les outils d'automatisation, les ressources SaaS et les services cloud.

L'adoption d'approches DevSecOps permet de réduire le coût moyen d'une fuite de données de

**38,4 %<sup>9</sup>**.



Les outils de sécurité et de conformité à privilégier incluent plusieurs fonctions et capacités essentielles.

### **Analyses proactives**

Pour améliorer vos niveaux de sécurité et de conformité, commencez par mieux les comprendre. Optez pour des outils qui fournissent des analyses automatisées, assurent une surveillance régulière des systèmes et vous alertent en cas de problème, sans trop mobiliser le temps et l'énergie de vos équipes.



### **Réponse hiérarchisée**

Les outils qui offrent des solutions de correction normatives vous évitent d'avoir à chercher vous-même les mesures à appliquer, ce qui représente un gain de temps et réduit le risque d'erreurs. Les créneaux pour l'application des correctifs sont limités, et la hiérarchisation des mesures en fonction des potentielles conséquences et des systèmes affectés permet d'optimiser leur utilisation.

### **Résultats personnalisables**

Certains contrôles de vulnérabilité et de conformité ne s'appliquent pas forcément à certains systèmes en raison de leur utilisation, configuration ou charge de travail. Dans l'idéal, optez pour des outils qui vous permettent de définir un contexte métier afin de réduire le nombre de faux positifs, de gérer les risques et de fournir une vue réaliste de l'état de la sécurité et de la conformité.

### **Rapports lisibles**

Les outils qui génèrent des rapports clairs et lisibles sur les systèmes à jour, ceux qui nécessitent un correctif et ceux qui ne sont pas conformes aux politiques de sécurité augmentent l'auditabilité et vous permettent de mieux comprendre l'état de votre environnement.

### **Interface unifiée**

Les outils qui vont au-delà de la gestion d'un seul composant ou d'une seule couche de votre environnement simplifient les opérations de sécurité et permettent de mieux comprendre le niveau de sécurité et de conformité dans l'entreprise. Les outils unifiés peuvent également fournir un contexte amélioré pour les analyses et conseils de correction.



### **Données exploitables**

Les outils qui fournissent des informations adaptées à votre environnement vous aident à identifier plus rapidement les problèmes de conformité et les vulnérabilités, les systèmes affectés et les conséquences potentielles sur votre activité. Ils permettent également de hiérarchiser et planifier les mesures de correction.

# Davantage de sécurité et de conformité avec les solutions Red Hat

Red Hat suit une approche globale en matière de gestion des risques liés à la sécurité et à la conformité, qui augmente la rapidité, l'évolutivité et la stabilité dans l'ensemble de l'environnement informatique, des serveurs bare metal et virtuels aux infrastructures de cloud public, privé ou hybride, jusqu'aux déploiements d'edge computing. Les solutions Red Hat® impliquent à la fois les individus, les processus et les technologies pour optimiser l'efficacité opérationnelle, stimuler l'innovation et améliorer la satisfaction des salariés.

La plateforme **Red Hat Enterprise Linux** se trouve au cœur de cette stratégie. Base d'exploitation stable et intelligente pour l'informatique moderne et les déploiements de cloud hybride d'entreprise, elle offre un avantage optimal à votre entreprise. D'une efficacité constante sur toutes les infrastructures, elle vous permet de déployer des applications, des charges de travail et des services en utilisant les mêmes outils, quel que soit votre environnement.

La sécurité est un élément clé de l'architecture et du cycle de vie de la plateforme Red Hat Enterprise Linux. Les systèmes multicouches de défense contre les fuites utilisent des contrôles de sécurité automatisés et reproductibles pour réduire le risque d'exposition aux vulnérabilités. Les mises à niveau de sécurité essentielles et les correctifs en direct sont inclus dans votre souscription Red Hat Enterprise Linux et vous aident à maintenir votre environnement à jour et sécurisé.

66

Depuis notre passage à Red Hat Enterprise Linux, nous avons **observé une accélération de la détection et de l'analyse des bogues et vulnérabilités**<sup>10</sup>.

—  
Yuki Miyamoto

Infrastructure informatique/Système d'infrastructure en ligne, division Technologies de l'information, Square Enix Co., Ltd.

Les outils de gestion de Red Hat s'intègrent à Red Hat Enterprise Linux afin de vous fournir les fonctionnalités dont vous avez besoin pour gérer efficacement les risques de vulnérabilités et la conformité.



Les outils et références configurables réduisent le nombre de faux positifs et vous donnent une vue précise de l'état de vos infrastructures.



Les fonctionnalités d'automatisation améliorent la précision de la configuration et des correctifs tout en réduisant les erreurs humaines.



Les vues personnalisables fournissent rapidement des informations pertinentes aux bons utilisateurs.



Les mesures de correction automatisées et proactives accélèrent la résolution des problèmes, sans recourir au service d'assistance.



Une vaste bibliothèque de ressources fournit des informations détaillées et ciblées 24 heures sur 24, 7 jours sur 7.



Les options sur site et SaaS vous permettent de déployer les outils selon vos préférences.



Les API se connectent aux outils et interfaces de sécurité, conformité et gestion dont vous disposez déjà et que vous connaissez bien.



Les capacités de détection des vulnérabilités et des logiciels malveillants analysent les systèmes à la recherche de CVE (Common Vulnerabilities and Exposures) et de signatures de logiciels malveillants.



L'optimisation des ressources vous aide à dimensionner correctement vos déploiements de cloud public sur la base d'indicateurs de calcul, de mémoire et de performances.

# Outils intégrés

Les outils de gestion Red Hat reposent sur des années d'expérience en matière de développement Linux et d'assistance. Ils fonctionnent ensemble pour rationaliser l'administration informatique, ce qui permet à votre équipe d'éviter les pertes de temps et les dépenses d'énergie inutiles, et améliore la sécurité, l'efficacité et la fiabilité de votre environnement.



## Analyse, observation et gestion des systèmes Red Hat

Incluse avec la plateforme Red Hat Enterprise Linux et fournie en tant que service, la solution **Red Hat Insights** analyse en permanence les plateformes et applications pour prévoir les risques, recommander des actions et suivre les coûts, de manière à faciliter la gestion des environnements de cloud hybride. Grâce à Insights, vous pouvez contrôler l'efficacité, la stabilité et les performances, gérer les risques liés à la sécurité et à la conformité, ainsi que suivre et optimiser les dépenses dans les différents clouds.

**26 %** d'accélération de la résolution des incidents de sécurité<sup>11</sup>

**24 %** de hausse d'efficacité des équipes chargées de la sécurité informatique<sup>11</sup>

**76 %** de temps d'arrêt non planifiés en moins<sup>11</sup>



## Rationalisation et automatisation de la gestion du système

**Red Hat Satellite** est une solution de gestion d'infrastructure pensée pour le provisionnement et la maintenance des systèmes Red Hat Enterprise Linux, quel que soit leur environnement : physique, virtuel, dans le cloud ou en périphérie. Elle rationalise le provisionnement, l'application de correctifs et d'autres tâches répétitives de gestion des systèmes à grande échelle. Cette solution accroît ainsi l'efficacité de l'exploitation tout en assurant la sécurité et la disponibilité des systèmes ainsi que la conformité aux politiques.

**56 %** de gain d'efficacité lors de l'application des correctifs<sup>12</sup>

**56 %** de gain d'efficacité de l'infrastructure informatique<sup>12</sup>

**28 %** de réduction des coûts totaux d'exploitation<sup>12</sup>

<sup>11</sup> Aperçu d'IDC sur la valeur métier, commissionné par Red Hat, « **La valeur métier de Red Hat Insights** », document n° US51795124, février 2024

<sup>12</sup> Livre blanc d'IDC commissionné par Red Hat, « **Red Hat Satellite Helps Enterprise Organizations Optimize Infrastructure with Automation Tools** », document n° US46109220 août 2021

## Découvrez les réussites de clients

# Met Office

Le Meteorological Office, le service météorologique national du Royaume-Uni, fournit quotidiennement des services liés à la météo et aux conditions climatiques à des personnes situées dans le monde entier. Soucieux d'établir une approche globale de la gestion des serveurs, le Met Office a adopté la solution Red Hat Insights en complément de Red Hat Satellite. Avec l'aide d'un responsable de compte technique Red Hat, ce service a considérablement amélioré sa visibilité sur son environnement de serveurs.

Dans un premier temps, il a testé Red Hat Insights sur plusieurs de ses machines qui présentaient des problèmes connus. Ceux-ci ont été immédiatement détectés, ce qui a convaincu l'équipe informatique de procéder à un déploiement à plus grande échelle. L'équipe s'est appuyée sur Red Hat Satellite, conformément aux processus internes de gestion du changement, pour simplifier l'installation d'Insights dans l'ensemble de ses systèmes.

Insights a considérablement simplifié la hiérarchisation des tâches, la détection des problèmes et la compréhension de leur gravité ainsi que l'identification des systèmes concernés. Cette solution a également aidé le Met Office à optimiser son parc de serveurs en identifiant les problèmes de configuration et en les corrigeant.

Le service de météorologie entend continuer à utiliser les deux solutions Red Hat pour gérer l'ensemble de son environnement et renforcer sa posture de sécurité d'une manière plus proactive.

”

J'ai compris que Red Hat Insights pouvait nous offrir une vue d'ensemble et nous permettre d'adopter une **approche plus holistique de la gestion de nos systèmes**. La solution Red Hat Satellite détecte parfaitement les problèmes sur chaque machine, alors que la force de Red Hat Insight réside dans sa capacité à traiter les problèmes communs sur l'ensemble des systèmes, au lieu de procéder machine par machine.

—  
**Chris Wilkinson**

Ingénieur système senior,  
Meteorological Office, Royaume-Uni.

# Vous souhaitez vous lancer ?

Votre entreprise dépend de votre infrastructure informatique et de vos applications. En adoptant des approches et outils efficaces de gestion des vulnérabilités et des risques liés à la conformité, vous protégez votre entreprise.

Nous proposons une plateforme Linux de confiance qui intègre les outils et services de gestion nécessaires pour assurer la sécurité de l'exploitation et des innovations.



## Analyse des risques à l'aide de Red Hat Insights

- ▶ [En savoir plus](#) sur Red Hat Insights
- ▶ [Rapport d'analyste](#) sur Red Hat Insights

## Gestion à grande échelle à l'aide de Red Hat Satellite

- ▶ [En savoir plus](#) sur Red Hat Satellite
- ▶ [Rapport d'analyste](#) sur Red Hat Satellite