Sécurité et conformité de Red Hat Enterprise Linux

Une base fiable pour l'exécution de vos charges de travail dans le cloud hybride

Grâce à Red Hat Enterprise Linux, assurez la sécurité et la conformité de votre infrastructure informatique et préparez-la pour les audits. Ce système d'exploitation répond aux principales exigences de sécurité et de conformité :

- Capacités de sécurité modernes et multicouches pour réduire les risques
- Application automatisée des correctifs et mesures de correction pour minimiser les temps d'arrêt
- Sécurisation des processus et de la validation des cycles de vie de développement
- Outils de mise en conformité intégrés pour répondre aux normes de sécurité
- Contrôles de sécurité cohérents dans l'ensemble du cloud hybride
- Sécurité des charges de travail dans les environnements de cloud public

La clé : sécuriser le système d'exploitation

Les failles de sécurité sont de plus en plus nombreuses et sophistiquées, c'est pourquoi il est essentiel d'intégrer des fonctionnalités de sécurité dans l'ensemble de l'infrastructure. Les systèmes d'exploitation (la base sur laquelle s'exécutent les applications) ont besoin de fonctionnalités de sécurité étendues et approfondies pour se protéger contre les vulnérabilités et répondre aux exigences de conformité.

La solution Red Hat® Enterprise Linux® fournit une base de sécurité fiable sur laquelle vous pouvez faire évoluer vos applications et déployer des technologies émergentes de manière cohérente, que ce soit sur des systèmes bare metal, dans des environnements virtuels, dans le cloud ou en périphérie du réseau. Ses capacités de sécurité et de mise en conformité vous aident de plusieurs manières :

- **Atténuer les risques :** gérez la sécurité et réduisez les risques de faille avant que vos données, vos systèmes ou votre réputation ne soient atteints.
- **Sécuriser les systèmes :** automatisez les contrôles de sécurité et maintenez-les dans la durée, à grande échelle, en évitant autant que possible les temps d'arrêt.
- **Garantir la conformité :** rationalisez les normes de conformité dans les environnements fortement réglementés.

Réduire les risques pour les données, les systèmes et la réputation

Mises à niveau et correctifs de sécurité critiques : améliorez la disponibilité et la résilience grâce à des correctifs du noyau en temps réel et la résolution des vulnérabilités de sécurité. Résolvez rapidement les problèmes de sécurité majeurs sans redémarrage, afin de garantir la disponibilité des applications critiques.

Listes d'autorisations pour les applications (fapolicyd) : bloquez les accès non autorisés en créant des listes de programmes autorisés à s'exécuter sur des machines ou réseaux spécifiques. Utilisez les politiques prédéfinies ou personnalisez-les pour détecter les applications modifiées ou empêcher leur exécution.

Sécurité de la chaîne d'approvisionnement : réduisez les risques liés aux cycles de vie des logiciels avec des pratiques de développement plus sécurisées qui incluent une analyse statique du code dans l'ensemble de la base. Ainsi, vous évitez la plupart des failles de sécurité avant le déploiement et améliorez le projet Open Source communautaire.

Gestion évolutive des vulnérabilités : gérez les vulnérabilités avec des paramètres de sécurité évolutifs à l'aide de la solution Red Hat Insights. Personnalisez les politiques de sécurité, appliquez-les dans l'ensemble de vos systèmes, surveillez les risques et prenez des mesures de correction si nécessaire.

Automatiser les contrôles de sécurité à grande échelle, à long terme

Mécanisme de racine de confiance matérielle sécurisé : utilisez des mécanismes de racine de confiance matérielle pour garantir l'intégrité des logiciels sur vos systèmes. Fournissez des paramètres de sécurité cohérents pour les jetons matériels externes, notamment des cartes à puce et des boîtes noires transactionnelles (HSM).

Technologie NBDE (Network Bound Disk Encryption) : automatisez le déverrouillage des systèmes chiffrés sur site ou dans le cloud hybride, sans gestion manuelle des clés de chiffrement. Grâce à cette couche supplémentaire de protection, vos données ne sont disponibles que lorsqu'elles sont sécurisées.

facebook.com/redhatinc
@RedHatFrance
linkedin.com/company/red-hat

Chiffrement modernisé et évolutif : protégez vos données avec des paramètres de chiffrement personnalisables et cohérents dans l'ensemble du système pour répondre aux exigences de conformité. Gérez le chiffrement à l'échelle du système avec une méthode simple à commande unique.

Contrôles d'accès obligatoires SELinux : effectuez des contrôles d'accès granulaires sur les fichiers, processus, utilisateurs et applications pour minimiser les risques de réattribution inadaptée des privilèges. Personnalisez les accès selon les applications ou les conteneurs. Ce niveau de contrôle renforce la confidentialité et l'intégrité des données et protège les processus des entrées non vérifiées.

Gestion centralisée des identités : gérez les authentifications et les autorisations des utilisateurs via des contrôles d'accès basés sur les rôles ou sur des politiques, à grande échelle, dans l'ensemble de l'environnement. Intégrez facilement ces contrôles à d'autres solutions de gestion des accès et des identités ou à des répertoires.

Répondre aux exigences de conformité et rationaliser les audits

Certifications de sécurité vérifiées : répondez aux normes de conformité des clients. Red Hat met un point d'honneur à vérifier la conformité de chaque version mineure de son système d'exploitation Red Hat Enterprise Linux avec les normes FIPS et à certifier chaque version Extended Update Support (EUS) selon les critères communs.

Outils de conformité intégrés : analysez les configurations et recherchez les vulnérabilités sur un système local pour valider sa conformité. Générez des rapports et des références OpenSCAP, puis utilisez l'automatisation pour corriger les systèmes non conformes. Intégrez les solutions Red Hat Smart Management et Red Hat Insights pour gérer la conformité à grande échelle.

Enregistrement de session : enregistrez les activités d'administration et obtenez un fichier lisible pour répondre aux exigences de sécurité en cas d'audit ou permettre la relecture des sessions afin de faciliter la résolution des problèmes. Choisissez facilement les utilisateurs ou groupes que vous souhaitez enregistrer.

Rôles système : automatisez les configurations de sécurité et maintenez la cohérence sur l'ensemble des systèmes au fil du temps, afin d'assurer la sécurité et la conformité à grande échelle. Déployez votre solution Red Hat Enterprise Linux et gérez la sécurité avec un minimum de ressources en utilisant des rôles avec SELinux, les certificats, NBDE, l'enregistrement de session, le protocole SSH, les politiques de chiffrement et bien plus encore.

Découvrez tous les atouts de Red Hat Enterprise Linux

Contactez votre représentant Red Hat ou cliquez ici pour découvrir comment Red Hat Enterprise Linux peut vous aider à gérer la sécurité et la conformité sur l'ensemble de votre infrastructure de cloud hybride.

À propos de Red Hat

Red Hat aide ses clients à standardiser leurs environnements, à développer des applications cloud-native et à intégrer, automatiser, sécuriser et gérer des environnements complexes en offrant des services d'assistance, de formation et de conseil primés.

facebook.com/redhatinc
@RedHatFrance
linkedin.com/company/red-hat

EUROPE, MOYEN-ORIENT ET AFRIQUE (EMEA)
00800 7334 2835
europe@redhat.com

FRANCE
00 33 1 41 91 23 23
fr.redhat.com

fr.redhat.com
#F29077_0621