Optimiser la sécurité de Linux avec Red Hat

La valeur métier de Red Hat Enterprise Linux

IDC a observé que les entreprises ayant standardisé leurs environnements avec Red Hat Enterprise Linux ont profité d'avantages significatifs en matière de sécurité, notamment[1] :

- 33 % de gain d'efficacité pour les équipes de sécurité
- 46 % d'accélération des mises à jour de sécurité
- 47 % d'accélération de la réponse face aux vulnérabilités de sécurité

Des modèles de sécurité différents selon les distributions Linux

Dans le domaine de la sécurité des infrastructures informatiques, de nouvelles menaces apparaissent chaque jour et des réglementations de conformité sont ajoutées en permanence. L'adoption d'une plateforme de base axée sur la sécurité pour standardiser les environnements est une stratégie essentielle pour protéger les applications, processus et charges de travail. Si toutes les distributions Linux® sont Open Source, chacune suit une approche différente en matière de sécurité.

Lorsqu'elles choisissent une distribution Linux pour standardiser leurs environnements, les entreprises doivent évaluer différents aspects qui leur permettront de réduire les risques et de répondre aux exigences les plus récentes. Comment les fonctionnalités de sécurité de la distribution sont-elles développées ? Dans quelle mesure les mécanismes de protection de la distribution peuvent-ils être efficacement appliqués aux environnements ? Comment la distribution pourra-t-elle soutenir et améliorer la posture de sécurité au-delà du point de vente, pour protéger l'infrastructure contre les menaces émergentes, aujourd'hui comme demain ?

Red Hat® Enterprise Linux est un système d'exploitation sécurisé, qui repose sur plus de 30 années d'expérience dans le domaine des technologies Linux et qui est proposé par un leader technologique auquel font confiance plus de 90 % des entreprises du classement Fortune 500[2]. Cette solution applique une stratégie de *défense en profondeur* pour le développement de solutions, la configuration, la gestion et l'assistance. Cet aperçu explique comment ces éléments contribuent à renforcer la posture de sécurité et s'associent pour former un système d'exploitation fiable et axé sur la sécurité.

Une solution conçue pour un maximum de sécurité et de fiabilité

Les solutions Red Hat reposent sur une base Open Source créée par une communauté internationale, transparente et décentralisée d'ingénieurs qui placent la sécurité au cœur des technologies. Le système d'exploitation Red Hat Enterprise Linux prend en compte la sécurité dès le départ. Il facilite l'application des mécanismes de sécurité dès la phase d'assemblage et assure la surveillance et la correction des menaces émergentes.

Un cycle de développement logiciel axé sur la sécurité

Au moment de choisir une distribution Linux, il est important de tenir compte des normes suivies pendant la phase de développement.

Chez Red Hat, nous accordons la priorité à la sécurité pendant le cycle de développement. Nous nous basons sur le framework SSDF (Secure Software Development Framework) du NIST (National Institute of Standards and Technology), les recommandations du projet OWASP (Open Worldwide Application Security Project) et les normes ISO (Organisation internationale de normalisation).

Le service Red Hat Product Security favorise l'amélioration continue de la sécurité dans les pipelines de mise en production tout en soutenant les systèmes et les équipes qui s'efforcent d'assurer la confidentialité, la disponibilité et l'intégrité des produits et services Red Hat. Les nombreux clients Red Hat qui travaillent dans des secteurs hautement réglementés doivent avant tout garantir la sécurité de leur chaîne d'approvisionnement des logiciels avant de procéder au déploiement.

1 Livre blanc d'IDC, commissionné par Red Hat, « The Business Value of Standardizing on Red Hat Enterprise Linux », document n° US52594324, septembre 2024

2 Données client Red Hat et liste du classement Fortune 500, juin 2024

La sécurité intégrée à la production

La distribution Linux la plus adaptée à une entreprise doit permettre aux équipes d'appliquer efficacement les mécanismes de protection basés sur les meilleures pratiques de sécurité. Notre plateforme Linux intègre des mécanismes de sécurité sur plusieurs niveaux, notamment des configurations sécurisées par défaut, des contrôles d'accès basés sur le principe du moindre privilège et des processus automatisés.

Pour sécuriser leurs images, les utilisateurs de Red Hat Enterprise Linux peuvent tirer parti des différents profils de sécurité offrant des configurations par défaut. Ces références s'appuient sur les meilleures pratiques et permettent aux administrateurs d'appliquer la configuration dès la phase d'assemblage, et ainsi de s'assurer que leur déploiement respecte les exigences de conformité et de sécurité de l'entreprise. Cette approche permet non seulement de réduire les risques, mais aussi d'éviter les erreurs humaines lors de tâches qui seraient sinon effectuées manuellement après l'assemblage.

Une feuille de route pour gérer les menaces à venir

Les entreprises qui ont une posture de sécurité forte sont prêtes à faire face aux menaces à venir et capables de se conformer aux nouvelles exigences. Certaines distributions Linux imposent aux utilisateurs de se préparer eux-mêmes, ce qui les incite à se tourner vers des solutions communautaires.

La solution Red Hat Enterprise Linux est encadrée par une équipe produit et de développement qui surveille activement les nouvelles menaces et élabore des approches pour s'y préparer. Ces spécialistes Red Hat sont des membres actifs de la communauté axée sur la sécurité, et nombre d'entre eux sont impliqués dans le projet OpenSCAP, un framework Open Source qui permet de surveiller la sécurité et la conformité des systèmes Linux.

Respect des exigences globales en matière de conformité régionale

Pour choisir une distribution Linux, les entreprises doivent également prendre en compte les différents impératifs de conformité que fixent leurs équipes et leurs clients. La solution dispose-t-elle déjà d'un certain nombre de validations et de certifications de cybersécurité courantes, ou l'équipe devra-t-elle s'en occuper par la suite ?

Au fil des années, nous avons réalisé d'importants investissements pour permettre aux entreprises d'utiliser Red Hat Enterprise Linux afin de répondre aux exigences de sécurité globales strictes de leur région, ainsi que de tirer parti des meilleures pratiques de sécurité le plus efficacement possible. Avec plus de 100 bureaux répartis dans plus de 40 pays, nous savons que les réglementations en matière de conformité peuvent varier d'un pays à l'autre.

Pour répondre aux exigences de conformité régionales, nous avons obtenu un grand nombre de validations et de certifications pour nos produits et solutions, notamment Red Hat Enterprise Linux.

Méthodes de déploiement efficaces

Le respect des exigences en matière de sécurité et l'application des meilleures pratiques nécessaires peuvent constituer une charge pour les équipes de sécurité. Les étapes d'analyse, de validation et d'attestation peuvent prendre beaucoup de temps et nécessiter beaucoup de travail au sein de plusieurs équipes.

Le mode image pour Red Hat Enterprise Linux offre une méthode de déploiement basée sur une approche native pour les conteneurs, qui permet d'assembler, de déployer et de gérer le système d'exploitation. Il permet aux équipes chargées de la sécurité d'appliquer les outils de sécurisation des conteneurs (analyse, validation, chiffrement, attestation) aux éléments de base du système d'exploitation, ce qui simplifie considérablement leur travail. Non seulement cette approche réduit les risques, mais elle augmente aussi l'efficacité.

Red Hat Enterprise Linux aide les clients à atteindre leurs objectifs en matière de sécurité

Lorsque l'université du Sussex a dû migrer des serveurs essentiels vers un système d'exploitation entièrement pris en charge, elle a collaboré avec l'entreprise de consulting WM Promus pour adopter Red Hat Enterprise Linux. Ce changement lui a permis de réduire le risque de cyberattaque et d'obtenir une certification gouvernementale majeure comme preuve du niveau élevé de sécurité opérationnelle.

« L'université dispose d'un immense parc informatique. La migration vers Red Hat Enterprise Linux a limité les perturbations et permis à l'équipe de réduire les risques plus rapidement[3]. »

Eileen O'Mahony,
Directrice générale,
WM Promus

3 Étude de cas Red Hat, « WM Promus aide une université à renforcer l'efficacité et la sécurité », 23 octobre 2024

Gestion proactive des risques

Le système d'exploitation doit permettre aux équipes de toujours être informées des menaces et des problèmes liés à la sécurité.

Intégrée à Red Hat Enterprise Linux, la solution Red Hat Lightspeed facilite la gestion de bout en bout des systèmes. Elle permet aux utilisateurs du système d'exploitation d'identifier et de signaler les problèmes, de hiérarchiser les risques en fonction des effets potentiels sur l'activité, et même de déclencher l'action suivante dans une chaîne d'outils d'automatisation. Red Hat Lightspeed peut rechercher des CVE (Common Vulnerabilities and Exposures) et aider à hiérarchiser les mesures de correction en fonction du type de risque, de la gravité et des effets.

Cette solution permet également aux équipes de vérifier la conformité réglementaire avec les politiques OpenSCAP, de corriger les systèmes non conformes et de générer des rapports de conformité. Elle s'utilise aussi pour détecter rapidement les signatures de logiciels malveillants actifs dans les systèmes de l'ensemble de l'environnement de cloud hybride.

Prise en charge continue de la sécurité

Pour les entreprises, le choix d'une plateforme Linux pour standardiser leurs environnements aura des implications pendant de nombreuses années. Il leur est donc essentiel de déterminer le type de prise en charge offerte après le déploiement et par la suite.

Les utilisateurs de Red Hat Enterprise Linux peuvent travailler en toute confiance, avec 10 ans de prise en charge et de mises à jour pour les versions majeures, ainsi qu'un accès au portail client Red Hat qui fournit des informations sur les vulnérabilités de sécurité actuelles et les mesures à prendre pour limiter leurs effets. L'équipe chargée de la résolution des incidents de sécurité des produits Red Hat aide les utilisateurs à comprendre les risques et les effets des CVE émergentes, et fournit des conseils pour les corriger.

Des partenariats fiables et une collaboration durable

Nous participons à de nombreux programmes coordonnés de signalement responsable à l'échelle du secteur. Nous intervenons depuis longtemps au sein d'organismes de sécurité tels que FIRST (Forum of Incident Response and Security Teams), l'OpenSSF (Open Source Security Foundation) ou Oasis, ce qui nous permet de conserver notre statut de partenaire mondial pour la collaboration en matière de sécurité.

Nous sommes l'une des six entreprises au monde à participer au programme CVE (CVE.org) avec le statut Root. À ce titre, nous soutenons la mission de cet organisme qui vise à identifier, définir et cataloguer les vulnérabilités de sécurité rendues publiques. En plus d'exercer ce rôle central, nous bénéficions du statut de partenaire CNA (CVE Numbering Authority), ce qui nous permet d'attribuer des identifiants CVE aux vulnérabilités et de publier des rapports (CVE Records). Ainsi, lorsqu'un utilisateur de Red Hat Enterprise Linux prend connaissance d'une nouvelle CVE, une équipe de spécialistes de la sécurité maîtrisant la plateforme a déjà activement participé à la recherche, à l'évaluation et à l'analyse des étapes de correction à suivre.

Partage communautaire

Les utilisateurs d'autres distributions Linux peuvent aussi profiter de nos pratiques de sécurité. Fidèles à l'éthique Open Source, nous encourageons la communauté à collaborer pour définir des stratégies de résolution, d'application de correctifs et d'atténuation des risques qui affectent les systèmes Linux, afin de préserver la solide réputation de sécurité de Linux.

Notre équipe collabore avec d'autres équipes à travers le monde pour développer des pratiques de sécurité Open Source, notamment au travers de la création de la solution OpenSCAP, de notre participation à l'OpenSSF et de nos contributions à la base de données OSV.

Cette collaboration s'applique également au code Red Hat, que les membres de la communauté peuvent inspecter, auditer et réviser et auquel ils peuvent contribuer.

Optimiser la sécurité de Linux avec Red Hat

Lorsque vous adoptez Red Hat Enterprise Linux pour standardiser vos environnements, vous bénéficiez du soutien d'une entreprise qui prend la sécurité en compte dès la conception. Découvrez comment nous pouvons aider votre entreprise à assembler une plateforme Linux axée sur la sécurité.

À propos de Red Hat

Premier éditeur mondial de solutions Open Source d'entreprise, Red Hat s'appuie sur une approche communautaire pour fournir des technologies Linux, de cloud hybride, de conteneurs et Kubernetes fiables et performantes. Red Hat aide ses clients à développer des applications cloud-native, à intégrer des applications nouvelles et existantes ainsi qu'à gérer et automatiser des environnements complexes. Conseiller de confiance auprès des entreprises du Fortune 500, Red Hat propose des services d'assistance, de formation et de consulting reconnus et primés qui apportent à tout secteur les avantages de l'innovation ouverte. Situé au cœur d'un réseau mondial d'entreprises, de partenaires et de communautés, Red Hat participe à la croissance et à la transformation des entreprises et les aide à se préparer à un avenir toujours plus numérique.

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