Livre blanc

Vers des systèmes SAP sécurisés : Comment améliorer la sécurité et réduire les risques opérationnels ?

Index

Exercer une activité dans une économie numérique exige de l'agilité, et les infrastructures numériques d'entreprise doivent devenir véritablement solides face aux cybermenaces croissantes. À mesure que les organisations développent leur empreinte numérique, elles doivent s'assurer que leur infrastructure SAP est réellement sécurisée et capable de se défendre face à une surface d'attaque grandissante. SUSE permet aux organisations de garantir une plate-forme SAP sécurisée en améliorant la sécurité et en réduisant les risques opérationnels.

Les principaux défis liés à la sécurisation des systèmes SAP

Source : SAPinsider 2022

1 Détection des menaces potentielles

2 Suivi des correctifs/ mises à jour

3 Sécurisation du code personnalisé

4 Protection des données

Les organisations placent de plus en plus leurs workloads en dehors de leurs datacenters traditionnels, afin de s'adapter à des équipes plus dispersées, de connecter des périphériques IoT (Internet des objets) et de tirer parti de la flexibilité et de l'évolutivité des services de cloud public. Ce paysage en constante évolution, avec des surfaces d'attaque plus vastes, a entraîné une augmentation de la fréquence et de la sophistication des cybermenaces.

Dans le même temps, les réglementations sur la confidentialité, telles que le Règlement général sur la protection des données (RGPD) au sein de l'Union européenne, et les législations étatiques aux États-Unis, comme la loi californienne sur la protection des consommateurs et la loi sur la protection de confidentialité du Colorado, montrent que les organisations ont une plus grande responsabilité en ce qui concerne la protection des informations privées. Elles s'exposent également à de lourdes amendes si elles ne s'emparent pas de cette question.

En particulier, votre infrastructure SAP héberge des logiciels, des processus et des données stratégiques qui prennent en charge toutes vos opérations métiers. Si votre infrastructure tombe en panne en raison d'une cyberattaque ou si vos données SAP stratégiques sont compromises, votre organisation subira des coûts imprévus et pourra même perdre des ventes, des clients et sa réputation.

Malheureusement, les cybercriminels comprennent parfaitement l'importance de l'infrastructure et des données SAP, ce qui fait de ces dernières des cibles de choix pour les cyberattaques. Il est donc essentiel pour les organisations de mettre en oeuvre une stratégie complète de cyberrésilience SAP, afin d'améliorer la sécurité et de réduire les risques opérationnels.

L'importance stratégique de la protection de votre environnement SAP a été mise en évidence dans un rapport de SAPinsider, publié en 2022 et intitulé « Cybersecurity Threats to SAP Systems ». Ce dernier a révélé que certaines des principales menaces organisationnelles comprenaient des systèmes non corrigés, des attaques sur la chaîne d'approvisionnement, des attaques de ransomware et des connexions non sécurisées à d'autres systèmes.

Ce rapport a également identifié les principaux défis liés à la sécurisation des systèmes SAP, tels que la détection des menaces potentielles, le suivi des correctifs et des mises à jour, la sécurisation du code personnalisé et la protection des données.

Pour véritablement sécuriser votre système, vous avez besoin de solutions qui réduisent vos risques opérationnels dans tous les environnements : sur site, en hybride et dans le cloud public. Cela comprend les éléments suivants :

- Un système d'exploitation robuste et sécurisé
- Des outils d'automatisation, de monitoring et de gestion
- L'intégration des meilleures pratiques dans le code
- L'intégration transparente de la sécurité SAP
- Un environnement sécurisé et fiable pour les déploiements Edge et en conteneurs

SUSE est le seul acteur à disposer de l'expérience, des connaissances et de l'innovation nécessaires pour sécuriser, gérer et surveiller l'ensemble de votre plate-forme SAP, afin de vous faire bénéficier d'une véritable cyberrésilience SAP.

Les solutions stratégiques Linux sécurisent la chaîne d'approvisionnement des logiciels

Aujourd'hui, les organisations doivent améliorer leur agilité métier afin de s'adapter aux changements de manière rapide et rentable. Cela signifie qu'elles doivent pouvoir fonctionner dans un environnement traditionnel sur site ainsi que dans une infrastructure cloud évolutive.

La sécurisation de la chaîne d'approvisionnement des logiciels est une priorité absolue pour SUSE. C'est pourquoi la sécurité est au coeur de SUSE Linux. C'est autour d'elle que nous créons notre système d'exploitation, de manière à ce qu'il vous protège contre les futures failles de sécurité, intrusions et attaques. SUSE Linux fournit un environnement optimal pour toutes les applications,

La sécurisation de la chaîne d'approvisionnement des logiciels est une priorité absolue pour SUSE. C'est pourquoi la sécurité est au coeur de SUSE Linux. C'est autour d'elle que nous créons notre système d'exploitation, de manière à ce qu'il vous protège contre les futures failles de sécurité, intrusions et attaques.

qu'elles soient déployées sur site, dans le cloud ou en Edge.

SUSE s'efforce de sécuriser les pratiques et les composants impliqués dans la création et le déploiement de sa solution Linux. Nous veillons à ce qu'aucun cybercriminel ne puisse injecter de code malveillant dans nos versions, ce qui se reflète dans notre longue liste de certificats de sécurité premiers de l'industrie. Ils incluent notamment la norme américaine FIPS 140-2. Il s'agit d'une norme de sécurité gouvernementale pour la validation des modules cryptographiques. Ils incluent également le cadre de sécurité SLSA (Supply Chain Levels for Software Artifacts), ainsi qu'un autre certificat du gouvernement américain. Il s'agit de celui de la Defense Information Systems Agency (DISA).

SUSE Linux Enterprise Server (SLES) a également obtenu la certification CC (Common Criteria) EAL 4+ relative à la chaîne d'approvisionnement de logiciels. SUSE Linux Enterprise Server est désormais certifié EAL 4+ pour les architectures IBM Z, ARM et x86-64, ce qui signifie qu'il est conforme aux exigences de sécurité les plus strictes pour les infrastructures stratégiques. La certification CC (Common Criteria) EAL 4+ de SUSE pour la chaîne d'approvisionnement de logiciels comprend la production sécurisée, la livraison des mises à jour et la protection du capital de données numériques stratégiques.

Les fonctions propres à SAP renforcent la sécurité

Pour atteindre le plus haut niveau de protection, votre système d'exploitation doit s'intégrer étroitement à la sécurité SAP. SUSE Linux est conçu avec des technologies propres à SAP, notamment le pare-feu SAP et l'antivirus SAP. SUSE Linux Enterprise Server (SLES) a passé de nombreux tests réalisés par SAP, et a obtenu la certification Premium de SAP.

Les guides de sécurisation renforcée des systèmes SAP constituent un aspect important des puissantes fonctions de sécurité de SUSE. En accord avec les meilleures pratiques, ces derniers bloquent les cybercriminels en réduisant les vulnérabilités et les vecteurs d'attaque potentiels. En d'autres termes, il s'agit d'optimiser la résistance à une cyberattaque.

SUSE propose des images SUSE Linux Enterprise Server for SAP renforcées dans le cloud couvrant différents cas d'utilisation dans les infrastructures de cloud pour toutes les très grandes entreprises, garantissant ainsi la sécurité de tous les déploiements dans le cloud. SUSE propose également un guide de sécurisation renforcée de SUSE Linux Enterprise Server for SAP Applications pour SAP HANA. Les guides de sécurisation renforcée comprennent des commentaires de clients qui aident à identifier tous les paramètres de sécurité à prendre en compte. Ils ont été conçus pour fournir une aide lorsque certains scénarios se produisent dans la réalité.

SUSE vous permet de configurer, gérer et surveiller l'ensemble de votre sécurité SAP à partir de SUSE Manager, une solution de gestion d'infrastructure conçue pour simplifier et sécuriser l'ensemble de votre environnement, sur site, en périphérie ou dans le cloud. SUSE Manager vous permet d'utiliser OpenSCAP (Security Certification and Authorization Package), une solution standardisée de contrôle de la conformité pour les grandes infrastructures Linux. Cela vous permet de vérifier que vos systèmes respectent les directives de conformité ou qu'ils s'inscrivent dans les stratégies de sécurité, afin de vous assurer qu'ils sont configurés de manière optimale.

Les meilleures pratiques en matière de sécurité et les paramètres de configuration peuvent également être validés via Trento, la console Web native dans le cloud de SUSE. Celle-ci applique en permanence les meilleures pratiques, valide les configurations système et propose des correctifs pour tous les problèmes détectés.

Les outils de gestion des vulnérabilités et des correctifs permettent de contrer les menaces

La gestion des vulnérabilités et des correctifs joue un rôle essentiel dans la sécurisation d'un environnement SAP. Si les systèmes sont obsolètes, ils sont vulnérables aux cyberattaques. SUSE Manager fournit un outil centralisé de gestion des vulnérabilités qui renforce la visibilité sur l'ensemble de votre infrastructure SAP afin d'améliorer la détection des menaces potentielles.

> « Grâce à la fiabilité de SUSE Linux Enterprise Server, nous réalisons quatre cycles complets d'application de correctifs par an, avec très peu de problèmes. Même si nous modifions constamment l'environnement, la technologie SUSE fonctionne très bien. »
>
> Pino Lascala,
> Ingénieur technique serveur
> SA Power Networks

SUSE Manager vous permet de déployer, configurer, gérer, mettre à jour et surveiller tous les systèmes Linux de votre environnement de la même manière, quel que soit leur emplacement ou leur mode de déploiement. Une interface unique donne accès à une gamme complète de fonctions de gestion, ce qui vous permet d'effectuer toutes les tâches de gestion plus rapidement et avec moins d'erreurs, améliorant ainsi la productivité du service informatique et réduisant les interruptions de service des serveurs.

Lorsque SUSE Manager est combiné au service SUSE Linux Enterprise Live Patching, les organisations peuvent mettre en oeuvre des correctifs de stratégies de sécurité pour éliminer les vulnérabilités de type Zero Day. Vous pouvez également créer un double workflow pour l'application de correctifs, en appliquant un correctif immédiat pour les nouvelles vulnérabilités, sans interruption de service pour le kernel et les bibliothèques de votre système d'exploitation. En complément, appliquez des correctifs de maintenance régulièrement planifiés. Il n'est plus nécessaire de négocier des fenêtres de maintenance pour résoudre les vulnérabilités de type Zero Day.

SUSE Manager propose également des fonctions de test de contenu pour définir et appliquer des stratégies d'application de correctifs, créant ainsi un workflow sécurisé pour le processus d'application des correctifs. Cette solution permet de télécharger les correctifs à l'avance pour les préparer à l'installation. Vous pouvez ensuite commencer à appliquer chaque correctif dès qu'il est planifié, ce qui vous permet de gagner du temps dans les fenêtres de maintenance.

L'excellence opérationnelle garantit la sécurité des activités métiers

Pour garantir l'excellence opérationnelle, il est essentiel de maintenir le bon fonctionnement de vos systèmes SAP. Les interruptions de service imprévues mettent l'activité en pause et entraînent souvent des pertes d'opportunités commerciales et une réputation entachée. SUSE Linux intègre des fonctions conçues spécialement pour assurer le bon fonctionnement des environnements SAP, sans interruption. Par exemple :

- L'intégration de meilleures pratiques au code
- Des outils et assistants d'automatisation pour réduire les erreurs de configuration et les tâches manuelles
- Des outils de monitoring et de visualisation pour une vue en temps réel de la plate-forme SAP
- Une technologie haute disponibilité de pointe conçue pour des scénarios SAP plus résilients

> « Pour exploiter le grand potentiel de l'innovation dans l'agriculture, notre service informatique doit être en mesure de fonctionner avec agilité. Les solutions SUSE nous aident à livrer rapidement de nouveaux services numériques, sans compromettre la stabilité et la disponibilité. »
>
> Jan Ove Steppat,
> Architecte d'infrastructure Open Source,
> CLAAS GmbH & Co. KG

Les outils d'automatisation et les assistants de configuration guidés sont précieux pour améliorer la sécurité et la conformité, et réduire les interruptions de service inopinées ainsi que les pertes de données. Par exemple, si vous mettez à niveau le logiciel SAP HANA dans un système en cluster, un assistant peut automatiquement déconnecter et reconnecter le cluster, réduisant ainsi les risques d'erreur. Vous pouvez également automatiser le déploiement de machines virtuelles, ce qui peut être une tâche manuelle très chronophage dans les grandes organisations disposant de plusieurs sites.

Les outils de gestion, de monitoring et de visualisation du système fournissent une vue en temps réel de la plate-forme SAP, ce qui facilite l'identification des problèmes de sécurité potentiels. Vous pouvez surveiller de manière proactive vos serveurs, vos instances cloud et vos clusters haute disponibilité. Les outils de visualisation intégrés permettent de voir facilement ce qui se passe sur le réseau en affichant des statistiques pertinentes dans un format facile à utiliser.

Les outils de gestion des systèmes réduisent les risques opérationnels

Les meilleures pratiques sont intégrées au code du système d'exploitation SUSE Linux Enterprise Server for SAP Applications. Cela signifie que les configurations et les paramètres sont constamment vérifiés pour s'assurer qu'ils sont corrects et qu'ils ne présentent aucun risque de sécurité. Cela est essentiel, car les systèmes mal configurés ne sont, par nature, pas sécurisés.

Avec SUSE, vous avez accès à des catalogues de configuration soigneusement sélectionnés pour différents cas d'utilisation qui ont été éprouvés et validés par des clients professionnels au fil des ans.

La console Web Trento permet aux administrateurs de surveiller l'ensemble de la pile du système d'exploitation de votre environnement SAP, y compris les fonctions de haute disponibilité. Trento s'exécute en arrière-plan et effectue des vérifications sur SUSE Linux for SAP Applications afin de valider et de corriger les configurations système. Si Trento trouve une configuration incorrecte, il affiche le problème et fournit des conseils. Il peut même suggérer des commandes que les administrateurs peuvent simplement copier et coller pour corriger la configuration.

> « Par rapport à d'autres distributions Linux, nous avons découvert que SUSE Linux Enterprise Server for SAP Applications était de loin le plus facile à déployer et à configurer. Une fois déployée, la solution SUSE est également gagnante en matière de stabilité. »
>
> Seo Jun-hyeok,
> Responsable technologique, équipe de consulting, Lotte Data Communications

La sécurité pour une infrastructure SAP étendue

Votre infrastructure SAP s'étend au-delà des datacenters et du cloud, jusqu'aux environnements périphériques et mis en conteneurs, qui doivent également être sécurisés. SUSE offre un environnement sécurisé et fiable pour les conteneurs et les environnements Edge.

Rancher Prime est une plate-forme de gestion Kubernetes qui combine la sécurité, la stratégie et la gestion des utilisateurs pour les opérations multiclusters. Elle garantit que les applications exécutées dans des conteneurs (Rancher, EKS, AKS, OpenShift, etc.) peuvent être sécurisées, qu'elles soient connectées à SAP via des API ou via un middleware d'intégration.

SUSE NeuVector permet d'appliquer les meilleures mesures de sécurité et de conformité aux applications et à une infrastructure mises en conteneurs, du coeur au cloud, en passant par le Edge, en assurant la conformité avec le RGPD, la gestion des stratégies, l'analyse des conteneurs et le pare-feu de la couche application compatible avec les protocoles.

SUSE Edge est une solution spécialement conçue pour gérer le cycle de vie des périphériques edge. En connectant en toute sécurité les périphériques edge à votre infrastructure SAP, cette solution intègre la sécurité sur trois couches de gestion : le cycle de vie des applications, le cycle de vie Kubernetes et le système d'exploitation. SUSE Edge simplifie, centralise et automatise la gestion du cycle de vie de Kubernetes et Linux sur vos emplacements périphériques distribués.

SUSE : un partenaire SAP de confiance

SUSE est idéalement positionné pour sécuriser l'ensemble de votre infrastructure SAP dans n'importe quel environnement. SUSE est un partenaire SAP de confiance depuis des décennies, et est plébiscité par les organisations du monde entier. D'ailleurs, 85 % des mises en oeuvre SAP HANA reposent sur SUSE Linux. SUSE est une organisation certifiée ISO-27001 et 27701, ainsi qu'un leader du secteur en matière de certification de sécurité.

SUSE est la seule organisation qui dispose de la technologie, des connaissances et des décennies d'expérience nécessaires pour sécuriser votre environnement SAP du coeur de la plate-forme à la périphérie. SUSE Linux Enterprise Server for SAP Applications est une application approuvée par SAP, par des partenaires et par des organisations du monde entier. En faisant de SUSE votre plate-forme SAP, vous dynamiserez immédiatement vos opérations grâce à des meilleures pratiques, à des certifications de sécurité et à des certifications d'infrastructure de plate-forme SAP validées sur le marché. Et vous aurez la garantie de maintenir votre excellence opérationnelle grâce à l'automatisation, à la gestion et au monitoring SUSE.

SUSE vous donne accès à un environnement SAP sécurisé et vous garantit une sécurité renforcée et des risques opérationnels réduits.

Consultez le site www.suse.com/secure-sap pour plus d'informations.

SAP Endorsed App
Premium Certified

SUSE Linux Enterprise Server for SAP Applications est une application approuvée par SAP.

SUSE

2023

SUSE Maxfeldstrasse 5
90409 Nuremberg
www.suse.com

Pour en savoir plus, contactez SUSE aux numéros suivants :
+1 800 796 3700 (États-Unis/Canada)
+49 (0)911-740 53-0 (International)

Merci

SCFR0039 | © 2023 SUSE LLC. Tous droits réservés. SUSE et le logo SUSE sont des marques déposées de SUSE LLC aux États-Unis et dans d'autres pays. Toutes les marques commerciales de fabricants tiers appartiennent à leur propriétaire respectif.