



Le "Patching Paradox"

Plus un système est important, plus il doit être disponible, mais le besoin de disponibilité réduit la possibilité d'appliquer des correctifs.



Les défis

- La plupart des clients SAP ont du mal à se tenir au courant des mises à jour et des correctifs, ce qui se traduit par des serveurs non mis à jour
- Bien qu'il existe des politiques de sécurité, les environnements critiques tels que SAP sont souvent considérés comme des exceptions aux politiques d'application de correctifs



Les raisons

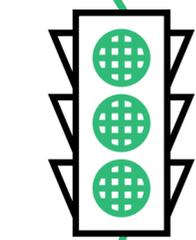
- Temps nécessaire, même pour un simple redémarrage du système SAP HANA
- Incapacité à négocier les fenêtres de maintenance
- Temps et efforts nécessaires pour que le service informatique applique un correctif à un système
- Complexité de la mise en oeuvre des politiques d'application de correctifs
- Manque d'outils de gestion des vulnérabilités



Le résultat

INTERRUPTIONS DE SERVICE ! Qu'il s'agisse d'une faille de sécurité ou d'une maintenance planifiée pour l'application de correctifs, le résultat est le même : des interruptions de service.

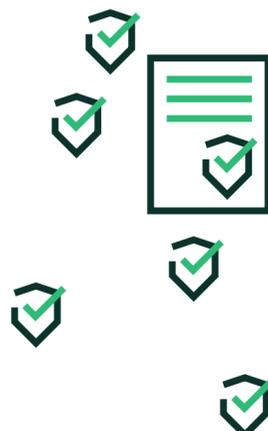
Mais les failles de sécurité doivent être évitées à tout prix, c'est pourquoi il est essentiel d'appliquer des correctifs dès le premier jour.



Les solutions

Appliquer des correctifs sans interruption de service

- SLE Live Patching applique des correctifs sans interruption de service
- L'application de correctifs en temps réel au kernel et aux bibliothèques permet de mettre en oeuvre la politique d'application de correctifs dès le premier jour
- Appliquez des correctifs pendant les heures de travail pour réduire la complexité opérationnelle



Identifier les vulnérabilités

- Appliquez et testez les correctifs pour réduire les risques opérationnels
- SUSE Manager analyse les vulnérabilités et définit un workflow d'application de correctifs pour améliorer la sécurité

Mettre en oeuvre une politique d'application de correctifs complète

- Mettez en place un programme de maintenance régulière incluant tous les correctifs
- Mettez en oeuvre une politique de correction des vulnérabilités dès le premier jour
- Automatisez l'application de correctifs, y compris les clusters



SUSE permet aux clients SAP d'éliminer le "Patching Paradox"



Suivez le parcours vers une plate-forme SAP sécurisée :
Rendez-vous sur suse.com/secure-sap/