ÉTUDE DE CAS

SAP transforme la sécurité des endpoints grâce à Tanium

Suite à plusieurs fusions et acquisitions, SAP a amélioré l'efficacité, réduit le temps de correction et amélioré la visibilité de la sécurité en consolidant les outils et en automatisant la sécurité des endpoints.

ORGANISATION

SAP SE

LIEU

Walldorf, Allemagne

NOMBRE DE ENDPOINTS

100 000

Une croissance continue entraîne une complexité informatique.

Après l'acquisition de trois sociétés de logiciels basés sur le cloud, SAP a fait face à un défi majeur en matière de sécurité : la gestion de milliers de nouveaux endpoints sur des unités commerciales cloisonnées.

Les acquisitions stratégiques ont constitué la pierre angulaire de la croissance de SAP. Au cours de ses 52 années d'exploitation, SAP a acquis plus de 50 entreprises de conception de logiciels. Parmi celles-ci, on peut citer trois fournisseurs de services de gestion des dépenses basés sur le cloud : Ariba, Concur et Fieldglass. Bien que cette croissance ait renforcé le portefeuille de SAP, elle a également créé un défi de sécurité : la gestion de milliers d'endpoints sur plusieurs systèmes hérités.

Initialement, SAP gérait ces entreprises séparément, chacune avec ses propres outils et processus de sécurité. Mais en 2018, SAP les a consolidées en une seule entité : La gestion intelligente des dépenses (ISM). D'un point de vue commercial, cette consolidation semblait logique. Cependant, du point de vue de la sécurité, elle créa une fragmentation qui rendit la gestion des vulnérabilités presque impossible.

Chaque entreprise comptait des workflows de sécurité différents, ce qui rendait difficile le maintien des SLA stricts de SAP :

- La plupart des vulnérabilités résolues dans les 90 jours
- Les vulnérabilités critiques en sept jours maximum

Unification de la plateforme de sécurité

Afin de maintenir la conformité et rationaliser les opérations de sécurité, ISM avait besoin d'une plateforme unique présentant plusieurs avantages :

- offrir une visibilité en temps réel
- automatiser les correctifs
- unifier les processus de sécurité dans toutes les unités commerciales

Cependant, avec des dizaines de milliers d'endpoints dans le monde entier, comment les équipes de sécurité d'Ariba, Concur et Fieldglass pouvaient-elles assurer la conformité ?

Selon Darren Sapper, « L'unique solution était de tout consolider en une seule équipe à l'aide d'une seule plateforme technologique. »

> **« La combinaison de ces trois secteurs d'activité a rendu difficile la conformité à nos SLA »**
>
> **Darren Sapper**
> Directeur principal responsable de la sécurité des plateformes et de la gestion intelligente des dépenses
> SAP

Mettre à l'échelle de la gestion des endpoints avec Tanium Automate

Pour relever ses défis croissants en matière de sécurité, SAP avait besoin d'une plateforme unique et unifiée capable de fournir une visibilité et une automatisation en temps réel dans son unité commerciale nouvellement consolidée, l'ISM.

SAP a découvert Tanium pour la première fois par l'intermédiaire de l'une de ses sociétés acquises, qui utilisait déjà la plateforme avec succès. Après un examen technique, l'équipe ISM a décidé d'étendre le rôle de Tanium, en faisant de cette solution sa seule solution de gestion des endpoints.

Adam Levinson, vice-président des services cloud gérés chez SAP ISM, a déclaré : « Grâce à Tanium, nous n'avons qu'une seule interface, une seule expertise, un seul outil à gérer, contre plusieurs auparavant. »

> « [Tanium] L'automatisation constitue la recette secrète qui regroupe toutes les capacités de Tanium. C'est un outil vraiment puissant. »

Darren Sapper
Directeur principal responsable de la sécurité des plateformes, et de la gestion intelligente des dépenses
SAP

Automatisation de la sécurité pour une efficacité optimisée

La pièce maîtresse du partenariat d'ISM est Tanium Automate, qui transforme les opérations de sécurité informatique en automatisant les tâches de sécurité répétitives et complexes.

Avec Tanium Automate, l'équipe peut :

- créer des playbooks personnalisés en plusieurs étapes qui orchestrent les workflows de sécurité avec peu ou pas de code
- déployer des mises à jour et des correctifs de manière transparente, réduisant ainsi le risque d'erreurs manuelles
- s'assurer que les équipes informatiques et de sécurité restent informées, améliorant ainsi le temps de réponse et la conformité

« L'automatisation constitue la recette secrète qui regroupe toutes les capacités de Tanium », a déclaré Darren Sapper. « C'est un outil vraiment puissant. »

Avant Tanium, l'équipe de gestion des endpoints ISM s'appuyait sur des workflows manuels en plusieurs étapes qui prenaient du temps et étaient sujets aux erreurs humaines. Cette stratégie était inefficace et présentait un risque accru.

Grâce à Tanium Automate, l'équipe réduit la complexité et gagne en efficacité :

- consolider jusqu'à 20 étapes de déploiement en un seul processus automatisé, réduisant ainsi la complexité opérationnelle
- réduire le risque d'erreurs manuelles en orchestrant les workflows de sécurité de manière contrôlée et prévisible
- accélérer les cycles de correction : la correction d'un centre de données prenait une semaine entière et ne prend désormais que quelques heures

« Lorsque vous réunissez 10 ou 20 étapes, l'erreur humaine reste toujours une possibilité », a expliqué Darren Sapper. « Tanium Automate élimine cette possibilité. »

Une vue unifiée pour la gestion de la sécurité

ISM gérait également les endpoints à l'aide de plusieurs solutions ponctuelles, ce qui contribuait à la complexité au sein des équipes. Cette centralisation dans la solution de Tanium a offert à l'équipe une plateforme unique pour gérer la sécurité et les opérations en temps réel.

Grâce à un ensemble de compétences, un outil et un seul écran, l'équipe ISM a considérablement amélioré la visibilité, le contrôle et les temps de réponse dans l'ensemble de son environnement.

> « Grâce à [Tanium] Automate, nous sommes en mesure de corriger un centre de données, ce qui prendrait normalement environ une semaine, en quelques heures seulement. »
>
> **Adam Levinson**
> VP responsable des services cloud gérés et de la gestion intelligente des dépenses
> SAP

Résultats

Patching plus rapide

- Réduction de 98 % du temps nécessaire à la correction d'un centre de données
- Réduction du temps de correction d'un centre de données d'une semaine complète à quelques heures seulement, améliorant considérablement l'efficacité opérationnelle

Identification plus rapide des vulnérabilités

- Tanium Automate permet la détection des vulnérabilités en temps réel sur plusieurs emplacements
- L'équipe a identifié et résolu un problème de fichier de configuration sur 95 emplacements en seulement deux minutes, un processus qui aurait auparavant pris des heures, voire des jours

> « Lorsque vous réunissez 10 ou 20 étapes, l'erreur humaine est toujours une possibilité : Tanium Automate élimine cette possibilité. »

Darren Sapper
Directeur principal responsable de la sécurité des plateformes et de la gestion intelligente des dépenses
SAP

TANIUM

Le pouvoir de la certitude.™

Rendez-nous visite sur www.tanium.com et suivez-nous sur LinkedIn et X.

© Tanium 2025