Imprivata gère et sécurise son environnement de conteneurs avec Splunk Cloud

Défis clefs

Pour faire gagner du temps à son personnel DevOps, Imprivata souhaitait se munir de capacités de journalisation centralisée et sécurisée et d'interrogation ad hoc dans des environnements de développement et de production en conteneurs fortement distribués.

Résultats clefs

Le passage à Splunk® Cloud a permis à Imprivata de réduire les coûts associés à la maintenance de son infrastructure locale, de rationaliser sa conformité en matière de sécurité et de donner à ses ingénieurs DevOps le temps de se consacrer à des tâches à plus forte valeur ajoutée.

imprivata

Industrie : Santé

Solutions : Opérations IT, sécurité

La sécurité des identités numériques est plus importante que jamais.

Imprivata, société de sécurité IT pour le secteur de la santé, fournit aux établissements de santé du monde entier une plateforme de sécurité et d'identité accessible de partout et offrant des capacités de gestion positive des identités et d'authentification multifacteurs. Imprivata sécurise la santé et instaure la confiance entre les personnes, les technologies et les informations afin de relever les défis stratégiques de conformité et de sécurité tout en améliorant la productivité et l'expérience des patients.

Aperçu de l'environnement cloud complet

Les équipes DevOps et de développement d'Imprivata collaborent à la maintenance de l'infrastructure d'outillage et d'automatisation de l'entreprise, en appliquant les bonnes pratiques pour garantir des performances optimales pendant les pics de production. Les équipes font depuis longtemps confiance à Splunk Enterprise pour recevoir des alertes, créer des tableaux de bord, produire des rapports sur les accords de niveau de service et résoudre les problèmes.

« Notre chance est que nous avons toujours utilisé Splunk ; nos logs système, d'Amazon Web Services, de pare-feu et de sécurité sont tous envoyés dans Splunk, » explique un responsable de l'équipe de la plateforme cloud d'Imprivata.

Résultats chiffrés

- Le personnel du NOC gère 100 % des incidents de production grâce à l'automatisation et à des manuels sans aucune remontée vers les équipes DevOps
- Simplification de la conformité HIPAA, SOC 2 Type II et RGPD
- Élimination des coûts liés à l'infrastructure locale et de la charge de gestion

Splunk est indispensable pour la visibilité et la stabilité de l'environnement opérationnel d'Imprivata, qui utilise les outils de conteneurisation Docker et Kubernetes ainsi que des contrôles d'automatisation Python pour superviser ses ressources déployées dans Amazon Web Services. Les développeurs Imprivata utilisent Docker sur leurs ordinateurs portables et, plutôt que de conserver les logs localement, ils les envoient dans Splunk Cloud pour en faciliter l'analyse.

Le responsable déclare : « Notre architecture cloud-native fortement distribuée implique de nombreux services et conteneurs qui sont autant de pièces mobiles. Vous pouvez examiner des logs mais ne jamais savoir par lequel commencer. Il serait impossible de savoir ce qui se passe sans Splunk. »

Il ajoute : « Chez Imprivata, nous regroupons tous les logs de l'infrastructure, des applications et des appliances locaux au même endroit, si bien que le dépannage des applications, de l'infrastructure et du système cloud se font tous dans un même emplacement : Splunk. Les tableaux de bord Splunk aident l'équipe de gestion des produits et les responsables techniques à évaluer les accords de niveau de service et à les mesurer dès le départ, favorisant ainsi une culture de la mesure et une compréhension commune du produit dès le début. »

Splunk Cloud permet une évolutivité rentable

Une initiative de migration des solutions locales vers le cloud et des besoins en croissance rapide ont incité Imprivata à passer de Splunk Enterprise à Splunk Cloud. Le volume de données que la société envoie à Splunk est d'environ 150 Go par jour, mais il y a eu des pics à 500 Go. Splunk Cloud permet à Imprivata d'obtenir des réponses à partir de ses données machine sans avoir à gérer une infrastructure. « Splunk Cloud réduit le coût d'exploitation de notre infrastructure tout en libérant notre équipe IT qui a le temps de se consacrer à des tâches à forte valeur ajoutée, » explique le responsable.

Normalisation de la conformité et des audits

Splunk Cloud simplifie également la conformité à la loi HIPAA sur la portabilité et la traçabilité de l'assurance santé et à d'autres réglementations, dont SOC 2 Type II et le règlement général sur la protection des données (RGPD). Imprivata peut analyser, visualiser et superviser les données machine de toutes les sources (systèmes de dossiers médicaux électroniques, dispositifs médicaux connectés, etc.) afin de superviser des environnements applicatifs complexes, d'harmoniser les fonctions d'audit et de réduire les risques et les coûts. Le contrat Splunk Cloud de l'entreprise comprend un accord de partenariat commercial (BAA) sur la protection des informations médicales personnelles (PHI) conformément aux directives HIPAA.

> Splunk Cloud m'a libéré de nombreuses tâches administratives et me permet ainsi d'aider mon équipe et nos partenaires au sein de l'entreprise à analyser nos activités, effectuer des analyses des causes profondes et atteindre des objectifs concrets. »
>
> **Responsable,** Équipe de la plateforme cloud, Imprivata

> La version de Splunk conforme à la norme HIPAA que nous utilisons nous protège par un BAA très avantageux et indispensable pour tous les fournisseurs avec lesquels nous travaillons. Si un rapport s'arrête ou que le planificateur ralentit, nous n'avons plus besoin d'en rechercher la cause. Nous laissons les experts de Splunk s'en charger. »
>
> **Responsable,** Équipe de la plateforme cloud,Imprivata

Le responsable explique : « En tant que société de sécurité dans le domaine de la santé, nous devons renforcer la sécurité à tous les niveaux. Et c'est pour cela que nous travaillons avec Splunk. Le BAA définit les violations et départage les responsabilités. Nous ne faisons pas affaire avec un fournisseur qui ne nous donne pas cette assurance. »

Des performances plus rapides, une grande valeur ajoutée pour l'entreprise

Le responsable estime qu'environ 100 ingénieurs d'Imprivata interagissent avec Splunk Cloud d'une manière ou d'une autre, parmi lesquels environ 25 ingénieurs de développement créent des applications cloud et peut-être 10 experts Splunk exécutent les recherches les plus sophistiquées en quelques minutes ou secondes. Imprivata a récemment connu son premier mois pendant lequel le personnel de niveau 1 et de niveau 2 du centre d'opérations réseau (NOC) actif 24 h/24 7 jours/7 a traité 100 % des incidents de production avec des systèmes d'automatisation et des manuels sans aucune remontée vers les équipes DevOps, ce qui a considérablement amélioré le temps moyen de réparation et évité des impacts sur les services grâce à une correction proactive des problèmes.

Grâce à ces gains d'efficacité et à l'externalisation des tâches d'administration et de gestion de l'infrastructure vers Splunk Cloud, Imprivata libère le temps de ses ingénieurs hautement qualifiés qui peuvent ainsi utiliser le système pour accomplir des tâches plus rentables pour l'entreprise. Ils consacrent leur temps précieux à résoudre les problèmes, étudier les indicateurs de performance et effectuer des analyses des causes profondes.

Le responsable explique : « Quand quelqu'un me pose une question, je peux lui montrer comment utiliser tout le potentiel de Splunk Cloud pour obtenir des informations utiles. Au lieu de nous contenter d'administrer Splunk, nous l'utilisons pour chercher de l'or. »

Téléchargez Splunk gratuitement ou commencez dès maintenant avec l'essai gratuit de la version cloud. Que ce soit dans le cloud ou sur des serveurs locaux, pour de grandes ou petites équipes, il existe un modèle de déploiement Splunk adapté à vos besoins.

splunk>

En savoir plus : www.splunk.com/asksales

www.splunk.com

20-15395-Tier2-Imprivata-A4-101-CS