splunk>

FICHE PRODUIT

Splunk® Cloud™

La plateforme SaaS leader en termes d'intelligence opérationnelle

AVANTAGES PRINCIPAUX

- **Instantané :** Essai instantané grâce à la Sandbox Splunk en ligne. Conversion instantanée du POC à la production.
- **Sécurisé :** Attestation SOC2 Type 2. Des environnements cloud dédiés pour chaque client.
- **Fiable :** SLA garantissant 100 % de temps de service Toutes les fonctionnalités Splunk Enterprise, y compris les applications, les API et les SDK. Peut évoluer jusqu'à 10 To et plus par jour.
- **Hybride :** Visibilité centralisée sur les déploiements Splunk Cloud (SaaS) et Splunk Enterprise (logiciels).

Présentation de Splunk Cloud

Splunk Cloud fournit des renseignements opérationnels au moyen d'un service dans le cloud. Il offre un moyen simple et rapide d'analyser les données machine générées par l'infrastructure technologique de votre organisation, avec tous les aspects pratiques du logiciel en tant que service (SaaS).

Les données machine sont l'un des segments les plus porteurs, les plus complexes et les plus riche du Big Data. Générées par les systèmes informatiques, les applications, les appareils technologiques, les capteurs et autres, les données machine contiennent un enregistrement catégorique des transactions des utilisateurs, des interactions avec les clients, du comportement du système, des menaces de sécurité et bien plus.

Avec Splunk Cloud, vous pouvez explorer, surveiller et analyser l'ensemble de vos données machine historiques et en temps réel, et produire des rapports. Dépannez les problèmes, étudiez les incidents de sécurité et surveillez votre infrastructure de bout en bout pour éviter les dégradations et les interruptions de service. Vous bénéficiez d'une vue en temps réel et de renseignements précieux sur l'expérience de vos clients, les transactions et d'autres données professionnelles essentielles. Splunk Cloud est disponible sous forme de service et rend vos données machine accessibles, utilisables et exploitables à l'échelle de votre entreprise.

Commencez dès maintenant avec la Sandbox Splunk en ligne gratuite et bénéficiez d'une visibilité centralisée sur toute l'infrastructure de votre organisation, qu'elle soit physique, virtuelle ou dans le cloud.

Un service conçu pour les entreprises

Une architecture pensée pour la disponibilité et la performance. Splunk Cloud est conçu pour assurer 100 % de disponibilité et des performances fiables. Chaque client reçoit un environnement cloud dédié, afin que les performances ne soient jamais affectées par les actions d'un autre client. Splunk Cloud permet également la mise en cluster et la réplication des données, toujours pour assurer la continuité du service et sa disponibilité. Ces caractéristiques sont garanties par notre SLA proposant 100 % de disponibilité.

Évolutivité et flexibilité. Pour plus de souplesse, Splunk Cloud supporte des pics de volumes allant jusqu'à 10x, et peut prendre en charge jusqu'à 10 To par jour.

Une sécurité robuste. Avec des environnements cloud dédiés mis en place pour chaque client, Splunk Cloud s'assure que vos données ne soient jamais en contact avec celles d'un autre client. Splunk cloud propose également des contrôles d'accès basés sur les rôles, des fonctions d'audit et le chiffrement des données en transit et au repos. Splunk Cloud a reçu les attestations SOC2 Type 1 et Type 2. Pour plus d'informations, consultez notre documentation technique : Protéger les données clients dans Splunk Cloud.

Plateforme SaaS complète d'intelligence opérationnelle

Toutes les fonctions de Splunk Enterprise avec tous les avantages du SaaS. Splunk Cloud propose toutes les fonctionnalités de la plateforme leader Splunk Entreprise et donne accès aux applications Splunk, y compris l'application Splunk pour la sécurité des entreprises.

Recherche hybride. Splunk Cloud offre une vision unique et transparente sur l'ensemble des déploiements Splunk Entreprise et Splunk Cloud, ce qui permet aux clients de déployer Splunk en tant que logiciel ou SaaS en fonction de leurs besoins opérationnels, tout en conservant une visibilité centralisée.

Collecte et indexation de toutes les données machine. Collectez et indexez en temps réel toutes les données machine, quels que soient leur source, leur format ou leur origine. Cela inclut les flux de données des applications standard et personnalisées, des serveurs d'applications, des serveurs web, des bases de données, les données de transfert issues des réseaux, des machines virtuelles, des équipements de télécommunications, des systèmes d'exploitation, des capteurs et bien d'autres sources. Il n'est pas nécessaire de « comprendre » les données au départ. Envoyez simplement vos données dans Splunk Cloud pour qu'il commence immédiatement à les recueillir et les indexer, et vous permette ainsi de les explorer et les analyser. Résolvez les problèmes des applications, examinez les incidents de sécurité, surveillez les réseaux et leurs performances, maintenez votre conformité et analysez les nouveaux produits et services.

Recherche et analyse. Que vous soyez responsable de la production , de la sécurité et de l'audit du service informatique, du développement d'applications ou de la collecte et de l'analyse des données de l'entreprise, la recherche constitue toujours le point de départ pour découvrir toutes les nouvelles possibilités que peuvent

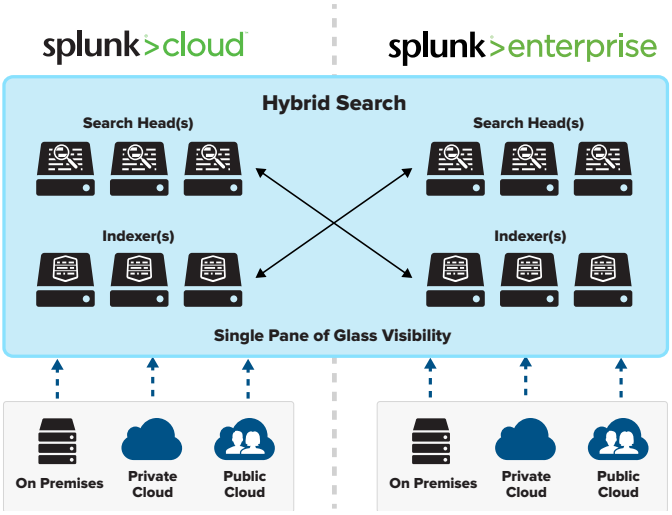

Figure 1 : La recherche hybride permet une visibilité centralisée et transparente.

vous offrir vos données. Splunk Cloud inclut le puissant langage de recherche Splunk, nommé Search Processing Language (SPL™). Sa simplicité d'utilisation permet au débutant de s'adapter facilement, tandis que la puissance de ses fonctionnalités séduit l'expert en analyse de données. Interagissez avec vos données pour en extraire de puissants renseignements. Agrandissez ou réduisez la fenêtre de temps pour révéler rapidement les tendances, les pics et les anomalies. Procédez à une analyse approfondie des résultats et éliminez toutes les perturbations afin de retrouver l'aiguille dans la botte de foin ; corrélez, analysez et prenez en charge les événements en temps réel. Utilisez des termes ou des expressions spécifiques, des opérateurs booléens et de puissantes fonctions d'analyse statistique et de création de rapports.

Plus de connaissances. Splunk Cloud retrouve automatiquement les informations importantes à partir de vos données machine dès l'étape de recherche. Vous avez donc la possibilité d'utiliser immédiatement vos nouvelles sources de données. Vous pouvez enrichir et conférer davantage de sens à vos données machine en identifiant, en nommant et marquant les champs et les termes spécifiques. Ajoutez les informations provenant de sources externes – bases de gestion des actifs, systèmes de gestion des configurations et répertoires d'utilisateurs – pour rendre le système plus intelligent pour tous les utilisateurs.

Surveillance et alerte. Transformez les recherches en alertes en temps réel pour un suivi permanent des seuils que vous avez fixé. Déclenchez automatiquement des actions telles que l'envoi de notifications par e-mail, par flux RSS ou encore pas l'exécution de scripts pour effectuer des actions correctives. Les alertes peuvent être configurées à différents niveaux de précision en fonction des différents seuils, tendances et autres recherches complexes (abandon des paniers d'achat, attaques en force brute et tentatives de fraude).

Rapport et analyse. Élaborez rapidement des graphiques complexes et des tableaux de bord présentant les tendances importantes, les valeurs minimales et maximales, un résumé des valeurs les plus importantes et la fréquence des occurrences. Créez de A à Z des rapports robustes et riches en informations, sans connaissances avancées des commandes de recherche. Accédez aux événements bruts depuis n'importe quel point du graphique. Enregistrez des rapports, intégrez-les à des tableaux de bord et affichez-les sur votre écran ou un support mobile. Créez des PDF à intervalles réguliers pour les communiquer à la direction, aux utilisateurs commerciaux ou aux autres membres du personnel informatique concernés.

Tableaux de bords et vues personnalisées. Combinez facilement différentes vues en tableaux de bord interactifs grâce à l'éditeur dédié. Les tableaux de bord intègrent différents tableaux et visualisations de vos données en temps réel afin de répondre aux besoins d'utilisateurs variés : direction, analystes commerciaux et de sécurité, audits, développeurs et administrateurs système. Les utilisateurs peuvent éditer les tableaux de bord à l'aide d'une interface simple proposant la fonction glisser-déposer, et changer de type de présentation à la volée grâce aux contrôles intégrés.

Apps Splunk. Splunk Cloud prend en charge les applications Splunk et d'autres contenus. Les applications Splunk répondent aux besoins des utilisateurs quels que soient leurs rôles, les cas d'utilisation et les technologies disponibles dans l'entreprise. Elles vous permettent de voir vos données sous un nouveau jour et vous offrent des vues prédéfinies sur les technologies des leaders du marché tels que Linux, Windows, VMware et d'autres.

Environnement développeur riche. Donnez à vos développeurs la possibilité d'intégrer les données et les fonctionnalités de Splunk Cloud dans les applications de l'entreprise à l'aide des kits de développement logiciels (SDKs) pour Java, JavaScript, C#, Python, PHP et Ruby.

Nos clients réussissent avec Splunk Cloud

FINRA, qui est le plus grand régulateur indépendant des sociétés de courtage opérant aux États-Unis, utilise Splunk Cloud à des fins de sécurité et de conformité. FINRA utilise, en outre, Splunk Cloud avec l'application Splunk pour AWS.

« Splunk Cloud fournit des applications qui vous permettent d'extraire une grande valeur de vos données. »

MindTouch, fournisseur leader de logiciels de gestion de clientèle dans le cloud, utilise Splunk Cloud pour bénéficier d'une visibilité et d'analyses en temps réel sur ses activités. Grâce à Splunk Cloud, MindTouch surveille ses logiciels cloud en temps réel et produit des analyses commerciales précieuses pour ses clients, renforçant ainsi leur satisfaction, la résolution proactive des problèmes et l'efficacité des opérations.

« Chez MindTouch, nous avons testé plusieurs services d'analyse de données machine et, en-dehors de Splunk, aucune n'était capable de supporter les rigueurs de nos fortes demandes, » explique Aaron Fulkerson, fondateur et CEO de MindTouch. « Nos produits jouent un rôle stratégique pour nos clients et les 100 % de disponibilité assurés par Splunk Cloud nous permettent de satisfaire leur attente : une continuité parfaite du service. Splunk Cloud nous a permis d'assurer une fiabilité de service 24h/24 et 7j/7. »

Backupify, fournisseur leader d'une solution de sauvegarde cloud à cloud, utilise Splunk Cloud pour établir des corrélations entre les événements de sources de données disparates et surveiller ses systèmes de production. Grâce à Splunk Cloud, Backupify est passé du premier contact commercial à la mise en production en moins d'une semaine, sans aucun effort opérationnel.

« Splunk Cloud nous a fait gagner des mois de développement, » confie Eugene Gorelik, directeur des DevOps de Backupify. « D'autre part, nous estimons avoir obtenu une réduction de 60 à 70 pour cent de nos délais de dépannage en production. »

Commencez dès aujourd'hui

Des abonnements annuels à Splunk Cloud sont proposés pour des volumes de données allant de 5 Go à plusieurs téraoctets par jour ; des options de volumes personnalisés sont disponibles en dehors de cette plage. Pour accéder à Splunk Cloud, veuillez nous contacter à l'adresse sales@splunk.com.

250 Brannan St., San Francisco, CA 94107 info@splunk.com | sales@splunk.com 866-438-7758 | 415-848-8400 apps.splunk.com

splunk> listen to your data™

www.splunk.com

Item # DS-Splunk-Cloud-116-A4_FR