Libérez la puissance du CASB

Les 5 principaux avantages de Lookout Secure Cloud Access

Table des matières

Présentation de Lookout Secure Cloud Access

Dans le paysage numérique actuel basé sur le cloud, les données sont plus précieuses que jamais. Et l'expansion constante de la surface d'attaque fait de la découverte, de la classification et de la protection des données un défi permanent.

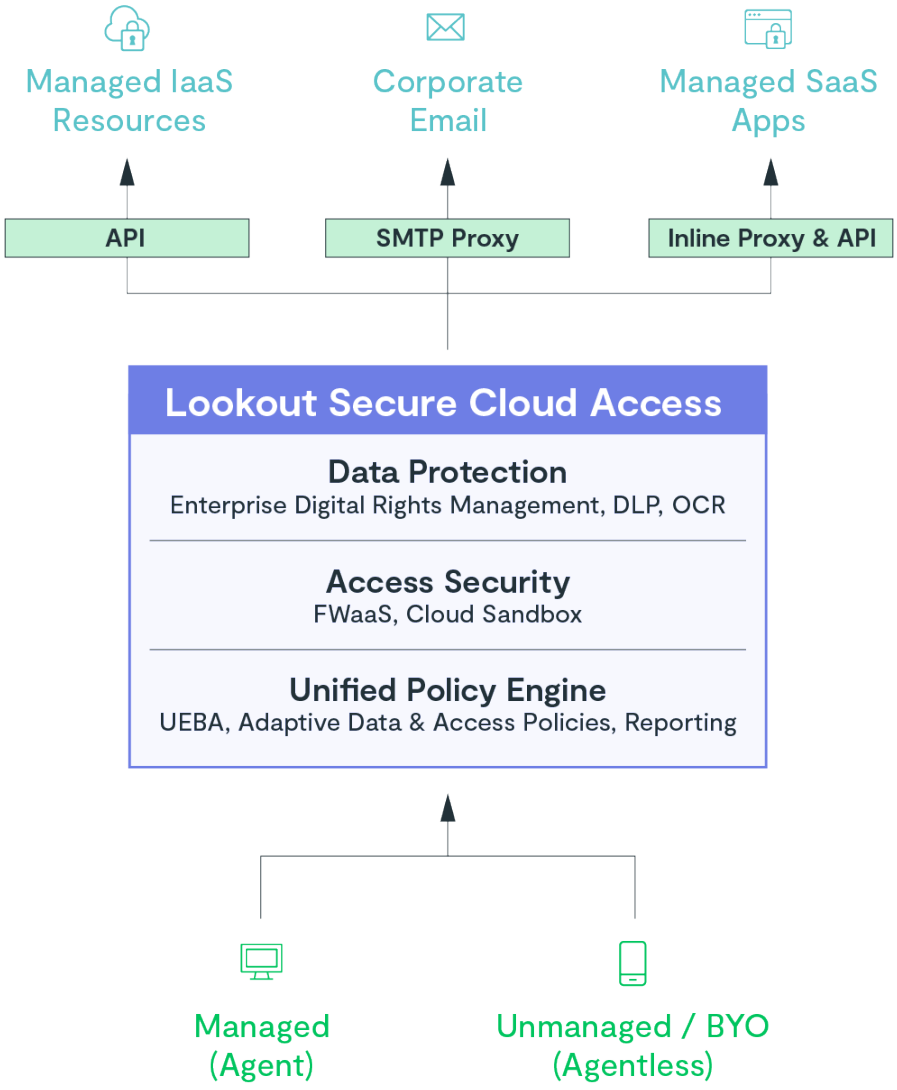
Les chiffres parlent d'eux-mêmes. Seulement 54 % des entreprises savent où sont stockées leurs données sensibles.[1] Un chiffre stupéfiant : 65 % des entreprises collectent tellement de données qu'elles sont incapables de les catégoriser ou de les analyser. [2] Les employés et les sous-traitants accédant aux données depuis divers emplacements et appareils, ce manque de visibilité présente un risque de sécurité majeur, en particulier lorsque les utilisateurs adoptent un comportement à haut risque.

Pour protéger efficacement les données, les entreprises ont besoin d'une visibilité sur l'endroit où se trouvent les données, comment elles sont partagées et qui y a accès.

Lookout Secure Cloud Access est un courtier de sécurité d'accès au cloud (CASB) construit sur la base du Zéro Trust. Un nombre croissant d'entreprises l'utilisent pour détecter, évaluer et protéger les données de toutes les applications cloud et SaaS.

Contrairement aux politiques statiques de sécurité des données des solutions des fournisseurs traditionnels, les politiques adaptatives de Lookout Secure Cloud Access vous donnent le contexte de chaque demande d'accès aux données ou aux applications. Cela réduit les faux positifs pour le partage de données et les tickets d'assistance informatique tout en améliorant la productivité des employés.

Lookout Secure Cloud Access vous permet de contrôler vos données à mesure qu'elles se déplacent, où qu'elles se déplacent. Son moteur de politiques centralisé offre des fonctionnalités granulaires et adaptatives de prévention des pertes de données (DLP), simplifiant la définition et l'application des politiques de sécurité dans toutes les applications cloud et Saas.



Ce livre blanc offre un aperçu de l'approche innovante de Lookout pour fournir des fonctionnalités CASB sur notre plateforme de sécurité unifiée. Il se concentre sur nos principes de conception fondamentaux, qui apportent une valeur stratégique essentielle aux entreprises cherchant à protéger leur actif le plus important : leurs données.

1. https://www.spirion.com/data-classification/
2. https://www.thalesgroup.com/en/markets/digital-identity-and-security/press-release/businesses-collect-more-data-than-they-can-handle-reveals-gemalto

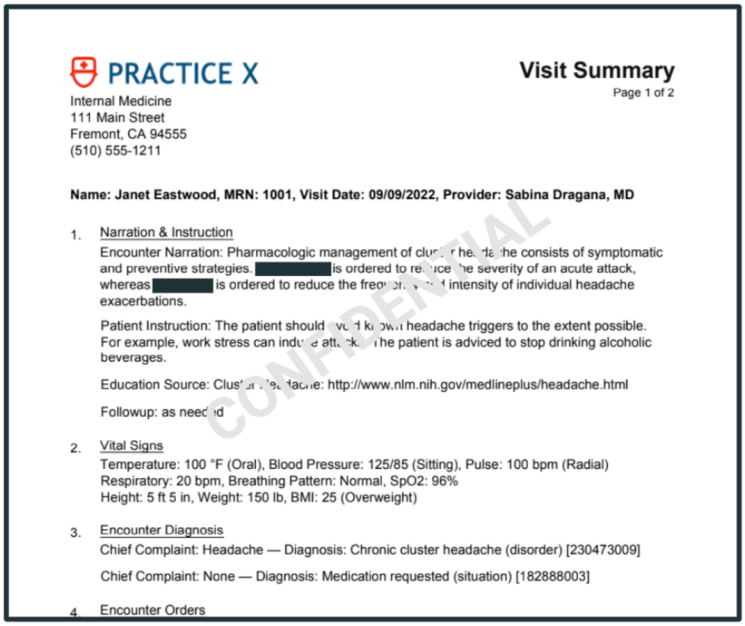
Bénéficiez d'un contrôle granulaire sur vos données

Votre entreprise repose sur une variété de parties prenantes utilisant plusieurs outils de collaboration. Tous ne sont pas abrités au sein de votre entreprise. Et cela présente un véritable défi. Vous devez assurer la sécurité des données, car elles sont partagées entre des sous-traitants et des partenaires externes. Ensuite, une fois les projets terminés, vous devez protéger les données qui ont été partagées.

Les fonctionnalités natives de gestion des droits numériques (DRM) de Lookout Secure Cloud Access offrent un contrôle complet sur les données sensibles, quelle que soit la personne qui les partage ou la manière dont elles sont partagées. Vos données sont en sécurité, que vos employés, sous-traitants et partenaires collaborent par courrier électronique ou via des outils tels que Slack, Microsoft Teams, Box, Dropbox, Google Drive et Microsoft OneDrive.

Contrairement à d'autres solutions de protection des données qui appliquent simplement des politiques pour autoriser ou refuser l'accès aux données, Lookout propose des politiques flexibles qui mettent en place des barrières de sécurité autour de cet accès.

Les technologies de correspondance exacte des données (EDM) et de reconnaissance optique de caractères (OCR) de Lookout identifient et protègent les données sensibles dans une variété de formats, y compris le texte, les images et autres documents numérisés. Lookout analyse les fichiers et les dossiers au fur et à mesure qu'ils sont partagés, et identifie et protège les informations confidentielles sur la base de politiques prédéfinies avec plusieurs options d'application.



PRACTICE X

Visit Summary

Page 1 of 2

Internal Medicine
111 Main Street
Fremont, CA 94555
(510) 555-1211

Name: Janet Eastwood, MRN: 1001, Visit Date: 09/09/2022, Provider: Sabina Dragana, MD

1. Narration & Instruction

Encounter Narration: Pharmacologic management of clu[redacted]he consists of symptomatic and preventive strategies. [redacted] is ordered to re[redacted]e severity of an acute attack, whereas [redacted] is ordered to reduce the freq[redacted] intensity of individual headache exacerbations.

Patient Instruction: The patient should [redacted] headache triggers to the extent possible. For example, work stress can indu[redacted] the patient is adviced to stop drinking alcoholic beverages.

Education Source: Clus[redacted]e: http://www.nlm.nih.gov/medlineplus/headache.html

Followup: as need[redacted]

2. Vital Signs

Temperature: 100 °F (Oral), Blood Pressure: 125/85 (Sitting), Pulse: 100 bpm (Radial)
Respiratory: 20 bpm, Breathing Pattern: Normal, SpO2: 96%
Height: 5 ft 5 in, Weight: 150 lb, BMI: 25 (Overweight)

3. Encounter Diagnosis

Chief Complaint: Headache — Diagnosis: Chronic cluster headache (disorder) [230473009]

Chief Complaint: None — Diagnosis: Medication requested (situation) [182888003]

4. Encounter Orders

Les politiques DRM de Lookout suppriment toutes les informations confidentielles liées aux réglementations sur la confidentialité en matière de santé et intègrent un filigrane pour empêcher le partage de données sensibles avec des utilisateurs non autorisés et ainsi garantir une conformité totale.

Lookout fournit une puissante fonctionnalité DRM native qui permet aux entreprises de contrôler l'accès aux données et au contenu, même après leur partage avec d'autres personnes. Les entreprises conservent le contrôle de leurs données même lorsqu'elles sont stockées sur des appareils non gérés.

- **Masquer ou censurer :** Lookout identifie les données sensibles telles que les numéros de sécurité sociale et les numéros de carte de crédit, ainsi que les données spécifiques aux régions et aux secteurs. Les administrateurs peuvent ainsi appliquer des politiques permettant le partage de données tout en masquant ou en supprimant les informations sensibles. Les outils dépourvus de fonctionnalité DRM peuvent identifier les documents sensibles, mais ils ne peuvent pas masquer ou censurer les informations. Le service informatique est donc obligé de bloquer le partage de données, ce qui entrave l'activité des employés.
- **Filigrane :** pour maintenir la sécurité des données, Lookout peut appliquer automatiquement des filigranes pour alerter les utilisateurs du contenu confidentiel des fichiers sensibles. Les filigranes découragent les employés de prendre des captures d'écran ou de partager les documents.
- **Chiffrer :** Lookout peut chiffrer les fichiers pour garantir que seuls les utilisateurs autorisés y ont accès. Cet accès peut expirer après une durée définie. Le chiffrement peut également être combiné avec d'autres règles de DLP. Par exemple, des informations confidentielles peuvent rester masquées au sein d'un fichier décrypté. Un employé ou un sous-traitant ne pourra donc plus accéder à des documents sensibles une fois qu'il aura quitté une entreprise.

Vous pouvez aller plus loin dans la protection des données en définissant des politiques dynamiques de gestion des droits numériques pour limiter les personnes autorisées à décrypter le contenu. Cela peut impliquer une combinaison d'options configurables telles que les informations d'identification des utilisateurs, les niveaux de risque des utilisateurs et la géolocalisation.

Les avantages des fonctionnalités DRM natives sont évidents : elles facilitent une collaboration sécurisée et améliorent la productivité tout en offrant une protection robuste pour les données sensibles.

Identifiez les anomalies, stoppez les menaces plus vite

Lookout Secure Cloud Access applique l'analyse du comportement des utilisateurs et des entités (UEBA) pour surveiller et évaluer en permanence les utilisateurs, les appareils et les activités. Votre équipe peut ainsi identifier les écarts par rapport au comportement normal, afin que vous puissiez rapidement remédier à un large éventail de menaces potentielles, notamment les menaces internes malveillantes, les comptes compromis et les menaces persistantes avancées (APT).

60 %

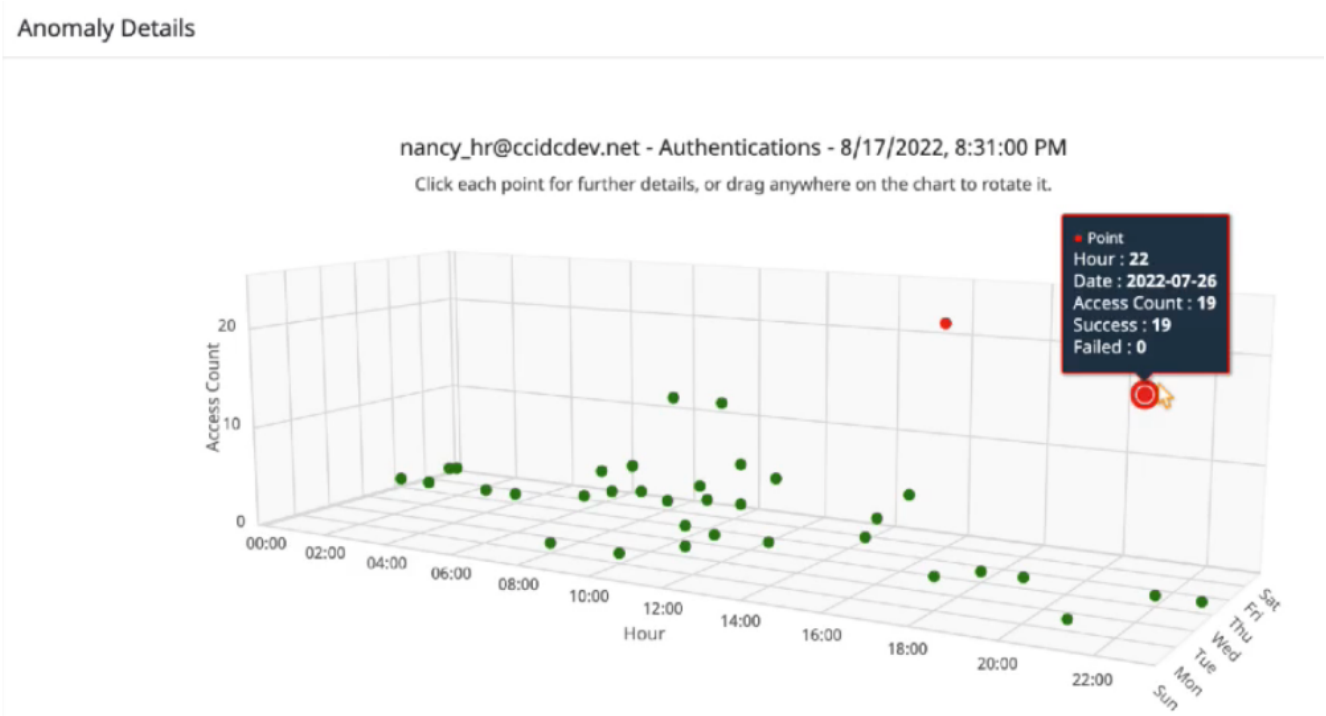
60 % des violations de données sont causées par des utilisateurs authentifiés. En surveillant le comportement des utilisateurs et en identifiant les téléchargements de données volumineux et les anomalies similaires, la technologie UEBA peut détecter les activités malveillantes telles que l'exfiltration de données ou la fraude.

L'UEBA surveille non seulement les anomalies de géolocalisation, mais identifie également les activités à risque telles que les téléchargements massifs d'utilisateurs individuels, l'utilisation d'appareils non gérés susceptibles d'être infectés par des malwares, les tentatives de connexion persistantes, les modifications de données ou l'accès des utilisateurs à de nombreux fichiers auxquels ils n'ont jamais accédé auparavant.

Surveillez les risques avec un accès adaptatif

Grâce à une analyse en temps réel des modèles d'utilisateurs, d'appareils et de localisation, Lookout génère des scores de risque utilisateur précis qui peuvent être personnalisés en fonction de vos politiques. Notre fonctionnalité d'accès adaptatif utilise l'apprentissage automatique pour analyser le comportement des utilisateurs, l'état de l'appareil et la localisation. Lookout attribue un score de risque à chaque utilisateur qui peut augmenter en fonction de l'utilisateur, de l'adresse IP, de l'activité de l'application et de la posture de l'appareil, puis détermine s'il convient d'accorder ou de refuser l'accès à des données spécifiques en fonction de ce score.

Un score de risque élevé peut déclencher des alertes pour le suivi de l'administrateur ou fournir automatiquement des actions supplémentaires basées sur des politiques de sécurité prédéfinies, telles que l'exigence d'une nouvelle authentification de l'utilisateur, le masquage ou la suppression de données, ou encore le blocage complet de l'accès des utilisateurs.



Les anomalies dans les activités de connexion déclenchent des alertes.
Ce graphique montre plusieurs connexions en dehors des dates et heures normales pour un utilisateur.

La solution Secure Cloud Access repose sur les principes du Zéro Trust. Elle valide le contexte d'un utilisateur avant d'accorder l'accès aux applications et aux données, puis vérifie en permanence les droits d'accès. Que les utilisateurs tentent d'accéder aux applications cloud et SaaS à partir d'appareils gérés ou non, ils sont authentifiés et autorisés en fonction de l'état de sécurité de leurs appareils, ainsi que de leurs profils de risque. Le niveau d'accès de chaque utilisateur peut être modifié dynamiquement en fonction des indicateurs de risque.

Réduisez la complexité et les coûts grâce à une plateforme de sécurité unifiée

À mesure que les réseaux et les cybermenaces ont évolué et sont devenus de plus en plus complexes, les développeurs ont créé de nouveaux produits et solutions pour relever les défis qu'ils représentent. Nous avons assisté à une prolifération de produits ponctuels, chacun conçu pour répondre à une menace de sécurité spécifique.

Par conséquent, certaines entreprises gèrent aujourd'hui jusqu'à 76 outils de sécurité. Les équipes sont débordées. Et faire appel à autant de fournisseurs représente un coût.

Ces conditions ont commencé à entraîner une consolidation au sein du marché de la sécurité. Mais ce dont les professionnels de la sécurité ont besoin, c'est d'une visibilité et d'une gestion à partir d'un emplacement unique : une plateforme de sécurité qui intègre diverses technologies de sécurité dans une architecture unique et unifiée.

Les piles de sécurité traditionnelles peuvent être complexes à gérer et coûteuses à acheter et à entretenir. De plus, chaque produit ponctuel possède sa propre console et sa propre interface d'administration. Les paquets doivent traverser plusieurs appareils avant d'atteindre leur destination, ce qui entraîne des problèmes de latence et de performance. Et l'accès basé sur VPN est lent et fastidieux. Sans parler de la mauvaise expérience utilisateur.

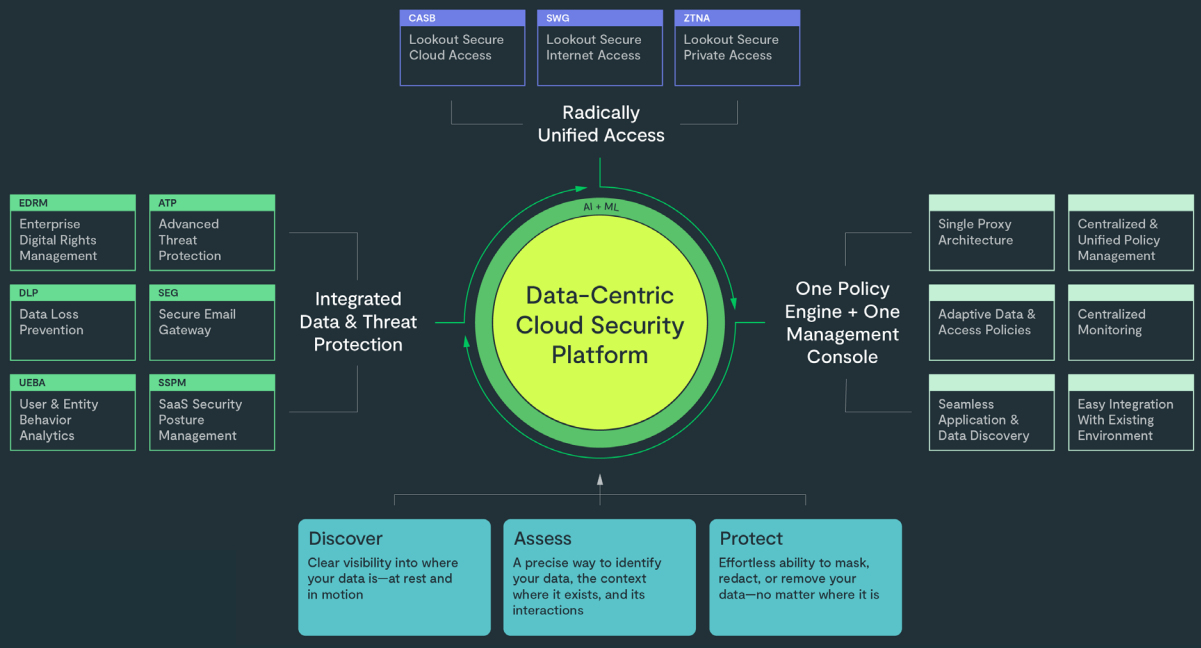
L'architecture de plateforme de sécurité unifiée de Lookout réduit à la fois le coût et la complexité de la gestion de la sécurité. Sa console unique et son interface d'administration vous permettent de dépenser moins pour gérer les politiques et les configurations des outils, intégrer de nouveaux services et traiter avec plusieurs fournisseurs. En comparaison, des produits ponctuels disparates ne s'intègrent pas toujours bien, voire même pas du tout. Ils nécessitent souvent que les équipes informatiques jonglent entre les plateformes, les écrans d'administration et les outils.

Lookout Secure Cloud Access propose des tarifs groupés et des coûts globaux inférieurs pour la configuration, l'administration et la maintenance d'une plateforme unifiée, ce qui peut également réduire les coûts de licence.

L'un des principaux avantages d'une plateforme de sécurité unifiée est qu'elle permet une application centralisée des politiques d'administration, de sorte que vous pouvez appliquer des politiques de sécurité cohérentes, y compris celles pour la DLP et la gouvernance des données, entre les utilisateurs, les appareils et les localisations. Le désalignement des politiques et les mauvaises configurations sont ainsi évités.

Même si l'application centralisée des politiques de Lookout permet une approche unifiée et cohérente de la sécurité du cloud, et offre une protection et une gouvernance étendues au sein d'environnements multicloud et multicentres de données, elle offre également un certain nombre d'avantages supplémentaires :

- **Latence et performances améliorées.** Les produits Lookout Cloud Security utilisent une architecture proxy unique, ce qui réduit le nombre de services par lesquels le trafic doit passer pour l'inspection et l'application des politiques.
- **UEBA en temps réel et criminalistique avancée.** Alimenté par un modèle de données de base unifié, l'UEBA fonctionne en temps réel pour détecter les menaces et y répondre. Cela permet d'améliorer la sécurité et de réduire le temps nécessaire pour enquêter et résoudre les incidents.
- **Suivi cohérent des menaces.** L'architecture de la plateforme de sécurité unifiée de Lookout donne à votre équipe de sécurité une compréhension claire des menaces auxquelles votre entreprise est confrontée, au niveau de toutes les applications et données, afin que vous puissiez les atténuer rapidement.



Répondez aux besoins de sécurité modernes avec un proxy d'application intelligent

Les proxys agissent comme intermédiaires entre les utilisateurs et les applications, en plus de fournir une couche de sécurité précieuse. Cependant, tous les proxys ne sont pas construits de la même façon, et les proxys traditionnels ont tendance à identifier uniquement les destinations comme étant bonnes ou mauvaises, sans fournir de contexte supplémentaire.

Le proxy de Lookout fournit du contexte. Par exemple, il identifie les différences de politique de sécurité entre l'utilisation personnelle et professionnelle d'applications telles que Google Workspace et Microsoft 365, puis adapte l'accès en fonction de ces politiques.

Étant donné que Lookout applique son proxy intelligent spécialement conçu sur une plateforme unifiée, il permet une approche cohérente et complète pour sécuriser tout le trafic Internet, les applications SaaS et les applications d'entreprise privées. Cette architecture proxy unique simplifie la gestion et le déploiement des outils de sécurité, tout en garantissant une application cohérente des politiques.

Le proxy intelligent de Lookout combine des fonctionnalités de sécurité avancées, une application unifiée des politiques et une visibilité complète pour offrir une protection robuste du trafic Internet et des données.

En permettant des fonctionnalités telles que le coaching des utilisateurs, la collaboration sécurisée et le refus du partage public de données sensibles, le proxy d'application intelligent de Lookout établit un équilibre parfait entre productivité et sécurité.

Profitez du cloud public pour une architecture hautement évolutive

Beaucoup trop de fournisseurs de services de sécurité (SSE) sont gênés par des architectures cloud propriétaires héritées pour le déploiement de points de présence (POP).

L'AWS Global Accelerator de Lookout comprend un réseau mondial de 109 points de présence dans 92 villes à travers 50 pays. Cet avantage stratégique est conséquent. Il vous permet de croître plus vite que vos concurrents. Lorsque vous avez besoin d'une nouvelle localisation POP, Lookout peut la déployer en quelques jours seulement, alors que d'autres fournisseurs ont généralement besoin de plusieurs mois.

Lookout permet aux clients d'évoluer n'importe où à la demande avec AWS. Cela vous permet de bénéficier des avantages des microservices cloud-first, une meilleure rapidité des outils et des fonctionnalités, ainsi que d'un meilleur délai de mise sur le marché.

Profitez du cloud public pour bénéficier de vitesse, d'évolutivité et de coûts hautement compétitifs. **76 % d'Internet est accessible depuis l'architecture cloud. 50 % des 1 million de sites les plus importants se trouvent dans le cloud et 42 % des 100 000 premiers sites sont sur Amazon.** En revanche, l'architecture du cloud privé n'a pas la vitesse ni l'agilité nécessaires pour répondre à la nécessité d'adapter votre entreprise de manière fiable et rapide.

Lookout Secure Cloud Access protège vos données dans le cloud

Chaque jour, vos employés chargent, téléchargent et partagent des données d'entreprise à partir de vos applications SaaS approuvées.
Bien que cela soit excellent pour la productivité, cela augmente le risque de fuite de données, de partage non autorisé, de violations de la réglementation ou d'incursions de malwares malveillants.

Lookout Secure Cloud Access protège vos données dans le cloud et vous permet de contrôler l'utilisation des applications cloud gérées et non gérées. Les avantages comprennent :

- L'accélération de la vitesse et de l'ampleur du déploiement ;
- La capacité d'identifier et de stopper les menaces plus vite, et ;
- Un coût réduit.

Franchissez le pas. Obtenez dès maintenant une évaluation des risques SaaS.

Nous avons décrit comment Lookout Secure Cloud Access peut vous aider à protéger vos données, à respecter les réglementations et à générer un retour sur investissement. Il vous suffit maintenant d'en apprendre davantage sur les performances de vos efforts actuels en matière de sécurité des données. Inscrivez-vous à notre évaluation gratuite des risques SaaS. Cette évaluation :

- Identifie les angles morts et les zones qui vous exposent à des risques ;
- Offre une visibilité sur les utilisateurs, les appareils et les données associés à vos applications SaaS, et ;
- Offre des informations exploitables sur la manière dont Lookout peut vous aider.

À propos de Lookout

Lookout, Inc. est une société de sécurité cloud centrée sur les données qui offre une sécurité Zéro Trust en réduisant les risques et en protégeant les données partout où elles sont, sans frontières ni limites. Nous protégeons les données sur les appareils, les applications, les réseaux et le cloud grâce à notre plateforme de sécurité unifiée, cloud-native et aussi fluide et flexible que le monde numérique moderne. Des entreprises de toutes tailles et des organismes gouvernementaux font confiance à Lookout pour protéger leurs données sensibles, leur permettant ainsi de vivre, de travailler et de se connecter librement et en toute sécurité. Pour en savoir plus sur Lookout Cloud Security Platform, visitez lookout.com et suivez-nous sur notre blog, LinkedIn et X (anciennement Twitter).

Pour plus d'informations, visitez
lookout.com

Demandez une démo à
lookout.com/request-a-demo