suridata

SSPM:

Sécuriser la promesse des applications SaaS

Notre mission est d'assurer la sécurité de vos applications SaaS.

Suridata offre la plate-forme SSPM la plus puissante du marché sécurisant des dizaines d'applications SaaS les plus courantes d'aujourd'hui.

Le moteur de profilage intelligent de Suridata signale les problèmes critiques en surveillant les configurations, les applications tierces et les risques d'accès. Suridata utilise alors un moteur de workflow sophistiqué pour s'assurer que les failles de sécurité les plus critiques sont atténuées en premier.

La priorisation favorise l'efficacité. La surveillance couvre vos actifs. La couverture automatisée vous protège.

Bienvenue chez Suridata.

suridata

75 E Santa Clara St, San Jose,
CA 95113, USA

7 Menachem Begin Rd.,
Ramat Gan, Israel

www.suridata.com
Info@Suridata.ai

Distribué en France par AMC SOFT
1, Pl Paul Verlaine 92100 Boulogne Billancourt
https://amcsoft.fr contact@amcsoft.fr Tel : +33680741316

Le SaaS est essentiel pour les entreprises (Mais effrayant pour les équipes de sécurité !)

Une étude Statista de 2022 montre qu'une organisation moyenne prend en charge 110 applications SaaS, soit un bond de 37 % par rapport à l'année précédente.
Les gestionnaires et les travailleurs apprécient la simplicité des applications SaaS pour acheter, apprendre et intégrer dans le travail quotidien de partage, de collaboration et d'intégration avec d'autres applications.
Les responsables de la sécurité deviennent nerveux lorsqu'ils apprennent que leur organisation exécute 110 applications SaaS. Des questions se posent : "Qui a accès à ces applications ?", "Quelles données sont générées ?" et "Comment mon équipe déjà occupée peut-elle prendre en charge 110 applications ?!"

37%

increase in SaaS applications in a single year

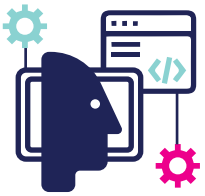
Les anciennes approches de la sécurité SaaS :

Sans intervention

Compter sur les utilisateurs professionnels pour comprendre suffisamment bien l'application et la sécurité pour établir et maintenir une approche de sécurité efficace est une attente irréaliste.

Réglez-le et oubliez-le

Les opérateurs de sécurité sont intimidés par la variété et la complexité des applications métier. Les contrôles SaaS natifs ne prennent en charge que les fonctions de sécurité de base. Les applications sophistiquées, sans surveillance constante, connaissent une sécurité dégradée au fil du temps.



Gérer manuellement

Les applications SaaS génèrent une énorme quantité de « bruit » dans les flux de menaces et les procédures de surveillance de la sécurité, submergeant rapidement même les équipes les plus dotées en ressources.

La nouvelle approche : SaaS, mais vérifiez !

En tant que professionnels de la sécurité, notre travail consiste à permettre l'utilisation d'applications SaaS tout en garantissant la sécurité des données critiques des organisations. La bonne nouvelle qui simplifie le défi est que les risques SaaS se répartissent en trois piliers clés :

Mauvaises configurations.

Problèmes dans les paramètres de sécurité entraînant des risques de pénétration du système.

Applications tierces (Plugins).

Connexion à des applications tierces non vérifiées avec des autorisations excessives entraînant une fuite de données.

Accès

Les informations enregistrées ou gérées dans le cloud peuvent être partagées à outrance.

Sans le savoir, les utilisateurs configurent leurs applications SaaS, ajoutent des plugins et partagent des données sans se rendre compte qu'ils mettent constamment l'ensemble de l'organisation en danger. C'est exactement là que SSPM entre en jeu.

SSPM est-il la bonne solution pour vous ?

SaaS Security Posture Management (SSPM) est une nouvelle catégorie créée par Gartner pour les solutions qui évaluent en continu les risques de sécurité SaaS. Avec l'explosion du nombre et de la complexité des applications SaaS, le potentiel de configurations non sécurisées et d'autorisations excessives est élevé. Une bonne solution SSPM promet d'identifier en permanence les erreurs de configuration et de hiérarchiser les expositions aux risques les plus élevés afin qu'elles puissent être traitées.

Comment fonctionne une bonne solution SSPM :

Maîtriser et gérer des centaines d'applications SaaS est accablant et consommateur de ressources. Suridata peut vous aider. Avec de nouvelles applications, plugins et intégrations ajoutés chaque jour, la seule façon de résoudre ces problèmes est une solution SSPM qui gère :

- la recherche, hiérarchisation et résolution des erreurs de configuration de sécurité
- la surveillance et l'analyse de toutes les applications tierces, la détection des applications à risque et de leur impact sur l'organisation
- l'identification des problèmes d'accès associés au partage excessif de données par les utilisateurs