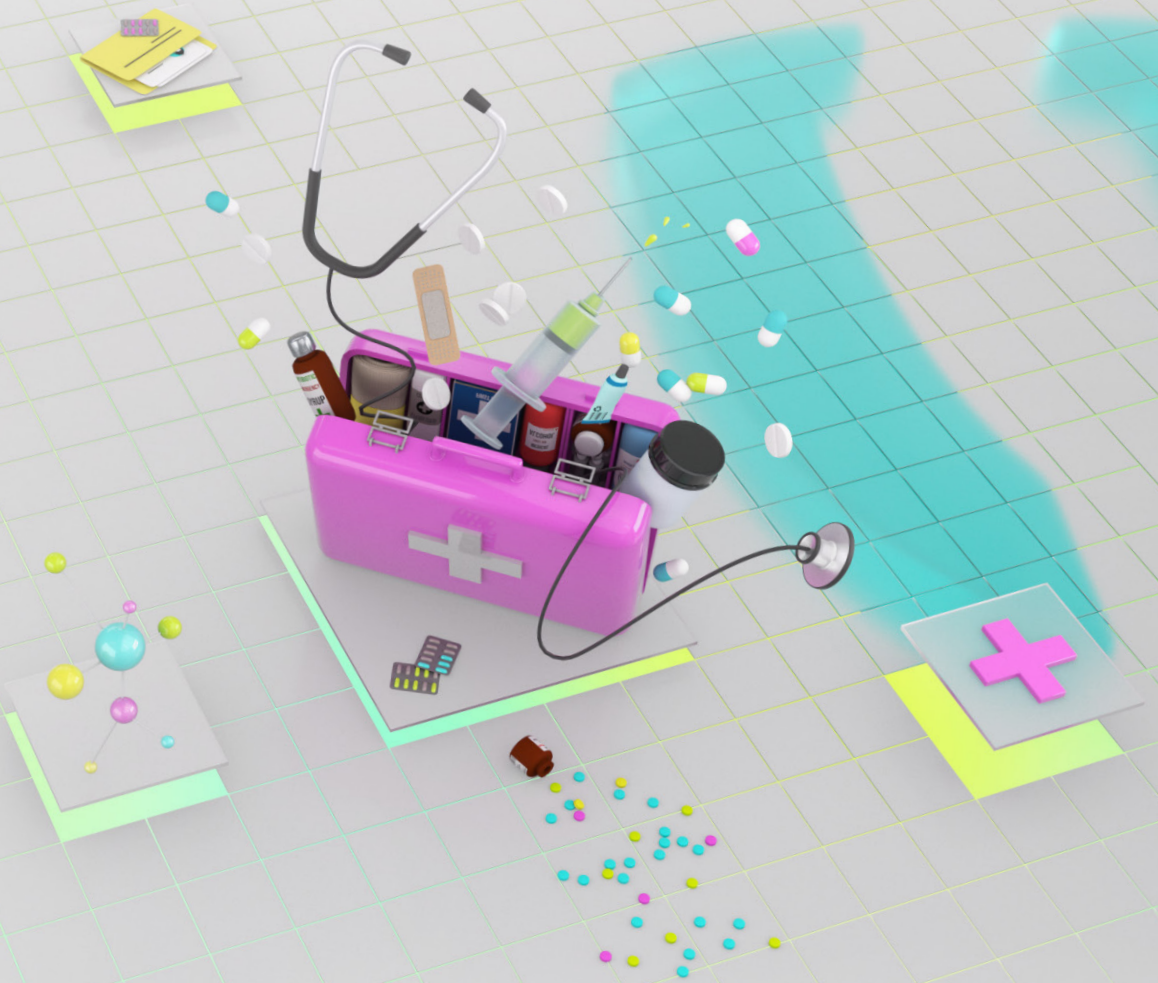
ADAPTIVE SHIELD

Sécurité SaaS dans l'e-Santé

Comment l'entreprise française, leader en Europe, a mis en œuvre un programme agile et robuste à grande échelle

L'ÉTUDE DE CAS RÉUSSIE DE Doctolib



À propos de Doctolib

Depuis 2013, Doctolib poursuit un seul objectif : construire le système de santé dont nous rêvons tous, aux côtés des soignants et des patients. Doctolib soutient 430,000 praticiens et aide 90 millions de personnes à travers l'Europe à prendre soin de leur santé. Avec près de 3 000 salariés, Doctolib est présent dans plus de 30 villes en France, mais aussi en Allemagne, en Italie et aux Pays-Bas.

L'entreprise dispose d'une équipe de sécurité très expérimentée, répartie en trois départements se concentrant sur différents domaines de sécurité : la sécurité des produits, la sécurité de l'entreprise et la sécurité de la plateforme. La sécurité SaaS est gérée par l'équipe de sécurité de l'entreprise, qui suit un processus spécifique pour l'adoption, la surveillance et la maintenance continue des applications critiques de Doctolib.

Le défi de la sécurité SaaS

Initialement, Doctolib utilisait des processus manuels pour sécuriser son écosystème SaaS, ce qui réduisait l'information à des aperçus ponctuels en guise de sécurité. Au fur et à mesure que l'entreprise adoptait davantage d'applications, elle s'est rendue compte que son approche actuelle de gestion de la sécurité et de la conformité à la réglementation du secteur de la santé n'était ni optimale ni évolutive.

L'équipe de sécurité avait besoin d'une visibilité continue sur la configuration des applications afin de garantir une sécurité et une conformité en accord avec les exigences réglementaires. De leur côté, les administrateurs d'applications des différents départements avaient également besoin d'une meilleure visibilité, notamment concernant les milliers d'employés utilisant ces applications et connectant parfois des centaines d'autres applications tierces ou extensions.

D'autres problèmes SaaS sont survenus. Les équipes d'autres départements commençaient à intégrer des applications à l'insu de l'équipe de sécurité. D'où la nécessité d'améliorer la collaboration avec les différents départements pour apprivoiser "une jungle SaaS indomptable".

Pour leur environnement IaaS et PaaS, Doctolib s'appuyait sur un Cloud Security Posture Management (CSPM) et cherchait une solution similaire pour maîtriser leur parc SaaS au vu de l'accroissement exponentiel d'applications en interne.

Processus d'évaluation SSPM

En 2022, Doctolib a mené un appel d'offres avec les trois principaux éditeurs SaaS Security Posture Management (SSPM). Au cours d'une preuve de concept (POC), l'équipe Doctolib a connecté ses applications les plus sensibles et les plus complexes à la plateforme SSPM d'Adaptive Shield.

Après avoir minutieusement comparé et évalué tous les éditeurs pure Player SSPM du marché, Doctolib a choisi Adaptive Shield comme partenaire privilégié.

La solution Adaptive Shield offre une couverture plus large d'applications prêtes à l'emploi s'alignant le mieux à la pile d'applications Doctolib et fournissant une plus grande profondeur de contrôle de sécurité. Adaptive Shield était aussi la seule à associer les utilisateurs à leurs appareils. Enfin, elle dispose d'une interface clients intuitive et simplifie considérablement la collaboration entre les équipes de sécurité et les administrateurs de chaque application.

« Avec Adaptive Shield, nous avons rapidement mis en place une solide politique Zéro Trust à l'échelle de tout notre écosystème SaaS. La plateforme renforce continuellement notre sécurité SaaS en se concentrant sur les erreurs de configuration, en gérant les identités, en détectant les applications non autorisées et en offrant une visibilité sur les appareils de nos utilisateurs SaaS. »

François-Xavier Le Quéré
Corporate IT Senior Security Engineer at Doctolib

Mise en œuvre réussie du programme de sécurité SaaS avec Adaptive Shield

L'équipe de Doctolib est devenue opérationnelle avec Adaptive Shield au premier trimestre 2023 et est passée d'une visibilité ponctuelle, obtenue par des audits manuels, à une visibilité continue et approfondie sur toutes ses applications critiques. L'équipe Customer Success d'Adaptive Shield a participé au processus d'intégration, aidant Doctolib à définir les objectifs et les indicateurs clés, à suivre les meilleures pratiques et à impliquer le personnel approprié à chaque étape. En plus des principales applications surveillées lors du POC, Doctolib a rapidement intégré le maximum d'applications SaaS dans la plateforme via des clés API. Pour la première fois, l'organisation pouvait facilement surveiller ses utilisateurs et leurs autorisations ainsi que les applications tierces inter-connectées à leurs applications SaaS les plus sensibles.

La gestion des appareils était une préoccupation majeure pour Doctolib. En effet, l'intégration d'Adaptive Shield avec Crowdstrike a permis aux membres de l'équipe de sécurité de visualiser les scores Zero Trust ainsi que les vulnérabilités critiques (CVE) des appareils associés, grâce à un inventaire complet des appareils.

L'équipe de sécurité a étendu l'accès à la plateforme Adaptive Shield à plusieurs départements, tels que les équipes GRC, Gestion des appareils, Gestion des risques et vulnérabilités, et SecOps, pour qu'ils puissent surveiller régulièrement leurs domaines respectifs. Ils ont également sollicité les administrateurs d'applications (App Owners) pour faciliter la collaboration et les aider à mieux comprendre les problèmes de configuration SaaS et leurs impacts sur la sécurité SaaS/Cloud du leader d'e-Santé.

Valeur ajoutée et résultats

Grâce à Adaptive Shield, Doctolib a considérablement renforcé la sécurité de son écosystème SaaS en un temps record. La société utilise la plateforme au quotidien qui gère et couvre ainsi tous les aspects de leur sécurité SaaS. L'entreprise a pu identifier les erreurs de configuration qui élargissent sa surface d'attaque et s'assure dorénavant que les applications soient conformes aux normes en vigueur. En plus des contrôles de sécurité présents nativement, Doctolib a créé plus de 40 contrôles de sécurité personnalisés afin que les applications soient aussi conformes aux politiques de sécurité spécifiques à l'entreprise. Grâce au suivi des utilisateurs via la plateforme, Doctolib a amélioré ses capacités de déprovisionnement, supprimant complètement l'accès aux employés qui étaient exclus de l'IdP, mais qui avaient toujours accès à différentes applications SaaS localement. Au cours de l'année, Doctolib n'a cessé d'améliorer sa posture de sécurité, notamment grâce aux deux nouveaux inventaires d'Adaptive Shield. L'inventaire de permissions offre une visibilité granulaire sur les droits et accès des utilisateurs, permettant ainsi d'ajuster correctement les permissions. Parallèlement, l'inventaire de données indique quels fichiers sont partagés publiquement, ce qui aide à limiter le risque de fuite de données.

Aujourd'hui, Doctolib surveille un grand nombre d'intégrations via la plateforme Adaptive Shield. Le leader d'e-Santé s'efforce d'obtenir un score de sécurité se rapprochant au mieux des 100 % sur chaque application et organise des points trimestriels avec les administrateurs d'applications pour mieux contrôler ces mauvais réglages et enfin maîtriser sa "jungle" SaaS.

À l'avenir

Maintenant que l'axe de la prévention des failles de sécurité SaaS est efficace, Doctolib s'attaque au grand axe de la détection en intégrant le module de détection et réponse aux menaces (ITDR) d'Adaptive Shield. Pour faciliter et centraliser les processus internes d'alerting, l'équipe prévoit également d'ajouter des workflows d'alertes intégrés à leurs SOAR/SIEM existants. Enfin, une des prochaines étapes de Doctolib repose sur l'intégration et la surveillance d'applications personnalisées (custom applications) développées en interne.