



Comment Cimpres sécurise les identités cloud sur plusieurs environnements SaaS et Cloud

ÉTUDE DE CAS



« Polyrise (désormais DatAdvantage Cloud) a répondu à tous nos besoins en permettant de détecter et traiter les accès abusifs ou inappropriés, menaces internes, fuites de données et usurpations de comptes survenant sur des services cloud stratégiques. »

Ian Amit, CSO de Cimpres



Cette étude de cas a été publiée par Polyrise, une entreprise acquise par Varonis en 2020.

[EN SAVOIR PLUS >](#)

EN BREF



Cimpres est une entreprise cotée en bourse (NASDAQ : CMPR) dont le siège est basé à Dublin, en Irlande. Ses 15 sites réunissent plus de 16 000 employés, et elle se spécialise dans la fabrication de produits sur mesure, notamment de la papeterie, de la signalétique et des vêtements.

LES PROBLÈMES

- Nombre élevé d'utilisateurs internes et d'autres BU
- Plusieurs sites et identités cloud à gérer et sécuriser
- Maintien de la visibilité sur les utilisateurs cloud disposant de trop de privilèges

LA SOLUTION

- **DatAdvantage Cloud** (anciennement Polyrize) cartographie et analyse les relations entre les utilisateurs et les données sur l'ensemble des applications et services cloud.

RÉSULTATS

- Surveillance de l'activité et alertes en cas d'accès abusifs ou inappropriés, de menaces internes, de fuites de données et d'usurpation de compte
- Corrélation des identités entre les environnements SaaS et IaaS

Les problèmes

Toute la beauté de Cimpres réside dans son organisation ouverte et distribuée qui permet de personnaliser des designs très rapidement, de fabriquer les produits selon le principe du flux-tendu et de les livrer avec des délais réduits. Malheureusement, ce modèle pose aussi un vrai problème de sécurité, car il implique l'existence de nombreux utilisateurs internes et d'autres BU basés sur différents sites et dont les identités cloud doivent être gérées et sécurisées.



« Le maintien d'une visibilité sur nos utilisateurs cloud disposant de trop de privilèges, les comptes inactifs et les shadow admins constituait une de nos principales difficultés, explique Ian Amit, le CSO de Cimpres. C'est à cause du risque posé par le téléchargement et le partage inappropriés de nos données stratégiques par le biais de divers services cloud que nous avons décidé de chercher de nouvelles solutions de sécurité axées sur les identités. »

La solution

Cimpres a invité Polyrize (désormais Varonis) à participer à une évaluation comparative réunissant des fournisseurs de sécurité classiques et plusieurs start-ups. « Nous nous penchons sur différents moyens de répondre à notre besoin d'élasticité en matière de mise en œuvre des droits depuis quelques années déjà, poursuit Ian Amit. Au cours du processus, Polyrize est vraiment apparue comme la solution la plus complète du marché. Elle propose une visibilité sur plusieurs plateformes, ce qui nous permet de nous concentrer sur les cas d'utilisation les plus risqués, mais aussi de réduire notre surface d'attaque, et ce en continu. »

Résultats

Après avoir configuré les processus de sorte à éliminer le grand nombre d'identités obsolètes qui avaient proliféré partout dans l'entreprise, ajuster les privilèges définis de manière incorrecte et éliminer les shadow admins, Cimpres utilise principalement Polyrize (aujourd'hui DatAdvantage Cloud) pour surveiller l'activité et détecter les menaces.



« Polyrize (désormais DatAdvantage Cloud) a répondu à tous nos besoins en permettant de détecter et traiter les accès abusifs ou inappropriés, menaces internes, fuites de données et usurpations de comptes survenant sur des services cloud stratégiques, conclut Ian Amit. Polyrize est capable de corréler les identités sur les environnements SaaS et IaaS pour s'assurer que même les attaques les plus sophistiquées seront détectées en temps réel. C'est un vrai atout dans notre environnement toujours plus hétérogène et tourné vers le cloud. »

Par ailleurs, l'équipe d'assistance de Cimpres lui communique régulièrement des informations lui permettant de se préparer aux menaces dans le cloud les plus récentes.



**Surveillez et détectez
les menaces sur vos
applications et dépôts de
données cloud stratégiques.**

[DEMANDER UNE DÉMO](#)