CASE STUDY

Renforcer le contrôle des droits d'accès à privilèges sans charge supplémentaire

Le fournisseur de services cloud 3DS OUTSCALE rationalise la gestion des droits d'accès à privilèges et renforce la sécurité grâce à l'automatisation de la supervision, de l'enregistrement et du contrôle des mots de passe avec One Identity Safeguard

L'essentiel

- **Entreprise**
  3DS OUTSCALE
- **Secteur**
  Fournisseur de services Cloud
- **Pays**
  France
- **Site web**
  https://fr.outscale.com/

Les défis

- L'investigation des incidents d'accès à privilèges occupait une personne de l'équipe à plein temps
- Les tâches répétitives de supervision et de reporting étaient source d'erreur
- Le manque de données en temps réel empêchait de gérer les incidents de manière proactive
- Les mots de passe étaient mutualisés pour éviter des processus de requêtes et de réactivation trop longs

Les résultats

- Le risque d'erreur humaine est éradiqué, ce qui renforce la sécurité et la conformité
- Grâce à une gestion proactive, les problèmes de sécurité sont identifiés avant toute incidence
- L'automatisation des mots de passe améliore la protection sans impacter la productivité

Solutions

- One Identity Safeguard

3DS OUTSCALE n'avait aucun moyen de gérer et de superviser les sessions par droit d'accès à privilèges de façon proactive, car les administrateurs partageaient les mots de passe pour éviter des processus de requête et de réactivation qui prenaient trop de temps. De plus, l'entreprise devait allouer tout le temps d'une personne de son équipe informatique à l'investigation des incidents d'accès à privilèges.

En déployant One Identity Safeguard, 3DS OUTSCALE a gagné en efficacité pour contrôler et superviser les droits d'accès à privilèges. De plus, en automatisant les processus relatifs aux mots de passe, l'entreprise a renforcé sa sécurité sans affecter la productivité.

Le fournisseur de services cloud 3DS OUTSCALE est spécialisé dans la protection des données de ses clients, mais aussi des accès internes à leurs systèmes. Édouard Camoin, responsable de la sécurité des systèmes d'information chez 3DS OUTSCALE, précise : « La donnée client est notre actif le plus important. Il faut la protéger en permanence. Toutefois, il ne faut pas oublier le contrôle d'accès interne. La sécurité doit être étanche de bout en bout ».

Resserrer les accès à privilèges

3DS OUTSCALE cherchait à améliorer la supervision des administrateurs détenant des droits d'accès à privilèges. Chez 3DS OUTSCALE, les administrateurs disposent d'habilitations de niveau un, deux ou trois. Les administrateurs de niveau un, souvent des fournisseurs, disposent de droits d'accès restreints aux systèmes internes et suivent des procédures de support bien précises. Par contre, les administrateurs de niveau deux et trois ont des droits d'accès à privilèges variables aux systèmes internes stratégiques sur lesquels repose le cloud central de 3DS OUTSCALE.

« Avec Safeguard, la façon dont nous supervisons les sessions à privilèges est bien plus efficace. Les données des sessions sont à portée de main et nous pouvons remonter à tout ce qui peut déclencher une alerte »

Édouard Camoin,
responsable de la sécurité des systèmes d'information chez 3DS OUTSCALE

Les administrateurs de niveau deux et trois peuvent accéder au cœur de l'infrastructure par le biais d'un hôte bastion. La supervision de chaque session administrateur par ce bastion et son reporting se faisaient en grande partie manuellement. Un membre de l'équipe était occupé à plein temps à investiguer les incidents potentiels de sécurité et à générer des rapports d'audit. Édouard Camoin explique : « Notre but consistait à contrôler et enregistrer les accès à privilèges pour avoir à disposition les données sur toutes les sessions. En cas d'apparition d'une brèche de sécurité, nous voulions être plus proactifs pour pouvoir la traiter avant qu'elle ne pose problème ».

Édouard Camoin voulait aussi supprimer tout risque dans la gestion des mots de passe des sessions à privilèges car le système habituellement utilisé soulevait des dangers, entre autres avec des mots de passe génériques. « Je voulais réduire le risque de ce processus en l'automatisant » ajoute-t-il.

Une solution facile à déployer

Pour réduire le risque associé aux accès, 3DS OUTSCALE a implémenté Safeguard de One Identity. Selon Édouard Camoin, les solutions ont été simples à déployer et à manager. 3DS OUTSCALE a opté pour le mode opératoire Instant On de Safeguard qui a permis de ne pas modifier les flux de travail des utilisateurs. Par conséquent, les administrateurs ont pu continuer à utiliser leurs applications client habituelles pour accéder aux serveurs et aux systèmes sans perturbation de leurs tâches quotidiennes. « Éviter de trop changer les habitudes des administrateurs a été un grand avantage de Safeguard pour faciliter son adoption » commente Édouard Camoin.

Économie d'une charge de travail d'une personne

3DS OUTSCALE n'a plus besoin qu'un membre de l'équipe travaille à plein temps à l'investigation des incidents potentiels de sécurité, parce que Safeguard enregistre toutes les sessions d'accès à privilèges. Ces sessions sont de plus indexées, ce qui facilite leur recherche. « Avec Safeguard, la façon dont nous supervisons les sessions à privilèges est bien plus efficace » indique Édouard Camoin. « Les données des sessions sont à portée de main et nous pouvons remonter à tout ce qui peut déclencher une alerte. De plus, toutes les preuves sont disponibles pour mener des audits et répondre aux exigences de conformité ».

L'erreur humaine éliminée, la sécurité se renforce

En supprimant le facteur humain de la supervision des accès à privilèges, 3DS OUTSCALE a éliminé l'erreur humaine. « Beaucoup de tâches de supervision simples et répétitives sont sujettes aux erreurs. Pour nous, cela posait un gros problème au plan de la sécurité et de la conformité » note Édouard Camoin. « Nous ne pouvons nous permettre aucune erreur ».

3DS OUTSCALE utilise aussi l'enregistrement des sessions à privilèges pour sensibiliser davantage les administrateurs à la sécurité. Édouard Camoin précise : « Nous reprenons les sessions pour aider les administrateurs à comprendre que nous devons rester concentrés sur la sécurité. C'est un outil de formation qui fonctionne bien ».

« Je n'ai plus l'impression que nous sommes impuissants jusqu'à ce qu'un incident survienne. Avec Safeguard, nous pouvons agir tout de suite, avant tout dommage »

Édouard Camoin,
responsable de la sécurité des systèmes d'information chez 3DS OUTSCALE

« Avec Safeguard, la façon dont nous supervisons les sessions à privilèges est bien plus efficace. Les données des sessions sont à portée de main et nous pouvons remonter à tout ce qui peut déclencher une alerte »

Édouard Camoin,
responsable de la sécurité des systèmes d'information chez 3DS OUTSCALE

La gestion proactive devient possible

Point essentiel pour Édouard Camoin, 3DS OUTSCALE peut gérer les droits d'accès à privilèges de façon proactive. En effet, Safeguard supervise les sessions en temps réel et peut lancer l'alerte si quelque chose sortant de l'ordinaire est repéré, par exemple une commande à risque ou une fenêtre de titre suspecte dans une connexion de graphe. « Je n'ai plus l'impression que nous sommes impuissants jusqu'à ce qu'un incident survienne » apprécie Édouard Camoin. « Avec Safeguard, nous pouvons agir tout de suite, avant tout dommage ».

Efficacité accrue grâce à l'automatisation

La sécurité associée aux mots de passe est bien plus rigoureuse, sans alourdir les charges de gestion. Grâce à Safeguard, les requêtes et la réactivation de mots de passe des administrateurs sont automatisées pour une efficacité maximum. 3DS OUTSCALE a également ajusté sur-mesure le processus d'approbation aux directives de l'entreprise. « Nous n'utilisons plus de mots de passe mutualisés » poursuit Édouard Camoin. « L'ensemble du processus d'allocation et de réactivation est plutôt fluide avec Safeguard, ce qui nous évite des retards ».

À propos de One Identity

La gamme de solutions de gestion des accès et des identités (IAM) de One Identity adapte l'IAM au terrain. Elle inclut notamment des solutions modulaires et intégrées centrées sur l'entreprise et prêtes pour l'avenir de la gouvernance des identités, de la gestion des accès et des privilèges.

Consultez tous les cas d'étude de One Identity à l'adresse OneIdentity.com/casestudies