Comment Toulouse Métropole s'appuie sur Varonis pour la gestion de ses incidents de sécurité

> La plateforme Varonis nous permet d'accompagner sereinement la forte croissance de nos volumes de données, y compris sur les nouveaux périmètres cloud, et d'analyser nos alertes de sécurité.

À propos de cette étude de cas :

Notre client est Toulouse Métropole, une métropole regroupant, avec d'autres intercommunalités, une partie de l'agglomération de Toulouse, dans la Haute-Garonne.

En bref

Les défis

- Gérer l'augmentation des besoins de stockage on-premises et sur un nombre croissant de services SaaS
- Assurer la conformité avec le RGPD et le RGS (Référentiel général de sécurité) et la confidentialité des données
- Renforcer les compétences des équipes en matière de sécurité

La solution

Plateforme Varonis de sécurité des données :

- Permet de suivre les accès aux comptes, documenter le renouvellement des mots de passe, et génère des rapports précieux lors des audits de conformité
- Permet de rattraper les erreurs des utilisateurs lors de la manipulation de leurs données
- Facilite la gestion des alertes de sécurité et leur analyse

Les résultats

- Visibilité sur l'ensemble des fichiers on-premises et dans le cloud
- Conformité RGPD et RGS
- Équipes de sécurité délivrées des tâches les plus fastidieuses et les moins valorisantes
- Prise en compte des alertes de sécurité et facilité d'analyse

Les défis

Faire face à une augmentation massive du volume de données

Outre un volume de données en augmentation constante (plus de 300TO), le périmètre de Toulouse Métropole a évolué, avec l'arrivée d'un nombre croissant de nouveaux services dans le cloud.

Assurer la surveillance des données sur la messagerie Microsoft 365, dans les espaces de stockage cloud, à travers les flux, et bien entendu toujours on-premises, devient un défi majeur.

> **« Sur un tel périmètre, retrouver rapidement les données après l'erreur d'un utilisateur pouvait devenir un véritable casse-tête, » explique Catherine Lopez, responsable d'exploitation SI, Toulouse Métropole.**

Protéger les données et assurer la conformité RGPD et RGS

Les audits RGS réclament de nombreux rapports afin d'évaluer la conformité des traitements de données et leur protection.

Sur un périmètre aussi vaste et complexe que celui de Toulouse-Métropole, cela s'avère une tâche colossale et très chronophage. Et la question se pose également pour générer des rapports de conformité RGPD.

VARONIS

Consacrer des heures à établir un rapport n'est pas une tâche très valorisante pour les équipes, et cela vient prendre du temps sur des missions plus valorisantes.

Gérer les alertes de sécurité et l'analyse des incidents

La gestion manuelle des alertes de sécurité et leur analyse pouvaient prendre des heures, consacrées essentiellement à lancer des scripts PowerShell. Outre la répétition des tâches pour les équipes, ne pas pouvoir répondre immédiatement en situation de suspicion est inenvisageable, à l'heure où les cyberattaques explosent.

« Avec l'augmentation des ransomware qui ciblent les collectivités et l'augmentation de la surface d'attaque de Toulouse Métropole, la gestion des incidents est devenue clé. »

La solution

Plateforme Varonis de sécurité des données

Afin de disposer d'une vision transverse et immédiate de ses données, qu'elles soient hébergées localement comme dans les différents environnements cloud, SharePoint Online, Exchange, et OneDrive, Toulouse Métropole s'appuie sur la plateforme Varonis.

Cliente depuis 2015, la Métropole a commencé par déployer la plateforme Varonis on-premises, afin de retrouver le contrôle de ses larges volumes de données dans un environnement Windows, Linux et cloud.

Aujourd'hui, avec la montée en puissance de Microsoft 365 (messagerie, stockage et espaces collaboratifs, qui permettent de partager des documents avec un contrôle limité de la sécurité informatique, la solution a été étendue aux environnements cloud de manière transparente.

Elle permet désormais de gérer sans couture l'ensemble des données de son système d'information hybride.

> **« Avant de choisir la plateforme Varonis, nous n'avions aucune visibilité de la traçabilité ni de l'exploitation de nos données, » précise Catherine.**

Répondre aux exigences des audits de conformité

Lors d'audits RGS (Référentiel général de sécurité), la plateforme Varonis permet à Toulouse Métropole de suivre précisément les accès aux comptes et le renouvellement des mots de passe. Au-delà de pouvoir éditer un état précis en quelques minutes pour répondre aux demandes des auditeurs, la plateforme de Varonis permet à la Métropole de protéger ses données, où qu'elles se trouvent.

> **Varonis nous permet de générer des rapports RGPD immédiatement et de répondre aux exigences en matière de protection des données. Et lors d'audits RGS, la plateforme édite une vue précise de la vie des comptes. Cela fait gagner du temps aux auditeurs, mais aussi à nos équipes.**

Détecter les menaces et analyser les alertes de sécurité

La plateforme Varonis permet de prévenir de tout comportement anormal et d'alerter immédiatement les équipes de sécurité, notamment pour prévenir Toulouse Métropole de toute tentative d'attaque par ransomware. Varonis accompagne ainsi les équipes de sécurité dans leurs tâches quotidiennes, tout en leur faisant gagner en compétence, sur les tâches liées à la réponse à incidents.

> **Des tâches qui prenaient deux heures nous prennent désormais 5 minutes. C'est un gain de temps non négligeable. Mais la plateforme Varonis nous permet surtout d'avoir une réponse immédiate lorsque l'on soupçonne une tentative d'attaque. Dans ce contexte, le délai moyen de résolution sert les équipes de sécurité.**

> **C'est sans doute l'aspect le plus précieux de Varonis : une intégration complète entre l'alerte et l'analyse.**

Les résultats

Un contrôle sur les données utilisateurs, où qu'elles soient hébergées

Toulouse Métropole a désormais une vision unifiée de ses données utilisateurs au sein de son système d'information hydride. Qu'elles soient hébergées localement, en tant que pièce-jointe dans la messagerie Microsoft 365 ou encore dans un espace de travail collaboratif sur le cloud, les données sont suivies, gérées et peuvent être récupérées simplement, même après qu'un utilisateur ait déplacé un répertoire entier par erreur.

Ainsi, les problématiques d'extension de la surface d'accès liés à ces ruptures de permissions deviennent immédiatement identifiables et contenues.

> **« Nous sommes passés de traitements manuels à des traitements automatiques, précâblés. Nous n'avons désormais plus qu'à paramétrer ce que l'on souhaite obtenir, et non à le concevoir, » ajoute Catherine.**

Une protection des données qui rime avec conformité

La Métropole est désormais en mesure de générer des rapports et des vues instantanées sur l'usage des comptes utilisateurs ou de leurs données, à la demande des auditeurs. Les équipes comme les auditeurs gagnent du temps et réduisent la charge.

Le temps ainsi libéré est mis à profit pour que les équipes montent en compétences sur des sujets de sécurité opérationnels, grâce notamment à l'accompagnement actif de Varonis pour aider les équipes à toujours mieux tirer parti de la solution.

> **Varonis nous permet de suivre les accès aux comptes utilisateurs et de documenter le renouvellement des mots de passe.**

Une sécurité renforcée contre les ransomware

La plateforme Varonis aide les équipes de Toulouse Métropole à mieux traiter les alertes et, grâce à un workflow d'analyse, évaluer et traiter le risque. Accompagnées par Varonis dans leur montée en compétence, les équipes disposent ainsi immédiatement des informations nécessaires à une analyse des événements, pour une sécurité du SI contre toute tentative d'attaque.

> **Nous nous reposons beaucoup sur la gestion des alertes de la plateforme Varonis, ainsi que les capacités d'analyse de ces dernières qu'elle offre aux équipes. Varonis nous permet de rendre des informations complexes nettement plus compréhensibles beaucoup plus rapidement et plus facilement.**

> **« Varonis a depuis toujours cette capacité à nous accompagner pour suivre l'évolution des technologies et de nos besoins dans le cloud et on-premises, » explique Catherine.**

« Grâce à Varonis, les équipes analysent aisément une situation juste après qu'elle a eu lieu, en s'appuyant sur des corrélations qui pourraient paraître simples, alors que derrière il y a des informations très verbeuses et très lourdes à creuser. »

VARONIS

Sécurisez vos données dans le cloud et on-premises.

Demander une démo