Varonis aide la Haute Autorité de Santé à mieux gérer la gouvernance de ses données

« «Nos données sont notre bien le plus précieux. Il est rassurant d'avoir un outil qui nous permette de savoir précisément ce qui est fait avec ! »

En France, la Haute Autorité de santé est une « autorité publique indépendante à caractère scientifique dotée de la personnalité morale » créée par la loi française du 13 août 2004 relative à l'assurance maladie. Sa vocation est scientifique.

POINTS CLÉS

Les défis

+ Réduire significativement le nombre d'interfaces d'administration de la sécurité
+ Disposer d'une vision unifiée sur l'ensemble de l'environnement Microsoft 365 après avoir migré dans le Cloud
+ Se préparer à l'arrivée de la directive européenne NIS2 sur le volet de la gouvernance des données

La solution

La Plateforme de Sécurité des Données de Varonis + Service de protection Varonis MDDR :

+ Offre une visibilité et un contrôle sur l'ensemble des données de l'entreprise
+ Découvre et protège les données sensibles dans le cloud et on-premises
+ Réduit de manière proactive l'exposition des données sensibles
+ Offre des alertes en temps réel sur les menaces potentielles, basées sur l'analyse comportementale

Les résultats

+ Offre une visibilité sur l'ensemble de l'écosystème M365
+ Approche de conformité NIS2 plus rassurante
+ Meilleure prise en compte des alertes et facilité d'analyse
+ Équipes de sécurité libérées des tâches les plus fastidieuses et les moins valorisantes

LES DÉFIS

La multiplication des interfaces nuit à la visibilité et à l'efficacité des équipes

Lors de sa migration vers Microsoft 365, les équipes IT de la Haute Autorité de Santé (HAS) à Toulouse se sont retrouvées face à une multiplication des interfaces d'administration : aux 22 outils de sécurité existants s'ajoutaient désormais toutes les consoles Microsoft 365 qui n'existaient pas auparavant.

> **« Nous nous sommes retrouvés face à toutes ces consoles, avec une problématique de personnel. Il nous fallait trouver une solution pour gérer l'ensemble d'une manière efficace. Nous savions que, sinon, nous n'y arriverions pas. L'équipe ne s'appropriait pas toutes ces interfaces, notamment en ce qui concerne la sécurité et la gouvernance »,** se souvient Jean-Yves Perier, adjoint au chef de service du Système d'Information, responsable de l'unité technique Sécurité et Assistance aux Utilisateurs.

La HAS se met alors en quête d'un outil capable d'agréger non seulement les interfaces des outils Microsoft 365, mais aussi — si possible — d'aller au-delà en intégrant d'autres produits de sécurité.

Assurer un meilleur contrôle sur les données dans le Cloud

Un autre défi est apparu au même moment : l'arrivée des outils de collaboration de Microsoft qui permettent aux utilisateurs de créer facilement des liens de partage qui peuvent facilement surexposer des informations sensibles à des collègues et même à n'importe qui sur l'internet.

Ces liens créent des angles morts pour les équipes informatiques et de sécurité.

> **« Là non plus, nous n'avions aucune visibilité sur ces partages ».**

Il nous fallait alors remédier à cela. D'autant que, même si la HAS ne gère que 500 utilisateurs en interne, ces partages sont ouverts à l'ensemble de sa communauté externe. Soit au total près de 10 000 utilisateurs, qui échangent au quotidien une grande quantité de documents.

La HAS faisait ainsi face à un double défi : celui de renforcer à la fois la gouvernance et le contrôle de ses données réparties à travers des environnements très hétérogènes, et de le faire de manière efficace avec une équipe réduite.

> **« Notre migration vers Microsoft 365 a révélé une grosse problématique en matière de personnel.**
>
> **L'équipe savait que si l'on ne trouvait pas rapidement un outil capable d'agréger toutes les interfaces d'administration, ça allait être très compliqué de gérer ce nouveau périmètre ».**

« Notre migration vers Microsoft 365 a révélé une grosse problématique en matière de personnel ».

LA SOLUTION

La Plateforme de Sécurité des Données de Varonis

Après la migration vers Microsoft 365 et face au double défi de l'explosion du nombre de consoles d'administration et du manque de visibilité sur les données partagées par une communauté étendue de 10 000 utilisateurs, les équipes internes ont rapidement compris qu'elles ne pourraient pas faire face seules.

> **« Nous avons souhaité un outil capable de consolider tout ça pour nous. Notre RSSI connaissait déjà Varonis sur la protection de l'AD, et la fonctionnalité de consolidation des interfaces venait d'être annoncée. Tout était aligné ! ».**

La HAS initie alors rapidement un PoC. S'ensuit, face au constat d'adoption rapide par les équipes, la décision de s'équiper de la Plateforme de Sécurité des Données de Varonis, en plus des solutions dédiées à la protection de l'AD.

Grâce à l'accompagnement des équipes Varonis, le déploiement et la prise en main de la solution a pu se faire en douceur :

> **« C'est crucial. Sans cela, nous n'utiliserions pas la solution aussi bien, et nous ne pourrions envisager une montée progressive dans la complexité de nos usages, de nos alertes et de nos scénarios ».**

Le déploiement a permis dans un premier temps d'intégrer 22 outils de sécurité existants en plus des interfaces d'administration de Microsoft 365.

Cette capacité à voir l'ensemble des consoles d'administration en un seul outil est bien entendu le bénéfice immédiat du projet en termes d'optimisation du quotidien. Mais hors de question de s'arrêter là pour autant : grâce à sa nouvelle supervision centralisée des consoles, la HAS a bien sûr immédiatement mis en place quelques alertes et de premiers rapports quotidiens et hebdomadaires.

> **« Ce sont pour le moment des alertes simples, par exemple sur les volumes de téléchargement, les connexions utilisateurs suspectes (qui, comment, d'où ?), etc. Mais cela permet déjà d'observer des choses et de commencer à faire de la pédagogie auprès des utilisateurs quand nous observons des écarts. »**

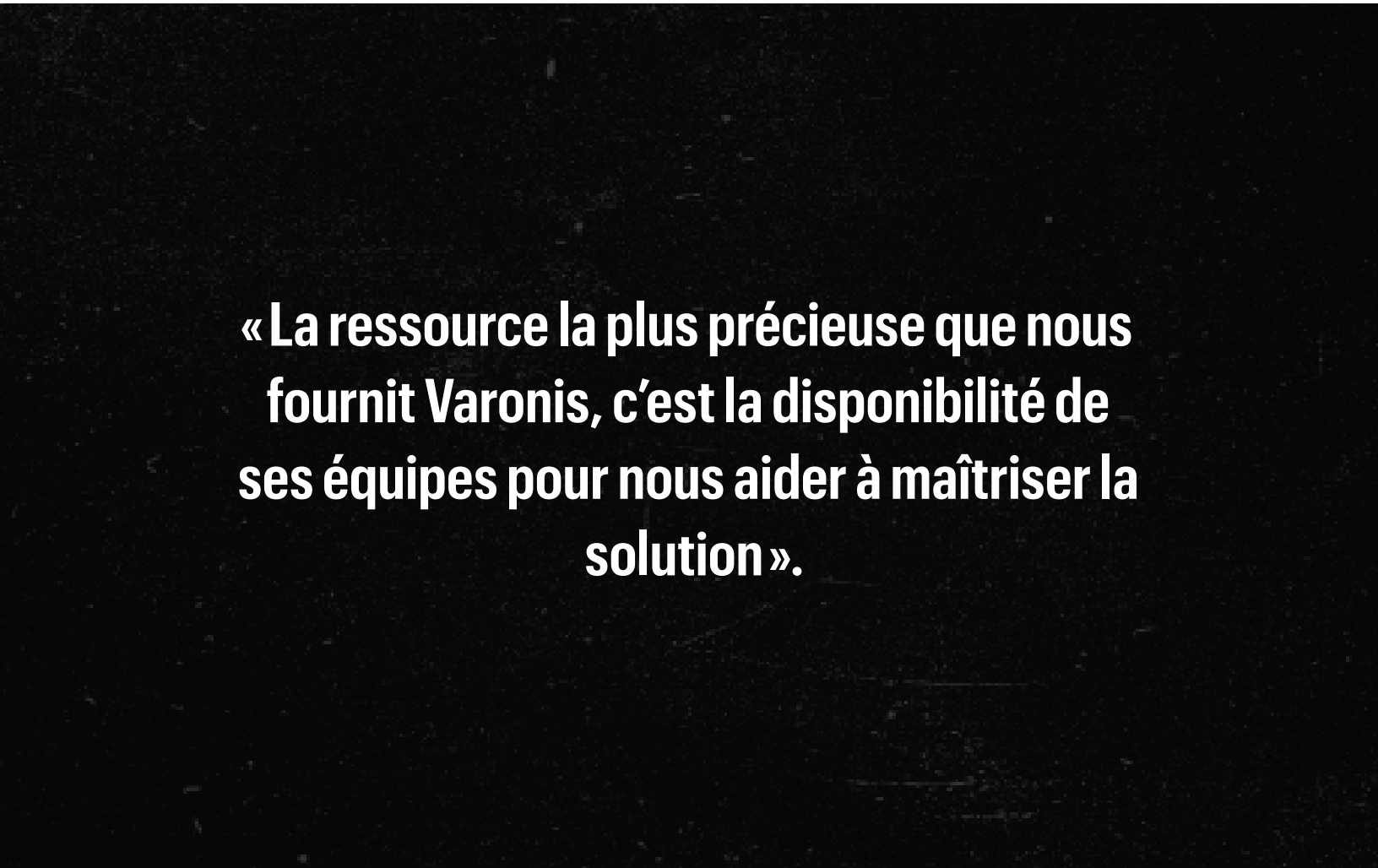
Et d'autres viendront, bien sûr…

> **« C'est un outil vraiment très bien fait, très puissant, mais complexe. Il est bon de prendre le temps de s'y familiariser. Et pour cela nous sommes bien aidés par les équipes Varonis, avec qui nous organisons des ateliers de travail toutes les 3 à 4 semaines afin d'avancer dans le déploiement de nouvelles règles et de nouveaux contrôles. Loin de nous faire perdre du temps, cette progressivité nous laisse également le temps de communiquer avec nos utilisateurs, là aussi pour faire de la pédagogie ».**

La plateforme Varonis permet aux équipes sécurité de contrôler le trafic interne et externe, et d'identifier rapidement des anomalies éventuelles. Et les équipes Varonis veillent 24/7.

Aujourd'hui, les alertes générées par ces premières règles sont veillées par les équipes Varonis 24/7, dans le cadre du service de réponse à incidents Varonis MDDR (Managed Data Detection & Response). Cela permet une vigilance de tous les instants, y compris pour une équipe interne réduite.

> **« Nous avons d'ailleurs pu tester l'efficacité du dispositif lorsque l'un de nos utilisateurs a décidé de renommer en masse les fichiers de son répertoire de travail ! La solution et les équipes de réponse à incident de Varonis ont identifié l'action et cela nous a permis de lever le doute rapidement ».**



LES RÉSULTATS

Des équipes sécurité plus performantes et moins surchargées dans la gestion des alertes

Grâce à la pplateforme Varonis, l'équipe dispose de plus de temps pour se concentrer sur les tâches et les alertes importantes. Ils ne perdent pas de temps.

> **« Aujourd'hui, pour gérer 22 outils de sécurité et l'ensemble des interfaces d'administration de la sécurité de Microsoft 365, j'y passe une demi-journée par semaine. Et encore, parce que je veux faire ça bien. Tout compris, avec l'équipe, nous devons y passer les ¾ d'une journée chaque semaine. Ce n'est vraiment rien à l'échelle de notre semaine ».**

Un temps réduit, mais cohérent avec un usage encore simple de la plateforme.

Gouvernance de la donnée et sécurisation de l'IA

L'usage est toutefois appelé à s'étendre. L'un des plus grands dangers est que les utilisateurs cherchent constamment à optimiser leur productivité, souvent en recourant à des outils non validés par l'entreprise, ce qui augmente les risques de fuite ou de mauvaise utilisation des données.

Outre un test du module Copilot destiné à identifier les dérives possibles de l'intelligence artificielle générative, notamment en termes de partage ou d'exfiltration de données sensibles, la HAS s'apprête à utiliser Varonis pour soutenir ses initiatives en matière de gouvernance des données.

> **« Notre bien le plus précieux, c'est nos données et notre image. Il est donc important, et rassurant, de disposer d'un outil capable de nous montrer clairement ce qui est fait avec ce bien précieux».**

Alerter sur les usages non conformes de la donnée

Dans le contexte de la mise en conformité avec la directive NIS2, l'un des prochains objectifs pour la HAS en matière de gouvernance de la donnée est notamment d'être en mesure de la classifier, et d'alerter lors de situations ou d'usages non conformes (telles que des données sensibles stockées dans un emplacement inapproprié).

> **« Nous avons déjà eu à livrer à notre direction un rapport sur l'exfiltration de données, et nous en aurions été incapables sans la solution Varonis. Savoir que la solution nous assiste est rassurant ».**
>
> **« Notre collaboration croissante avec Varonis nous offre la possibilité d'être en totale adéquation avec les pré-requis liés à la gestion et la protection de nos données. Elle nous simplifie la tâche au quotidien ! ».**
>
> **« L'outil nous rend plus sereins face à l'arrivée de la directive NIS2. Nous savons que si demain nous devons faire des recherches très critiques sur l'usage de nos données, et en particulier dans un contexte judiciaire, la plateforme Varonis sera essentielle. »**

« L'outil nous rend plus sereins face à l'arrivée de la directive NIS2. Nous savons que si demain nous devons faire des recherches très critiques sur l'usage de nos données, et en particulier dans un contexte judiciaire, la plateforme Varonis sera essentielle ».

Se tenir prêt pour la directive NIS2 ?

Et ce, par le biais d'une meilleure gouvernance de la donnée via l'usage de l'IA notamment.

Demandez une démo