

Customer stories

L'hôpital limbourgeois ZOL gère la complexité croissante avec une nouvelle plateforme de gestion des données



“

Auparavant, les ingénieurs devaient tous les jours déplacer les bandes et contrôler les back-ups. Aujourd'hui, ils disposent de plus de temps pour se consacrer à d'autres projets

**Kurt Gielen
ICT Operations
Manager** ”

Forte digitalisation dans l'hôpital

Le Ziekenhuis Oost-Limburg (ZOL) est un hôpital non universitaire et dynamique de 811 lits. Les activités sont réparties sur trois campus : le campus Sint-Jan à Genk, le campus Sint-Barbara à Lanaken et le Centre médical André Dumont à Waterschei. Un quatrième campus viendra bientôt s'y ajouter avec l'acquisition de l'hôpital Maas en Kempen à Maaseik.

Comme la plupart des acteurs de la santé, l'hôpital est confronté à une forte augmentation des applications digitales, tant pour gérer le bâtiment et son fonctionnement qu'à l'égard des patients, avec par exemple le Dossier Patient Informatisé (DPI). « Nous sommes donc de plus en plus dépendants de l'informatique, mais la complexité des systèmes augmente aussi considérablement », constate Kurt Gielen, ICT Operations Manager du ZOL.

Le système de back-up de l'hôpital n'était plus adapté à la croissance explosive de la quantité de données. Kurt Gielen : « Lorsque nous sommes passés au nouveau DPI, nous utilisons encore une technologie de back-up classique (bandes, disques durs classiques...) qui était en outre répartie sur différents centres de données. » Pour l'hôpital, le défi consistait, d'une part, à simplifier la gestion journalière et, d'autre part, à trouver une solution évolutive permettant à l'équipe informatique d'absorber une croissance forte et rapide en fonction de la capacité et de la performance.

La solution

Pour répondre à ce défi, le ZOL a collaboré avec Orange Cyberdefense. « Nous travaillons avec Orange Cyberdefense depuis des années pour notre réseau principal et nos solutions de sécurité. Ce partenaire est parti de cette approche pour élaborer une solution de back-up », explique Kurt Gielen.

La solution comprend deux volets : une solution Rubrik permettant d'organiser très simplement le back-up de l'hôpital dans une optique SLA, sur laquelle vient se greffer une solution de stockage d'objets 100 % compatible S3 de Cloudian. Grâce à cette dernière, l'hôpital est en mesure d'assumer une évolutivité presque illimitée.

Les avantages

Combiner deux technologies en une seule solution ne relève pas de l'évidence. Kurt Gielen : « Mais c'est justement l'atout majeur et la véritable plus-value de la collaboration avec Orange Cyberdefense. Cette entreprise fournit l'expertise adéquate et des ingénieurs qualifiés, et les déploie judicieusement pour parvenir à une solution performante. »

Les avantages de la solution Rubrik s'expriment surtout dans la gestion quotidienne considérablement simplifiée. C'est « installé puis oublié ». La solution offre également diverses nouvelles fonctionnalités qui aident beaucoup l'équipe informatique à développer un environnement de test et d'acceptation. Rubrik Live Mount, par exemple, permet de mettre très rapidement des bases de données à disposition à ces fins.

L'atout majeur de Cloudian réside dans le fait que, grâce à l'évolutivité modulaire et exabyte, l'hôpital ne doit plus se préoccuper des archives et de la capacité de stockage correspondante. « Nous avons déjà plus d'un pétaoctet de données dans nos archives et, grâce à la solution standardisée S3 de Cloudian, nous disposons d'une évolutivité illimitée. Nous pourrions donc, dans les années à venir, poursuivre notre croissance en fonction des besoins de l'hôpital qui ne cessent d'augmenter dans ce domaine », souligne Kurt.

Le résultat

La nouvelle solution a permis à l'hôpital d'améliorer considérablement son fonctionnement opérationnel et technique. Le processus de back-up est plus automatisé. Auparavant, les ingénieurs devaient tous les jours déplacer les bandes et contrôler les back-ups. Aujourd'hui, ils disposent de plus de temps pour se consacrer à d'autres projets (à plus grande valeur ajoutée).

Par ailleurs, l'équipe informatique est désormais en mesure de réaliser certaines choses qui étaient auparavant impossibles ou qui duraient très longtemps. Avant, il fallait compter 12 à 14 heures pour mettre en place un environnement de test. Aujourd'hui, cela ne prend que quelques minutes. Kurt : « Et bien que les patients et les médecins en soient un peu plus éloignés, il s'agit d'une solution avec laquelle nous pouvons également mettre leurs données en sécurité ou avec laquelle ils peuvent utiliser de manière sûre leurs données confidentielles. »

L'avenir

Cette nouvelle solution forme la base de la stratégie de gestion de données axée sur l'avenir. « La cybersecurity et les back-ups sont de plus en plus imbriqués, car le back-up est un point central où convergent toutes les données. Cela nous donne la possibilité d'analyser les données et de constater les anomalies. C'est la prochaine étape que nous voulons franchir », conclut Kurt Gielen.



Gestion simple : solution pour la forte augmentation de la complexité des systèmes informatiques.



Évolutivité : la quantité de données connaît une croissance explosive. Cette solution permet à l'hôpital d'absorber une croissance rapide en termes de capacité et de performance.



Résistant au ransomware : grâce au système de fichiers inaltérable, les cryptolockers ne sont pas en mesure de verrouiller les back-ups existants.



Grâce au savoir-faire et à l'expertise d'Orange Cyberdefense, le planning et la mise en œuvre ont été étonnamment simples.

Orange Cyberdefense

Orange Cyberdefense est l'entité du groupe Orange spécialisée en cybersécurité. En tant que prestataire de sécurité de référence en Europe, nous mettons tout en œuvre pour bâtir une société numérique plus sûre.

Nous sommes un prestataire de services de sécurité pilotée par les données et d'analyse de la menace, procurant une vision inégalée des menaces existantes ou émergentes.

Orange Cyberdefense jouit d'une expérience de plus de 25 ans dans le domaine de la sécurité de l'information, emploie plus de 250 chercheurs et analystes dans 16 SOC, 10 CyberSOC et 4 centres CERT répartis dans le monde entier ainsi que des équipes commerciales et de support dans 160 pays. Nous sommes fiers de pouvoir affirmer que nous proposons une protection globale avec une expertise locale et que nous assurons le support de nos clients tout au long du cycle de vie des menaces.

Pour toute information complémentaire, consultez le site <https://orangecyberdefense.com/>