

Cytiva

Unifier les opérations de sécurité de la biotechnologie, partout dans le monde



Nom

Cytiva

Secteurs

Entreprise/Biotechnologie

Localisation

International

Produits

Security Center hébergé, Synergis, Omnicast, ClearID, Plan Manager, Clearance, Mission Control

Partenaires

Johnson Controls



Comment Cytiva a réorganisé la sécurité physique sur ses sites mondiaux à l'aide de Genetec Security Center en mode hébergé et ClearID

Dotée d'une longue expérience dans la biotechnologie, Cytiva fournit des technologies et des services qui optimisent et accélèrent le développement et la fabrication de produits thérapeutiques. Présente dans plus de 40 pays, la société met en œuvre une innovation centrée sur le client, allant de la recherche biologique fondamentale au développement de vaccins novateurs, de médicaments biologiques et de nouvelles thérapies cellulaires et géniques. Avec plus de 100 sites à travers dans le monde, Cytiva sait que pour façonner l'avenir des sciences de la vie, il faut une maîtrise stricte de tous les aspects liés à la sécurité.

Trouver la solution optimale pour une vaste feuille de route numérique

Lorsque Cytiva a été acquise par une nouvelle société mère, il a fallu tout de suite transformer et moderniser les systèmes et l'infrastructure de sécurité physique. L'entreprise souhaitait abandonner les solutions locales obsolètes et disparates pour une approche axée sur le cloud afin de minimiser le poids de la gestion d'infrastructure pour ses équipes.

De grands projets d'expansion se profilant à l'horizon, elle recherchait par conséquent une solution de sécurité évolutive et tournée vers l'avenir, capable de satisfaire les besoins immédiats comme ceux de l'avenir.

Selon Larry Allen, Responsable Produits techniques pour les installations, la sécurité et la gestion de crise chez Cytiva : « Suite à l'acquisition, nous sommes devenus beaucoup plus autonomes en tant qu'entité. Nous avons davantage de liberté pour investir dans nos projets et faire évoluer notre sécurité physique comme nous le souhaitions. Notre premier objectif était de simplifier nos opérations

grâce à l'unification et de standardiser la vidéo et le contrôle d'accès sur une seule plateforme. Par ailleurs, nous souhaitions accéder à un ensemble de fonctionnalités, de modules externes et d'intégrations qui s'aligneraient sur notre feuille de route numérique. »

Pour assurer le bon déroulement du processus de la prise de décision au déploiement, Cytiva a fait appel à Johnson Controls, un Partenaire distributeur Genetec agréé possédant une vaste expertise dans les déploiements complexes d'entreprise. Après avoir écouté les exigences clés de Cytiva et aidé l'équipe à consolider un plan, Johnson Controls a conçu l'ensemble de l'architecture de la plateforme en s'appuyant sur la version hébergée de Genetec Security Center.

Mise en place d'un déploiement hybride

Aujourd'hui, l'équipe de Cytiva gère le contrôle d'accès et la vidéosurveillance à l'aide de Genetec Security Center sur 17 de ses sites de recherche et de fabrication les plus stratégiques. Chaque site compte en moyenne 20 caméras et 30 portes, mais les plus grands sites comptent jusqu'à 500 caméras et 550 points d'accès.

Selon Larry Allen, Security Center en mode hébergé fut à la fois un choix stratégique et une décision bien accueillie par l'équipe. « Nous travaillons dans le domaine du biotraitement, de la thérapie génique et de l'analyse cellulaire, pas dans les logiciels de sécurité physique. Auparavant, il était difficile de tenir le rythme des correctifs de vulnérabilité et des mises à jour logicielles, et tout simplement d'assurer la gestion de ces environnements. En choisissant Genetec Security Center en mode hébergé, nous minimisons la gestion du cycle

de vie du logiciel. Comme le fournisseur en gère l'essentiel, nous gagnons du temps et nous bénéficions d'une fiabilité accrue », explique Larry Allen.

Avec Security Center en mode hébergé, Cytiva a pu élaborer un modèle de déploiement hybride. De plus, le système de contrôle d'accès Synergis^{MC} est entièrement hébergé dans le cloud, tandis que le système de surveillance Omnicast^{MC} et tous les enregistrements vidéo sont gérés et stockés localement sur différents sites.

Sur certains petits sites de Cytiva, la société a installé le dispositif tout-en-un Streamvault^{MC}, préchargé avec les solutions de vidéosurveillance et de contrôle d'accès pour faciliter le déploiement. La fonction Federation^{MC} assure le lien entre tous les systèmes et offre une vue totalement unifiée de la sécurité.

« La version hébergée de Security Center nous permet d'étendre rapidement la sécurité sur l'ensemble des sites, nouveaux comme existants, en faisant appel aux services cloud en priorité. Cet aspect est essentiel pour nous, car lors d'une telle mise à niveau globale à l'échelle de l'entreprise, il devient inenvisageable de multiplier les serveurs. Le temps que notre équipe passerait à gérer ce matériel augmenterait le coût total de possession. Il arrive un moment où cela n'est plus rentable. Avec le mode hébergé et le déploiement hybride de Security Center, nous pouvons assurer nos opérations de façon bien plus économe », poursuit Larry Allen.

Avec une base solide en place, l'équipe de Cytiva ajoute progressivement de nouvelles caractéristiques et fonctionnalités pour renforcer la confiance et l'efficacité des opérateurs. Johnson Controls assure la formation et l'assistance sur site à l'équipe Cytiva. L'entreprise a également mis en place Plan Manager, l'interface cartographique de Security Center, pour aider les opérateurs à se retrouver sur chaque site et à traiter rapidement les alarmes ou les événements qui se déclenchent.

30 % de gain d'efficacité des ressources grâce à Genetec ClearID

Dans le cadre de la conception et du développement, Johnson Controls a également recommandé à Cytiva de mettre en œuvre Genetec ClearID^{MC}. Cette solution de gestion des accès physiques a non seulement contribué à standardiser et à simplifier les processus de demande d'accès des employés, mais des niveaux d'automatisation plus élevés ont également fait gagner beaucoup de temps au personnel.

« Depuis l'installation de Genetec ClearID, nous avons constaté un gain d'efficacité de 30 % en termes de ressources. Nous avons amélioré nos processus de flux de travail ; il nous faut moins de temps pour créer et gérer les identifiants et les droits d'accès des employés, ce qui représente un énorme avantage pour notre équipe », explique Larry Allen.

Avant ClearID, chaque site avait ses propres politiques et procédures concernant la gestion des demandes d'accès. La plupart du temps, un employé contactait l'équipe de sécurité et demandait un accès. Une fois certains critères remplis, l'équipe lui accordait l'accès manuellement en modifiant les droits d'accès du titulaire de carte dans l'ancien système de contrôle d'accès.

Selon Larry Allen, « il arrivait que les demandes d'accès passent entre les mailles du filet ou que quelqu'un n'obtienne pas l'approbation demandée. Avec ClearID, l'aspect libre-service représente l'avantage le plus important. Désormais, la demande d'accès peut être effectuée par l'employé, et l'ensemble du processus est automatisé jusqu'à ce que l'accès soit accordé par l'approbateur de la zone attribuée. »

Le module ClearID a également permis à l'équipe de Cytiva de renforcer la qualité des audits. « Désormais, lors d'un audit, nous pouvons rapidement démontrer que chaque étape, de la demande de l'employé à l'approbation et à l'octroi de l'accès par la personne autorisée, est enregistrée automatiquement par ClearID. Il n'y a aucune possibilité d'erreur humaine, donc du point de vue de l'audit, nous disposons de données de meilleure qualité pour renforcer la conformité réglementaire », poursuit Larry Allen.

Renforcer les bonnes pratiques de conformité et de cybersécurité

Avec plus de 100 sites à travers le monde, Cytiva s'engage à maintenir une sécurité de haut niveau tout en garantissant le respect des diverses réglementations. Il s'agit notamment du Règlement général sur la protection des données (RGPD), de la Biomedical Advanced Research and Development Authority (BARDA) et des Chemical Facility Anti-Terrorism Standards (normes antiterroristes des installations chimiques – CFATS), entre autres. Une part du respect de ces réglementations et du bon fonctionnement des opérations passe par le maintien des bonnes pratiques de cybersécurité et de respect de la vie privée.

« Auparavant, davantage de personnes devaient avoir accès à nos systèmes de sécurité physique pour traiter les demandes d'accès. Comme les processus d'octroi sont désormais tous automatisés dans ClearID, nous avons pu restreindre l'accès à l'application elle-même à un groupe très limité d'utilisateurs du système. Nos opérations de sécurité sont ainsi bien plus sûres et résilientes », résume Larry Allen.

Même pendant la phase de prise de décision, l'équipe doit s'assurer que chaque prestataire avec lequel elle s'associe et chaque solution qu'elle déploie respecte des normes très strictes de cybersécurité et de respect de la vie privée. Après avoir mis Genetec à l'épreuve au cours d'une évaluation complète, l'équipe de cybersécurité interne a été convaincue d'aller dans la bonne direction.

« De nombreuses entreprises n'ont pas beaucoup progressé dans le domaine de la cybersécurité, ou n'étaient pas en mesure de fournir les informations dont nous avions besoin. Genetec a répondu avec un grand nombre de documents pour étayer notre évaluation et a tout renvoyé en très peu de temps. Cette réactivité nous a permis de savoir qu'ils étaient non seulement préparés, mais également bien informés concernant tous les aspects de la cybersécurité », a déclaré Allen.

En Europe, l'équipe a également commencé à tester Genetec Clearance^{MC} pour plus de respect de la vie privée et pour mieux répondre aux exigences du RGPD. Ce système de gestion des preuves numériques basé sur le cloud servira bien sûr à simplifier les enquêtes en compilant les preuves dans un emplacement central ; mais l'équipe peut également utiliser Clearance pour répondre rapidement aux demandes d'informations des citoyens, automatiser les périodes de conservation des données et activer l'anonymisation automatique afin de mieux protéger l'identité des individus.

Renforcer la sécurité dans le domaine de la biotechnologie grâce aux bons partenariats

Bien que Cytiva ait fait d'énormes progrès dans la modernisation de sa sécurité physique, sa feuille de route numérique comprend encore plusieurs étapes. D'autres extensions de site et des ajouts de fonctionnalités sont prévus selon un plan échelonné sur 3, 5 et 10 ans.

Les priorités actuelles incluent la mise en place et l'essai du module d'aide à la décision Genetec Mission Control^{MC}. Parce qu'il guide les opérateurs dans la réponse aux incidents à l'aide de procédures opérationnelles standard, l'équipe estime que cet outil lui permettra de renforcer davantage la conformité et la sécurité.

À l'avenir, Cytiva tient à tirer le meilleur parti de ses investissements afin d'en récolter les fruits d'un point de vue opérationnel ; par exemple, en ajoutant des caméras spécialisées dans le but de surveiller certains sites de fabrication dont les processus sont fortement réglementés. La société envisage également de mettre en place des centres d'opérations régionaux qui contribueront à rationaliser la sécurité et la réponse aux incidents sur l'ensemble des sites mondiaux.

« Genetec Security Center et le module ClearID nous ont permis de standardiser nos politiques et nos opérations de sécurité sur l'ensemble de nos sites. Nous avons également pu optimiser nos ressources car nous travaillons plus efficacement au sein d'une seule plateforme unifiée. Notre partenariat avec Johnson Controls et Genetec a joué un rôle déterminant dans notre succès. Nous abordons en toute confiance la poursuite de notre feuille de route numérique, surtout en sachant que tout est centré sur cette solution robuste et unifiée », conclut Larry Allen.



« Il arrivait que les demandes d'accès passent entre les mailles du filet ou que quelqu'un n'obtienne pas l'approbation demandée. Avec ClearID, l'aspect libre-service représente l'avantage le plus important. Désormais, la demande d'accès peut être effectuée par l'employé, et l'ensemble du processus est automatisé jusqu'à ce que l'accès soit accordé par l'approbateur de la zone attribuée. »