Global Headquarters

Genetec Inc.
2280 Alfred Nobel Blvd.
Montreal, Quebec H4S 2A4
Canada

T: +1 514.332.4000

Media Alert

Les principales tendances qui marqueront le secteur de la sécurité physique en 2021 selon Genetec

Ces tendances incluent les applications innovantes des technologies de sécurité, l'attention particulière donnée au respect de la vie privée, les préoccupations grandissantes en matière de cybersécurité, l'adoption du cloud hybride et la plus forte vigilance vis-à-vis des fournisseurs.

MONTRÉAL, le 7 janvier 2021—Genetec Inc. ("Genetec"), un leader des solutions de sécurité unifiée, de sécurité publique, d'opérations et de business intelligence, partage aujourd'hui les 5 tendances qui se démarqueront sur le marché de la sécurité physique en 2021.

Les solutions de sécurité innovantes aideront les entreprises à surmonter la pandémie
Si l'optimisme est de mise dans le monde pour 2021, les organisations devront rester créatives sur la façon dont elles utilisent, mettent à jour et redéploient leurs systèmes de sécurité dans leurs installations. Elles pourront ainsi réfléchir plus largement au rôle de la sécurité physique et à ce qu'elle peut accomplir au-delà des applications traditionnelles, pour apporter plus de valeur. Cette résilience et cette ingéniosité ont déjà été observées au cours des derniers mois, de nombreuses organisations s'adaptant rapidement aux nouveaux besoins et défis posés par le Covid-19 en utilisant leurs technologies de sécurité physique comme un outil stratégique dans la lutte contre la pandémie. De bien des façons, les difficultés exceptionnelles engendrées par la situation actuelle ont mis plus encore en lumière le rôle et l'importance du secteur de la sécurité physique. Et une fois que la pandémie sera enfin derrière nous, nous pensons que les organisations continueront à considérer leur technologie de sécurité physique et les données associées comme stratégiques et potentiellement structurantes pour l'entreprise.

Les entreprises se concentreront sur la protection de la vie privée
Dans un effort pour assurer la sécurité des personnes pendant la pandémie de Covid-

19, de nombreuses organisations se sont empressées de mettre en place des dispositifs de "détection de fièvre" et d'autres systèmes nouveaux, sans nécessairement prendre le temps d'examiner les implications en matière de respect de la vie privée. Les préoccupations du grand public quant au respect de la vie privée dans le cadre de la recherche des cas contacts au Covid-19 et d'autres défis sociaux continueront de croître – obligeant le secteur de la sécurité physique à s'attaquer de front à la question de la vie privée et à trouver des solutions appropriées. Plutôt que d'entraver le développement de nouvelles technologies, le respect de la vie privée s'avérera être une force motrice dans la poursuite d'une conception responsable et innovante, encourageant les concepteurs éthiques et avant-gardistes à adopter les méthodologies de "Privacy by Design". Cela implique d'intégrer de manière proactive le respect de la vie privée dans la conception et le fonctionnement des systèmes informatiques, des infrastructures réseau et des pratiques commerciales, de la première ligne de code à l'interface utilisateur. Et dans le secteur de la sécurité physique, la conception d'une solution logicielle tenant compte du respect de la vie privée dès la conception signifie que les organisations n'auront pas à choisir entre la protection de la vie privée des individus et la garantie de leur sécurité physique. La protection de la vie privée devrait toujours être une option par défaut, et non l'inverse ; les développeurs de technologies de sécurité qui la prennent au sérieux bénéficieront d'avantages certains, mais surtout de la confiance de leurs clients.

Les risques de cybersécurité vont continuer de croître

Si la cybersécurité est un problème de longue date, elle restera malheureusement une préoccupation forte en 2021. Des écoles et hôpitaux aux entreprises privées, les cyberattaques ont augmenté au cours de l'année dernière. Rien qu'au troisième trimestre 2020, Trends Micro a recensé près de 4 millions de menaces par email et plus d'un million de visites sur des URL malveillantes liées au Covid-19.

La plupart d'entre elles peuvent être reliées au passage éclair au télétravail, qui a forcé les entreprises à redoubler d'efforts pour maintenir leurs activités tout en essayant de sécuriser leurs actifs. Dans la nouvelle réalité d'aujourd'hui, un périmètre informatique sécurisé n'existe plus, et avec peu de certitude sur le moment où l'on reprendra le travail au bureau ou sur un campus, les écoles, les entreprises et les gouvernements devront repenser leur stratégie de cybersécurité et mettre en place des mesures pour dissuader les pirates et protéger leurs organisations. Ils devront prendre des mesures

décisives pour renforcer leur posture de cybersécurité, sous peine de compromettre la sécurité de leur propriété intellectuelle et d'exposer des données sensibles et des informations personnelles. Il est essentiel de choisir des fournisseurs de confiance et de déployer des solutions de sécurité physique qui s'accompagnent de couches de cyberdéfense. Les équipes de sécurité sont bien conscientes que le chiffrement intégré, l'authentification multifacteurs et la gestion des mots de passe constituent les premières lignes de défense. Au-delà, l'exploitation d'autres fonctionnalités peut améliorer la posture de cybersécurité, notamment la possibilité d'accéder à des scores de risque de cybersécurité, des alertes de vulnérabilité du système et des rappels automatiques pour les mises à jour des micrologiciels et des matériels.

Un focus renforcé sur la confiance dans la chaîne logistique

Les technologies de sécurité physique font désormais partie intégrante de la stratégie informatique des organisations et sont heureusement soumises aux mêmes évaluations que leurs autres technologies. Certains gouvernements découragent déjà l'utilisation de produits provenant de certains fournisseurs, invoquant d'éventuelles failles de confiance et de sécurité. Les utilisateurs finaux, en particulier dans les grandes entreprises, prennent plus de temps pour s'intéresser aux fabricants, aux fournisseurs et aux distributeurs avec lesquels ils choisissent de travailler. Ils posent notamment aux fournisseurs des questions plus pointues sur la manière dont ils gèrent les menaces émergentes et communiquent sur les vulnérabilités de leurs produits et sur leur écosystème de partenaires, ainsi que sur leurs politiques en matière de données et de respect de la vie privée. Pour qu'un fournisseur de solutions de sécurité soit considéré comme un partenaire fiable et réputé auprès de ses clients, il va devoir satisfaire à des exigences plus strictes dans le cadre des processus d'approvisionnement.

La demande de solutions cloud hybride va poursuivre sa croissance

Selon un récent rapport de Forrester intitulé "Predictions 2021: Cloud Computing Powers Pandemic Recovery", l'infrastructure de cloud public mondiale va croître de +35 % pour atteindre une valeur marchande de 120 milliards de dollars au cours de l'année prochaine. La pandémie est en grande partie responsable de cette augmentation de la demande en cloud. Avec la montée en flèche des usages en ligne et du télétravail, la transition numérique déjà enclenchée s'est considérablement accélérée à l'échelle mondiale.

Afin de ne pas simplement survivre mais de prospérer, les professionnels de la sécurité physique devront suivre l'exemple des services informatiques et s'orienter vers le cloud. Au cours de l'année à venir, les responsables de la sécurité physique devraient s’affranchir de la distinction entre systèmes de sécurité cloud et sur site, et adopter un modèle de déploiement hybride pour leur infrastructure de sécurité physique. Cela leur permettra de mettre en œuvre des systèmes ou des applications cloud spécifiques tout en conservant les systèmes existants sur site.

Grâce à une approche cloud hybride, les directeurs de la sécurité deviendront plus agiles dans leurs prises de décisions sur la manière dont ils peuvent améliorer l'évolutivité, la redondance et la disponibilité, et répondre ainsi aux besoins changeants de leur organisation. Ils pourront également migrer rapidement vers des technologies plus récentes, minimiser l'empreinte matérielle, renforcer la cybersécurité et réduire les coûts. Les offres cloud doivent devenir une option incontournable, leur permettant de s'adapter rapidement aux changements et d’assurer la continuité des activités.

À propos de Genetec

Genetec développe des logiciels, matériels et services Cloud basés sur une architecture ouverte et destinés au secteur de la sécurité physique et publique. Son produit phare, Security Center, est une plateforme unifiée sur IP de vidéosurveillance, de contrôle d'accès et de reconnaissance automatique de plaques d'immatriculation (RAPI). Innovateur mondial depuis 1997, Genetec, dont le siège est à Montréal, au Canada, commercialise ses solutions auprès des entreprises et des organismes gouvernementaux via un réseau intégré de revendeurs, de partenaires de distribution certifiés, d'intégrateurs et de consultants au sein de plus de 80 pays. Fondée sur le principe de l'innovation, Genetec reste aux avant-postes des nouvelles technologies qui unifient les systèmes de sécurité physique sur IP.

Pour plus d'informations sur Genetec, rendez-vous sur :

www.genetec.com/fr

Contacts Presse :

Amérique du Nord
Véronique Froment
HighRez
Veronique@highrezpr.com
Tél: +1 603.537.9248