

Para liberación inmediata

Genetec comparte sus predicciones sobre las tendencias de seguridad física para 2021

Las tendencias clave incluyen aplicaciones innovadoras de tecnología de seguridad, enfoque en la privacidad, preocupaciones crecientes de ciberseguridad, adopción de la nube híbrida y un mayor escrutinio de los proveedores.

CIUDAD DE MÉXICO, 12 de enero de 2021 —[Genetec Inc.](#) (“Genetec”), un proveedor líder de tecnología de seguridad unificada, seguridad pública, operaciones y soluciones de inteligencia empresarial, compartió hoy sus cinco principales predicciones para la industria de la seguridad física en 2021.

Las soluciones innovadoras de seguridad ayudarán a las empresas a prosperar después de la pandemia

Aunque el mundo sigue siendo optimista para el año 2021, las organizaciones tendrán que seguir siendo creativas en cuanto a la forma en que utilizan, actualizan y redistribuyen sus sistemas de seguridad en sus instalaciones. Esto les permitirá empezar a pensar más ampliamente sobre el papel de la seguridad física y lo que pueden hacer más allá de las aplicaciones tradicionales para ofrecer más valor. Ya hemos visto pruebas de esta resiliencia e ingenio en los últimos meses con muchas organizaciones que se han adaptado rápidamente a las nuevas necesidades y desafíos que plantea el COVID-19, utilizando su tecnología de seguridad física como herramienta estratégica en la lucha contra la pandemia. En muchos sentidos, las extraordinarias dificultades que ha traído consigo la situación actual han hecho que se preste mayor atención al papel y la importancia de la industria de la seguridad física. Y una vez que la pandemia esté finalmente en el espejo retrovisor, creemos que las organizaciones continuarán viendo su tecnología de seguridad física y los datos relacionados, tanto estratégicos como de estructuración empresarial.

Las empresas se centrarán en la protección de la privacidad

En un esfuerzo por mantener a la gente segura durante la pandemia del COVID-19, muchas organizaciones se apresuraron a implementar dispositivos de "detección de fiebre" y otros

sensores nuevos sin tener necesariamente el tiempo para considerar las implicaciones de privacidad. La preocupación por la privacidad pública relacionada con el rastreo de contactos del COVID-19 y otros desafíos sociales seguirá creciendo. Estos temas sensibles requerirán que la industria de la seguridad física aborde la privacidad de frente y encuentre soluciones adecuadas. En lugar de obstaculizar el desarrollo de nuevas tecnologías, la privacidad resultará ser una fuerza motriz en la búsqueda de un diseño responsable e innovador, alentando a los desarrolladores con visión de futuro y ética a adoptar las metodologías de [Privacidad por Diseño](#). Esto supone la incorporación proactiva de la privacidad en el diseño y el funcionamiento de los sistemas de TI, la infraestructura de redes y las prácticas comerciales, desde la primera línea de código hasta los proveedores terceros seleccionados para la asociación e integración. Adicionalmente, en la industria de la seguridad física, el desarrollo de una solución de software teniendo en cuenta la privacidad desde el principio, significa que las organizaciones no tendrán que elegir entre proteger la privacidad individual y garantizar su seguridad física. La privacidad debería ser siempre la opción predeterminada y no al revés, y los desarrolladores de tecnología de seguridad que la tomen en serio obtendrán claras ventajas, en particular la confianza de sus clientes.

Los riesgos de seguridad cibernética seguirán aumentando

Si bien la seguridad cibernética ha sido un problema durante algún tiempo, lamentablemente seguirá siendo una preocupación vital en 2021. Desde escuelas y hospitales, hasta empresas privadas y gobiernos, ha habido un aumento de los ciberataques durante el último año. Sólo en el tercer trimestre de 2020, [Trend Micro](#) informó de que había casi 4 millones de amenazas por correo electrónico y más de 1 millón de visitas a URL maliciosas relacionadas con el COVID-19.

Gran parte de esto se puede relacionar con el cambio repentino al trabajo remoto, que dejó a las empresas luchando por mantener el negocio en marcha mientras que también intentaban asegurar los activos corporativos. Este cambio resaltó el hecho de que el perímetro tradicional en TI ya no existe. Las empresas, las organizaciones y los gobiernos tendrán que adoptar medidas decisivas para reforzar su postura cibernética o arriesgarse a socavar la seguridad de su propiedad intelectual, sus datos sensibles y su información personal. Elegir proveedores de confianza y desplegar soluciones de seguridad física que vengan con capas de defensa cibernética es fundamental. Los equipos de seguridad entienden que la encriptación incorporada, la autenticación multifactorial y la administración de contraseñas son las primeras líneas de defensa. Más allá de eso, aprovechar otras características como el índice de riesgo de ciberseguridad, las alertas de

vulnerabilidad del sistema y los recordatorios automatizados de actualizaciones de firmware y hardware, son ventajas significativas en este entorno de riesgo elevado.

Mayor atención a la confianza en la cadena de suministro

La tecnología de seguridad física se ha convertido en una parte integral de la estrategia de TI de una organización y, afortunadamente, ahora está bajo el mismo nivel de escrutinio que otros elementos del pilar tecnológico de una organización. Algunos gobiernos ya están desalentando el uso de ciertos productos de los fabricantes de seguridad, citando la confianza y las vulnerabilidades de seguridad. Los usuarios finales, especialmente en el espacio empresarial, están dedicando más tiempo a escrutar a los fabricantes, proveedores y distribuidores con los que deciden trabajar. Esto incluye hacerles a los proveedores preguntas más concretas sobre cómo gestionan las amenazas emergentes, qué tan comunicativos son sobre las vulnerabilidades de los productos y su ecosistema de socios, y cuáles son sus datos y políticas de privacidad. Para que un proveedor de soluciones de seguridad física sea considerado un socio de confianza y de buena reputación para sus clientes, tendrá que cumplir requisitos más estrictos como parte del proceso de adquisición.

La demanda de soluciones de nubes híbridas seguirá creciendo

Según el reciente [informe de Forrester, Predicciones 2021: Cloud Computing Powers Pandemic Recovery](#), la infraestructura pública global de nubes crecerá un 35% hasta un valor de mercado de 120.000 millones de dólares durante el próximo año. A medida que el uso en línea y el trabajo remoto se dispararon durante la pandemia, se aceleró enormemente el cambio global hacia la transformación digital, que ya estaba en marcha.

Para prosperar, los profesionales de la seguridad física tendrán que seguir el liderazgo de los departamentos de TI. El año que viene, los líderes de la seguridad física deberían dejar de lado la división entre sistemas de seguridad en la nube y en sitio y adoptar un modelo de despliegue híbrido en su infraestructura de seguridad física. Esto les permitirá implementar sistemas o aplicaciones específicas en la nube, manteniendo los sistemas existentes en sitio.

Con un enfoque de nube híbrida, los directores de seguridad serán más ágiles a la hora de tomar decisiones sobre cómo pueden mejorar la escalabilidad, la redundancia y la disponibilidad para adaptarse a las necesidades cambiantes de su organización. También podrán migrar rápidamente a tecnologías más nuevas, minimizar la huella de hardware,

impulsar la ciberseguridad y reducir los costos. Las ofertas de nubes deben convertirse en una opción esencial para adaptarse rápidamente a los cambios y garantizar la continuidad de la empresa.

--Fin--

Acerca Genetec

Genetec Inc. es una empresa de tecnología innovadora con un amplio portafolio de soluciones que abarca seguridad, inteligencia y operaciones. El producto estrella de la empresa, Security Center, es una plataforma de arquitectura abierta que unifica videovigilancia, control de acceso, reconocimiento automático de placas (ALPR), comunicaciones y analíticas, todo basado en redes IP. Genetec también desarrolla soluciones y servicios basados en la nube diseñados para mejorar la seguridad y aportar nuevos niveles de inteligencia operativa para gobiernos, empresas, transporte y las comunidades en las que vivimos. Fundada en 1997 y con sede en Montreal, Canadá, Genetec sirve a sus clientes globales a través de una extensa red de integradores, socios de negocios certificados y consultores en más de 80 países.

Para más información sobre Genetec, visita: [genetec.com/es](https://www.genetec.com/es)

© Genetec Inc., 2021. Genetec y el logotipo de Genetec son marcas comerciales de Genetec Inc. y pueden estar registradas o pendientes de registro en varias jurisdicciones. Otras marcas comerciales utilizadas en este documento pueden ser marcas comerciales de los fabricantes o proveedores del producto respectivo.

Contacto de Prensa:

México

Verónica Ballesteros

Infosol

vballesteros@infosol.com.mx

Tel: +52(55) 5560-1000