NOTA DE PRENSA
09 / 09 / 2021

Ingecom comercializa las soluciones de protección de datos de Netwrix

> El fabricante permite recuperar el control de los datos sensible y críticos para el negocio, independientemente de dónde estén.

Ingecom, Value Added Distributor (VAD) especializado en soluciones de ciberseguridad y ciberinteligencia, ha firmado un acuerdo de distribución con Netwrix, líder en protección de datos sensibles y críticos para el negocio, independientemente de dónde estén. La alianza alcanzada es para comercializar las soluciones del fabricante en España y Portugal.

“Estamos muy contentos de asociarnos con Ingecom y seguir creciendo juntos en Iberia –afirma Jesús Sáez, Country Manager Spain & Portugal de Netwrix– Las empresas están buscando soluciones que les permitan proteger sus datos sensibles de manera sencilla y con la penetración de Ingecom en el mercado podemos llegar a esas compañías y capacitarlas para identificar y clasificar su información sensible con la máxima precisión; reducir su nivel de riesgo y detectar las amenazas a tiempo para evitar filtraciones de datos, ayudando además a reducir costes operativos de IT y asegurando el cumplimiento normativo", añade Sáez.

Por su parte, Javier Modúbar, CEO de Ingecom, apunta que: “Estamos encantados de firmar un acuerdo con Netwrix ya que aporta a nuestro portfolio tecnologías de búsqueda y clasificación de la información, complementando así nuestros proyectos de protección de datos. Por otra parte, este fabricante dispone de un abanico de soluciones que permite cubrir muchos otros requerimientos de seguridad de los clientes como es la protección de usuarios privilegiados”.

“En cuanto a la estrategia global de Ingecom y MultiPoint Group, Netwrix nos ayuda a consolidarla dado que lleva bastantes años trabajando con el VAD israelí, obteniendo buenos resultados y ahora ha apostado también por firmar con nosotros en Iberia”, comenta el máximo responsable de Ingecom.

Fundada en 2006 y con oficinas centrales en Irvine (California), Netwrix ofrece productos de seguridad y gobernanza de información avanzados y sencillos de utilizar. Con demasiada frecuencia, las organizaciones abordan el control del acceso a sus datos sólo después de sufrir una filtración de datos. El fabricante presenta como alternativa la posibilidad de anticiparse a que esto ocurra ayudando a habilitar un sólido gobierno de acceso a los datos (*data access governance*) en los servidores de archivos del cliente, así como en los sistemas de colaboración como SharePoint y SharePoint Online, ofreciéndole a la empresa una visión profunda de sus datos no estructurados, incluyendo información sobre posibles brechas de seguridad, permisos efectivos y patrones de acceso a los datos. Gracias a Netwrix, las compañías pueden asegurarse de que cuentan con todos los controles de seguridad de acceso adecuados para evitar infracciones.

Mitigar el riesgo de fuga de datos

Con Netwrix Data Classification resuelve los retos de las organizaciones relacionados con los datos, como la mitigación del riesgo de fugas de datos, el aprovechamiento de todo el valor de su contenido, el aumento de la productividad de los empleados y la superación de las auditorías de cumplimiento con menos esfuerzo.

La solución permite que los clientes puedan identificar la información sensible y reducir su exposición a riesgos, tanto si los datos están en las instalaciones del cliente como en la nube, poniendo en cuarentena automáticamente la información crítica o sensible almacenada en ubicaciones no seguras o a las que acceden grandes grupos de usuarios con el objetivo de minimizar su exposición hasta que pueda tomar una decisión meditada de corrección.

Evaluación continua de riesgos

Netwrix propone una evaluación continua de riesgos de TI para que el cliente pueda identificar las vulnerabilidades que ponen en riesgo sus activos de información y la continuidad del negocio. El fabricante cuenta con la solución Netwrix Auditor que facilita la comprensión del perfil de riesgo actual de la compañía, la priorización de su respuesta, el conocimiento de los pasos a seguir para remediar cada problema, el ajuste de los niveles de riesgo a su entorno particular y la revisión del nuevo perfil de riesgo para evaluar el éxito de sus esfuerzos. Repitiendo este proceso, la organización puede mejorar continuamente su postura de seguridad, así como proporcionar pruebas a la dirección o a los auditores de su cumplimiento de las políticas internas o de la normativa externa. El software Netwrix Auditor detecta las amenazas a la seguridad, demuestra el cumplimiento y aumenta la

eficiencia del equipo de TI.

> ## La importancia de asegurar el dato

Las soluciones de Netwrix vienen a sumarse a una robusta propuesta del portfolio de Ingecom en torno a protección del dato, como es el caso de las soluciones de Forcepoint, ReSec y SealPath.

Por una parte, Forcepoint con su DLP (Data Loss Prevention) previene la pérdida de los datos mediante la identificación de manera automática de los incidentes de datos que presentan el mayor riesgo.

En cuanto a ReSec, el fabricante utiliza su tecnología patentada de Desarme y Reconstrucción de Contenido (CDR) para asegurar que cada documento que llega a la una organización esté libre de amenazas después de procesado. Esta solución proporciona protección completa contra todo tipo de amenazas de malware, tanto conocidas como desconocidas, incluyendo ransomware.

Mientras que SealPath utiliza tecnología IRM (Information Risk Management) para encriptar el dato y protegerlo, tanto dentro de la red de la empresa como fuera de ella, controlando quién accede a la información y con qué permisos.

Recordemos que el dato es uno de los cinco puntos (junto con el humano, el dispositivo, las aplicaciones y la infraestructura) a los que atacar en el ámbito de la ciberseguridad y que, según el informe *2021 Netwrix Cloud Data Security Report*, "los incidentes más comunes que experimentaron las agencias gubernamentales el año pasado en la nube fueron el phishing (reportado por el 39% de las organizaciones), la fuga accidental de datos (24%) y los ataques dirigidos a la infraestructura (22%). La fuga de los datos fue la más difícil de detectar de las tres; el 27% de las organizaciones necesitaron días para señalarla; además, la resolución de la fuga de datos también llevó más tiempo que otros incidentes, requiriendo de días, en el 32% de los casos, y meses en el 23% de las ocasiones".

Contacto de prensa:

JAVIER MODUBAR ALVAREZ

info@ingecom.net
944395678
http://www.ingecom.net