“Que la red funcione no significa que esté sana”

Netmetrix apuesta por observabilidad independiente e inteligencia artificial para anticipar fallos, optimizar capacidad y reforzar la seguridad en entornos críticos donde la continuidad del servicio es esencial.

Pablo Alvarez. CEO y fundador Netmetrix

Netmetrix Solutions es una empresa tecnológica europea especializada en hacer visible lo que ocurre en redes, ciberseguridad y sistemas críticos. Combina testing y validación, observabilidad de red y servicios profesionales para ofrecer datos fiables sobre rendimiento, disponibilidad y riesgos reales. A diferencia de un fabricante, actúa como partner independiente en entornos multi-vendor, ayudando a fijar una línea base de “normalidad” y a detectar desviaciones antes de que se conviertan en incidentes. Su objetivo: reforzar la continuidad, la eficiencia y la protección de servicios críticos, donde fallar no es una opción.

Pregunta. ¿Por qué es clave saber qué está pasando en la red, aunque “parezca que todo va bien”?
Respuesta. Porque que algo “funcione” no significa que esté sano. Muchos problemas empiezan como señales pequeñas: latencia creciente, jitter, microcortes o congestión puntual. Sin visibilidad no se ven tendencias ni se compara contra una línea base objetiva, y se acaba reaccionando cuando el impacto ya es real para el negocio: caída de servicios, mala experiencia o pérdida de productividad. En seguridad ocurre algo parecido: un atacante puede moverse lateralmente durante horas o días sin generar alertas evidentes. Observar la red permite detectar anomalías, priorizar y optimizar capacidad antes de que el problema se convierta en una crisis operativa o reputacional.

P. ¿Por qué la monitorización debería ser independiente de los propios equipos de red y seguridad?
R. Porque si la “medición” depende del mismo dispositivo que estás intentando vigilar, se introduce sesgo y un punto único de fallo. Si un router, un firewall o un WAF se satura, puede dejar de registrar eventos, perder paquetes o degradar su telemetría justo cuando más la necesitas. Una capa independiente —sondas, taps o plataformas externas— mantiene la observabilidad y, aunque el equipo esté al límite, permite auditar de forma objetiva y comparar fabricantes y disponer de trazas externas verificables y configuraciones sin casarte con ninguno. Además, mejora tanto la respuesta a incidentes como el cumplimiento normativo en sectores críticos.

“Una capa independiente mantiene la observabilidad cuando los equipos están al límite y permite auditar la red de forma objetiva, sin sesgos ni dependencias de fabricante”

P. ¿Qué ventaja tiene apostar por un especialista de nicho como Netmetrix?
R. La especialización acorta el camino entre el dato y la decisión. Un proveedor de nicho vive en el detalle: conoce patrones de rendimiento, fallos típicos y métodos de prueba en 5G, SD-WAN o entornos mission-critical, y diseña métricas y tests ajustados al caso real. Además, la independencia multi-vendor evita que la visibilidad no esté condicionada por un fabricante en concreto. A esto se suma el acompañamiento en consultoría, puesta en marcha y transferencia de conocimiento para que el cliente no dependa de configuraciones manuales eternas.

P. ¿Cómo puede ayudar la IA (AIOps) en la monitorización y la seguridad de redes, desde hoy?
R. La inteligencia artificial aporta valor cuando reduce ruido y acelera el diagnóstico. Puede aprender la línea base, detectar anomalías, correlacionar eventos de distintas capas y sugerir causas probables. En seguridad ayuda a priorizar alertas y a detectar movimientos laterales. Pero no es magia: requiere datos de calidad, buena telemetría y supervisión humana. El verdadero valor aparece cuando se integra en los procesos operativos: menos tiempo “mirando pantallas” y más tiempo resolviendo.

Más información
www.netmetrix.es