ESPECIAL **ZERO TRUST**

Zero Trust en la era de la IA: identidad, dato y decisiones en tiempo real

CHECK POINT™

netskope

SAMSUNG

zscaler™

IR A PÁGINA SIGUIENTE

Zero Trust en la era de la IA: identidad, dato y decisiones en tiempo real

Zero Trust nació para resolver un problema muy concreto: dejar de confiar en la red corporativa como espacio seguro. Pero la irrupción de la inteligencia artificial está obligando a revisar de nuevo el modelo. Ahora ya no sólo hay que controlar usuarios y dispositivos. También empiezan a entrar en juego los agentes, automatismos, APIs y procesos capaces de actuar por sí solos dentro de las organizaciones.

Rosalía Arroyo

El concepto Zero Trust fue formulado hace más de una década por John Kindervag, analista de Forrester Research, como respuesta a la confianza implícita sobre la que se construyeron muchas redes corporativas tradicionales. La idea era sencilla, pero disruptiva: no confiar en nada por defecto y verificar siempre. Con el tiempo, organismos como el National Institute of Standards and Technology (NIST) ayudaron a convertir ese planteamiento en un marco de referencia más estructurado.

Durante años, Zero Trust se asoció principalmente a la eliminación del perímetro y al refuerzo del control del acceso. Sin embargo, el contexto actual está obligando a ampliar el enfoque. La adopción acelerada de la IA, la expansión del SaaS y el crecimiento de identidades no humanas están cambiando las reglas del

juego. Ya no se trata únicamente de quién accede, sino también de quién actúa, con qué datos, y bajo qué condiciones.

La IA está modificando además algunos de los pilares sobre los que se construía Zero Trust. Hasta hace relativamente poco, la mayoría de las arquitecturas estaban pensadas para usuarios humanos y accesos razonablemente predecibles. Ahora conviven asistentes inteligentes, agentes autónomos, integraciones automáticas y procesos capaces de ejecutar tareas de forma independiente. Eso multiplica las identidades y obliga a extender el modelo mucho más allá del usuario tradicional.

También cambia la velocidad. Los ataques se automatizan, evolucionan más rápido y generan volúmenes mucho mayores de actividad, lo que hace que las políticas basadas en reglas se queden cortas. Cada vez resulta más necesario tomar decisiones dinámicas capaces de evaluar identidad, dispositivo, comportamiento, ubicación, sensibilidad del dato o contexto de uso prácticamente en tiempo real.

Además, hay un tercer elemento que gana protagonismo: el dato. Con herramientas de IA generativa y aplicaciones SaaS, la información se mueve constantemente entre plataformas, usuarios y modelos. El reto ya no es únicamente controlar quién entra, sino qué información utiliza, cómo la comparte y con qué propósito.

> Zero Trust ya no gira solo alrededor del usuario: agentes, automatismos y APIs están cambiando el modelo

Qué sigue vigente y qué no

En su planteamiento original, Zero Trust proponía dejar de considerar la red interna como un espacio confiable. Ese principio sigue siendo válido, pero muchas organizaciones lo han aplicado de forma parcial. En la práctica, el concepto ha terminado reduciéndose en numerosos casos a la sustitución de la VPN o al despliegue de controles de acceso más estrictos.

La realidad es que Zero Trust nunca se limitó al acceso remoto. El propio NIST lo define como una arquitectura que abarca identidad, dispositivos, aplicaciones, datos y operaciones. El problema es que muchos proyectos siguen construyéndose alrededor de una única capa.

El resultado son entornos donde se verifica la identidad, pero no el contexto; donde se controla el acceso, pero no el uso posterior de la información; o donde existe visibilidad, pero no capacidad real de respuesta. Aunque sobre el papel, la organización pueda considerar que ha avanzado hacia Zero Trust, en la práctica sigue dependiendo de decisiones estáticas y de relaciones de confianza heredadas.

La IA cambia el escenario

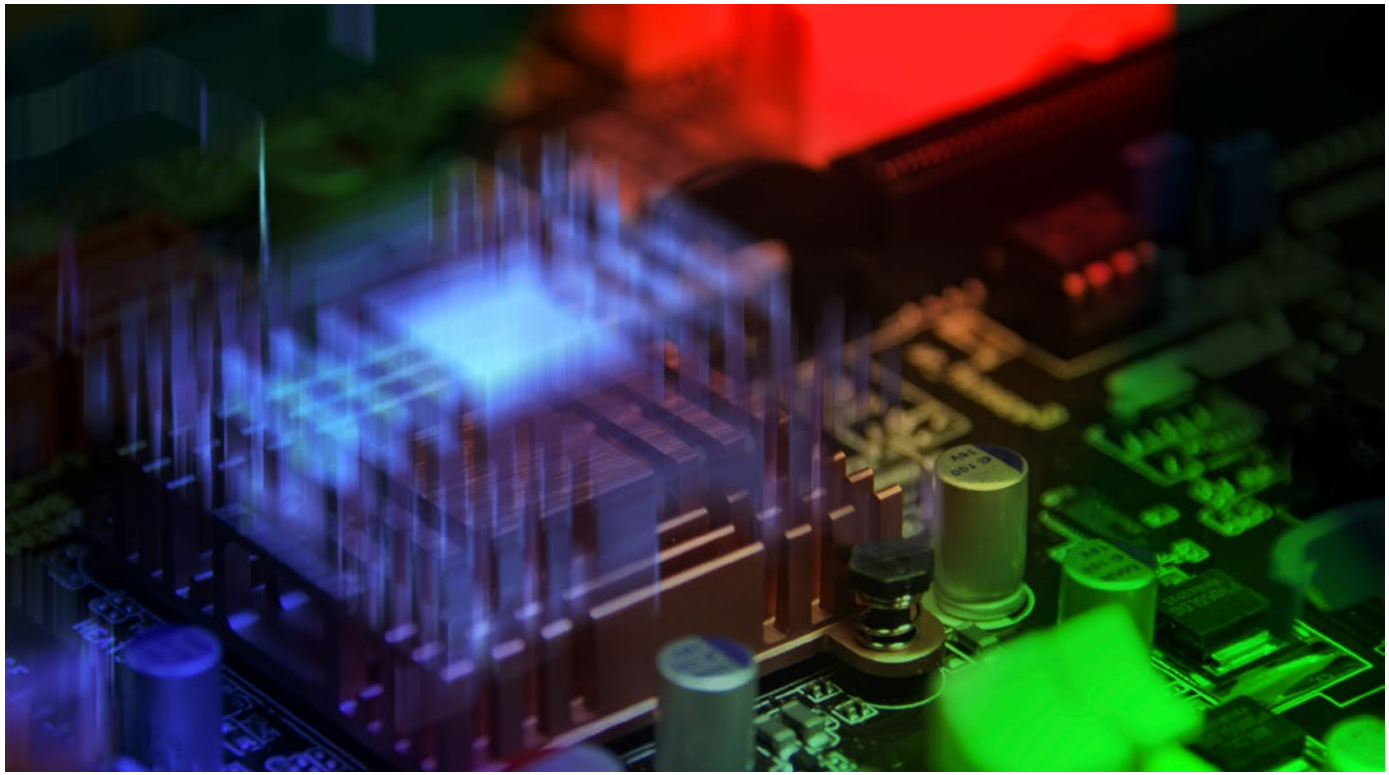
La inteligencia artificial añade una nueva dimensión al problema. No solo amplía la superficie de ataque, sino que, como decíamos, multiplica las entidades que interactúan con sistemas y datos. A los usuarios se suman ahora agentes, automatismos, APIs y procesos que operan con distintos niveles de autonomía.

Este cambio no es menor. Reconociendo que

estos sistemas plantean retos distintos a los de las identidades tradicionales, ya existen iniciativas específicas para abordar la seguridad de los agentes de IA. Para las organizaciones, esto implica gestionar un ecosistema mucho más complejo, en el que conviven identidades humanas y no humanas.

El problema es que muchas organizaciones han perdido la cuenta de las identidades no humanas que operan dentro de sus entornos. APIs, tokens, certificados, cuentas de servicio, integraciones entre aplicaciones o agentes capaces de ejecutar acciones de forma autónoma amplían continuamente la superficie de exposición. Y buena parte de esas identidades siguen fuera de los modelos clásicos de gobierno y supervisión, pese a que en muchos grandes entornos corporativos ya superan en número a las humanas.

El riesgo no está solo en el acceso. También en el comportamiento. Un agente automatizado puede consultar información, lanzar procesos, interactuar con otros sistemas o tomar decisiones sin intervención humana directa. Y si algo falla, el impacto puede escalar rápidamente.



El dato pasa al centro

El otro gran desplazamiento tiene que ver con el dato. Durante años, la seguridad se articuló alrededor del perímetro y, más tarde, del acceso. Ahora el foco empieza a situarse directamente sobre la información.

El auge del SaaS y de la inteligencia artificial generativa ha acelerado esta transición. Los datos ya no residen en un único entorno ni permanecen bajo un control centralizado. Se mueven constantemente entre aplicaciones, servicios y plataformas, muchas veces fuera de la visibilidad directa de IT.

Un mismo usuario puede consultar información corporativa desde un copiloto conectado a SaaS, reutilizarla en un asistente externo y combinarla después con otros flujos automatizados sin que la organización tenga una trazabilidad completa de ese recorrido.

Las cifras ayudan a dimensionar el problema. El

informe “Cost of a Data Breach 2025” de IBM sitúa el coste medio de una brecha en torno a los 4,5 millones de dólares, con un peso creciente de incidentes relacionados con accesos indebidos o exposición de información en entornos cloud. Por su parte, Gartner estima que en 2026 más del 80 % de las organizaciones habrá integrado APIs o modelos de IA generativa en sus procesos, incrementando notablemente los flujos de datos y los puntos de exposición.

La IA generativa está acelerando además un fenómeno que preocupa especialmente a CIOs y CISOs: el uso de herramientas fuera del control corporativo. Empleados que introducen información sensible en asistentes públicos, agentes conectados a repositorios internos o automatismos capaces de combinar datos de distintas fuentes están ampliando la superficie de riesgo mucho más rápido de lo que evolucionan muchas políticas de gobierno.

Lo que empieza a imponerse son controles capaces de interpretar el contexto de cada interacción: quién accede, desde dónde, con qué dispositivo y para qué propósito.

> La IA está desplazando el foco desde quién accede hacia qué comportamiento se espera de cada identidad

Decidir en tiempo real

Uno de los cambios más relevantes tiene que ver con la velocidad de decisión. Durante años, las políticas de seguridad se definían a priori y se aplicaban de forma relativamente rígida. Ese enfoque pierde eficacia en un entorno donde el riesgo cambia constantemente.

La combinación de IA, automatización y entornos distribuidos obliga a tomar decisiones en tiempo real. Esto implica cruzar señales de identidad, dispositivo, comportamiento, ubicación y sensibilidad del dato para evaluar cada acceso o acción.

El problema es que los atacantes también están acelerando. La automatización permite lanzar campañas más rápidas, adaptar malware en tiempo real o explotar credenciales robadas a gran escala. Frente a eso, las decisiones defensivas ya no pueden depender únicamente de revisiones manuales o políticas rígidas.

Aquí aparece uno de los grandes desafíos operativos. Muchas organizaciones disponen ya de herramientas de visibilidad y telemetría, pero no de mecanismos eficaces para traducir esa información en decisiones automatizadas. La distancia entre lo que se observa y lo que realmente se hace sigue siendo uno de los principales problemas.

El volumen de alertas tampoco ayuda. Los SOC gestionan cada vez más señales procedentes de endpoints, identidades, red, SaaS o cloud, mientras los equipos continúan teniendo dificultades para escalar operaciones y responder con rapidez. Eso está empujando al mercado hacia modelos más integrados y hacia un mayor uso de automatización e IA aplicada a operaciones de seguridad.

Del dispositivo al contexto: un modelo por capas

En este escenario, el concepto de perímetro pierde relevancia. En su lugar, emerge un mo-

La IA acelera el riesgo: las cifras que preocupan a los CISOs

La adopción de IA generativa está avanzando más rápido que los controles de seguridad. El informe "Cost of a Data Breach 2025" de IBM y el Ponemon Institute refleja hasta qué punto muchas organizaciones están perdiendo visibilidad sobre cómo se utilizan los datos en entornos de IA.

Entre los datos más relevantes destacan:

- **El 97 % de las organizaciones que sufrieron incidentes relacionados con IA no tenía controles de acceso adecuados sobre estos sistemas.**
- **El 63 % carecía de políticas específicas de gobierno de IA o mecanismos para controlar el llamado "shadow AI".**
- **Sólo el 17 % dispone de controles técnicos capaces de impedir que los empleados suban información sensible a herramientas públicas de IA.**
- **Los incidentes vinculados a "shadow AI" cuestan de media 670.000 dólares más que una brecha convencional.**
- **Las organizaciones que utilizan IA y automatización en seguridad reducen el coste medio de una brecha en 1,9 millones de dólares frente a aquellas que no las utilizan.**

El informe refleja además un problema creciente para los equipos de seguridad: la pérdida de control sobre el movimiento del dato. Muchas organizaciones ya no saben qué información está siendo utilizada por asistentes de IA, APIs o aplicaciones SaaS conectadas a modelos generativos.

https://www.ibm.com/reports/data-breach

En la práctica, esto obliga a extender el modelo Zero Trust a estos nuevos actores. Ya no basta con proteger la infraestructura o el acceso; es necesario controlar cómo operan los agentes, qué información utilizan y qué acciones pueden ejecutar.

Errores que siguen repitiéndose

A pesar de la evolución del discurso, hay errores que continúan apareciendo. Uno de los más habituales es abordar Zero Trust como un proyecto tecnológico aislado, en lugar de como un cambio de modelo. Otro consiste en centrarse únicamente en una capa —normalmente el acceso— sin integrar el resto.

También es frecuente encontrar organizaciones que han invertido en visibilidad, pero no han dado el salto hacia la automatización. O que han reforzado la autenticación sin revisar los privilegios existentes, manteniendo niveles de acceso innecesarios.

A esto se suma la adopción de IA sin una estrategia de seguridad clara. Muchas empresas están incorporando estas tecnologías para mejorar productividad o automatizar procesos, a

> Muchas organizaciones tienen visibilidad, pero todavía no saben traducirla en decisiones automatizadas

menudo más rápido de lo que son capaces de adaptar sus modelos de gobierno o sus políticas de acceso.

Otro error habitual es pensar que Zero Trust puede implantarse como un proyecto cerrado. La realidad es mucho menos ordenada. Nuevos usuarios, dispositivos, aplicaciones, integraciones y ahora también agentes inteligentes obligan a revisar continuamente las relaciones de confianza dentro de la organización.

Un modelo que ya no puede ser parcial

Todo apunta a que Zero Trust está evolucionando hacia un modelo más amplio, en el que identidad, dispositivo, acceso, dato y contexto deben trabajar de forma conjunta.

La cuestión ya no es únicamente si confiar o no, sino cómo verificar continuamente y cómo limitar cada acción en función del riesgo. En un entorno donde humanos y máquinas comparten decisiones y acceso, la seguridad depende de la capacidad de entender qué está ocurriendo en cada momento y actuar en consecuencia.

Para CIOs, CISOs y CTOs, el reto es claro: pasar de modelos fragmentados a una visión integrada que permita gobernar no solo quién accede, sino también qué hace y con qué impacto.

En el fondo, el gran cambio es que las organizaciones ya no solo tienen que decidir en quién confían. También necesitan entender qué están haciendo realmente humanos y máquinas dentro de sus sistemas, y hasta dónde están dispuestas a dejarles actuar. CST

CIOs y CISOs ante el nuevo Zero Trust: controlar sin frenar la automatización

Para entender cómo están afrontando las organizaciones esta nueva etapa de Zero Trust, hemos querido tomar el pulso a distintos responsables de tecnología y ciberseguridad. El objetivo: conocer cómo está cambiando la gestión de identidades en un entorno donde la IA, los agentes y los procesos automatizados empiezan a tener cada vez más peso dentro de las operaciones. También cómo están intentando equilibrar automatización, control y agilidad sin frenar el negocio ni aumentar el riesgo.

Rosalía Arroyo

Las respuestas dejan claro que uno de los grandes cambios afecta directamente a la identidad, uno de los pilares clásicos de Zero Trust. El modelo ya no gira únicamente alrededor de usuarios y dispositivos; ahora también entran en juego agentes, automatismos, APIs y procesos capaces de tomar decisiones o ejecutar acciones de forma autónoma.

En la práctica, esto está desplazando el foco desde la simple verificación de acceso hacia el comportamiento esperado de cada entidad. Manuel Asenjo Ayllón, CIO & CISO de Écija Abogados, resume bien este cambio al señalar que "el perímetro ya no lo definen solo las personas; ahora también lo marcan los procesos". En su organización, la gestión de identidades no humanas se ha convertido en "una prioridad real", hasta el punto de tratar cada automatismo "como una identidad crítica más, con su radio de acción acotado y bajo supervisión constante".

La experiencia no es teórica. Según explica, ya han vivido "casos reales de procesos que se han desviado de su curso con resultados totalmente inesperados", algo que está empujando a reforzar modelos de microsegmentación y privilegios mínimos también sobre agentes automatizados.

> "El perímetro ya no lo definen solo las personas; ahora también lo marcan los procesos"
>
> **Manuel Asenjo,**
> CIO & CISO, **Écija Abogados**

La misma preocupación aparece en la visión de Willy Obispo, jefe del Centro de Ciberseguridad

del Ayuntamiento de Madrid, quien considera que “cualquier organización ahora también tiene que proteger las identidades no humanas”. Desde su punto de vista, el crecimiento de automatismos convierte la gestión de identidades en “un servicio crítico en sí mismo”, donde el contexto gana cada vez más importancia y el nivel de confianza debe reducirse incluso dentro de sistemas internos.

La IA está cambiando además la propia naturaleza de la identidad. Para Jesús Alonso, Head of EMEA Cybersecurity de Bridgestone, el modelo tradicional basado en user/device está evolucionando hacia esquemas mucho más dinámicos. “Estamos pasando de una gestión de la identidad estática a dinámica”, explica, apoyándose en identidades temporales y permisos de un solo uso que desaparecen una vez completada la tarea para reducir superficie de ataque.

En ese escenario, la supervisión ya no se limita únicamente a verificar usuarios o accesos. Alonso señala que ahora también es necesario validar “la integridad del código”, de manera que un agente o script pierda automáticamente sus privilegios si su comportamiento cambia o el modelo ha sido alterado.

> “No se trata de poner más o nuevas barreras, sino de construir un marco seguro preestablecido, conocido y aceptado por la organización”
>
> **Willy Obispo,** jefe del Centro de Ciberseguridad del **Ayuntamiento de Madrid**

"Estamos pasando de una gestión de la identidad estática a dinámica"

Jesús Alonso, Head of EMEA Cybersecurity, **Bridgestone**

El trasfondo de todas estas reflexiones apunta a una misma dirección: Zero Trust empieza a desplazarse desde la pregunta clásica de "quién accede" hacia otra mucho más compleja: qué está haciendo realmente cada identidad y si ese comportamiento encaja con lo esperado.

La automatización también está generando nuevas preocupaciones en el plano ofensivo. José Luis Corona García, IT Manager en Betapack, reconoce que una de sus principales inquietudes es "la automatización que están utilizando los atacantes", especialmente en ámbitos como malware desarrollado con IA, fraude del CEO o deepfakes con clonación de voz.

En su caso, la aproximación a Zero Trust está muy condicionada por la necesidad de proteger entornos especialmente sensibles y complejos, donde todavía conviven sistemas legacy y arquitecturas aisladas. "Mis proyectos de Zero Trust pasan por securizar entornos aislados con equipos legacy", resume.

Automatización, control y negocio: el equilibrio que buscan las empresas

El otro gran desafío que aparece en las respuestas tiene que ver con el equilibrio entre automatización, control y agilidad. La IA permite acelerar procesos, analizar volúmenes masivos de información y automatizar decisiones, pero también introduce riesgos difíciles de gobernar si no existen límites claros.

En el caso de Manuel Asenjo, la automatización ya está ayudando a gestionar "volúmenes de datos que hasta hace poco eran inabarcables". Sin embargo, la supervisión humana sigue siendo irrenunciable, especialmente en

ámbitos sensibles como el jurídico. “La supervisión humana no es un paso opcional: es el nodo de control final y obligatorio en cada flujo de trabajo”, afirma. La tecnología aporta eficiencia, pero el criterio profesional continúa siendo “la garantía última de seguridad jurídica y ética para nuestros clientes”.

La necesidad de combinar automatización y supervisión también aparece en la visión de Willy Obispo. A su juicio, el error sería intentar responder al nuevo escenario añadiendo más fricción. “No se trata de poner más o nuevas barreras”, explica, sino de construir “un marco seguro preestablecido, conocido y aceptado por la organización”.

Desde su punto de vista, la clave está en automatizar también el control. Si identidad, permisos y rutas de acceso están correctamente modelados, la automatización no solo acelera operaciones, sino que también reduce errores y superficie de exposición. Eso sí, advierte de que determinados activos críticos o entornos TIER0 deben seguir manteniéndose bajo niveles de control mucho más estrictos.

Jesús Alonso coincide en esa idea de automatizar la seguridad para no frenar el negocio. Su planteamiento pasa por combinar prevención, detección y respuesta “lo más automatizada posible”, apoyándose en guardarraíles que permitan mantener el riesgo dentro de límites definidos previamente.

> “Ahora mismo, mi principal preocupación es la automatización que están utilizando los atacantes”
>
> **José Luis Corona García,**
> IT Manager en **Betapack**

El objetivo no es eliminar el riesgo —algo imposible en entornos cada vez más automatizados—, sino contenerlo. “Si una decisión automatizada es errónea, el impacto está confinado”, resume. La estrategia consiste en mantener máxima agilidad dentro de entornos controlados y segmentados para evitar que un fallo escale.

En paralelo, otras organizaciones están optando por un enfoque más gradual y basado en visibilidad. José Luis Corona García reconoce que, antes de imponer restricciones sobre herramientas de IA generativa, están priorizando identificar cuándo y cómo se utilizan dentro de la compañía para después establecer políticas internas de buenas prácticas.

Ese enfoque refleja una realidad que empieza a repetirse en muchas empresas: antes de bloquear, las organizaciones necesitan entender cómo se está utilizando la IA y dónde aparecen realmente los riesgos. Porque el reto ya no consiste únicamente en impedir accesos no autorizados, sino en gobernar un entorno donde humanos, agentes y automatismos comparten datos, decisiones y capacidad operativa.

“Zero Trust no es solo identidad: también es controlar qué accede, cómo y bajo qué condiciones”

La evolución de Zero Trust está obligando a muchas organizaciones a replantearse algo más que sus herramientas de seguridad. La expansión de la IA, la proliferación de entornos híbridos y el crecimiento de automatismos dentro de las empresas están elevando la complejidad hasta un punto donde ya no basta con añadir nuevas capas de protección o desplegar soluciones aisladas.

Rosalía Arroyo

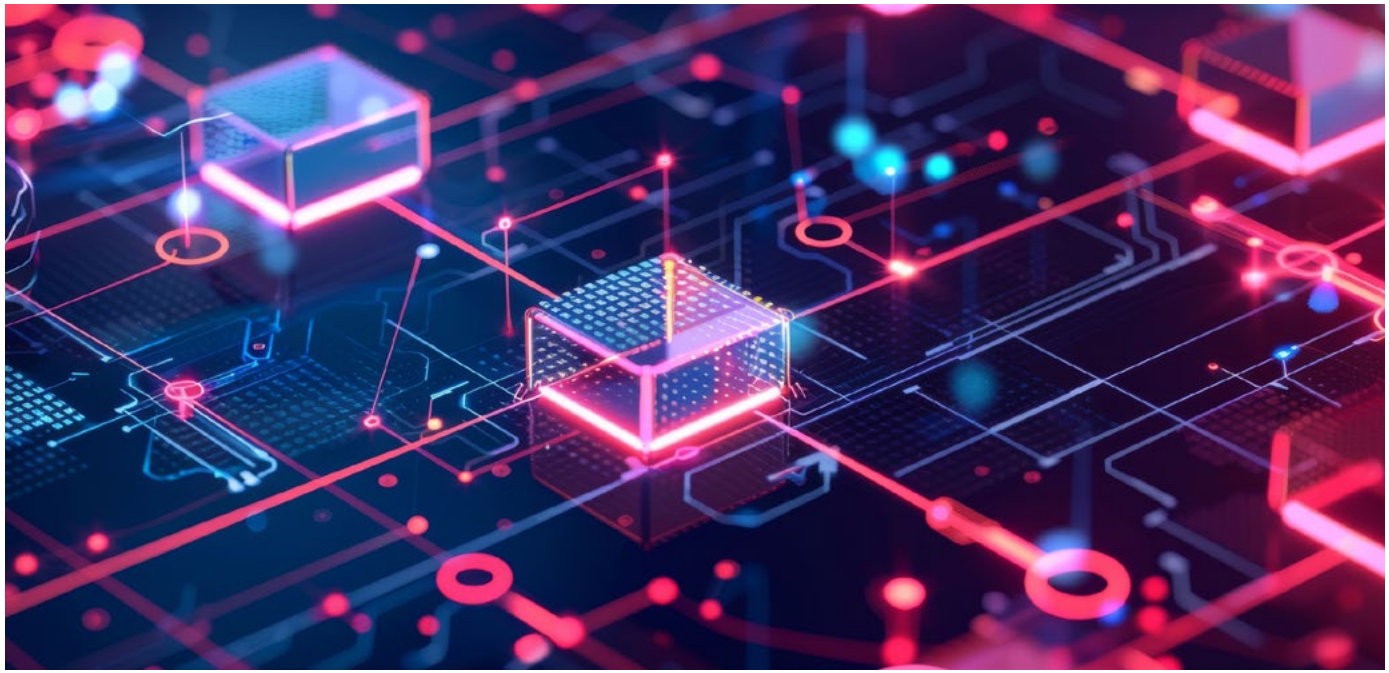
Para Eusebio Nieva, Sales Engineer Manager Iberia y evangelista de Check Point Software Technologies, uno de los principales problemas sigue siendo que muchas compañías creen haber adoptado Zero Trust cuando en realidad solo han reforzado el acceso remoto o la autenticación. “En algunas ocasiones se confunde Zero Trust con VPN, MFA o Single Sign-On”, explica. Son piezas importantes, reconoce, pero insuficientes si detrás sigue existiendo una lógica basada en confiar en todo lo que ocurre dentro del perímetro corporativo.

Desde su punto de vista, el verdadero cambio está en la capacidad de controlar no solo quién accede, sino también qué puede hacer, en qué contexto y bajo qué condiciones. “No solamente es importante la identidad”, resume. Lo relevante es “qué accede, cómo accede, en qué momento y con qué permisos”.

Ese planteamiento cobra todavía más importancia con la llegada de identidades no humanas. Agentes, APIs, automatismos o procesos autónomos obligan a ampliar el alcance tradicional de Zero Trust. El problema ya no pasa únicamente por validar usuarios, sino por entender cómo interactúan aplicaciones, procesos y datos dentro de la organización.

Eusebio Nieva, Sales Engineer Manager Iberia y evangelista de **Check Point Software Technologies**

> “Desde 2018, cerca del 80 % de nuestras detecciones estaban basadas en inteligencia artificial”



En paralelo, las empresas siguen teniendo dificultades para gestionar la complejidad acumulada durante años. Herramientas desconectadas, arquitecturas fragmentadas y múltiples soluciones puntuales terminan creando más fricción operativa. “Existen demasiados silos”, señala Nieva, y orquestar todas esas piezas “es algo que muy pocas corporaciones se pueden permitir de forma sencilla”.

Ese escenario está empujando al mercado hacia modelos más integrados y propuestas de plataforma. Nieva considera que no es solo una tendencia comercial, sino una necesidad real derivada de la dificultad de operar entornos cada vez más distribuidos. Cuantas más herramientas distintas intervienen, más difícil resulta integrarlas y automatizar procesos de seguridad de forma coherente.

Aun así, insiste en que las organizaciones tampoco quieren quedarse atrapadas en plataformas completamente cerradas. Ahí sitúa Check Point su estrategia “Open Garden”, basada en integrarse con soluciones de terceros y compartir inteligencia, automatización y capacidades de monitorización más allá de su propio ecosistema.

“La complejidad es el enemigo número uno”, afirma. Y cuanto más heterogéneo es el entorno, más difícil resulta conseguir que todas las piezas trabajen de forma coordinada.

La IA está acelerando todavía más esa presión. Según Nieva, uno de los mayores puntos de fricción aparece precisamente cuando las empresas intentan desplegar proyectos de inteligencia artificial rápidamente y la seguridad queda relegada a un segundo plano. “Muchas veces la gran sacrificada es la seguridad”, reconoce.

La prioridad suele ser poner el proyecto en marcha, demostrar resultados y justificar la inversión. Y eso, en muchas ocasiones, deriva en

> “La piedra angular de la transición postcuántica es saber qué tienes y dónde lo tienes”

atajos o controles insuficientes. Al mismo tiempo, la inteligencia artificial introduce amenazas distintas, desde automatismos maliciosos hasta nuevas formas de manipulación o explotación de modelos.

La propia IA ocupa ya una parte central de la estrategia de Check Point. Nieva recuerda que la compañía llevaba años utilizando modelos de inteligencia artificial tradicional para tareas de detección antes del auge de la IA generativa. “Desde 2018, cerca del 80 % de nuestras detecciones estaban basadas en inteligencia artificial”, afirma. Ahora el objetivo pasa por utilizar agentes capaces de monitorizar infraestructuras, detectar configuraciones anómalas o identificar cambios no autorizados prácticamente en tiempo real. También por automatizar tareas relacionadas con investigación, threat hunting o generación

Eusebio Nieva, Sales Engineer Manager Iberia y evangelista de **Check Point Software Technologies**

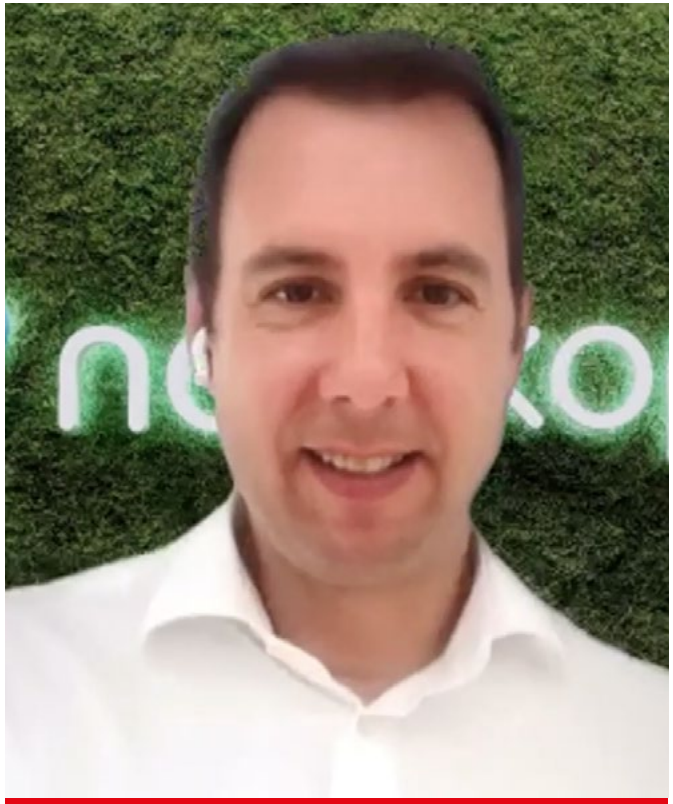
de políticas de seguridad. La idea es ayudar a los equipos de seguridad a operar más rápido sin incrementar todavía más la carga operativa. Ese enfoque conecta directamente con otro de los conceptos que Check Point lleva años defendiendo: prevention first. Para Nieva, la prevención sigue siendo el mecanismo más eficaz dentro de cualquier estrategia de seguridad. “Todo aquello que puedas poner en modo preventivo evitará trabajo posterior”, resume.

El problema, explica, es que muchas soluciones no ofrecen suficiente fiabilidad como para activarse directamente en bloqueo sin miedo a afectar a producción. Por eso insiste tanto en reducir falsos positivos y aumentar el nivel de confianza de las detecciones. “Cuando decimos que algo es malicioso y debe bloquearse, lo hacemos con muchísima confianza”, afirma.

Netskope: “La visibilidad ya no es suficiente: hay que entender cómo se mueve el dato”

La llegada masiva de la IA generativa a las empresas está obligando a revisar algunos de los pilares clásicos de Zero Trust. La conversación ya no gira únicamente alrededor del acceso o de la identidad; ahora el foco empieza a desplazarse hacia el dato, el contexto y la capacidad de tomar decisiones en tiempo real.

Rosalía Arroyo



Nacho Franzoni Martínez,
Solutions Engineer Manager de **Netskope**

Explica Nacho Franzoni Martínez, Solutions Engineer Manager de Netskope, que muchas compañías siguen centrando su estrategia en asistentes corporativos como Copilot o versiones empresariales de ChatGPT, pero la realidad es bastante más amplia. Netskope calcula que una gran organización utiliza de media alrededor de 130 aplicaciones de IA generativa diferentes.

Ese crecimiento está obligando a replantear también cómo se interpreta Zero Trust. Para Franzoni, el concepto sigue apoyándose en los mismos principios, pero necesita adaptarse a un escenario donde ya no solo intervienen usuarios humanos.

“Las IA trabajan primordialmente con tokens”, explica. También cambian los protocolos, los tipos de actividad y la forma en la que se intercambia la información. Frente al clásico tráfico HTTPS aparecen nuevos modelos de interacción ligados a agentes, automatismos o APIs capaces de operar de forma autónoma.

Aun así, hay algo que para Netskope no cambia: la necesidad de controlar el dato. “La clave sigue siendo entender qué información se mueve”, resume. Da igual que detrás exista un usuario, un agente o un automatismo; el problema continúa siendo identificar si ese dato es sensible, quién lo utiliza y bajo qué contexto.

Ahí es donde Franzoni sitúa una de las principales evoluciones del mercado. “La visibilidad es un must en seguridad”, afirma. Si no se entiende qué ocurre dentro del entorno corporativo,

> “La visibilidad ya no es suficiente: hay que entender cómo se mueve el dato”

resulta imposible prevenir o responder correctamente.

Pero, en su opinión, la visibilidad por sí sola ya no basta. El siguiente paso consiste en interpretar contexto: qué usuario accede, desde qué dispositivo, a qué instancia SaaS se conecta y qué tipo de actividad está realizando. “No es lo mismo un download que un upload o un share”, explica.

Más contexto y menos silos

La complejidad sigue siendo otro de los grandes problemas para muchas organizaciones. Franzoni considera que uno de los errores más habituales es pensar que Zero Trust es simplemente una tecnología concreta y no un modelo de seguridad mucho más amplio.

En opinión del directivo de Netskope, muchas compañías no tienen una única consola desde la que operar”, lo que complica la gestión de políticas, la automatización y la capacidad de aplicar controles coherentes entre acceso, SaaS, cloud o protección del dato.

Por eso Netskope lleva tiempo apostando por modelos SSE donde red, acceso, inspección de tráfico y protección de la información funcionan de forma integrada. La idea es evitar la proliferación de herramientas aisladas y reducir silos operativos. Un enfoque que se extiende también hacia la convergencia entre SSE, DSPM y protección del dato. Franzoni insiste en que el problema no es solo proteger información en tránsito, sino también entender qué ocurre cuando está en reposo o en uso.

“No se trata de tener diferentes soluciones para cada estado del dato”, señala. El objetivo es trabajar con un único motor de protección capaz

> “Una gran organización utiliza de media alrededor de 130 aplicaciones de IA generativa”

de aplicar las mismas políticas independientemente de si la información está en un OneDrive, moviéndose por Teams o utilizándose dentro de una aplicación de IA generativa.

Riesgo y decisiones en tiempo real

Otro de los grandes cambios que observa Netskope tiene que ver con la capacidad de tomar decisiones dinámicas basadas en riesgo. Para Franzoni, la tecnología ya permite avanzar mucho más allá de la simple detección, y explica que ya no se trata solo de ver o bloquear tráfico malicioso, sino de entender el riesgo asociado al usuario, al dato, al dispositivo o incluso a la instancia SaaS concreta a la que alguien intenta conectarse.

Esa capacidad depende también de la experiencia de usuario. Franzoni reconoce que cualquier proyecto de seguridad fracasa si introduce demasiada fricción porque “no hay proyecto de seguridad que se sostenga con una mala experiencia de usuario”.

Ahí entra en juego la infraestructura NewEdge de Netskope, basada en más de 130 puntos de presencia distribuidos globalmente. La idea es acercar inspección, políticas y capacidades de seguridad al usuario sin penalizar rendimiento ni acceso a aplicaciones SaaS.

La compañía está reforzando además capacidades específicas para IA, incluyendo guardrails, control de tráfico MCP o detección avanzada de información sensible mediante modelos de machine learning capaces de identificar código fuente, imágenes, whiteboards o fotografías de tarjetas bancarias.

Nacho Franzoni Martínez, Solutions Engineer Manager de **Netskope**

“El perímetro ya no está en la red: ahora está en el dispositivo”

La expansión del trabajo distribuido y la llegada de la inteligencia artificial están devolviendo protagonismo al dispositivo dentro de las estrategias de seguridad. Lo que durante años muchas organizaciones consideraron un elemento más del puesto de trabajo empieza a convertirse en una pieza crítica dentro de Zero Trust, especialmente ahora que usuarios, agentes y automatismos operan continuamente sobre información corporativa desde entornos móviles.

Rosalía Arroyo

“Prácticamente no hay nada que no puedas hacer desde el móvil”, dice Enrique Martín, director de Gran Cuenta de Samsung Electronics, para quien el desplazamiento del trabajo hacia dispositivos móviles está obligando también a revisar cómo se interpreta Zero Trust. Hasta ahora, el modelo se apoyaba principalmente en la validación del usuario y del acceso, pero la aparición de agentes capaces de actuar en nombre de las personas cambia el escenario.

Recuerda el directivo que, cuando hablamos de agentes de IA, “tú le estás dejando tus datos a un agente externo para que haga tareas en tu nombre”, por lo que aparece una nueva preocupación: hasta dónde puede acceder ese agente, cuánto tiempo conserva la información o qué ocurre si alguien copia esos datos mientras se utilizan.

“La IA tiene acceso a tus datos y hay que proteger esos datos”, insiste. El problema ya no es únicamente verificar la identidad o proteger la conexión. También hay que asegurar la información que utilizan esos agentes y garantizar que no pueda manipularse el modelo o las reglas con las que opera.

Enrique Martín,
director de Gran Cuenta de **Samsung Electronics**

Ahí es donde Samsung sitúa buena parte de su discurso alrededor de la seguridad anclada

> “Prácticamente no hay nada que no puedas hacer desde el móvil”

en hardware. Para Martín, cualquier estrategia Zero Trust necesita apoyarse en una “certeza absoluta” sobre el dispositivo desde el que se trabaja. Saber que el firmware es el correcto, que el sistema operativo no ha sido alterado y que nadie ha manipulado la base sobre la que funciona todo lo demás.

La raíz de confianza

“La seguridad se construye desde los cimientos”, viene a plantear durante la conversación. Ese es precisamente el papel que Samsung atribuye a Samsung Knox. La plataforma busca trasladar la confianza más allá del software y apoyarla directamente en hardware explica Martín, defendiendo la necesidad de una raíz de confianza ligada al silicio sobre la que construir firmware, kernel, sistema operativo y aplicaciones.

La compañía lleva años desarrollando ese enfoque y lo ha reforzado con tecnologías como Knox Vault, donde determinados datos y procesos sensibles quedan aislados del sistema operativo principal mediante un procesador y una memoria independientes. El objetivo es proteger credenciales, biometría o información utilizada por modelos de IA incluso aunque el sistema operativo llegue a verse comprometido.

Protección continua y movimiento lateral

La preocupación no está solo en proteger el dispositivo durante el arranque. También en mantener esa supervisión mientras se utiliza. “Necesitas saber qué está pasando en tiempo real”, explica Martín, añadiendo que eso implica combinar protección local, telemetría y capacidad de integración con centros de operaciones de seguridad.

> “La IA tiene acceso a tus datos y hay que proteger esos datos”

Enrique Martín, director de Gran Cuenta de **Samsung Electronics**

Uno de los riesgos que más preocupa a los responsables de ciberseguridad es el movimiento lateral. Para reducir ese riesgo, Samsung está reforzando capacidades de verificación continua e integración con SIEM y SOC corporativos. “El dispositivo tiene que reportar lo que está pasando”, resume.

Ahí encaja también Knox Matrix, una propuesta basada en defensa colaborativa entre dispositivos del ecosistema. La idea es que móviles, PCs y otros equipos puedan detectar anomalías entre ellos y aislar automáticamente elementos comprometidos antes de que el problema escale.

IA, movilidad y Zero Trust

La presión regulatoria añade otro factor adicional. Normativas como NIS2 o DORA están obligando a las organizaciones a demostrar capacidad real de control, trazabilidad y reacción. “Ya no vale con decir que tienes el software actualizado; tienes que demostrarlo”, afirma Martín.

En entornos con miles de dispositivos móviles, eso convierte la gestión centralizada y la visibilidad continua en elementos clave dentro de Zero Trust.

En el fondo, la visión de Samsung parte de una idea bastante clara: si el trabajo, los datos y ahora también la IA se están desplazando hacia la movilidad, la seguridad tiene que hacerlo también.

“La inteligencia artificial va a potenciar todavía más el uso en movilidad”, sostiene Enrique Martín, quien considera que muchas organizaciones todavía no han dado al dispositivo el peso que realmente tiene ya dentro de su estrategia Zero Trust. “A lo mejor deberías subir un poco más arriba la gestión de tu parque móvil”, concluye.

“Zero Trust ya no solo protege el acceso: también tiene que proteger el uso del dato”

La irrupción de la IA está obligando a muchas organizaciones a replantear cómo entienden Zero Trust. Lo que nació hace años como un modelo centrado principalmente en validar identidades y limitar accesos empieza ahora a enfrentarse a un escenario mucho más complejo, marcado por automatismos, agentes capaces de actuar de forma autónoma y decisiones que deben tomarse prácticamente en tiempo real.

Rosalía Arroyo

Gonzalo Oltra del Valle,
Enterprise Regional Director para Iberia de **Zscaler**

Tiene claro Gonzalo Oltra del Valle, Enterprise Regional Director para Iberia de Zscaler, que ahora Zero Trust no solo protege el acceso, “sino también el uso y la filtración de la información”.

El cambio, según señala, está relacionado con la necesidad de entender no solo quién accede, sino también “el qué y el por qué”. La llegada de agentes de IA capaces de tomar decisiones autónomas obliga a incorporar nuevos niveles de control, supervisión y gobernanza alrededor de cómo se utiliza la información dentro de las organizaciones.

Desde la perspectiva de Zscaler, muchas compañías siguen abordando Zero Trust de forma demasiado tecnológica y poco estratégica. Afirma Oltra que “se está ejecutando como un proyecto de integración de soluciones”, cuando en realidad debería plantearse como una transformación progresiva del modelo de seguridad. Ahí es donde la compañía sitúa uno de los errores más habituales: intentar trasladar arquitecturas heredadas al cloud sin modificar realmente la lógica de acceso. En el caso de ZTNA, por ejemplo, Oltra insiste en que no se trata de replicar la VPN “pero en la nube”. En su opinión el objetivo ya no es abrir un túnel hacia la red corporativa, sino restringir el acceso únicamente a aplicaciones concretas y validar continuamente

> “Ahora en Zero Trust hay que identificar no solo el quién, sino también el qué y el porqué”

identidad, contexto y estado del dispositivo antes de conceder permisos.

Para conseguirlo, considera imprescindible realizar primero un trabajo profundo de discovery. Entender qué aplicaciones existen, qué dispositivos acceden y cómo se están utilizando realmente los recursos corporativos.

Eliminar superficie de ataque

Según Oltra, el enfoque clásico sigue intentando proteger el perímetro y asegurar el camino hacia el dato, mientras que Zero Trust Exchange busca proteger directamente la interacción entre usuario, aplicación y dato, independientemente de dónde se encuentren.

“La IA no puede atacar lo que no ve y lo que no encuentra”, afirma, añadiendo que reducir superficie de ataque sigue siendo una de las mejores defensas frente a amenazas cada vez más rápidas y automatizadas.

La velocidad es precisamente otro de los factores que está obligando a replantear cómo se toman decisiones de seguridad. Explica Oltra que el modelo de Zscaler está diseñado para operar inline, inspeccionando tráfico y aplicando controles mientras la conexión se produce, sin depender de listas estáticas o reglas predefinidas. “Pasamos de observar a intervenir”, resume. La idea es que las decisiones se tomen en tiempo real y directamente en el punto donde circula el tráfico.

Más contexto y menos fricción

Ese modelo depende cada vez más de combinar múltiples señales de contexto. Identidad,

> “La IA no puede atacar lo que no ve y lo que no encuentra”

ubicación, dispositivo, comportamiento o riesgo asociado al acceso forman parte de las variables que la plataforma analiza continuamente para decidir qué hacer en cada interacción.

Oltra insiste en que uno de los grandes retos es conseguir todo eso sin penalizar experiencia de usuario. “No hay que pedir nada al usuario”, explica. La plataforma absorbe complejidad y toma decisiones automáticamente desde la nube, aplicando políticas dinámicas sin obligar al usuario a intervenir constantemente.

La IA está acelerando también la evolución de la propia propuesta de Zscaler. Según explica, la protección del dato y el uso seguro de modelos de IA ya no se entienden como módulos independientes, sino como una extensión natural de la arquitectura Zero Trust.

“La evolución es pasar de controlar accesos a

Gonzalo Oltra del Valle, Enterprise Regional Director para Iberia de **Zscaler**

controlar todas las interacciones con el dato”, resume.

Zero Trust en la era de la IA

Oltra considera que el mercado está entrando en una nueva fase donde la diferencia ya no se limita únicamente a capacidades técnicas concretas, sino al propio diseño de la arquitectura. Mientras algunos enfoques intentan adaptar tecnologías heredadas al cloud, Zscaler está evolucionando hacia modelos basados en lo que denomina “security data fabric”, apoyándose además en capacidades adquiridas tras la compra de Avalor.

La idea es ampliar visibilidad más allá del tráfico que circula por el proxy e integrar información procedente de distintas fuentes para construir una visión más amplia del riesgo.