Adopción segura de GenAI con Zero Trust:

Uso seguro de aplicaciones de GenAI pública

DOCUMENTO TÉCNICO

Tabla de contenido

Introducción

La IA generativa (GenAI) está transformando la manera de operar de los gobiernos, permitiéndoles mejorar la productividad, agilizar los procesos y brindar un mejor servicio a los ciudadanos. Sin embargo, para aprovechar el potencial transformador de GenIA y mitigar sus riesgos inherentes simultáneamente, los organismos deben aplicar los principios Zero Trust. Este paradigma garantiza que no se confíe de manera predeterminada en ninguna entidad, humana o máquina, asegurando una visibilidad continua y una verificación rigurosa de cada interacción.

Este documento técnico es el primero de la serie “Adopción segura de GenAI con Zero Trust”, una estrategia integral diseñada para ayudar a los organismos gubernamentales a navegar de manera segura el panorama de GenAI. La serie tiene tres fases:

- La fase 1, en este documento, se centra en asegurar las aplicaciones de GenAI pública para abordar riesgos como la fuga de datos y el uso no autorizado/no sancionado de la IA (“IA oculta”).
- La fase 2 explorará la adopción de herramientas de IA agéntica para aumentar la productividad de los empleados de manera segura.
- La fase 3 se centrará en la implementación segura de sistemas GenAI para servicios a los ciudadanos, garantizando que los sistemas y datos gubernamentales permanezcan protegidos.

Cada fase hace hincapié en un enfoque proactivo y en capas para equilibrar la innovación con una gobernanza y seguridad sólidas.

Uso seguro de GenAI pública

Información general

Los gobiernos tienen cada vez más consciencia del potencial transformador de la IA generativa (GenAI) para sus operaciones y los servicios que prestan a los ciudadanos. Esta tecnología ofrece una vía para lograr aumentos importantes de productividad y la evolución de los servicios a los ciudadanos a través de distintas aplicaciones. Estas soluciones van desde la comprensión del sentir público y la provisión de chatbots impulsados por la IA para ayuda de los ciudadanos y de TI, hasta facilitar la traducción de idiomas y la automatización de procesos internos como la redacción de descripciones de puestos de trabajo, el resumen de reuniones y la creación de anuncios públicos.

Las entidades gubernamentales que adoptaron estas medidas en sus comienzos ya están observando mejoras en la experiencia y la satisfacción de los empleados. El surgimiento de modelos de lenguaje grandes (LLM) de acceso público, como ChatGPT, ha impulsado la experimentación en todo el sector público a medida que las organizaciones buscan comprender y aprovechar las capacidades de la IA. Este interés generalizado subraya las oportunidades para mejorar la eficiencia y la prestación de servicios con la integración de estas herramientas avanzadas de IA.

Sin embargo, la integración de GenAI, especialmente a través de LLM públicos y modelos de terceros, plantea desafíos de seguridad importantes. El uso no autorizado de herramientas de IA (“IA oculta”) puede exponer datos confidenciales de los ciudadanos, registros comerciales o propiedad intelectual. El riesgo se amplifica aún más en los flujos de trabajo que incluyen la generación aumentada de recuperación (RAG) o el protocolo de contenido de modelos (MCP) y los agentes de IA, que podrían comprometer datos confidenciales y plantear riesgos para la seguridad nacional debido a la posibilidad de que actores patrocinados por estados o entidades maliciosas se aprovechen de estas vulnerabilidades con fines de espionaje, sabotaje o disrupción de infraestructuras críticas. Además, la GenAI presenta una amplia superficie de ataque que las medidas de seguridad tradicionales no están preparadas para gestionar eficazmente, porque a menudo se basan en controles binarios restrictivos o carecen de una visibilidad integral en diferentes entornos.

Para aprovechar el potencial de la GenAI, los organismos deben adoptar un enfoque Zero Trust con seguridad robusta, visibilidad y simplicidad para el usuario. Los siguientes pasos describen un proceso que los organismos pueden seguir para aprovechar la GenAI, mitigando de manera proactiva los riesgos de fuga de datos y evitando una carga excesiva para los equipos de seguridad:

1. Establezca marcos y políticas de gobernanza de la IA
2. Integre estrecha-mente la experiencia del usuario y la capacitación
3. Elija la arquitectura adecuada y priorice la seguridad
4. Implemente la protección de datos desde el principio
5. Utilice un enfoque de protección por capas

Analicemos más profundamente estos pasos.

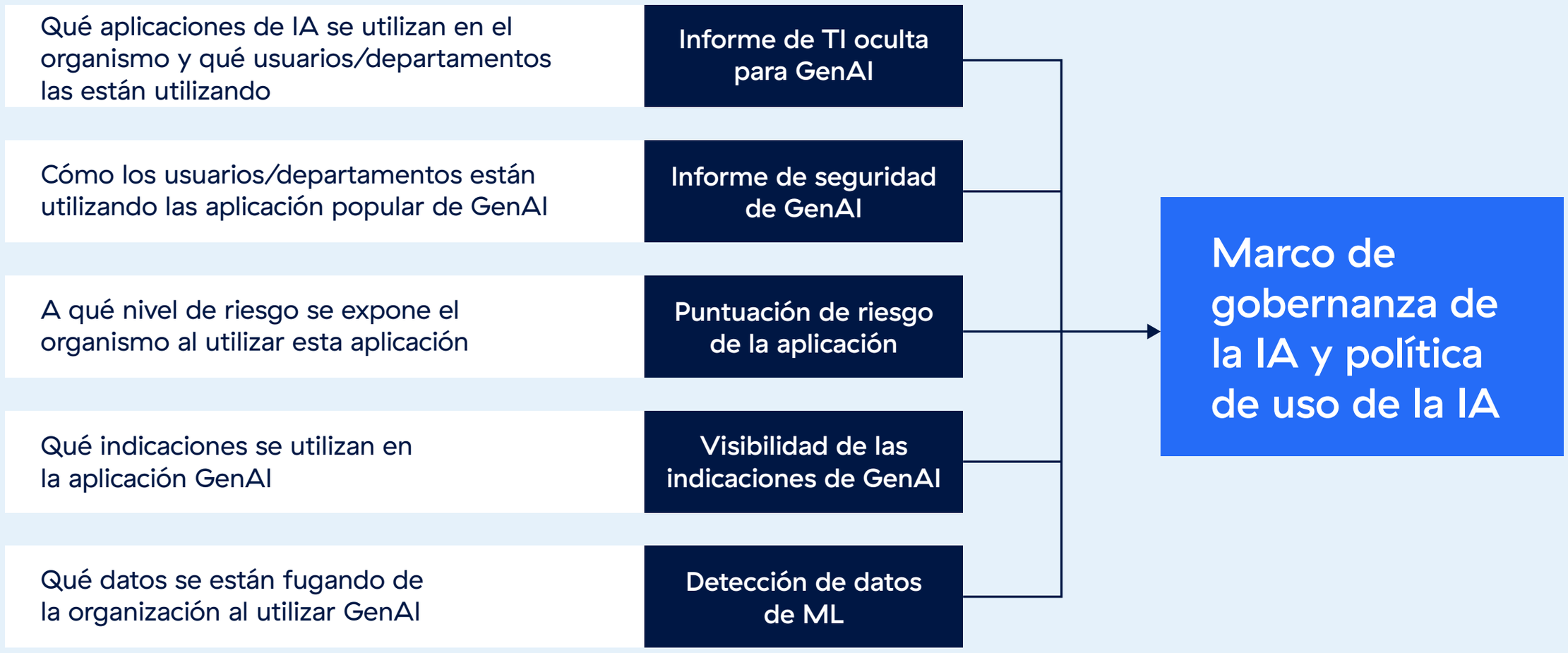
1. Establezca marcos y políticas de gobernanza de la IA

Para aprovechar plenamente los beneficios de la GenAI, los organismos deben implementar medidas de seguridad sólidas que aborden directamente los riesgos sin obstaculizar la productividad del usuario. Esta sección explora cómo los organismos pueden adoptar un enfoque Zero Trust para las aplicaciones de GenAI, garantizando al mismo tiempo que los controles de seguridad no entorpezcan la experiencia del usuario.

El desarrollo de marcos y políticas de gobernanza de la IA es esencial para asegurar la adopción de la GenIA dentro de los organismos estatales. Esto suele incluir la creación de un grupo de trabajo o un organismo de gobierno específico para supervisar el desarrollo y la implementación de políticas. Por ejemplo, el Grupo de Trabajo en GenAI de Alabama sirve de modelo con su enfoque de equipo colaborativo e interfuncional. Los organismos también deberían aprovechar los marcos Zero Trust establecidos, como el modelo de madurez Zero Trust de CISA y NIST 800-207, junto con marcos de seguridad específicos para la IA como el Marco de gestión de riesgos de IA de NIST (AI RMF), que remarca funciones centrales como la gobernanza, el mapeo, la medición y la gestión, o TRISM de Gartner®, para guiar sus esfuerzos. Mediante la adopción de un grupo de trabajo especializado y la utilización de estos marcos probados, los organismos pueden acelerar la integración segura de las tecnologías de GenAI en todos los departamentos.

Para respaldar este proceso, Zscaler proporciona información que ayuda a los organismos a rastrear el uso de la IA en sus entornos, evaluar los posibles riesgos relacionados con las aplicaciones de GenAI e identificar casos de fuga de datos. Aprovechar los informes de Zscaler permite a los organismos acceder a datos críticos sobre cómo se están utilizando actualmente las herramientas de GenAI.

Puntos de datos proporcionados por Zscaler para respaldar la creación de un marco de gobernanza de la IA y una política de uso de la IA



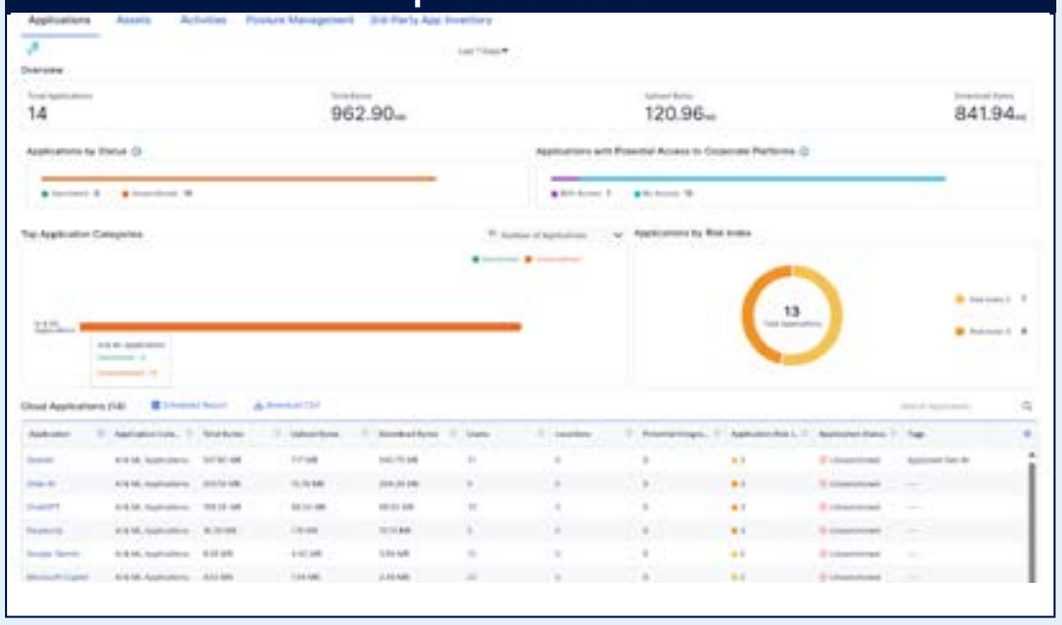
Comprensión del uso actual de la IA

Comprender el uso actual de la IA es un paso clave para crear marcos de gobernanza. Al analizar qué aplicaciones de GenAI se están utilizando, cómo se están aplicando y los factores de riesgo asociados, los organismos pueden identificar dónde son más necesarias las políticas. Este enfoque basado en datos garantiza que el marco siga siendo relevante, práctico y adaptado para abordar eficazmente los desafíos y oportunidades únicos del organismo.

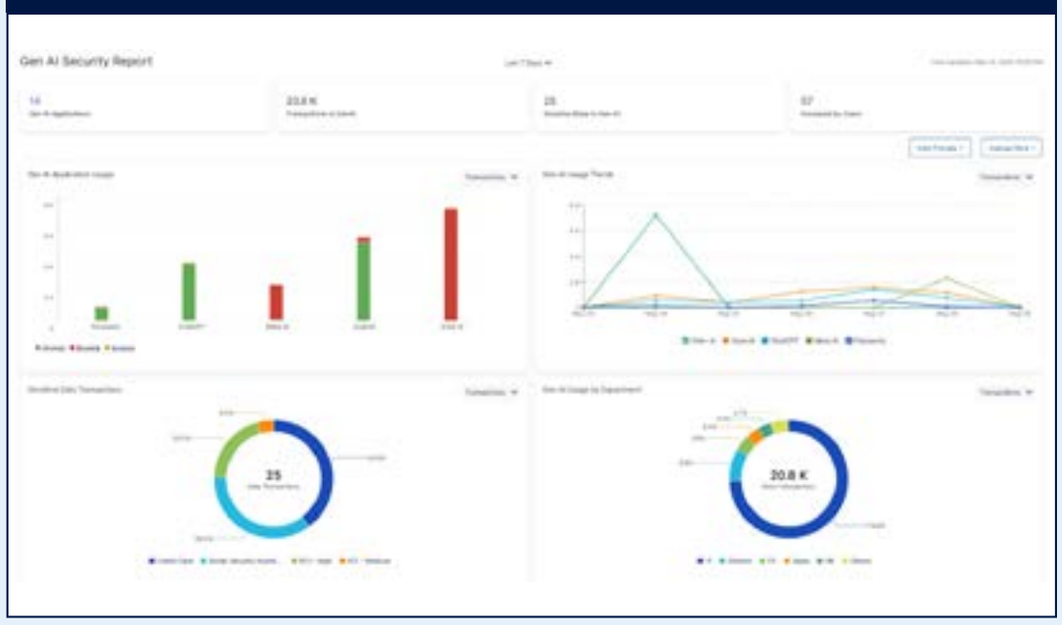
Zscaler proporciona informes detallados sobre el uso de la IA que ofrecen transparencia sobre qué aplicaciones de GenAI se están utilizando en los distintos organismos y el alcance de su uso. Estos datos pueden segmentarse aún más para mostrar patrones de uso dentro de departamentos o suborganismos específicos, lo que proporciona a las organizaciones una visión más clara de su panorama de uso de la IA.

Conocimientos sobre el uso de la IA oculta

Detección de aplicaciones de TI ocultas para GenAI

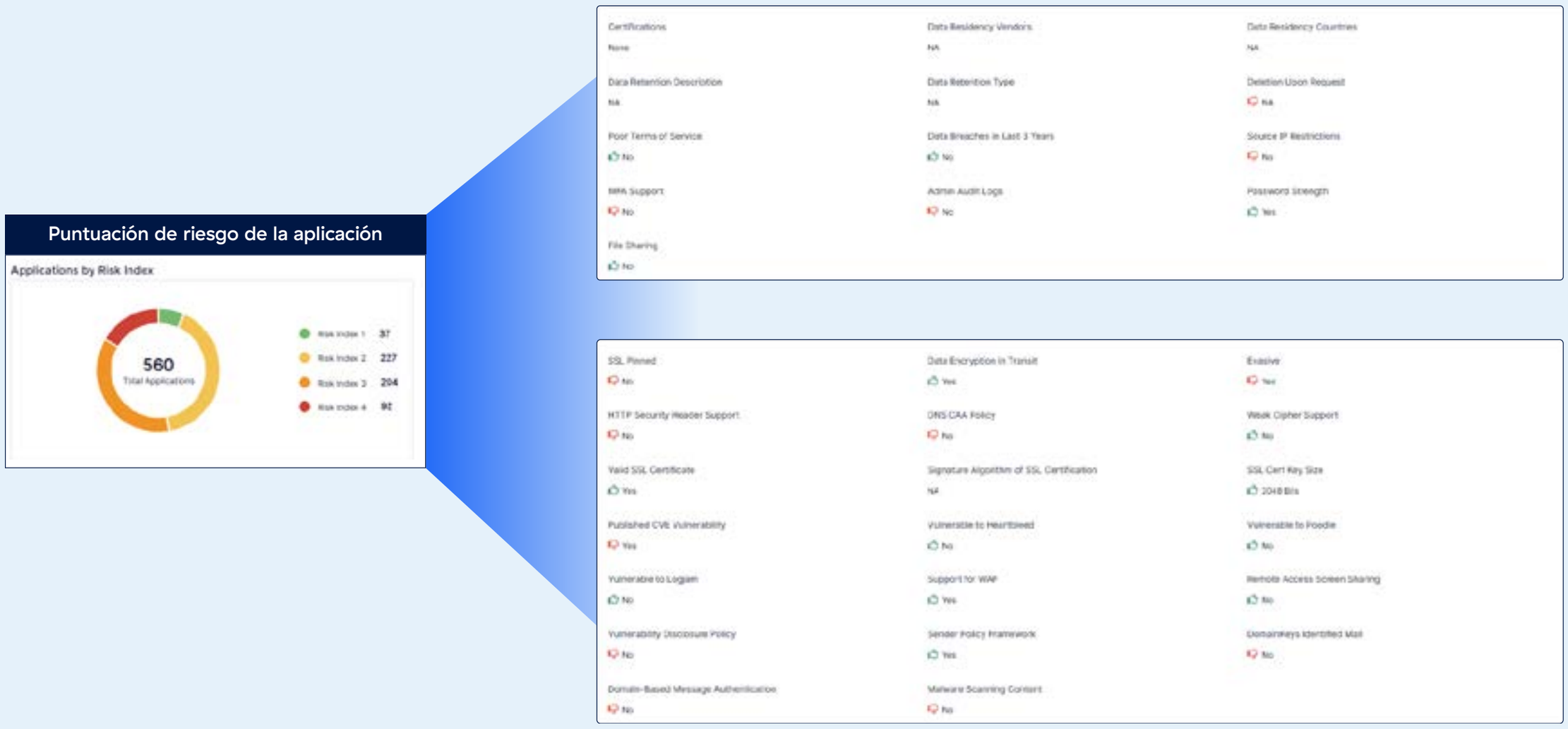


Informe de seguridad de GenAI



Gracias a esta visibilidad, los organismos pueden profundizar en los factores de riesgo asociados a estas aplicaciones. El equipo ThreatLabz de Zscaler, junto con inteligencia de amenazas externas, evalúa estos riesgos y les asigna puntuaciones agregadas que van del 1 al 5, lo que simplifica el análisis de riesgos para los responsables de tomar las decisiones. Los organismos también tienen la flexibilidad de adaptar estas puntuaciones en función de sus prioridades y requisitos únicos. Las evaluaciones de riesgos pueden incluir factores clave como vulnerabilidades de seguridad o problemas de cumplimiento normativo, lo que permite a los responsables de las políticas centrar los recursos en las áreas más relevantes para su misión y necesidades de seguridad. En el siguiente informe se muestran algunos ejemplos de factores de riesgo, como vulnerabilidades de seguridad o incumplimiento normativo, lo que permite a los responsables de las políticas del organismo priorizar las áreas que son importantes para el organismo respectivo.

Riesgos asociados al uso de la IA oculta

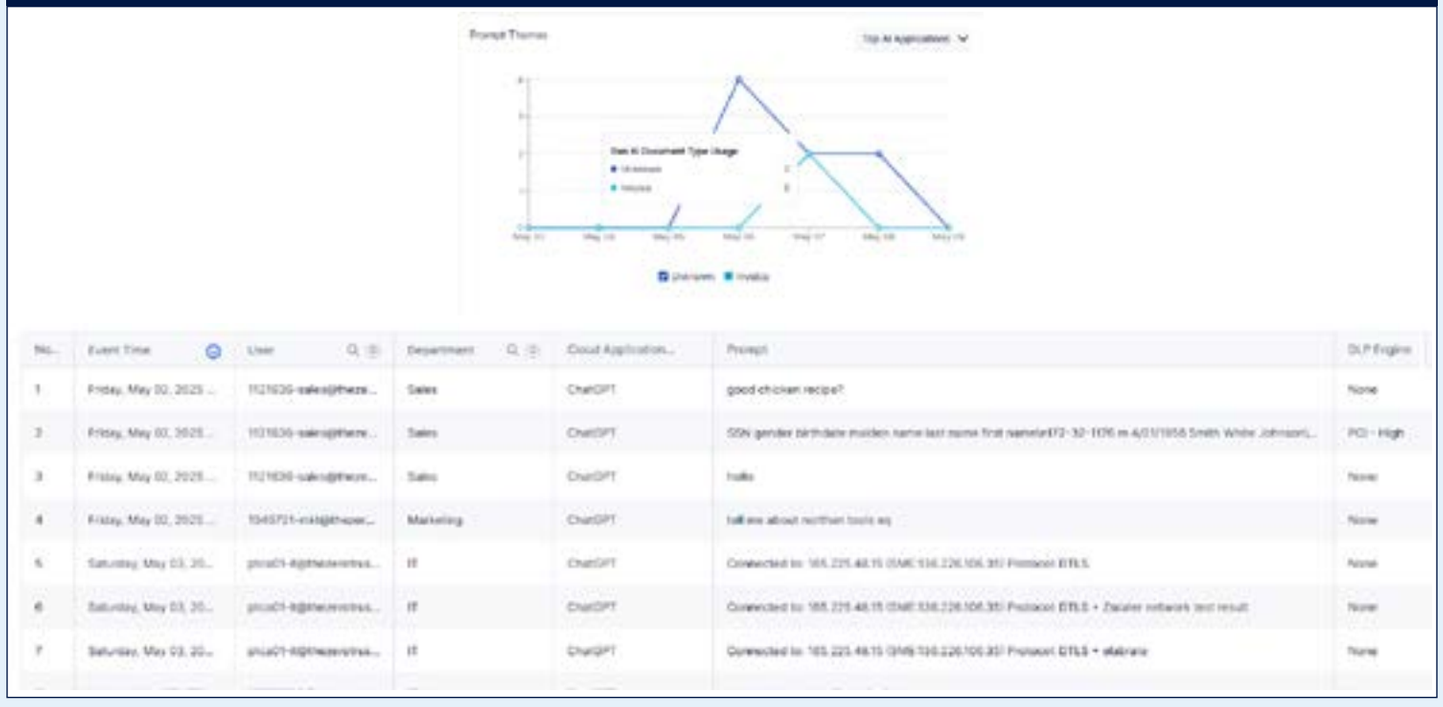


Conocimiento detallado de las interacciones de los usuarios con las aplicaciones de GenAI

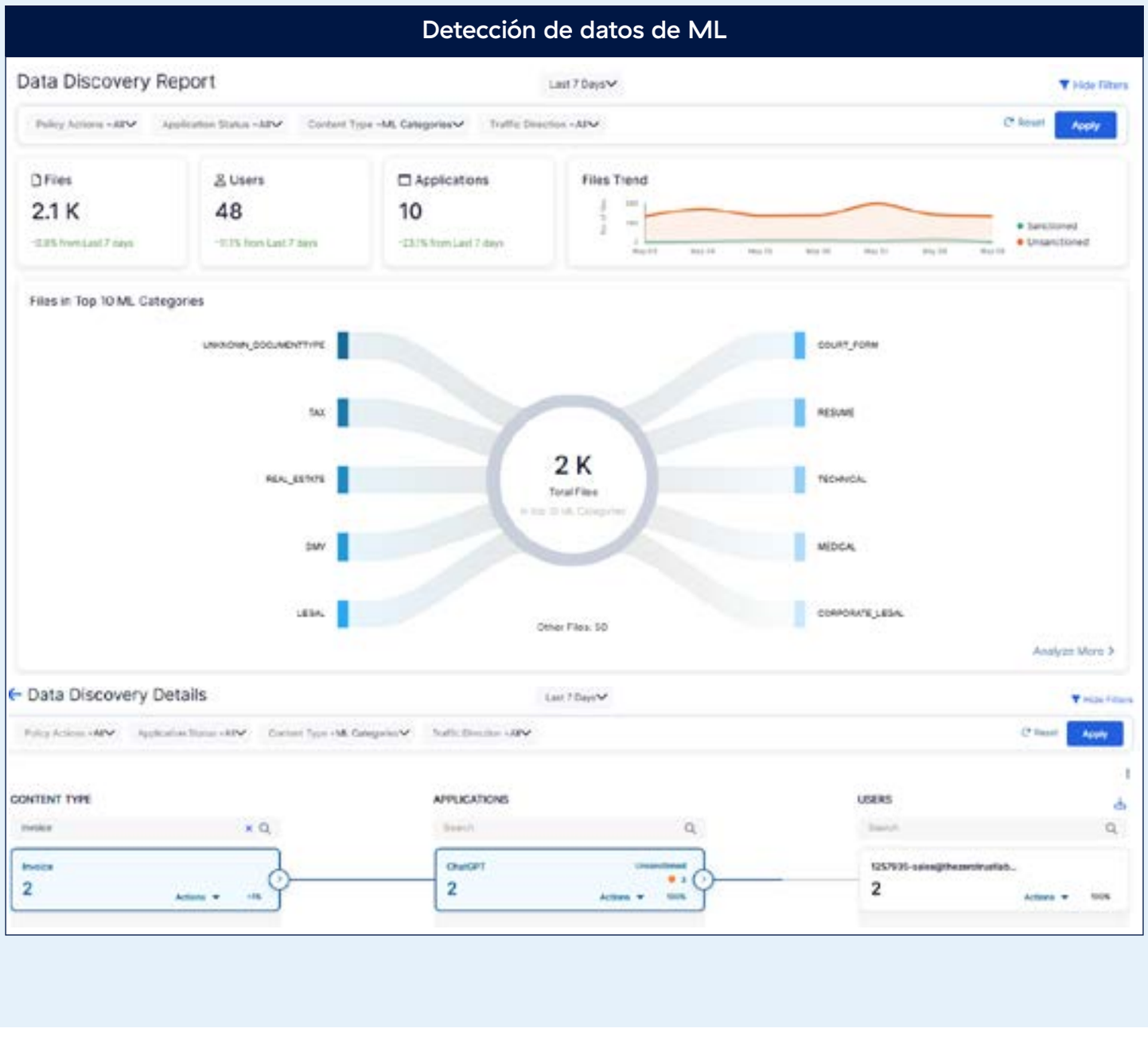
Zscaler va más allá de la visibilidad a nivel de aplicación al proporcionar conocimientos detallados de cada transacción, solicitud e interacción del usuario en las aplicaciones de GenAI. Esto incluye datos detallados sobre lo que introducen los usuarios no solo a través de transferencias de archivos, sino también mediante métodos como entradas por teclado, actividades del portapapeles y otras entradas compatibles. Estos datos son de gran valor para los organismos, ya que les ayudan a comprender mejor el tipo de datos que se comparten, a perfeccionar las políticas de seguridad y a garantizar el cumplimiento de las normas de gobernanza. Además, este nivel de visibilidad es esencial para las auditorías y se puede exportar sin problemas al SIEM del organismo para un seguimiento y análisis exhaustivos.

Informe sobre las fugas de datos actuales fuera del organismo

Visibilidad de las indicaciones de GenAI



Detección de datos de ML



Visibilidad de datos desconocidos

Zscaler mejora aún más la visibilidad al identificar datos que los organismos podrían desconocer que se fugan a través de las aplicaciones de GenAI. Gracias a las capacidades basadas en IA/ML, el informe ML Discovery de Zscaler va más allá de las reglas tradicionales de DLP de “solo supervisión” para detectar y clasificar de manera proactiva los datos confidenciales que se comparten con herramientas públicas de GenAI. Esto permite a los propietarios de datos y a los administradores de seguridad identificar fugas de datos desconocidas o no reconocidas y tratarlas antes de que se conviertan en problemas críticos.

Esta profunda visibilidad de los datos permite a los organismos identificar de manera proactiva datos de alto riesgo que podrían quedar expuestos a los LLM públicos. También ayuda a establecer o refinar la propiedad de la información confidencial, desarrollar políticas de uso e implementar directrices personalizadas para proteger conjuntos de datos clave.

Al combinar los conocimientos sobre usuarios, aplicaciones, riesgos de las aplicaciones, indicaciones y patrones de datos, Zscaler ayuda a crear políticas y procedimientos específicos que coinciden con los objetivos de la organización. Estos conocimientos impulsan la asignación de recursos y ayudan a definir roles y responsabilidades dentro del marco de gobernanza Zero Trust, lo que permite a los organismos adoptar un enfoque proactivo que equilibra la innovación con la definición de una estrategia integral de mitigación de riesgos.

2. Integre estrechamente la experiencia del usuario y la capacitación

La experiencia y la capacitación del usuario desempeñan un papel central en la adopción segura y exitosa de la IA generativa (GenAI) en los organismos estatales. Para garantizar una adopción sin problemas, es esencial diseñar las medidas de seguridad y la capacitación de usuarios de manera que les permitan seguir siendo productivos al tiempo que se ofrece una protección sólida. En la medida de lo posible, debe evitarse la introducción de nuevas herramientas o aplicaciones, especialmente aquellas que puedan suponer una carga de aprendizaje adicional para los usuarios. Además, para maximizar su impacto, los controles de seguridad eficaces deben ir acompañados de una capacitación continua de los usuarios. Las plataformas deben integrarse perfectamente con los canales y flujos de trabajo existentes, incorporando al mismo tiempo mecanismos de interacción y retroalimentación del usuario. Esto ayudará a los organismos a alinearse desde el principio con marcos como el Marco de gestión de riesgos de IA del NIST (AI RMF).

He aquí algunas capacidades clave de la plataforma que respaldan este enfoque:

Acceso sin interrupciones a GenAI

El objetivo principal de las herramientas de GenAI es liberar a los usuarios de tareas repetitivas y permitirles centrarse en las tareas que se benefician del criterio humano. Las medidas de seguridad para GenAI no deben interrumpir los flujos de trabajo de los usuarios. Zscaler facilita esto al eliminar la necesidad de usar software adicional o navegadores gestionados. Por ejemplo,

- **Agente único de Zscaler** El mismo agente de Zscaler que garantiza el acceso seguro a aplicaciones públicas y privadas también gestiona los controles de GenAI, proporcionando un acceso sin interrupciones y sin introducir herramientas adicionales.

- **Casos de acceso seguro sin agente**
  Los usuarios pueden usar su navegador nativo y su flujo de trabajo existente (por ejemplo, mediante el portal de la aplicación IDP) para acceder a las aplicaciones seguras de GenAI sin la necesidad de un agente.

- **Controles de seguridad flexibles** En lugar de supeditar el uso de la IA a las opciones de “permitir o bloquear” únicamente, Zscaler ofrece aislamiento del navegador basado en la nube. Esta funcionalidad redirige a los usuarios que acceden a las aplicaciones de GenAI a un entorno de navegador aislado alojado en la nube de Zscaler. Esto permite a los usuarios mantener una experiencia de navegador nativa al tiempo que se aplican medidas de seguridad avanzadas, como prevenir la actividad del portapapeles, la impresión o la carga de archivos. Este diseño garantiza la aplicación de las políticas de seguridad sin interrumpir la experiencia del usuario, todo ello gestionado a través de una plataforma unificada y un único agente de Zscaler para simplificar la administración.

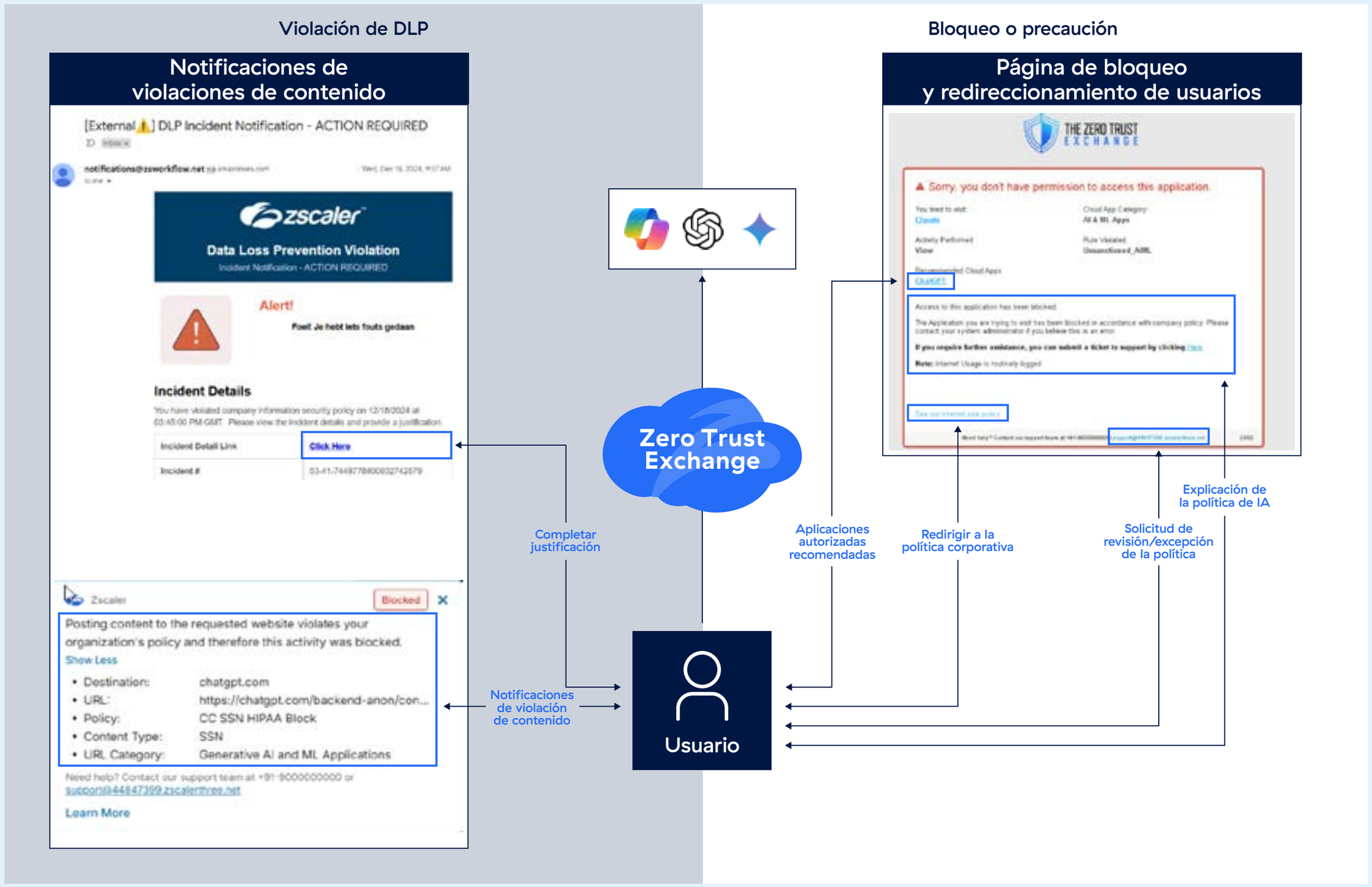
Estos controles pueden implementarse con un impacto mínimo en la infraestructura o los puntos finales existentes, lo que permite a los organismos implementar políticas de seguridad preservando una experiencia de usuario fluida y manteniendo el esfuerzo administrativo al mínimo.

Capacitación y retroalimentación integradas del usuario

La capacitación continua sobre el uso seguro de GenAI y las violaciones es esencial, especialmente dada la rápida evolución de GenAI. La capacitación debe ser regular, continua e integrada directamente en el flujo de trabajo y las herramientas habituales del usuario. Zscaler lo respalda mediante notificaciones dinámicas: cuando un recurso se bloquea, aísla o marca por violaciones de contenido, los usuarios reciben alertas personalizadas. Por ejemplo, si se bloquea una aplicación GenAI no autorizada, Zscaler sugiere alternativas aprobadas, lo que ayuda a redirigir el comportamiento de los usuarios y a mantener la productividad. En escenarios de violación del uso de datos, Zscaler se integra con herramientas conocidas como el correo electrónico y Slack, lo que facilita a los usuarios proporcionar justificaciones o recibir comentarios personalizados en las herramientas que ya utilizan.

Al integrar la capacitación de usuarios en los flujos de trabajo de seguridad, los organismos pueden establecer una base de gobernanza sólida para las aplicaciones de GenAI. Este enfoque no solo garantiza que los usuarios comprendan cómo interactuar de manera segura con la tecnología, sino que también ayuda a crear un marco escalable para gestionar los incidentes relacionados con la GenAI y perfeccionar las políticas de uso de la IA en toda la organización.

Capacitación y retroalimentación con Zscaler



3. Priorice la seguridad y elija la arquitectura adecuada

A medida que la superficie de ataque se amplía con la creciente adopción de herramientas de IA, las organizaciones deben elegir una plataforma que no solo proteja contra las amenazas impulsadas por IA, sino que también permita el uso seguro de aplicaciones de GenAI, construida sobre una arquitectura Zero Trust y con autorización de FedRAMP. Zscaler ofrece una solución integral que combina seguridad, facilidad de uso y cumplimiento para los organismos que adoptan GenAI.

Los organismos pueden comenzar a aprovechar las capacidades seguras de la GenAI de Zscaler con cambios mínimos en su infraestructura existente. Se puede reenviar tráfico a la plataforma a través de la aplicación Zscaler, que es compatible con los principales sistemas operativos, incluidos Windows, Mac, iOS, Android y Linux, o a través de un dispositivo de sucursal, o simplemente un navegador para la implementación sin agente. Una vez conectado, Zscaler se asegura de que los usuarios estén autenticados y autorizados antes de acceder a cualquier recurso en Internet, incluidas las aplicaciones de GenAI. Actuando como proxy, Zscaler inspecciona todas las sesiones TLS establecidas con las aplicaciones de GenAI, proporcionando a los organismos visibilidad completa y control granular sobre cómo interactúan los usuarios con estas herramientas. Esta arquitectura permite a los organismos ofrecer conocimientos detallados sobre cómo los usuarios utilizan las aplicaciones de GenAI y proporciona múltiples controles líderes en la industria para proteger los datos de los organismos.

Inspección de HTTPS y WebSocket seguro con Zscaler

Control de acceso

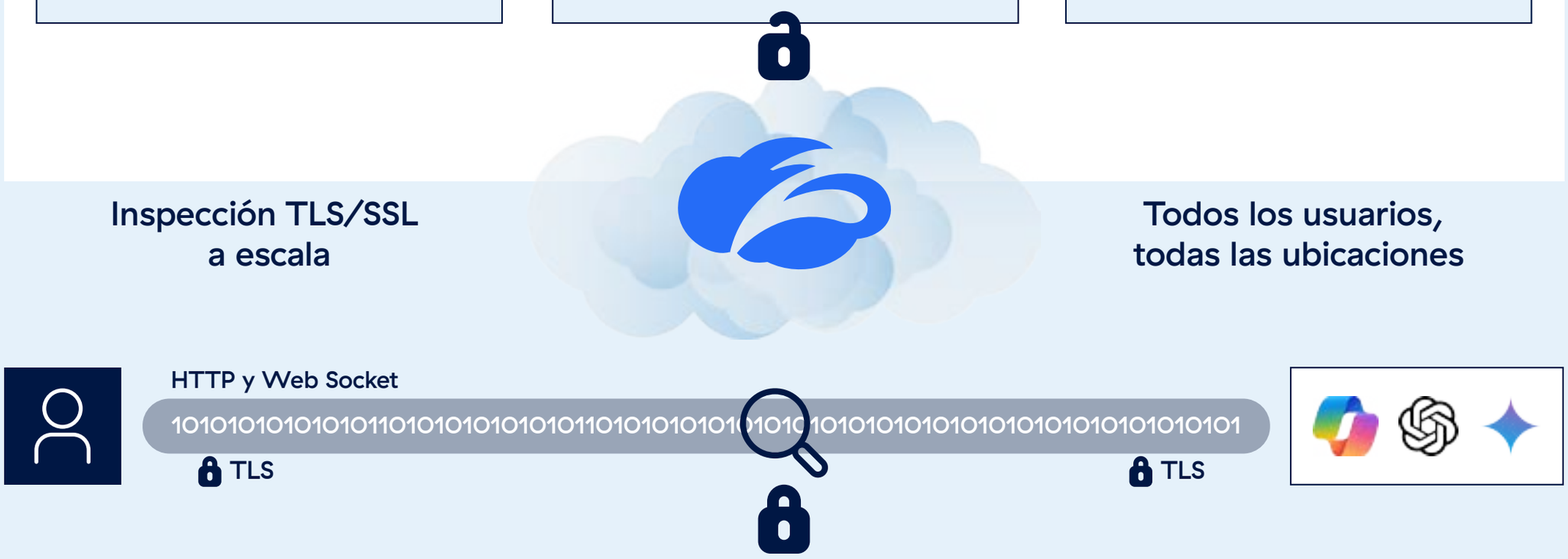
- Filtrado URL
- Firewall en la nube
- Controles granulares de aplicaciones en la nube
- Restricciones de tenencia
- Seguridad del DNS

Prevención de amenazas

- Protección contra malware
- Cloud Sandbox
- Protección contra amenazas avanzadas (IPS)
- Aislamiento del navegador en la nube

Protección de datos

- DLP en línea
- EDM/IDM
- Controles de tipo de archivo
- Controles de GenAI
- Aislamiento del navegador en la nube



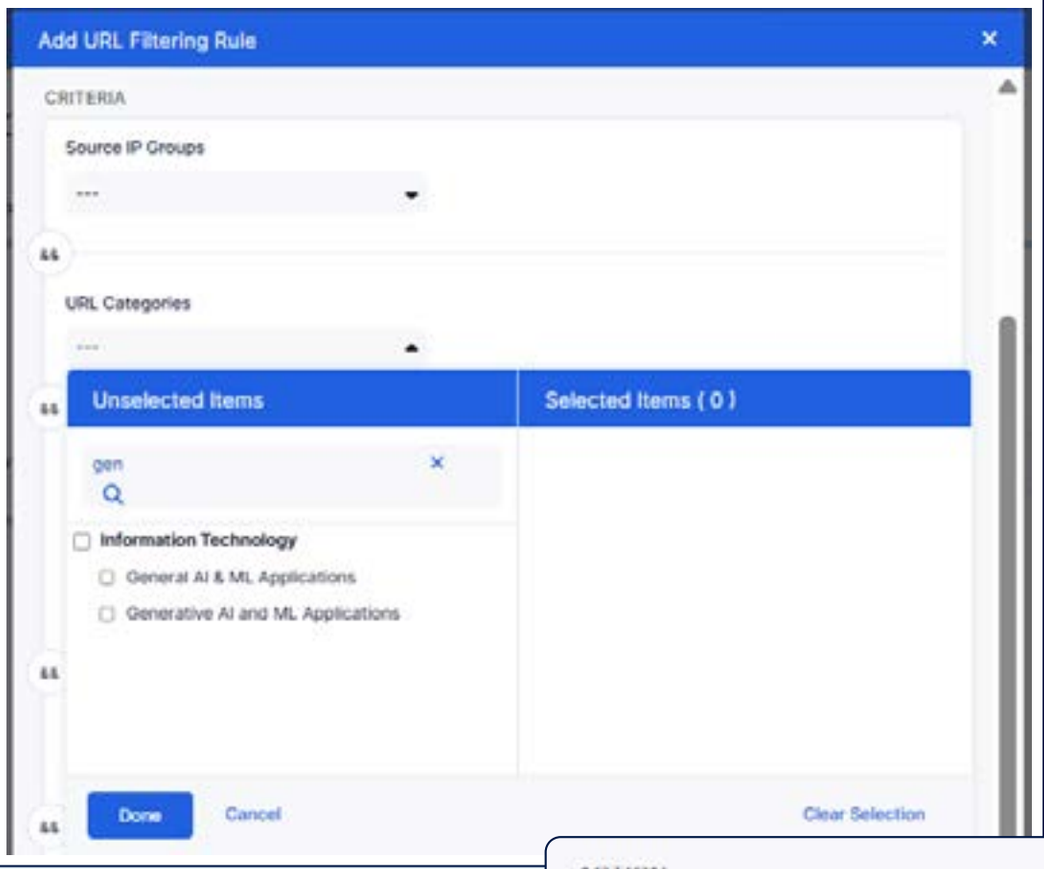
Automatice la detección y gestión de aplicaciones de GenAI

Con la implementación de TLS, los organismos obtienen acceso a todo el conjunto de capacidades de Zscaler, incluido el control granular de las aplicaciones de GenAI y aprendizaje automático (ML). Una ventaja clave reside en la categoría de aplicaciones de IA y ML de Zscaler, cuidadosamente seleccionadas por el equipo de ThreatLabz. Esta categoría engloba una amplia variedad de aplicaciones de IA, entre ellas algunas herramientas populares como ChatGPT, Gemini, MetiAI, Claude y otras.

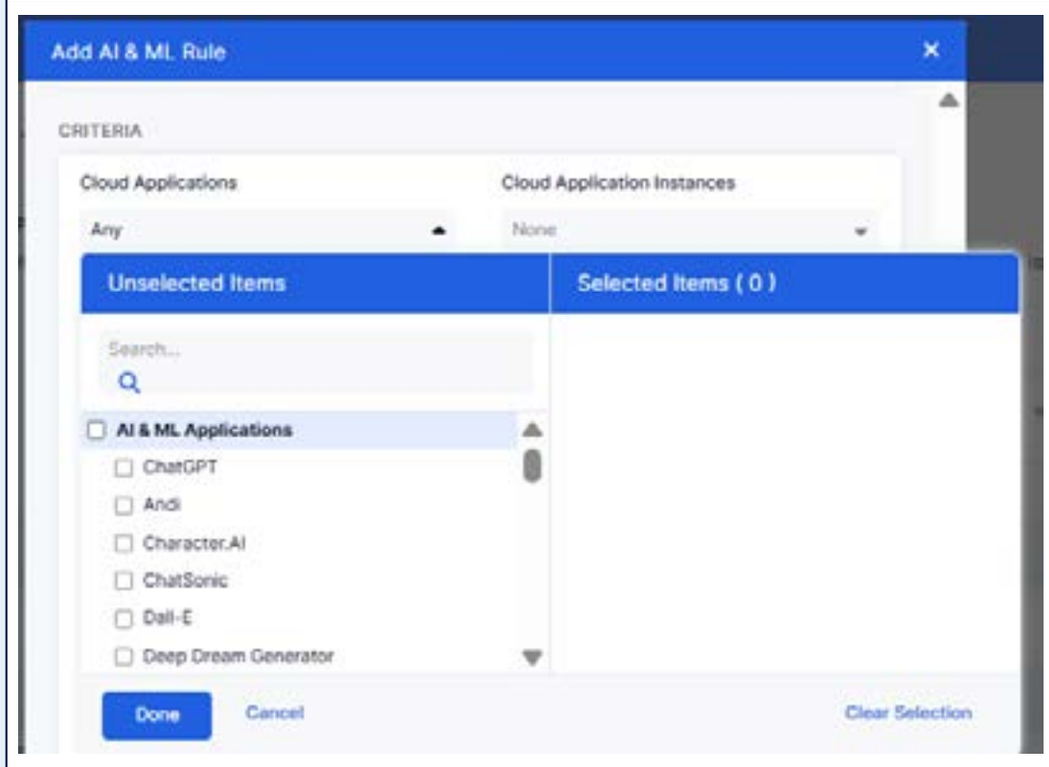
Mediante esta categoría, los organismos pueden aplicar políticas para bloquear de manera predeterminada las aplicaciones de GenAI desconocidas o no verificadas, y garantizar que solo se pueda acceder a las herramientas aprobadas. Las nuevas aplicaciones que van surgiendo, se agregan automáticamente a estas categorías, lo que ahorra a los organismos el esfuerzo de descubrirlas manualmente y enviar actualizaciones. Además, los organismos tienen la flexibilidad de ampliar o personalizar esta lista agregando dominios personalizados para que se adapten mejor a sus necesidades específicas. Zscaler también ofrece categorías específicas como “Aplicaciones de IA y ML generales” y “Aplicaciones de IA y ML generativos”, que, combinadas con la lista más amplia de “Aplicaciones de IA en la nube”, ofrecen una cobertura significativa para reducir los riesgos de seguridad que plantean las aplicaciones de GenAI. Este enfoque por capas permite a los organismos gestionar eficazmente el acceso a los cientos de aplicaciones que se desarrollan y publican cada semana.

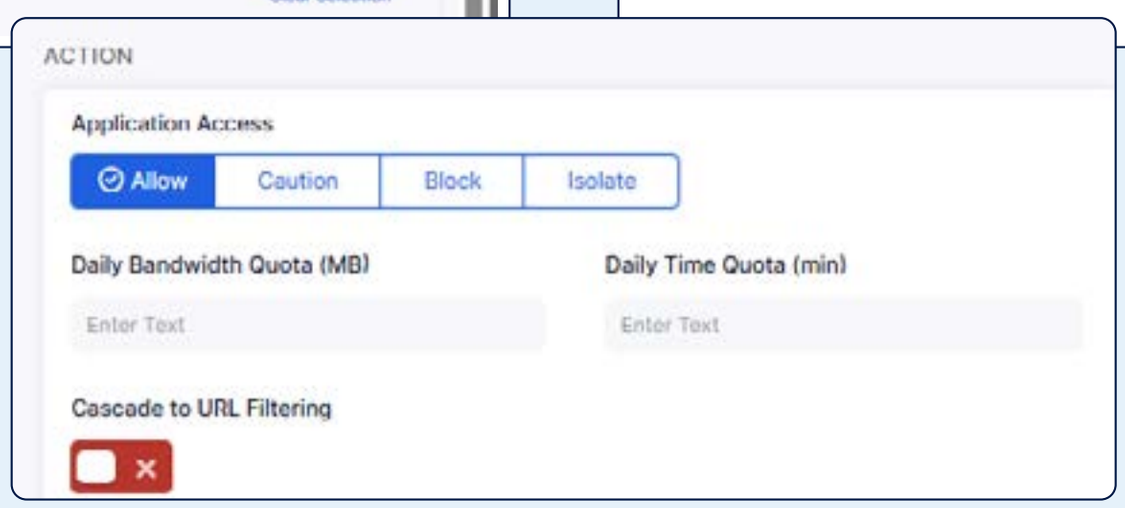
Selección de categorías amplias y aplicaciones específicas de IA

Categorías de URL para la red amplia



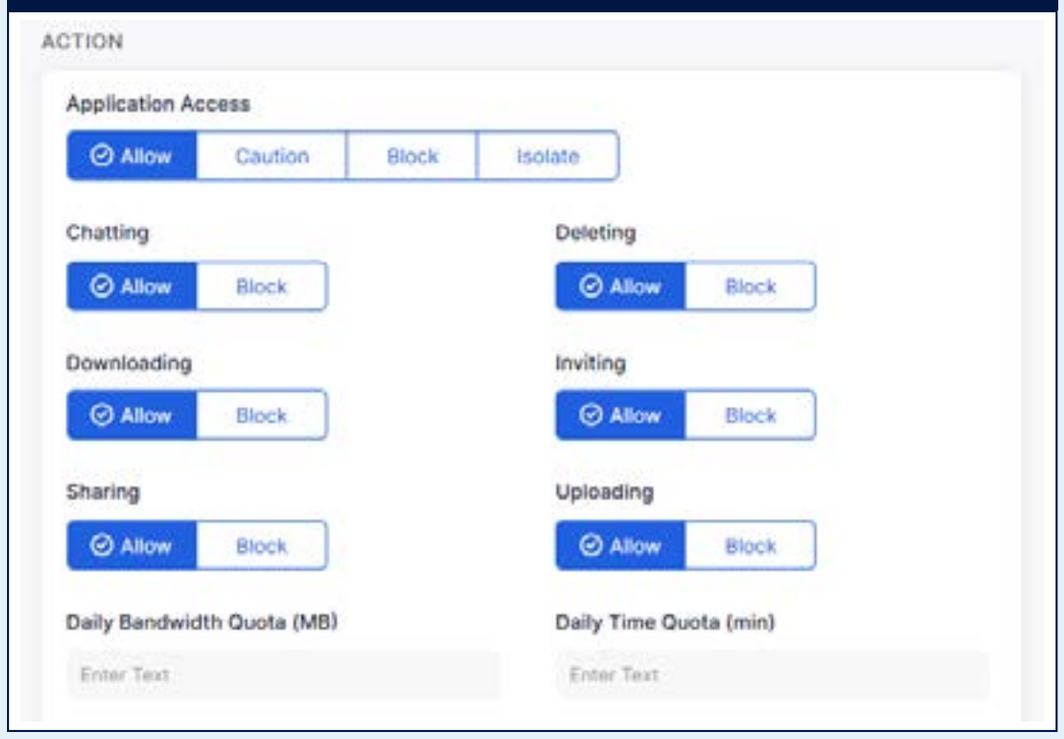
Aplicación de GenAI para controles granulares



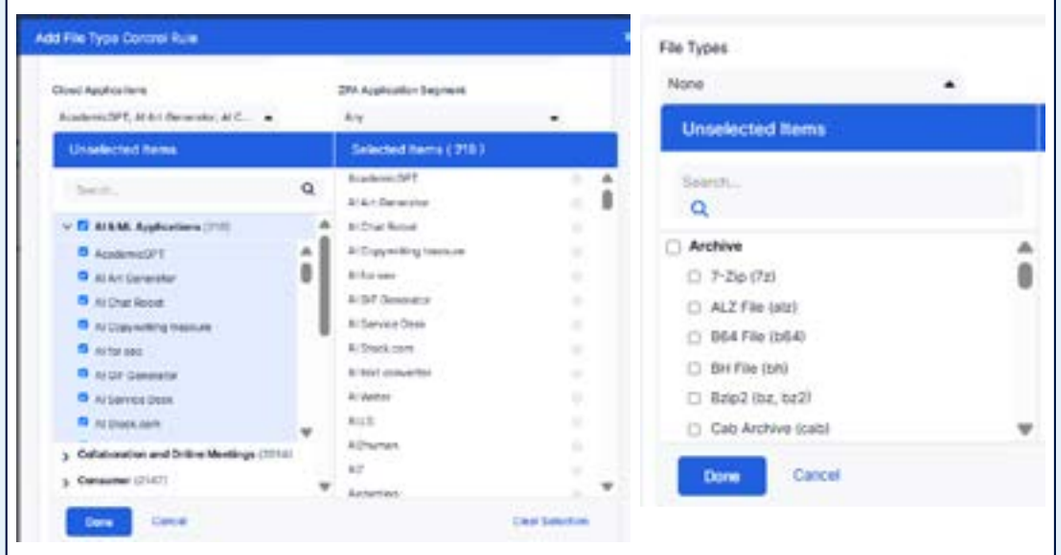


Controles granulares para aplicaciones SaaS, web y de IA

Controles granulares de la aplicación de GenAI



Controles de carga de archivos de la aplicación de GenAI



Permita aplicaciones autorizadas mediante el control de seguridad de aplicaciones SaaS

Además de mantener una lista muy completa de aplicaciones de IA, Zscaler proporciona controles detallados sobre cómo los usuarios interactuarán con las aplicaciones de GenAI. Estos controles son muy fáciles de aplicar, muy potentes y están consolidados en una plataforma única. La parte izquierda de la imagen muestra algunos ejemplos de controles granulares aplicables, cuando una política de seguridad de ChatGPT incluya controles granulares como permitir el chat, pero bloquear la carga de archivos o restringir el uso compartido de chats. Los organismos pueden aplicar estas medidas a nivel departamental o incluso a nivel de cada usuario. Estos controles granulares pueden refinarse aún más si se restringen los tipos de archivos que los usuarios pueden cargar a las aplicaciones de GenAI, como se muestra a la derecha. Este control de archivos también puede incluir la restricción de la carga de documentos cifrados.

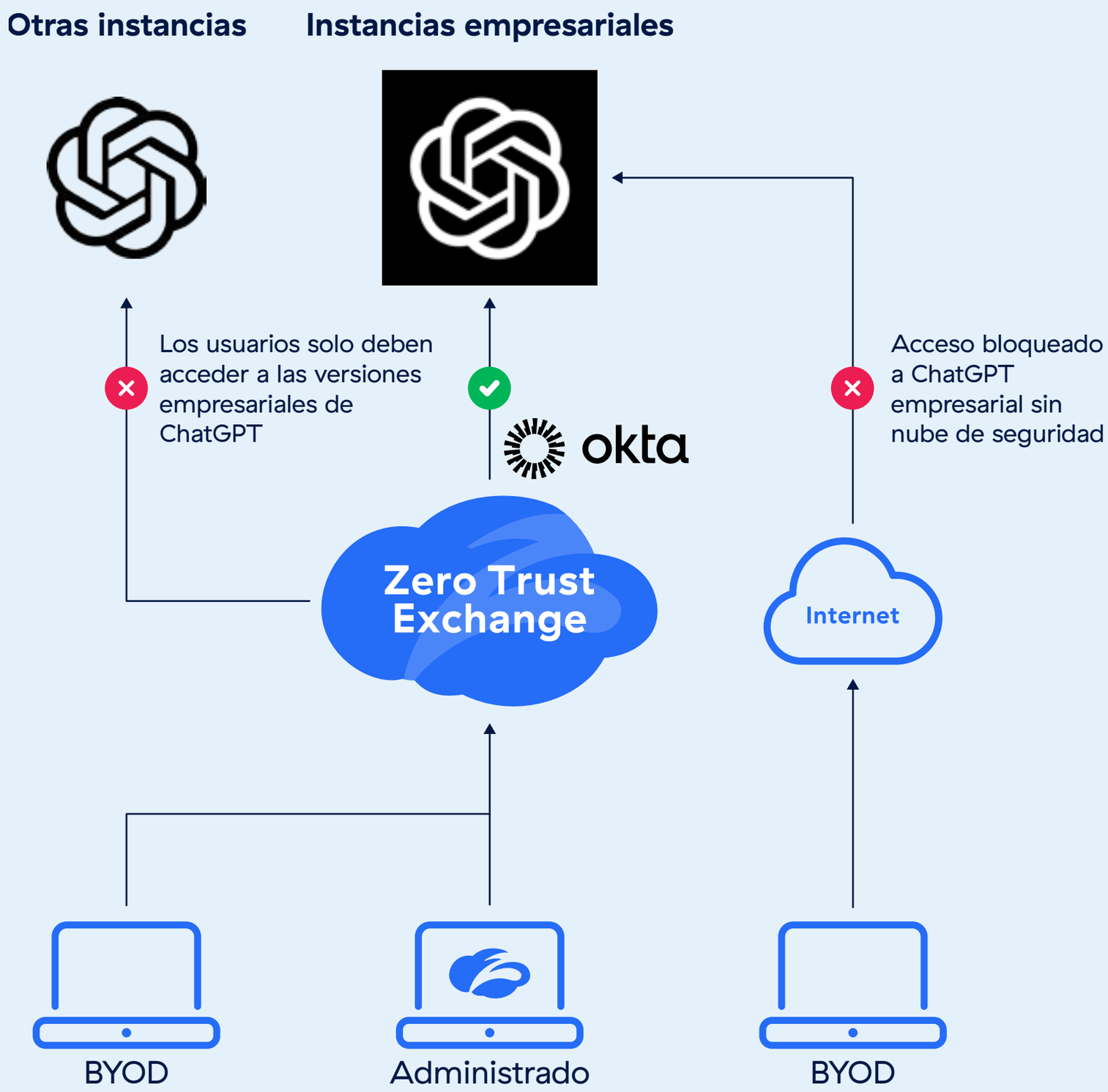
Restrinja el acceso a las instancias empresariales de las aplicaciones de GenAI

Los organismos deberían considerar seriamente el uso de versiones de las aplicaciones de GenAI para empresas para garantizar una mayor seguridad y control. Las versiones empresariales, como ChatGPT Enterprise, otorgan a los organismos la propiedad y el control totales de sus datos y conversaciones comerciales, sin que los datos corporativos contribuyan al entrenamiento del modelo. Estas soluciones cumplen con la norma SOC2 y proporcionan cifrado tanto en tránsito como en reposo. Además, simplifican la gestión de usuarios con funciones como el acceso basado en equipos, la verificación de dominio, el inicio de sesión único (SSO) y conocimientos sobre el uso, lo que permite una implementación segura a gran escala.

Las instancias empresariales de las aplicaciones de GenAI deben combinarse con SSO para maximizar la seguridad y proporcionar a los organismos una mayor visibilidad y control sobre el uso de las aplicaciones. Con la implementación de SSO, los organismos pueden aplicar políticas que bloqueen el acceso a las versiones no empresariales de las aplicaciones de GenAI. Por ejemplo, el control de usuarios de Zscaler para ChatGPT garantiza que solo se pueda acceder a los usuarios aprobados, mientras que los demás quedan restringidos automáticamente. Además, los organismos pueden implementar controles en la capa de gestión de identidades y accesos (IAM) mediante listas blancas para asegurarse de que las versiones empresariales sean la única instancia de uso de GenAI y para garantizar que solo se acceda a través de entornos seguros como la plataforma en la nube de Zscaler. Para ampliar aún más el acceso seguro, las instancias empresariales de GenAI también pueden ponerse a disposición de dispositivos no administrados o BYOD mediante el acceso BYOD sin agente de Zscaler.

Un enfoque simple de “permitir todo o bloquear todo” no es suficiente en el panorama actual de GenAI. Los organismos deben adoptar una estrategia de seguridad por capas con controles granulares adaptados a las diferentes interacciones de las aplicaciones. La consolidación de estas capacidades en una plataforma unificada no solo agiliza la implementación, sino que también simplifica el cumplimiento de los principios Zero Trust básicos, garantizando el acceso con privilegios mínimos, la visibilidad continua y la protección integral para cada interacción con GenAI.

Control de acceso a instancias autorizadas de aplicaciones de IA



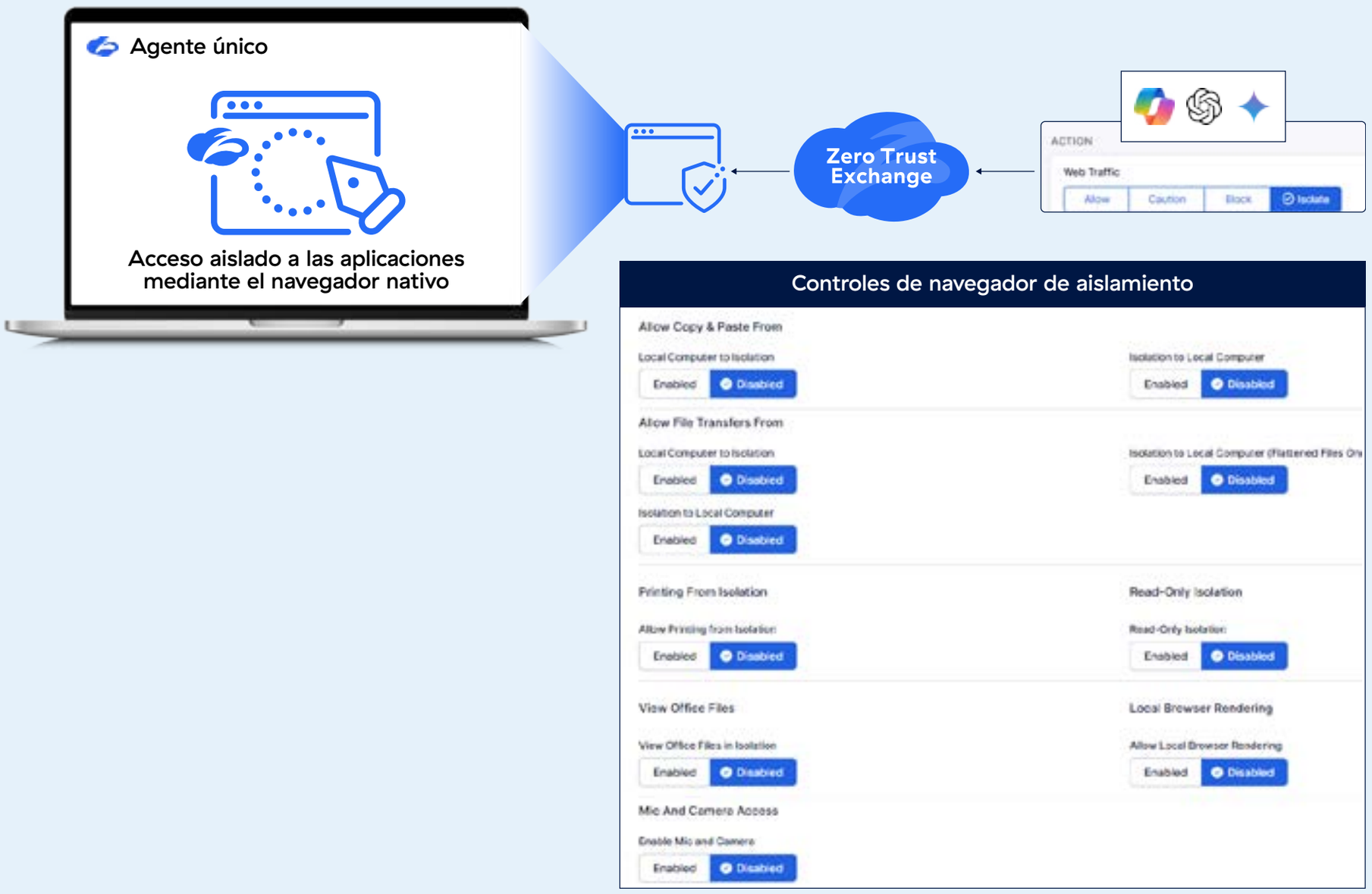
Reduzca el riesgo de las aplicaciones de GenAI no autorizadas

Cuando se necesita acceso a aplicaciones de GenAI que no están autorizadas (que carecen de licencia empresarial y de inicio de sesión único (SSO)), estas aplicaciones considerarse de alto riesgo. Los datos cargados en dichas aplicaciones pueden utilizarse para entrenar los modelos de GenAI, lo que podría exponer información confidencial. Para abordar este mayor riesgo, los organismos deben implementar capas adicionales de controles de seguridad para garantizar una supervisión más estricta de las interacciones de datos.

Zscaler ofrece una solución eficaz para gestionar este riesgo a través de su navegador Zero Trust. Esta herramienta permite a los organismos proporcionar acceso seguro a aplicaciones de GenAI no autorizadas con controles avanzados, como la limitación de acciones (por ejemplo, transferencia de archivos, impresión y uso del portapapeles). Además, el navegador Zero Trust impide que las aplicaciones de GenAI ejecuten código directamente en el navegador del usuario, y en su lugar, representa las interacciones en páginas aisladas. Esto ayuda a proteger contra la individualización, el seguimiento mediante cookies de terceros y otras vulnerabilidades, al tiempo que permite a los usuarios seguir utilizando el mismo navegador instalado por el organismo.

Este enfoque puede implementarse de dos maneras: con el agente unificado de Zscaler o mediante un modelo sin agente. Para los dispositivos de propiedad del organismo, se recomienda una implementación basada en agentes para garantizar que todo el tráfico se enrute a través de la plataforma de aplicación de Zscaler. En situaciones donde no se puede instalar un agente, la opción sin agente de Zscaler proporciona una alternativa segura, garantizando el acceso supervisado a las aplicaciones de GenAI sin comprometer la seguridad.

Controles granulares para proteger las aplicaciones de IA aisladas y, al mismo tiempo, equilibrar la experiencia del usuario



4. Implemente la protección de datos desde el principio

AI adoptar la GenAI, no implementar una sólida protección de datos desde el primer momento puede ocasionar fugas de datos, violaciones de las normas de privacidad y una pérdida de confianza pública, lo que en última instancia socava el éxito de estas herramientas. La naturaleza conversacional y fácil de usar de las aplicaciones de GenAI pública aumenta el riesgo de que los usuarios expongan involuntariamente datos confidenciales del gobierno. Sin una supervisión cuidadosa, acciones simples como copiar y pegar información o subir archivos podrían fugar detalles confidenciales debido al contexto o a la integración con otros sistemas. Esto destaca por qué la integración de medidas sólidas de protección de datos debería ser una parte fundamental de cualquier estrategia pública de adopción de GenAI para los gobiernos estatales y locales.

Zscaler permite a los organismos enfrentar estos riesgos directamente con sus avanzadas capacidades de prevención de pérdida de datos (DLP). La solución DLP de Zscaler para GenAI, diseñada para proteger la información confidencial desde el principio, identifica y bloquea el intercambio de datos confidenciales, ya sea a través de una solicitud, carga de archivos o uso indebido, antes de que puedan llegar a los modelos públicos de GenAI. Este enfoque proactivo se asegura de que los organismos puedan adoptar GenAI al tiempo que protegen la información confidencial y mantienen el cumplimiento normativo.

Acelere la adopción de DLP

Iniciar un proceso de protección de datos puede resultar complicado para muchas organizaciones, especialmente a la hora de equilibrar la necesidad de otorgar acceso a las herramientas de GenAI con la implementación de estrictas medidas de seguridad. Zscaler aborda este desafío al ofrecer una plataforma optimizada diseñada para apoyar a equipos ligeros, lo que permite una rápida adopción de GenAI con controles de protección de datos eficaces. Este enfoque garantiza que los organismos puedan escalar su marco de seguridad de manera eficiente en diversos departamentos y bases de usuarios.

Para los organismos que ya hayan integrado reglas para otros destinos de Internet, resulta sencillo extender esas políticas a las aplicaciones de GenAI. Zscaler también integra directamente en las aplicaciones de IA y ML los motores de DLP y los diccionarios existentes utilizados para otros canales, lo que reduce la redundancia y acelera la implementación. Si un organismo parte de cero, Zscaler proporciona diccionarios predefinidos que se pueden aplicar a las aplicaciones de GenAI con tan solo unos clics para evitar la fuga de datos confidenciales. Además, los documentos o conjuntos de datos conocidos pueden protegerse mediante EDM/IDM, y el etiquetado de protección de información de Microsoft (MIP) puede proteger aún más los datos cifrados o clasificados de cualquier exposición.

Para perfeccionar aún más las políticas, las capacidades de detección del aprendizaje automático (ML) de Zscaler identifican información confidencial previamente desconocida y fugas de datos dentro de las aplicaciones de GenAI, lo que permite a los organismos actualizar continuamente su estrategia de protección. Ya sea con el ajuste de los diccionarios existentes o la creación de reglas de detección personalizadas mediante expresiones regulares o palabras clave, los organismos pueden adaptarlos a sus necesidades. Zscaler también se integra con soluciones de copia de seguridad de datos como Rubrik, lo que simplifica la identificación y protección de datos.

Aceleración de la implementación de DLP con Zscaler

Implementar el Día O

Datos específicos del organismo con EDM e IDM

Diccionarios predefinidos que deben utilizar los organismos gubernamentales

- Números de enrutamiento bancario ABA
- Documento de finanzas corporativas
- Documento legal corporativo
- Documento judicial
- Credenciales y secretos
- Tarjetas de crédito
- Información sobre enfermedades
- Licencia de conducir (Estados Unidos)
- Información sobre medicamentos
- Estados financieros
- Documento de inmigración
- Documento de seguros
- Documento de factura
- Documento legal
- Documento médico
- Información médica
- Documento inmobiliario
- Números de Seguro Social (EE. UU.)
- Documento fiscal
- Número de identificación fiscal (EE. UU.)
- Documento del Departamento de Transporte y Automotores
- Información sobre tratamientos

Etiquetas AP/MI

Supervisión continua y visibilidad

Identificar fugas de datos y aplicaciones desconocidas

Datos recopilados de incidentes

Aportaciones y comentarios de los usuarios

Refinar y ajustar | Según sea necesario

Crear expresiones regulares/palabra clave para diccionarios personalizados

Palabras clave individual y de varias palabras con proximidad

Ampliar EDM + IDM a las soluciones de copia de seguridad de datos

La aplicación de políticas en tiempo real y la visibilidad detallada permiten a los equipos de TI proteger los datos confidenciales sin una complejidad adicional ni supervisión manual. Este enfoque simplificado facilita la adopción rápida y segura de las herramientas de GenAI, aprovechando sus beneficios de productividad al tiempo que garantiza el cumplimiento y la confianza pública, según el principio de “Nunca confiar, siempre verificar” de Zero Trust.

Simplifique la gobernanza de DLP

Un desafío común en la implementación de la prevención de pérdida de datos (DLP), especialmente en grandes organismos u organizaciones de servicios compartidos, es el volumen de incidentes que los equipos SOC y los propietarios de datos necesitan gestionar. Estos incidentes pueden variar desde exigir un seguimiento de los empleados para justificar sus acciones, reforzar la capacitación de los usuarios, gestionar excepciones o mantener un registro de auditoría. Sin un sistema eficiente, esto se puede volver demasiado rápidamente.

La automatización del flujo de trabajo simplifica este proceso al proporcionar una solución centralizada para gestionar los incidentes de protección de datos relacionados con la GenAI. Proporciona una visión completa de todos los incidentes en un solo lugar, incluidos los metadatos y detalles de las acciones o datos específicos que desencadenaron la violación. Esta centralización permite a los administradores revisar, priorizar y solucionar rápidamente los incidentes según sea necesario.

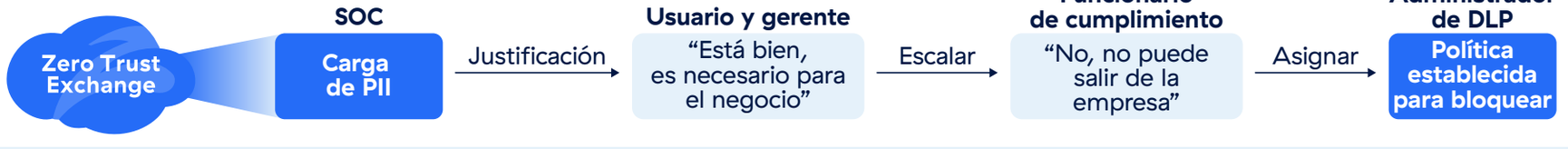
Una característica clave de la automatización de flujos de trabajo es su capacidad para agrupar incidentes en función de sus características compartidas y asignar prioridades. Estos grupos pueden luego asignarse a administradores específicos para su resolución particular. La automatización juega un papel importante aquí al permitir flujos de trabajo que notifican o capacitan a los usuarios finales involucrados en incidentes, solicitan justificaciones o ascienden los problemas a gerentes o propietarios de datos para su aprobación. Los flujos de trabajo automatizados también pueden activar acciones para solucionar incidentes sin intervención manual.

Al aprovechar la automatización del flujo de trabajo en DLP, los organismos pueden reducir significativamente los tiempos de resolución, disminuir las cargas operativas del SOC y obtener conocimientos prácticos sobre las áreas de riesgo. Estos datos pueden utilizarse para perfeccionar aún más las políticas o mejorar los programas de capacitación. Esto garantiza que los usuarios estén mejor preparados para operar de manera segura y reduce la probabilidad de incidentes en el futuro.

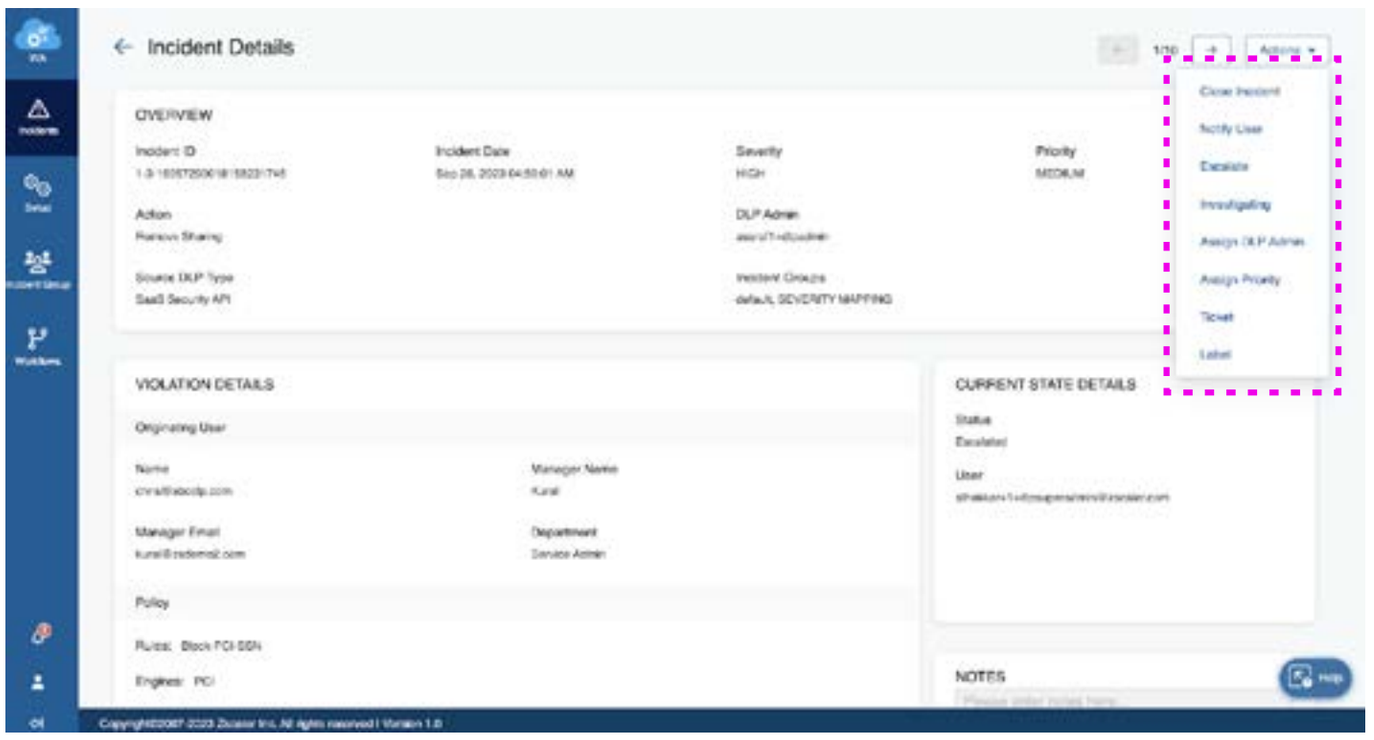
Optimice la gestión de incidentes con la gestión de casos y capacitación de usuarios

Automatización del flujo de trabajo

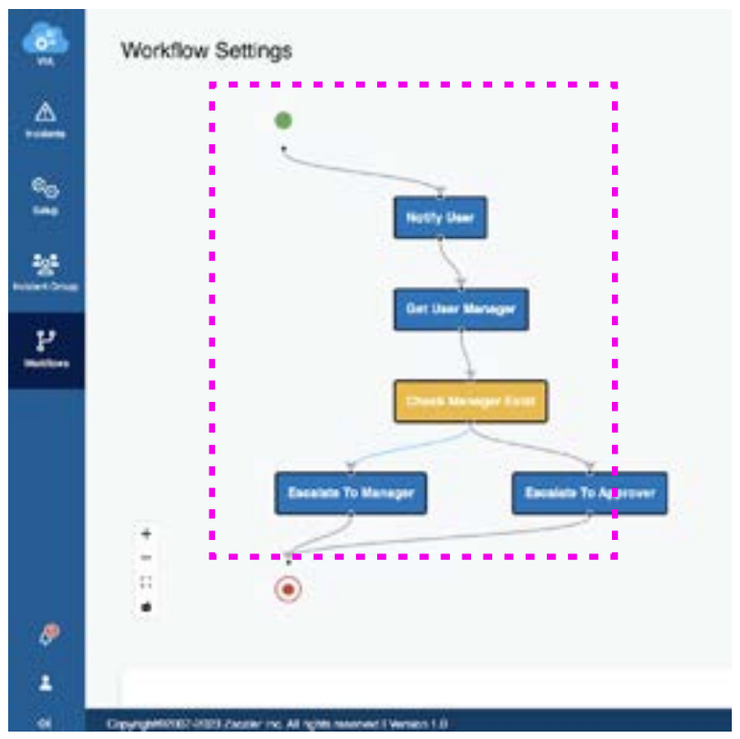
Justificar los incidentes a la vez que permite la capacitación de los usuarios



Gestione, asigne y escale incidentes fácilmente



Definir rutinas para flujos de trabajo



5. Integración de todos los elementos y uso de un enfoque por capas

Los gobiernos estatales y locales están adoptando la IA generativa (GenAI) para lograr nuevas eficiencias y mejorar los servicios, pero hacerlo de manera segura es fundamental. Con miles de herramientas de GenAI disponibles, junto con riesgos como la fuga de datos y el uso no autorizado, los organismos necesitan una estrategia clara que priorice la seguridad, integre los principios Zero Trust y, al mismo tiempo, permita la productividad. Un enfoque por capas simplifica este proceso al agrupar las aplicaciones según el riesgo, aplicar controles de seguridad personalizados y automatizar la gestión de incidentes para reducir la presión sobre los equipos de TI. Esta estrategia ayuda a los organismos a proteger los datos confidenciales, agilizar las operaciones y capacitar a los usuarios para que aprovechen de manera segura las aplicaciones de GenAI, todo ello dentro de un marco escalable y manejable.

Implemente controles en capas

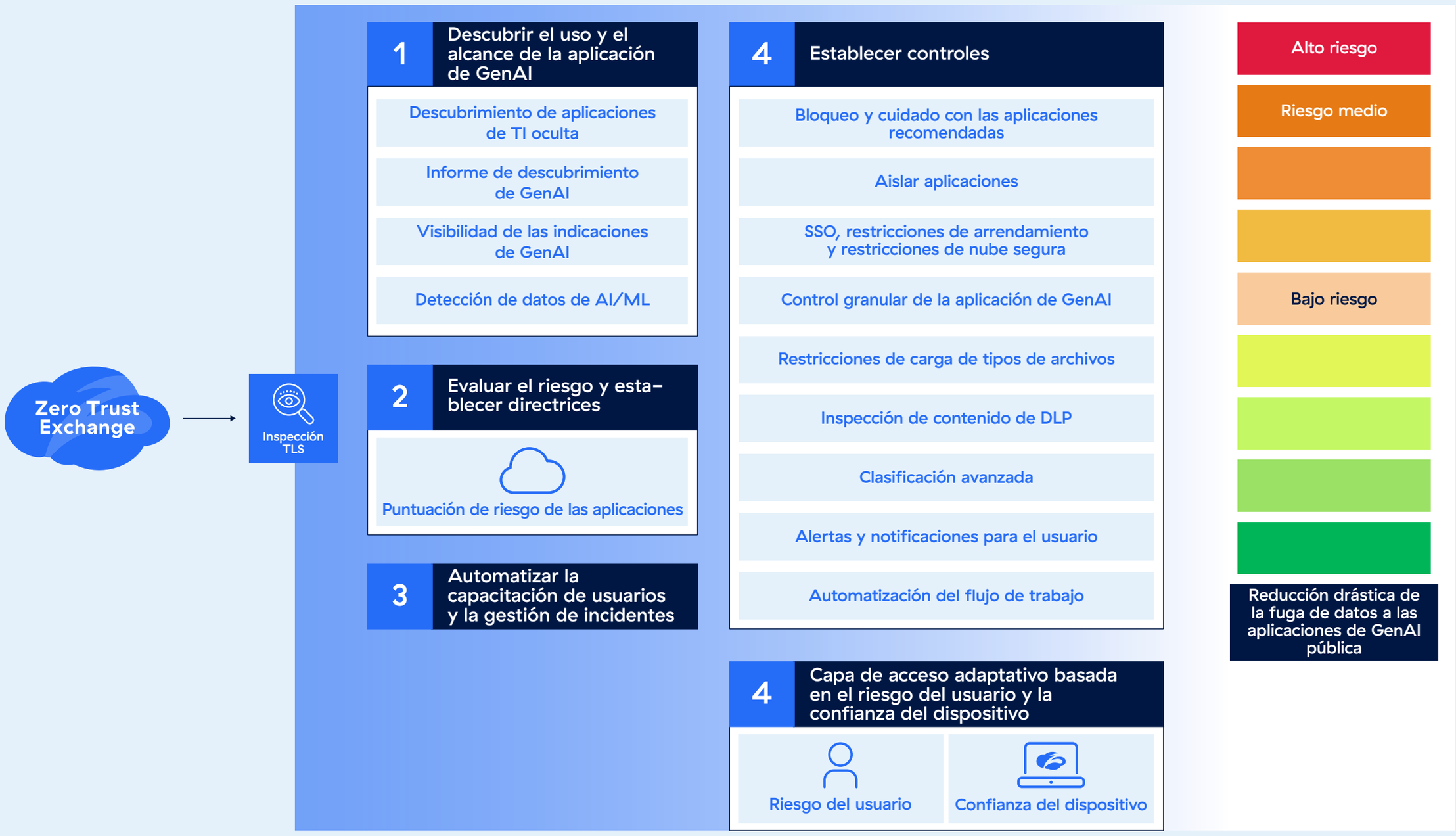
En esta sección, exploraremos cómo los organismos pueden integrar los diversos elementos de la adopción segura de GenAI utilizando un enfoque por capas. Con miles de herramientas de GenAI ya disponibles y otras nuevas que aparecen cada semana, la gestión de políticas e incidentes sin una estrategia bien pensada puede resultar rápidamente abrumadora.

Un enfoque por capas simplifica este proceso al organizar el acceso e implementar controles de datos adaptados a los niveles de riesgo. Este método no solo reduce la carga de trabajo de los administradores de seguridad, sino que también minimiza significativamente los riesgos de fuga de datos y reduce el número de incidentes que deben abordar los equipos de TI y seguridad. Al adoptar este enfoque estructurado, las organizaciones pueden aprovechar de manera segura y eficaz el poder de la GenAI al tiempo que mantienen la eficiencia operativa.

Como se mencionó anteriormente, las herramientas como el descubrimiento de aplicaciones de TI oculta, los informes de descubrimiento de GenAI y la visibilidad de las indicaciones de GenAI proporcionan conocimientos valiosos sobre cómo deberían evolucionar las políticas de IA y cómo se pueden personalizar los controles de seguridad para satisfacer las necesidades cambiantes. Estos conocimientos constituyen la base de un enfoque práctico y por capas para la gestión de aplicaciones de GenAI.

Una manera útil de implementar este enfoque es categorizar las aplicaciones de GenAI en tres grupos: alto riesgo, riesgo medio y bajo riesgo. Las aplicaciones de alto riesgo deben bloquearse por completo para evitar la exposición a vulnerabilidades innecesarias. Se puede acceder a las aplicaciones de riesgo medio con controles de seguridad reforzados, como el aislamiento del navegador y medidas de protección de datos más estrictas. Se puede permitir el acceso nativo a las aplicaciones de bajo riesgo, pero con restricciones centradas en el contenido o las acciones específicas que los usuarios pueden realizar.

Enfoque por capas para la protección de aplicaciones de IA



Esta estructura permite a los organismos adoptar un enfoque Zero Trust para la GenAI. Según este modelo, se bloquean de manera predeterminada las aplicaciones desconocidas, recién lanzadas o no aprobadas. Las aplicaciones aprobadas pero no autorizadas se aíslan con capas de seguridad adicionales, mientras que las aplicaciones totalmente autorizadas se benefician de una experiencia de usuario más fluida con protecciones personalizadas. Para facilitar su implementación y gestión, los organismos pueden utilizar herramientas como etiquetas de aplicación personalizadas y perfiles de riesgo. Estas herramientas permiten a los equipos de seguridad definir políticas predefinidas que se aplican automáticamente a las aplicaciones en función del riesgo asignado. Con tan solo etiquetar una aplicación, se aplican las políticas adecuadas, lo que reduce el esfuerzo administrativo al mínimo al tiempo que se mantiene un control sólido.

Automatización de los flujos de trabajo de incidentes

Otra capa fundamental a considerar es la gestión de incidentes. Es imprescindible que los organismos reduzcan el número de incidentes que el centro de operaciones de seguridad (SOC) o los administradores de datos deben gestionar manualmente. Por ejemplo, las violaciones de gravedad media y baja deben registrarse a los fines de auditoría y cerrarse automáticamente sin necesidad de una intervención manual significativa. Sin embargo, dado que aún representan violaciones de políticas, se debe notificar a los usuarios y solicitarles una justificación; un paso que resulta esencial para reforzar la capacitación de los usuarios y fomentar la rendición de cuentas.

Con Zscaler, las políticas de inspección de contenido para GenAI permiten a los organismos definir el nivel de gravedad de las violaciones, que luego se transmiten a las herramientas de automatización de flujos de trabajo. Esta función permite a los administradores diseñar flujos de trabajo adaptados a la gravedad de cada incidente. Se pueden utilizar atributos adicionales como la gravedad y otras características compartidas para categorizar los incidentes en grupos, y estos grupos se pueden asociar a flujos de trabajo automatizados. Este enfoque simplifica la manera en que se procesan los incidentes, garantizando el abordaje adecuado de las violaciones y aliviando significativamente la carga de los equipos SOC.

Reflexiones finales

Para transformar sus operaciones, empoderar a sus empleados y servir mejor a los ciudadanos, los organismos gubernamentales deben liderar en la implementación de la inteligencia artificial generativa (GenAI). Sin embargo, su adopción debe estar respaldada por una arquitectura Zero Trust. Al garantizar que cada usuario, dispositivo e interacción sea verificado, supervisado y controlado, indistintamente de la ubicación o la aplicación, los organismos pueden asegurar con confianza las iniciativas de GenAI con una sólida protección de datos, una gobernanza clara y experiencias de usuario optimizadas en el centro de su estrategia.

Zscaler permite a los organismos gubernamentales aprovechar los beneficios de productividad de la GenAI con un enfoque seguro y por capas que simplifica la gobernanza, agiliza la implementación e incorpora una seguridad sólida en cada interacción. Los organismos pueden reducir drásticamente los riesgos y escalar sus estrategias de adopción con una carga mínima para los equipos de TI y seguridad si establecen marcos de gobernanza de IA, automatizan el descubrimiento y la gestión de aplicaciones de GenAI, controlan el uso de instancias de aplicaciones de GenAI e implementan capacidades de DLP avanzadas desde el principio.

Dado que el panorama de la GenIA continúa evolucionando, se anima a los líderes de los organismos a adoptar un enfoque estratégico y gradual para su adopción. Comience por proteger el acceso a las aplicaciones de GenAI pública, desbloquee de manera segura una mayor productividad con la IA agéntica (documento futuro). Por último, exploraremos cómo extender de manera segura las capacidades de GenAI a los servicios centrados en el ciudadano, garantizando la protección de los sistemas en cada paso. Con Zscaler, los organismos pueden implementar estas fases con confianza, acelerando la innovación y manteniendo los más altos estándares de seguridad de datos y cumplimiento normativo.

Comuníquese con su equipo de cuenta o contáctenos para programar un taller específico para su organización.

Acerca de Zscaler
Zscaler (NASDAQ: ZS) acelera la transformación digital para que los clientes puedan ser más ágiles, eficientes, resistentes y seguros. Zscaler Zero Trust Exchange protege a miles de clientes de ciberataques y pérdida de datos al conectar de manera segura usuarios, dispositivos y aplicaciones en cualquier ubicación. Distribuido en más de 150 centros de datos en todo el mundo, Zero Trust Exchange basado en SSE es la plataforma de seguridad en la nube en línea más grande del mundo. Obtenga más información en **zscaler.com/mx** o síganos en Twitter **@zscaler**.

+1 408.533.0288 Zscaler, Inc. (Oficinas centrales) • 120 Holger Way • San José, CA 95134 zscaler.com/mx

zscaler™

Zero Trust Everywhere