Adopción segura de GenAI con Zero Trust:

Uso seguro de aplicaciones de GenAI pública

DOCUMENTO TÉCNICO

Índice

Introducción 3

Uso seguro de GenAI pública 4

Descripción general 4

1. Establecer marcos y políticas de gobernanza de la IA 5

Comprensión del uso actual de la IA 6

Información detallada sobre las interacciones de los usuarios con las aplicaciones GenAI 7

Visibilidad de datos desconocida 8

2. Integrar estrechamente la experiencia del usuario y la capacitación 9

Acceso sin problemas a GenAI 9

Capacitación y retroalimentación integradas para usuarios 11

3. Priorizar la seguridad y elegir la arquitectura adecuada 12

Automatizar la detección y la gestión de aplicaciones de GenAI 13

Permitir aplicaciones sancionadas a través del control de seguridad de aplicaciones SaaS 14

Restringir el acceso a instancias empresariales de aplicaciones GenAI 14

Reducir el riesgo de aplicaciones de GenAI no autorizadas 16

4. Implementar la protección de datos desde el principio 17

Acelerar la adopción de DLP 17

Simplifique la gobernanza de DLP 19

5. Unir todo y utilizar un enfoque en capas 20

Implementar controles en capas 21

Automatización de flujos de trabajo de incidentes 22

Reflexiones finales 23

Introducción

La IA generativa (GenAI) está transformando el modo en que operan los gobiernos, permitiéndoles mejorar la productividad, agilizar los procesos y brindar un mejor servicio a sus ciudadanos. Sin embargo, para aprovechar el potencial transformador de GenAI y al mismo tiempo mitigar sus riesgos inherentes, las agencias deben aplicar los principios Zero Trust. Este paradigma garantiza que ninguna entidad (humana o máquina) sea confiada por defecto, asegurando una visibilidad continua y una verificación rigurosa en 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 las agencias gubernamentales a navegar de forma segura en el panorama de GenAI. La serie incluye tres fases:

- La fase 1, descrita en este documento, se centra en asegurar las aplicaciones públicas de GenAI para abordar riesgos como la filtración de datos y el uso no autorizado o no aprobado de IA (“IA en la sombra”).

- La fase 2 explorará la adopción de herramientas de inteligencia artificial de Agentic para impulsar la productividad de los empleados de forma segura.

- La fase 3 se centrará en la implementación segura de sistemas GenAI para servicios ciudadanos, garantizando que los sistemas y datos gubernamentales permanezcan protegidos.

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

Uso seguro de GenAI pública

Resumen

Los gobiernos son cada vez más conscientes del potencial transformador de la IA generativa (GenAI) para sus operaciones y los servicios que brindan a los ciudadanos. Esta tecnología ofrece un camino hacia importantes ganancias de productividad y la evolución de los servicios ciudadanos a través de diversas aplicaciones. Estos van desde comprender el sentimiento público y proporcionar chatbots impulsados por IA para brindar soporte ciudadano y de TI hasta facilitar la traducción de idiomas y automatizar procesos internos como la redacción de descripciones de puestos, el resumen de reuniones y la creación de anuncios públicos.

Los primeros en adoptar esta tecnología dentro del gobierno ya están presenciando mejoras en la experiencia y la satisfacción de los empleados. La aparición de modelos de lenguaje grande (LLM) de acceso público, como ChatGPT, ha estimulado 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 mediante la integración de estas herramientas de IA avanzadas.

Sin embargo, la integración de GenAI, particularmente a través de LLM públicos y modelos de terceros, introduce desafíos de seguridad considerables. El uso no autorizado de herramientas de IA ("IA en la sombra") puede exponer datos confidenciales de ciudadanos, registros comerciales o propiedad intelectual. El riesgo se amplifica aún más en los flujos de trabajo que implican Retrieval Augmented Generation (RAG), Model Content Protocol (MCP) y agentes de IA, ya que pueden comprometer datos sensibles y suponer riesgos para la seguridad nacional al ofrecer oportunidades a actores patrocinados por el Estado o a entidades maliciosas para explotar estas vulnerabilidades con fines de espionaje, sabotaje o interrupción de infraestructuras críticas. Además, GenAI presenta una amplia superficie de ataque que las medidas de seguridad tradicionales, que a menudo se basan en controles binarios restrictivos o carecen de visibilidad integral en diferentes entornos, no están bien equipadas para gestionar de manera efectiva.

Para aprovechar el potencial de GenAI, las agencias deben adoptar un enfoque Zero Trust con seguridad sólida, visibilidad y simplicidad para el usuario. Los siguientes pasos describen un proceso que las agencias pueden adoptar para aprovechar la GenAI, al tiempo que mitigan de manera proactiva los riesgos de fuga de datos y evitan una carga indebida para los equipos de seguridad:

1. Establecer marcos y políticas de gobernanza de la IA
2. Integrar estrechamente la experiencia del usuario y la capacitación
3. Elija la arquitectura adecuada y priorice la seguridad
4. Implementar la protección de datos desde el principio
5. Utilice un enfoque en capas para la protección

Analicemos estos pasos con más detalle.

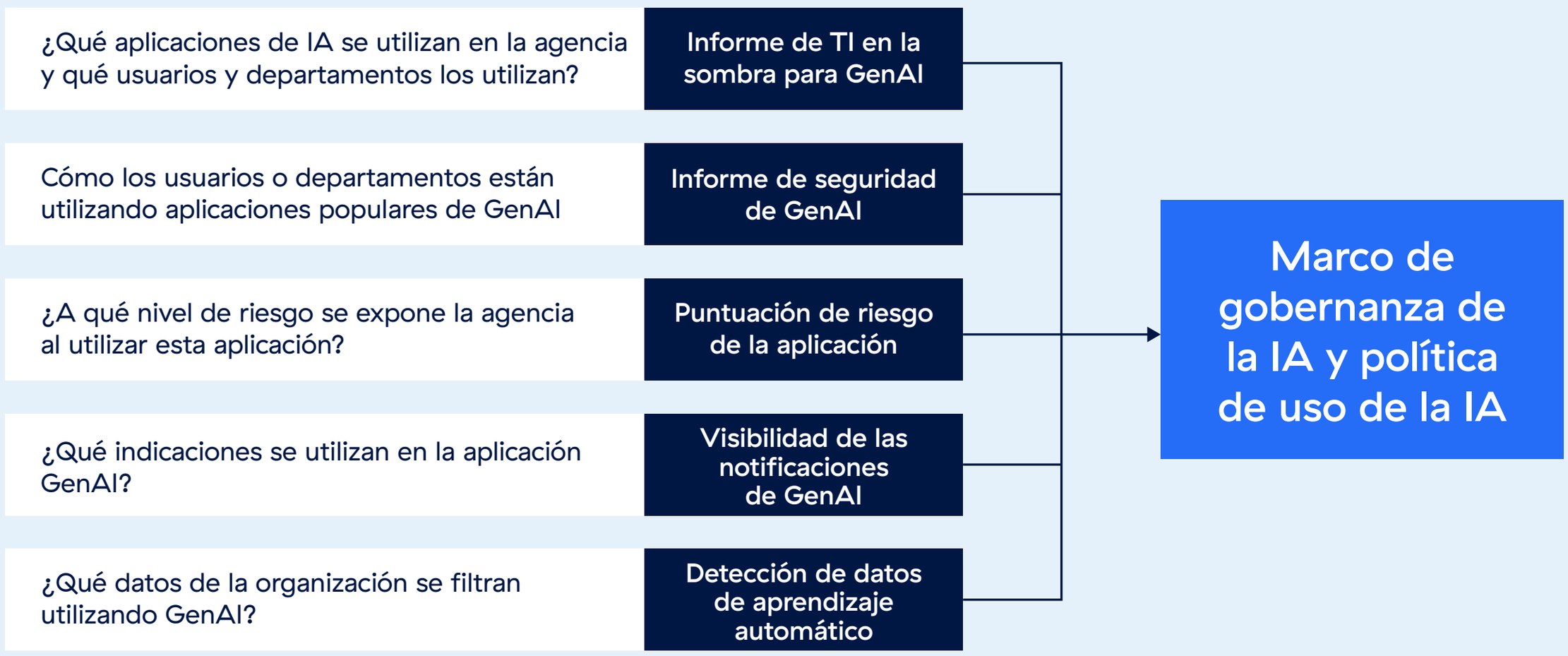
1. Establecer marcos y políticas de gobernanza de la IA

Para aprovechar al máximo los beneficios de GenAI, las agencias deben implementar medidas de seguridad sólidas que aborden directamente los riesgos sin obstaculizar la productividad del usuario. Esta sección explora cómo las agencias pueden adoptar un enfoque Zero Trust para las aplicaciones GenAI y al mismo tiempo garantizar que los controles de seguridad no impidan una experiencia de usuario fluida.

El desarrollo de marcos y políticas de gobernanza de la IA es esencial para garantizar la adopción de GenAI en las agencias estatales. Esto a menudo implica la creación de un grupo de trabajo o un órgano de gobernanza dedicado a supervisar el desarrollo y la implementación de políticas. Por ejemplo, el Grupo de Trabajo GenAI de Alabama sirve como modelo con su enfoque de equipo colaborativo y multifuncional. Las agencias también deberían aprovechar los marcos Zero Trust establecidos, como el modelo de madurez de Zero Trust de CISA y NIST 800-207, junto con marcos de seguridad específicos de IA como el Marco de Gestión de Riesgos de IA del NIST (AI RMF), que enfatiza funciones centrales como gobernanza, asignación, medición y gestión, o TRISM de Gartner, para guiar sus esfuerzos. Al adoptar un grupo de trabajo específico y utilizar estos marcos probados, las agencias pueden acelerar la integración segura de las tecnologías GenAI en todos los departamentos.

Para respaldar este proceso, Zscaler proporciona información que ayuda a las agencias a rastrear el uso de IA en sus entornos, evaluar los riesgos potenciales vinculados a las aplicaciones GenAI e identificar instancias de fuga de datos. El aprovechamiento de los informes de Zscaler permite a las agencias acceder a datos críticos sobre cómo se utilizan actualmente las herramientas GenAI.

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



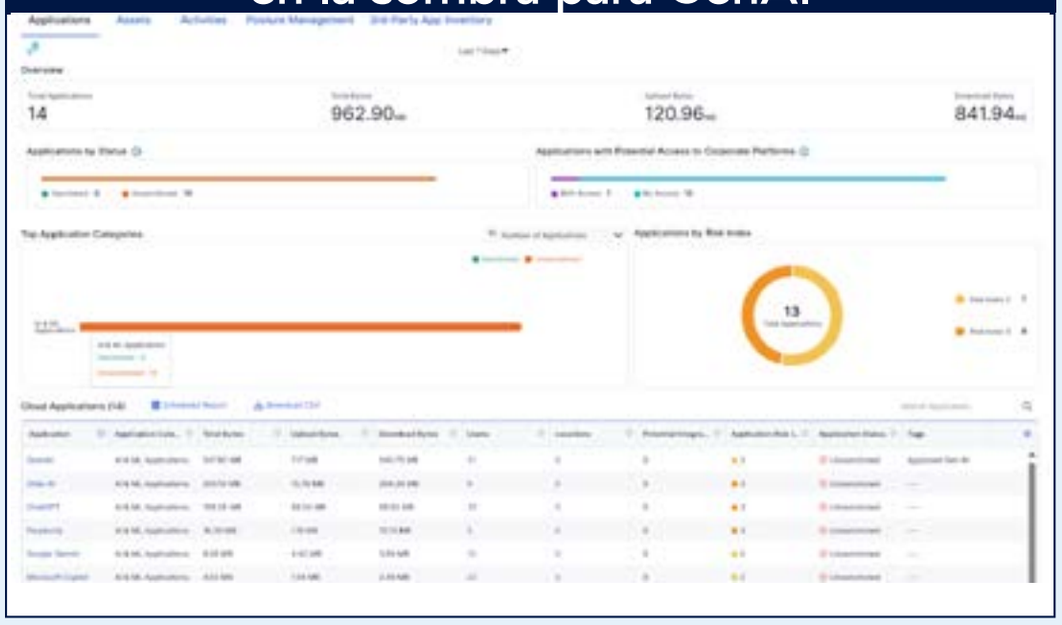
Comprender el uso actual de la IA

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, las agencias pueden identificar dónde son más necesarias las políticas. Este enfoque basado en datos garantiza que el marco siga siendo relevante, procesable y adaptado para abordar eficazmente los desafíos y oportunidades únicos de la agencia.

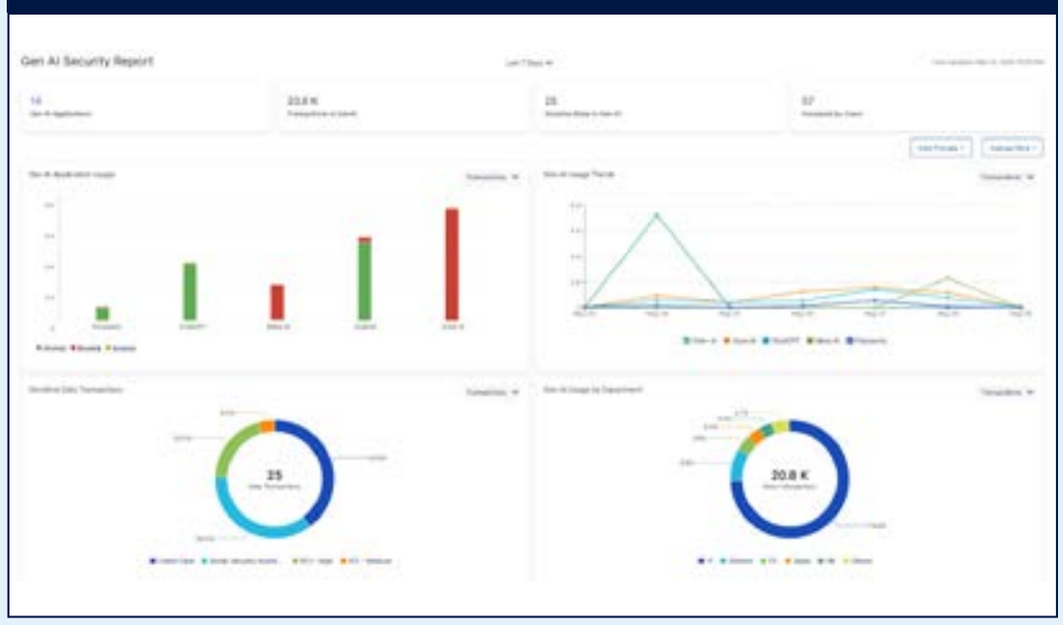
Zscaler proporciona informes detallados sobre el uso de IA que ofrecen transparencia sobre qué aplicaciones GenAI se utilizan en las agencias y el alcance de su uso. Estos conocimientos se pueden segmentar aún más para mostrar patrones de uso dentro de departamentos o subagencias específicas, lo que brinda a las organizaciones una visión más clara de su panorama de uso de IA.

Perspectivas sobre el uso de la IA en la sombra

Detección de aplicaciones de TI en la sombra para GenAI

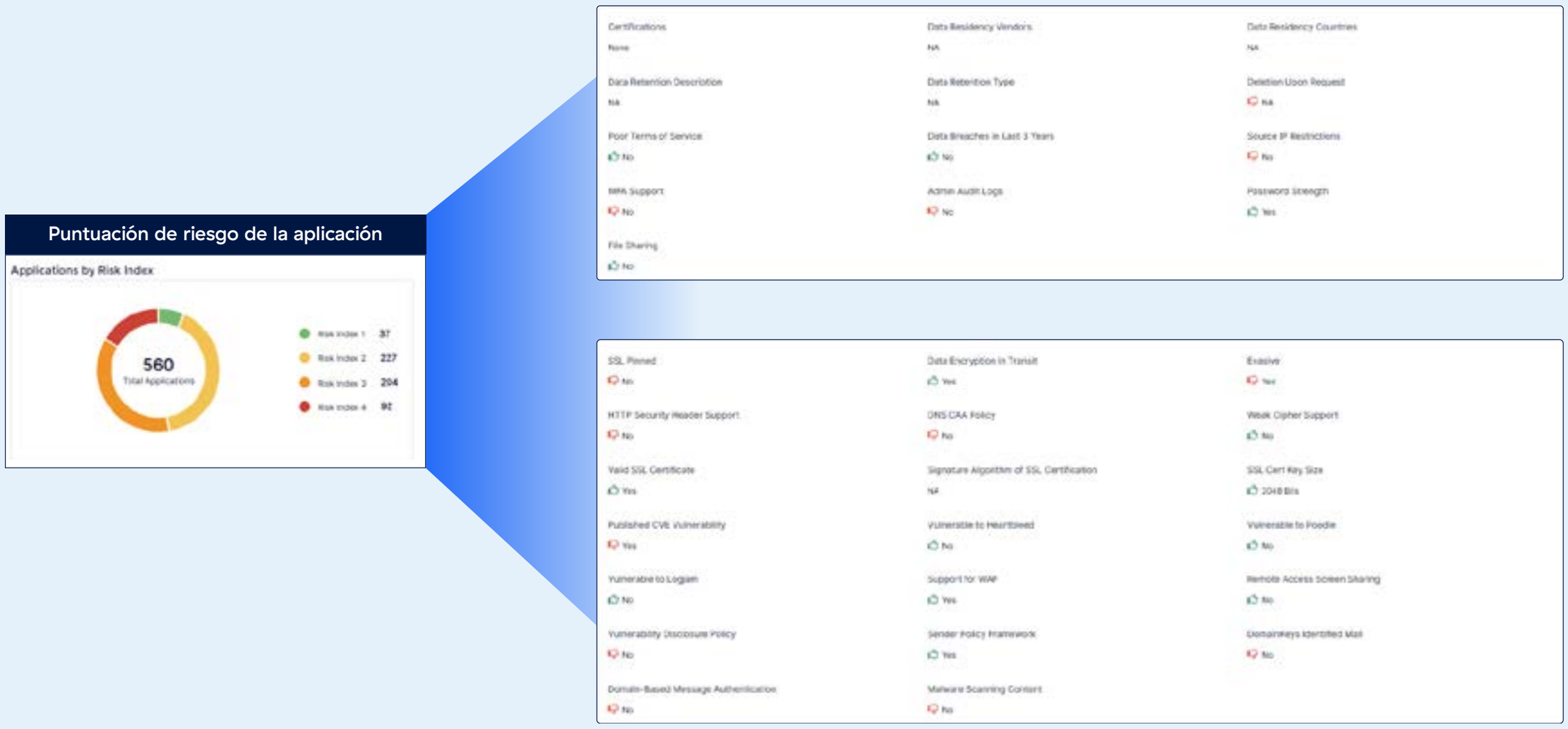


Informe de seguridad de GenAI



Con esta visibilidad, las agencias obtienen la capacidad de profundizar en los factores de riesgo asociados a estas aplicaciones. El equipo ThreatLabz de Zscaler, en coordinación con información de amenazas de terceros, evalúa estos riesgos y les asigna puntuaciones agregadas que van del 1 al 5, simplificando el consumo de riesgos para los tomadores de decisiones. Las agencias también tienen la flexibilidad de personalizar 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 concentrar los recursos en las áreas más relevantes para su misión y sus necesidades de seguridad. En el siguiente informe se muestran algunos ejemplos de factores de riesgo, como las vulnerabilidades de seguridad o el incumplimiento normativo, que permiten a los responsables de políticas de la agencia priorizar las áreas más importantes para dicha entidad.

Riesgo asociado con el uso de IA en la sombra

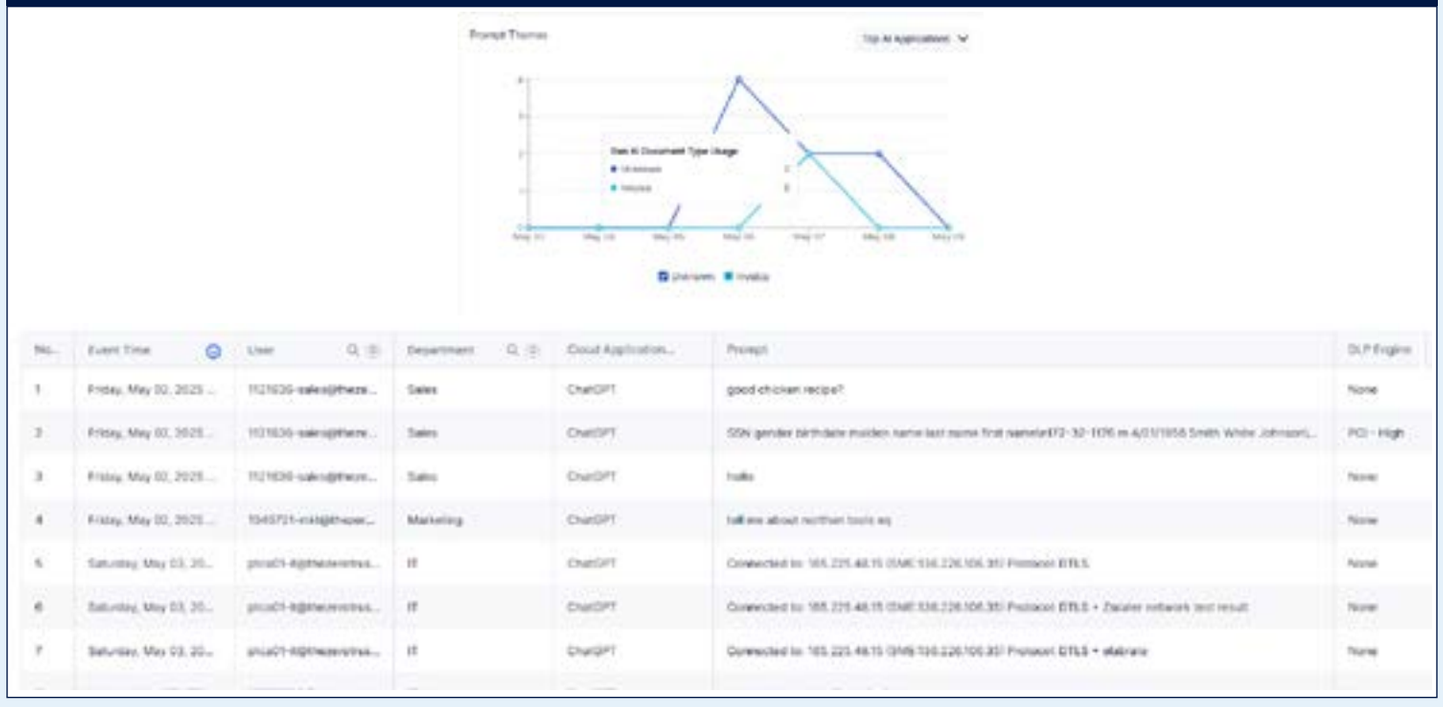


Información detallada sobre las interacciones de los usuarios con las aplicaciones GenAI

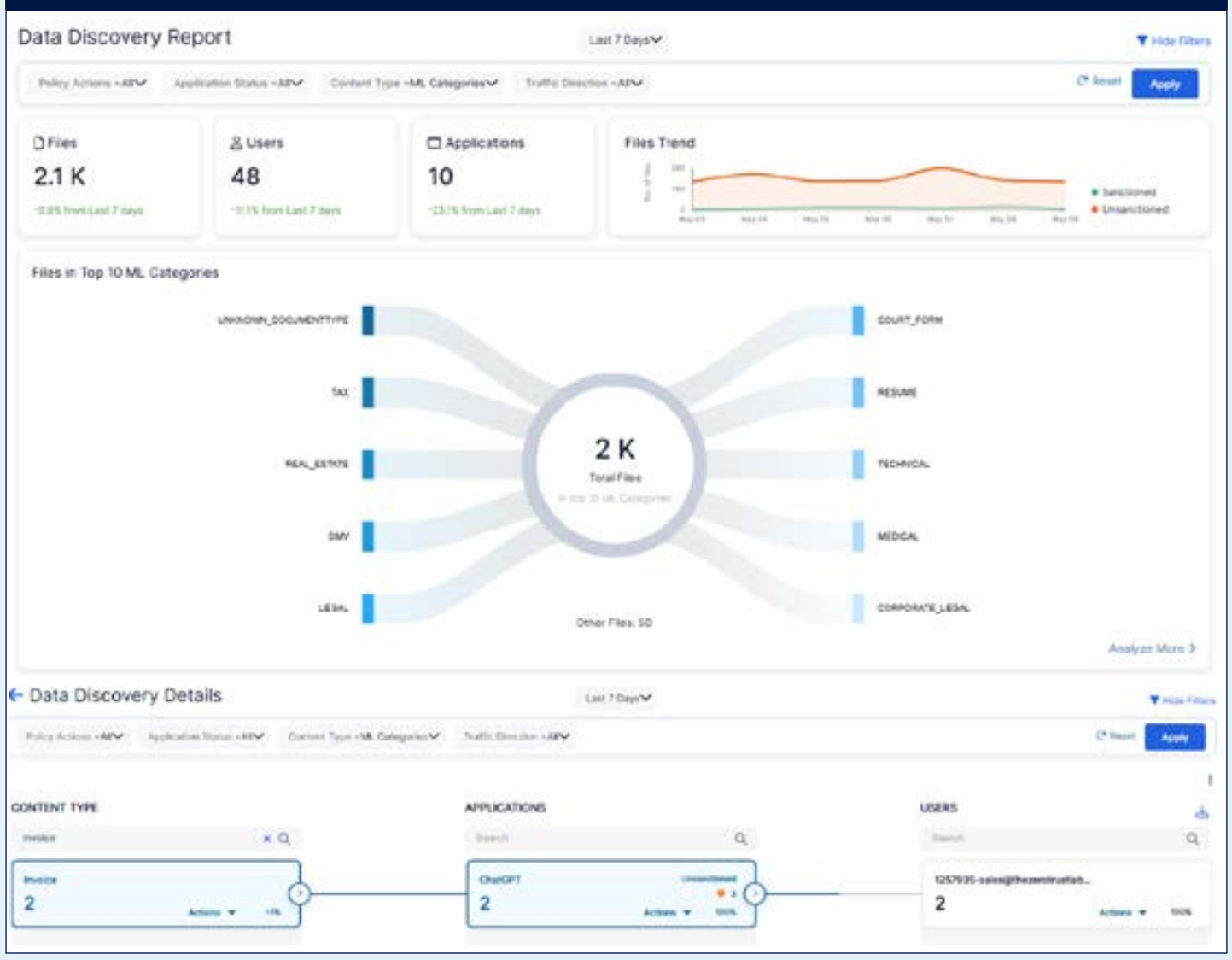
Zscaler va más allá de la visibilidad a nivel de aplicación al proporcionar información granular sobre cada transacción, solicitud e interacción del usuario dentro de las aplicaciones GenAI. Esto incluye datos detallados sobre lo que los usuarios ingresan no sólo a través de transferencias de archivos, sino también mediante métodos como entradas de teclado, actividades del portapapeles y otras entradas compatibles. Estos conocimientos son invaluables para las agencias, ya que les ayudan a comprender mejor el tipo de datos que se comparten, perfeccionar las políticas de seguridad y garantizar el cumplimiento de los estándares de gobernanza. Además, este nivel de visibilidad es esencial para fines de auditoría y puede exportarse sin problemas al SIEM de la agencia para un seguimiento y análisis exhaustivos.

Informe sobre la fuga de datos actual fuera de la Agencia

Visibilidad de las solicitudes de GenAI



Detección de datos de aprendizaje automático



Visibilidad de datos desconocida

Zscaler mejora aún más la visibilidad al identificar datos que las agencias pueden no saber que se filtran a través de las aplicaciones GenAI. Mediante capacidades impulsadas por IA y aprendizaje automático, el informe ML Discovery de Zscaler va más allá de las reglas tradicionales de DLP de “solo supervisión” para detectar y clasificar de forma proactiva los datos sensibles que se comparten con herramientas públicas de GenAI. Esto permite a los propietarios de datos y administradores de seguridad identificar fugas de datos desconocidas o no reconocidas y abordarlas antes de que se conviertan en problemas críticos.

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

Al combinar información sobre usuarios, aplicaciones, riesgos de aplicaciones, indicaciones y patrones de datos, Zscaler respalda la creación de políticas y procedimientos específicos que se alinean 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 de Zero Trust, lo que permite a las agencias adoptar un enfoque con visión de futuro que equilibra la innovación con la definición de una estrategia integral de mitigación de riesgos.

2. Integrar estrechamente la experiencia del usuario y la capacitación

La experiencia y la capacitación del usuario juegan un papel central en la adopción segura y exitosa de la IA generativa (GenAI) dentro de las agencias estatales. Para garantizar una adopción sin problemas, es esencial que las medidas de seguridad y la capacitación de los usuarios estén diseñadas de manera que les permitan seguir siendo productivos y, al mismo tiempo, ofrecer protecciones sólidas. Siempre que sea posible, se debe evitar introducir otra herramienta o aplicación, especialmente aquellas que puedan introducir nuevas herramientas generales que los usuarios deberán aprender. Además, los controles de seguridad efectivos deben ir acompañados de una educación continua de los usuarios para maximizar su impacto. Las plataformas deben integrarse perfectamente con los flujos de trabajo y canales existentes, incorporando al mismo tiempo mecanismos de interacción y retroalimentación del usuario. Esto ayudará a las agencias a alinearse con marcos como el Marco de Gestión de Riesgos de IA del NIST (AI RMF) desde el principio.

A continuación se presentan algunas capacidades clave de la plataforma que respaldan este enfoque:

Acceso sin problemas a GenAI

El objetivo principal de las herramientas GenAI es liberar a los usuarios de tareas repetitivas y permitirles concentrarse en el trabajo que se beneficia del juicio humano. Las medidas de seguridad de GenAI no deben interrumpir los flujos de trabajo de los usuarios. Zscaler facilita esto al eliminar la necesidad de software adicional o navegadores administrados. 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 IA generativa, ofreciendo un acceso fluido sin necesidad de introducir herramientas adicionales.

- **Acceso seguro sin agente**
  Los usuarios pueden utilizar su navegador nativo y su flujo de trabajo existente (por ejemplo, mediante el portal de aplicaciones del IdP) para acceder a las aplicaciones seguras de GenAI sin necesidad de un agente.

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

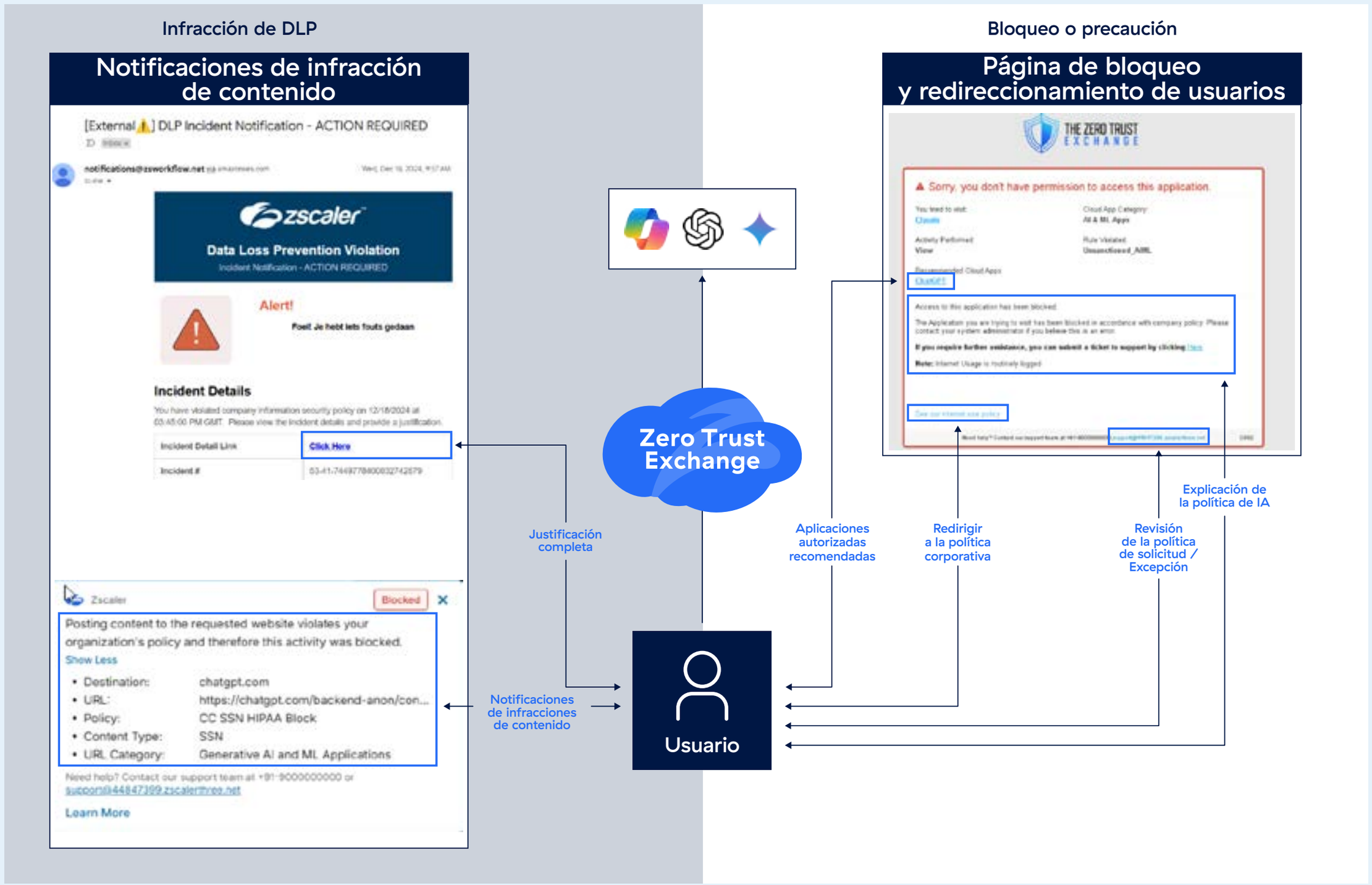
Estos controles se pueden implementar con un impacto mínimo en la infraestructura o los puntos finales existentes, lo que permite a las agencias implementar políticas de seguridad al mismo tiempo que preservan una experiencia de usuario perfecta y mantienen el esfuerzo administrativo al mínimo.

Capacitación y retroalimentación de usuarios integrada

La educación continua sobre el uso seguro de GenAI y sus infracciones 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 nativas del usuario. Zscaler admite esto a través de notificaciones dinámicas: cuando un recurso está bloqueado, aislado o marcado por infracciones de contenido, los usuarios reciben alertas personalizadas. Por ejemplo, si se bloquea una aplicación GenAI no autorizada, Zscaler sugiere equivalentes aprobados, lo que ayuda a redirigir el comportamiento de los usuarios y mantener la productividad. En escenarios de infracción del uso de datos, Zscaler se integra con herramientas familiares como el correo electrónico y Slack, lo que facilita que los usuarios proporcionen justificaciones o reciban comentarios personalizados en las herramientas que ya usan.

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

Capacitación y retroalimentación de usuarios con Zscaler



3. Priorizar la seguridad y elegir la arquitectura adecuada

A medida que la superficie de ataque se expande con la creciente adopción de herramientas de IA, es crucial que las organizaciones elijan una plataforma que no solo proteja contra las amenazas impulsadas por IA, sino que también permita el uso seguro de las aplicaciones GenAI, construidas sobre una arquitectura Zero Trust y con autorización FedRAMP. Zscaler ofrece una solución integral que combina seguridad, usabilidad y cumplimiento para las agencias que adoptan GenAI.

Las agencias pueden comenzar a aprovechar las capacidades seguras de GenAI de Zscaler con cambios mínimos en su infraestructura existente. El tráfico se puede reenviar 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 una implementación sin agente. Una vez conectado, Zscaler garantiza que los usuarios estén autenticados y autorizados antes de acceder a cualquier recurso en Internet, incluidas las aplicaciones GenAI. Al actuar como proxy, Zscaler inspecciona todas las sesiones TLS establecidas con aplicaciones GenAI, lo que proporciona a las agencias visibilidad total y control granular sobre cómo los usuarios interactúan con estas herramientas. Esta arquitectura permite a las agencias brindar información profunda sobre cómo los usuarios utilizan las aplicaciones GenAI y proporciona múltiples controles líderes en la industria para proteger los datos de las agencias.

Inspección de HTTPS y WebSockets seguros con Zscaler

Control de acceso

- Filtrado URL
- Cloud Firewall
- Controles granulares de aplicaciones en la nube
- Restricciones de tenencia
- Seguridad 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 GenAI
- Aislamiento del navegador en la nube

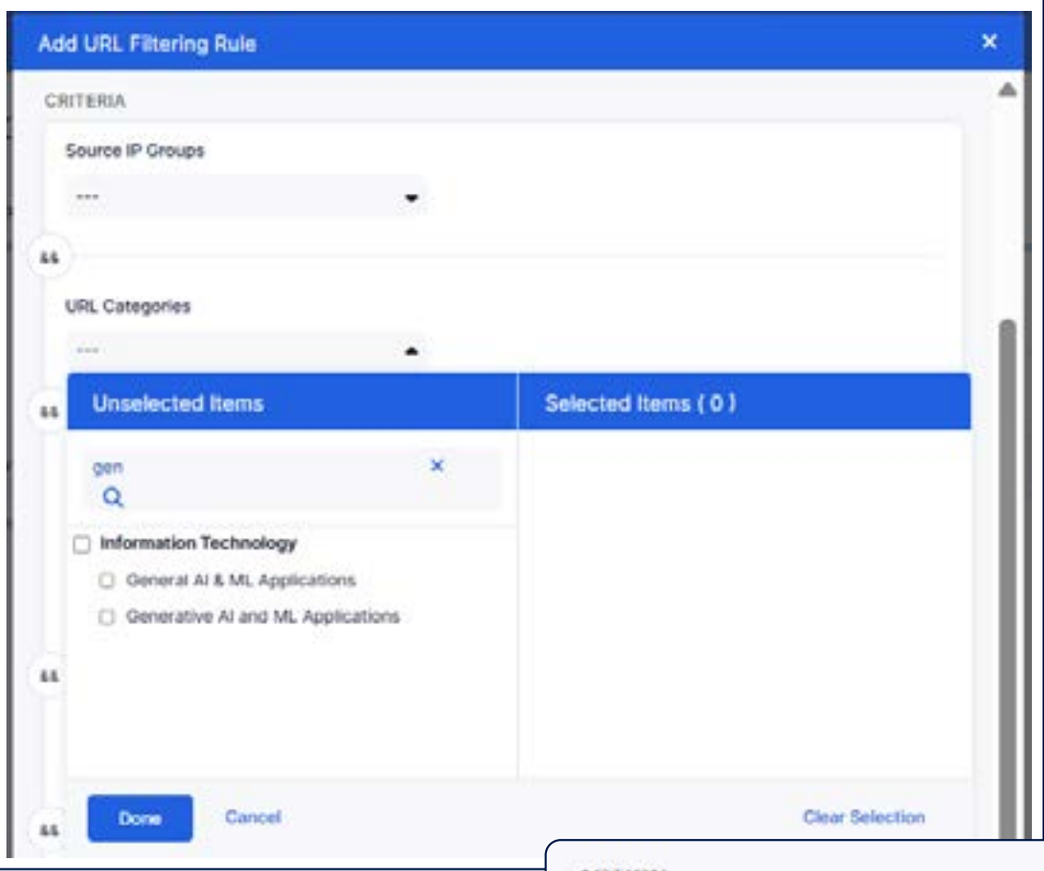
Automatizar el descubrimiento y la gestión de aplicaciones GenAI

Con la inspección TLS implementada, las agencias obtienen acceso al conjunto completo de capacidades de Zscaler, incluido el control granular sobre GenAI y aplicaciones de aprendizaje automático.
Una ventaja clave reside en la categoría Aplicaciones de IA y ML de Zscaler, supervisada por el equipo de ThreatLabz. Esta categoría abarca una amplia gama de aplicaciones de inteligencia artificial, incluidas herramientas populares como ChatGPT, Gemini, MetiAI, Claude, etc.

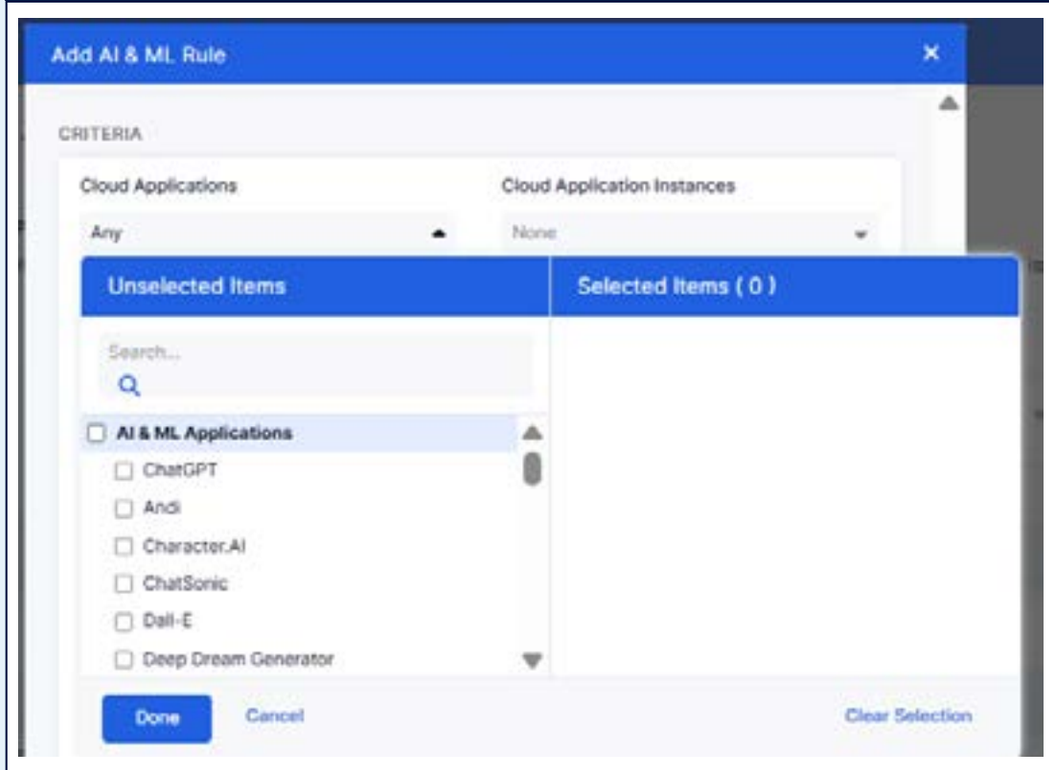
Al utilizar esta categoría, las agencias pueden aplicar políticas para bloquear aplicaciones GenAI desconocidas o no aprobadas de forma predeterminada, garantizando así que solo se pueda acceder a las herramientas aprobadas. A medida que surgen nuevas aplicaciones, se agregan automáticamente a estas categorías, lo que ahorra a las agencias el esfuerzo de descubrirlas manualmente y enviar actualizaciones. Además, las agencias tienen la flexibilidad de ampliar o adaptar esta lista agregando dominios personalizados para alinearla mejor con sus necesidades específicas. Zscaler también ofrece categorías específicas como “Aplicaciones generales de IA y aprendizaje automático” y “Aplicaciones de IA generativa y aprendizaje automático” que, al combinarse con la lista más amplia “Aplicaciones de IA en la nube”, proporcionan una cobertura significativa para reducir los riesgos de seguridad que presentan las aplicaciones de GenAI. Este enfoque en capas permite a las agencias gestionar eficazmente el acceso a cientos de aplicaciones que se desarrollan y lanzan cada semana.

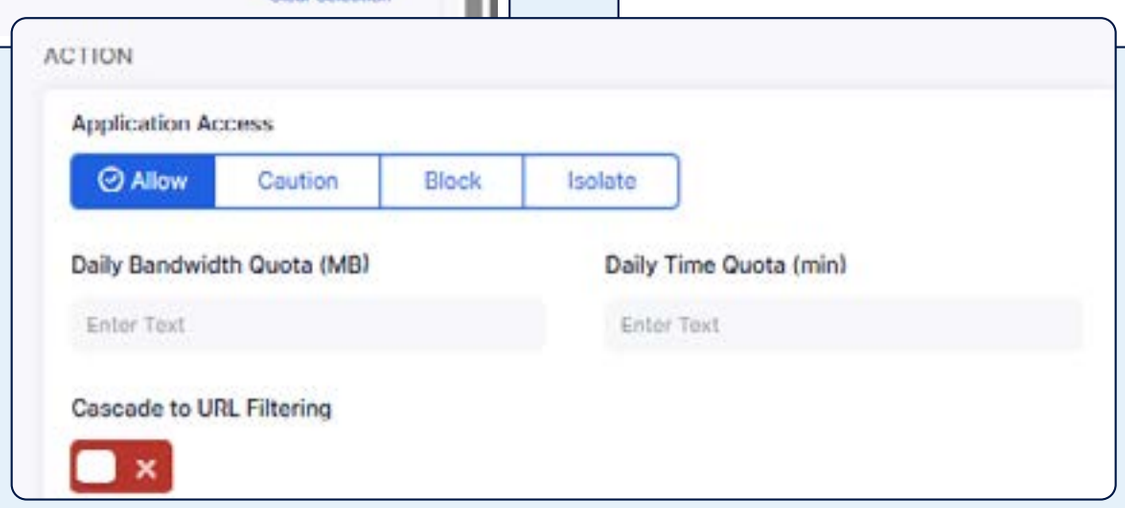
Selección de categorías amplias y aplicaciones de IA específicas

Categorías de URL para Wide Net



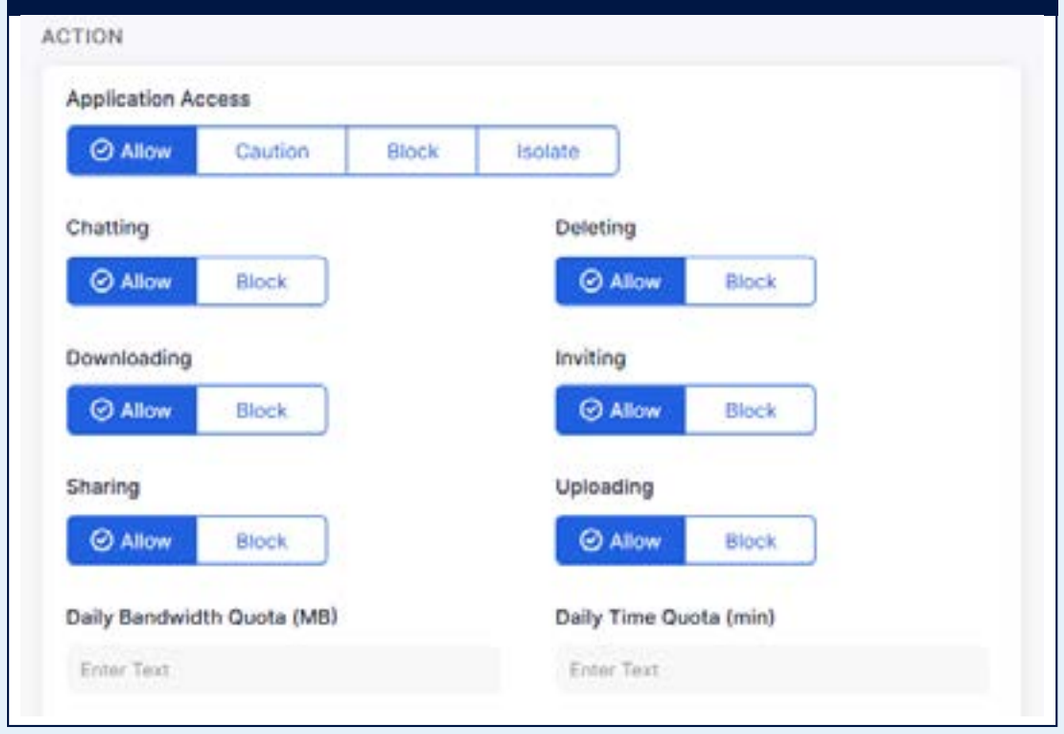
Aplicación GenAI para controles granulares



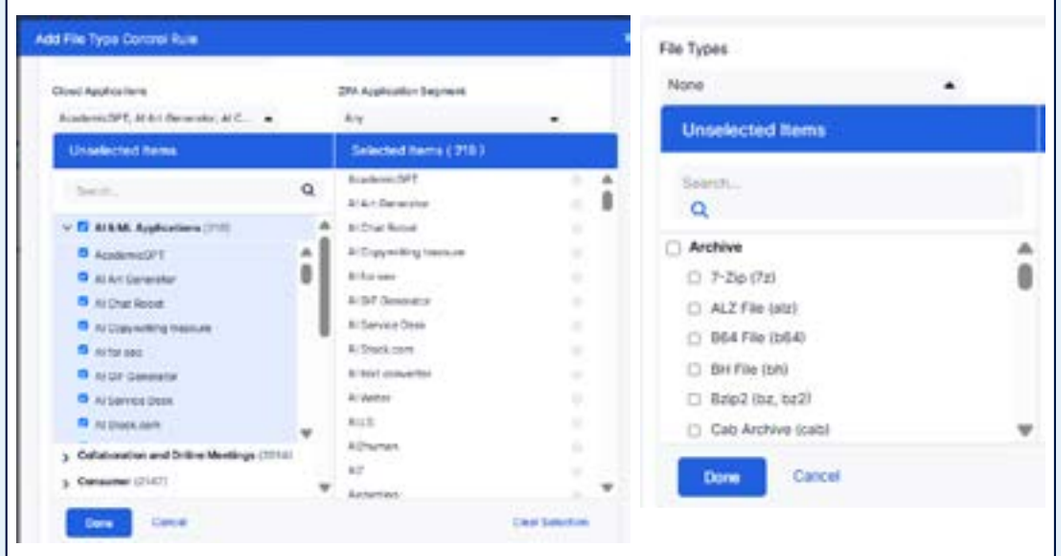


Controles granulares para aplicaciones SaaS, web y de inteligencia artificial

Controles granulares de la aplicación GenAI



Controles de carga de archivos de aplicaciones de GenAI



Permitir aplicaciones sancionadas a través del control de seguridad de aplicaciones SaaS

Además de mantener una lista completa de aplicaciones de IA, Zscaler proporciona controles granulares de cómo los usuarios interactuarán con las aplicaciones de genAI. Estos controles son increíblemente simples de aplicar, muy potentes y están consolidados dentro de una sola plataforma. El lado izquierdo de la imagen muestra algunos de los ejemplos de controles granulares que se pueden aplicar, en caso de que una política de seguridad de chatGPT pueda incluir controles granulares como permitir el chat, pero bloquear la carga de archivos o restringir el uso compartido de chats. Las agencias pueden aplicarlos a todo el departamento o incluso a cada nivel de usuario. Estos controles granulares se pueden refinar aún más restringiendo los tipos de archivos que los usuarios pueden cargar en las aplicaciones GenAI, como se muestra a la derecha. Este control de archivos también puede incluir la restricción de cargas de documentos cifrados.

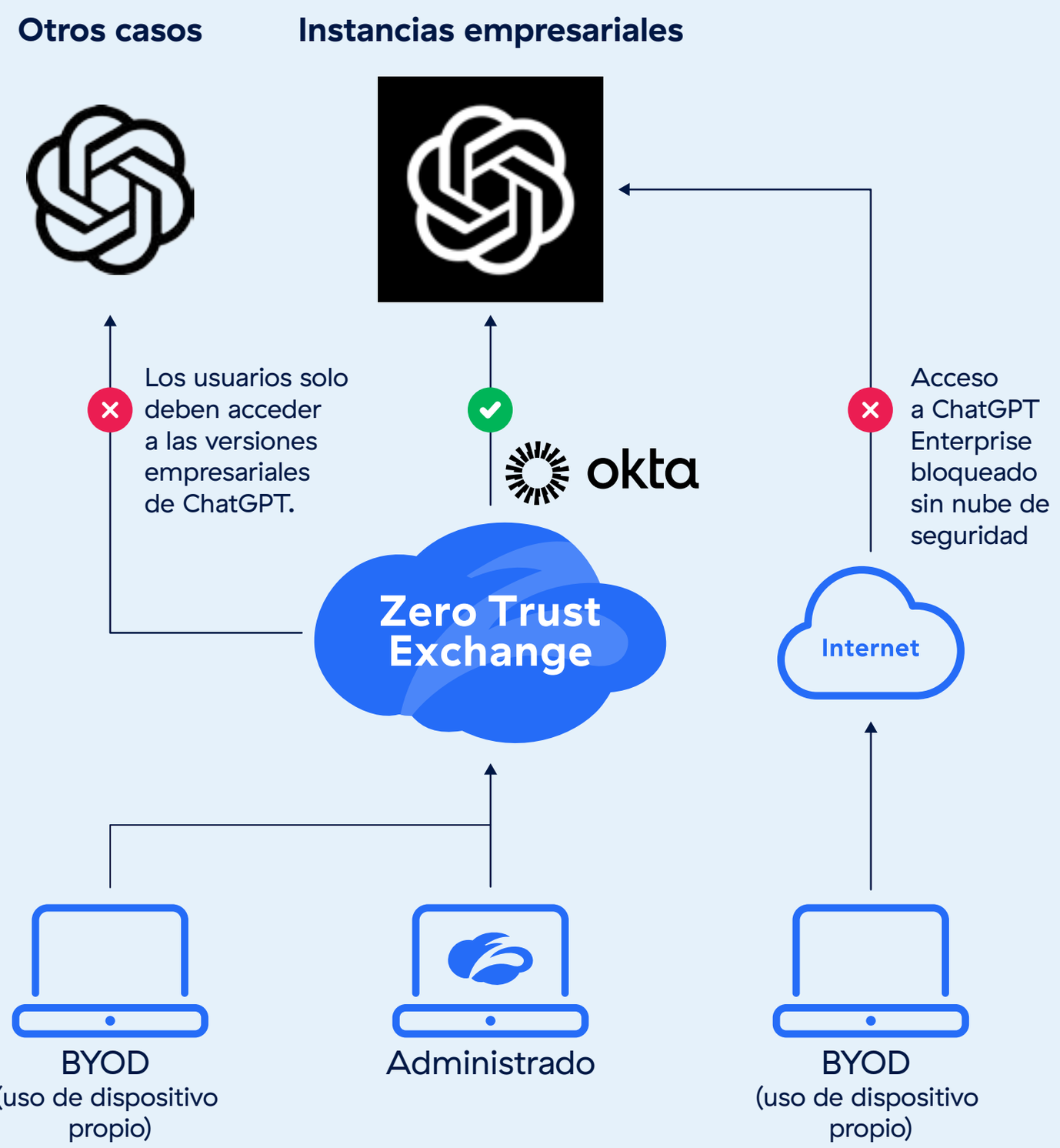
Restringir el acceso a instancias empresariales de aplicaciones de GenAI

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

Las instancias empresariales de las aplicaciones GenAI deben combinarse con SSO para maximizar la seguridad y brindar a las agencias mayor visibilidad y control sobre el uso de las aplicaciones. Con el SSO implementado, las agencias pueden aplicar políticas que bloqueen el acceso a versiones no empresariales de las aplicaciones GenAI. Por ejemplo, el control de arrendamiento de Zscaler para ChatGPT garantiza que solo se pueda acceder a los inquilinos aprobados, mientras que otros quedan restringidos automáticamente. Además, las agencias pueden implementar controles en la capa de Gestión de Identidad y Acceso (IAM) mediante listas blancas para garantizar que las versiones empresariales sean la única instancia de uso de GenAI y para garantizar que el acceso se produzca en entornos seguros como la plataforma en la nube de Zscaler. Para ampliar aún más el acceso seguro, las instancias GenAI empresariales 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” es insuficiente en el panorama GenAI actual. Las agencias deben adoptar una estrategia de seguridad en 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 la adhesión a los principios básicos de Zero Trust, garantizando acceso con el mínimo privilegio, visibilidad continua y protección integral para cada interacción de GenAI.

Control de acceso a instancias autorizadas de aplicaciones de IA



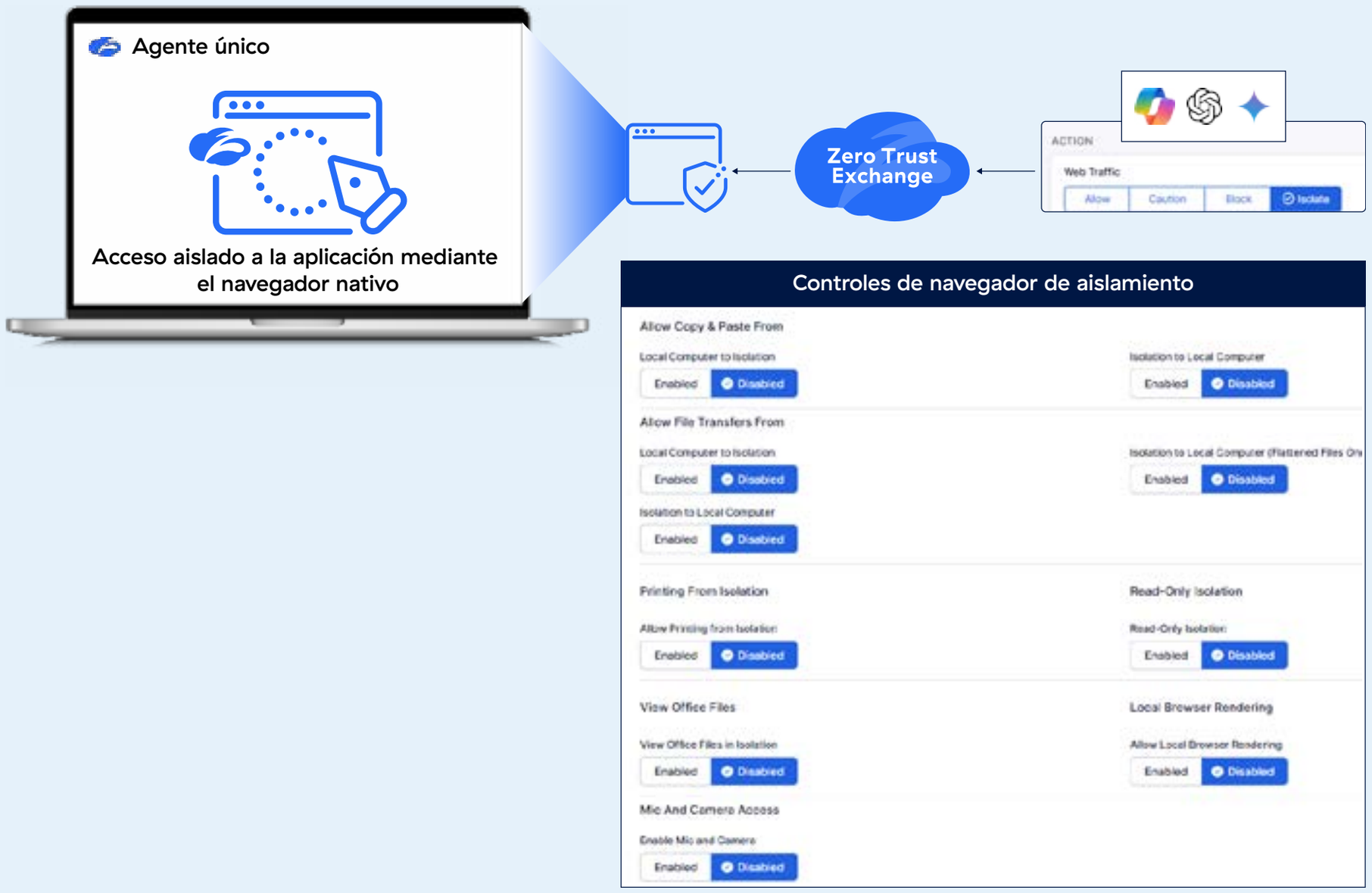
Reducir el riesgo de aplicaciones GenAI no autorizadas

Cuando se necesita acceso para aplicaciones GenAI que no están sancionadas (carecen de licencias empresariales e inicio de sesión único (SSO)), estas aplicaciones GenAI deben tratarse como de alto riesgo. Los datos cargados en dichas aplicaciones pueden usarse para entrenar los modelos GenAI, exponiendo potencialmente información confidencial. Para abordar este mayor riesgo, las agencias 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 Zero Trust Browser. Esta herramienta permite a las agencias proporcionar acceso seguro a aplicaciones GenAI no autorizadas con controles avanzados, como limitar acciones como transferencias de archivos, impresión y uso del portapapeles. Además, Zero Trust Browser evita que las aplicaciones de GenAI ejecuten código directamente en el navegador del usuario, y en su lugar representan interacciones en páginas aisladas. Esto ayuda a proteger contra la toma de huellas dactilares, el seguimiento de cookies de terceros y otras vulnerabilidades, al mismo tiempo que permite a los usuarios seguir usando el mismo navegador implementado por la agencia.

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

Controles granulares para proteger aplicaciones de IA aisladas y equilibrar la experiencia del usuario



4. Implementar la protección de datos desde el principio

No implementar una protección de datos sólida desde el comienzo de la adopción de GenAI puede generar infracciones de datos, infracciones de las normas de privacidad y una pérdida de confianza pública, lo que en última instancia socavará el éxito de estas herramientas. La naturaleza conversacional y fácil de usar de las aplicaciones públicas de GenAI aumenta el riesgo de que los usuarios expongan involuntariamente datos gubernamentales confidenciales. Acciones simples como copiar y pegar información o cargar archivos pueden, sin una supervisión cuidadosa, filtrar detalles confidenciales debido al contexto o la integración con otros sistemas. Esto resalta por qué la incorporación de medidas sólidas de protección de datos debería ser una parte central de cualquier estrategia pública de adopción de GenAI para los gobiernos estatales y locales.

Zscaler permite a las agencias abordar estos riesgos de frente con sus capacidades avanzadas de prevención de pérdida de datos (DLP). Creada para proteger información confidencial desde el principio, la solución DLP de Zscaler para GenAI identifica y bloquea el intercambio de datos confidenciales (ya sea a través de un mensaje, carga de archivos o uso indebido) antes de que puedan llegar a los modelos públicos de GenAI. Este enfoque proactivo garantiza que las agencias puedan adoptar GenAI mientras protegen la información confidencial y mantienen el cumplimiento.

Acelerar la adopción de DLP

Para muchas organizaciones, iniciar un proceso de protección de datos puede parecer una tarea desafiante, especialmente cuando se trata de equilibrar la necesidad de otorgar acceso a las herramientas GenAI con la implementación de sólidas medidas de protección. Zscaler aborda este desafío ofreciendo una plataforma optimizada diseñada para respaldar equipos reducidos, lo que permite una rápida adopción de GenAI con controles efectivos de protección de datos. Este enfoque garantiza que las agencias puedan escalar su marco de seguridad de manera eficiente en diversos departamentos y bases de usuarios.

Para las agencias que ya tienen reglas en línea aplicadas a otros destinos de Internet, extender esas políticas a las aplicaciones GenAI es sencillo. Zscaler también integra motores DLP y diccionarios existentes utilizados para otros canales directamente en aplicaciones de IA y aprendizaje automático, reduciendo la redundancia y acelerando la implementación. Si una agencia está comenzando desde cero, Zscaler proporciona diccionarios predefinidos que se pueden aplicar a las aplicaciones GenAI con solo unos pocos clics para evitar que se filtren datos confidenciales. Además, los documentos o conjuntos de datos conocidos pueden protegerse mediante las funciones EDM/IDM, y el etiquetado de Microsoft Information Protection (MIP) puede reforzar la protección de los datos cifrados o clasificados frente a su posible exposición.

Para refinar aún más las políticas, las capacidades de detección de aprendizaje automático (ML) de Zscaler identifican información confidencial previamente desconocida y fugas de datos dentro de las aplicaciones GenAI, lo que permite a las agencias desarrollar continuamente su estrategia de protección. Ya sea ajustando diccionarios existentes o creando reglas de detección personalizadas utilizando expresiones regulares o palabras clave, las agencias pueden adaptarlas para que se ajusten a sus necesidades. Zscaler también se integra con soluciones de respaldo de datos como Rubrik, simplificando la identificación y protección de datos.

Aceleración de la implementación de DLP con Zscaler

Implementación de día O

Datos específicos de la agencia con EDM e IDM

Diccionarios predefinidos que deberían utilizar los organismos gubernamentales

- Números de ruta bancaria de la 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 seguro,
- Factura,
- Documento legal,
- Documento médico.
- Información médica,
- Documento inmobiliario,
- Números de la Seguridad Social (EE. UU.),
- Documento fiscal,
- Número de identificación fiscal (EE. UU.),
- Documento del Departamento de Transporte y Automotores,
- Información sobre tratamientos.

Etiquetas AP / MIP

Visibilidad y supervisión continua

Identificar fugas de datos y aplicaciones desconocidas

Datos recopilados de incidentes

Aportaciones y comentarios de los usuarios

Refinar y ajustar | Según sea necesario

Crea expresiones regulares para diccionarios personalizados / Palabra clave

Palabras clave de una o varias palabras con proximidad

Ampliar EDM y IDM para soluciones de copia de seguridad de datos

La aplicación de políticas en tiempo real y la visibilidad granular permiten a los equipos de TI proteger datos confidenciales sin complejidad adicional ni supervisión manual. Este enfoque optimizado facilita la adopción rápida y segura de las herramientas de GenAI, aprovechando sus beneficios de productividad y al mismo tiempo garantizando el cumplimiento y la confianza pública, alineándose con el principio "Nunca confíes, siempre verifica" 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 agencias u organizaciones de servicios compartidos, es el volumen de incidentes que los equipos SOC y los propietarios de datos necesitan gestionar. Estos incidentes pueden abarcar desde requerir un seguimiento con el empleado para justificar la acción, reforzar la formación del usuario, gestionar excepciones o mantener un registro de auditoría. Sin un sistema eficiente, esto puede volverse rápidamente abrumador.

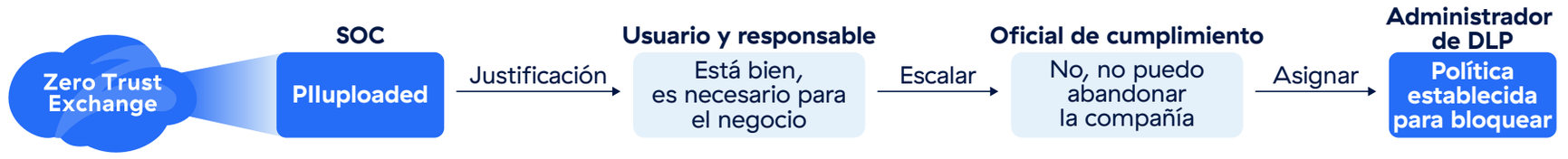
La automatización del flujo de trabajo simplifica este proceso al ofrecer una solución centralizada para gestionar incidentes de protección de datos relacionados con GenAI. Proporciona una vista completa de todos los incidentes en un solo lugar, incluidos los metadatos y los detalles de las acciones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

Una característica clave de la automatización del flujo de trabajo es su capacidad de agrupar incidentes en función de características compartidas y asignar prioridades. Estos grupos pueden luego asignarse a administradores específicos para una resolución específica. 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 escalan problemas a gerentes o propietarios de datos para su aprobación. Los flujos de trabajo automatizados también pueden desencadenar acciones para remediar incidentes sin intervención manual.

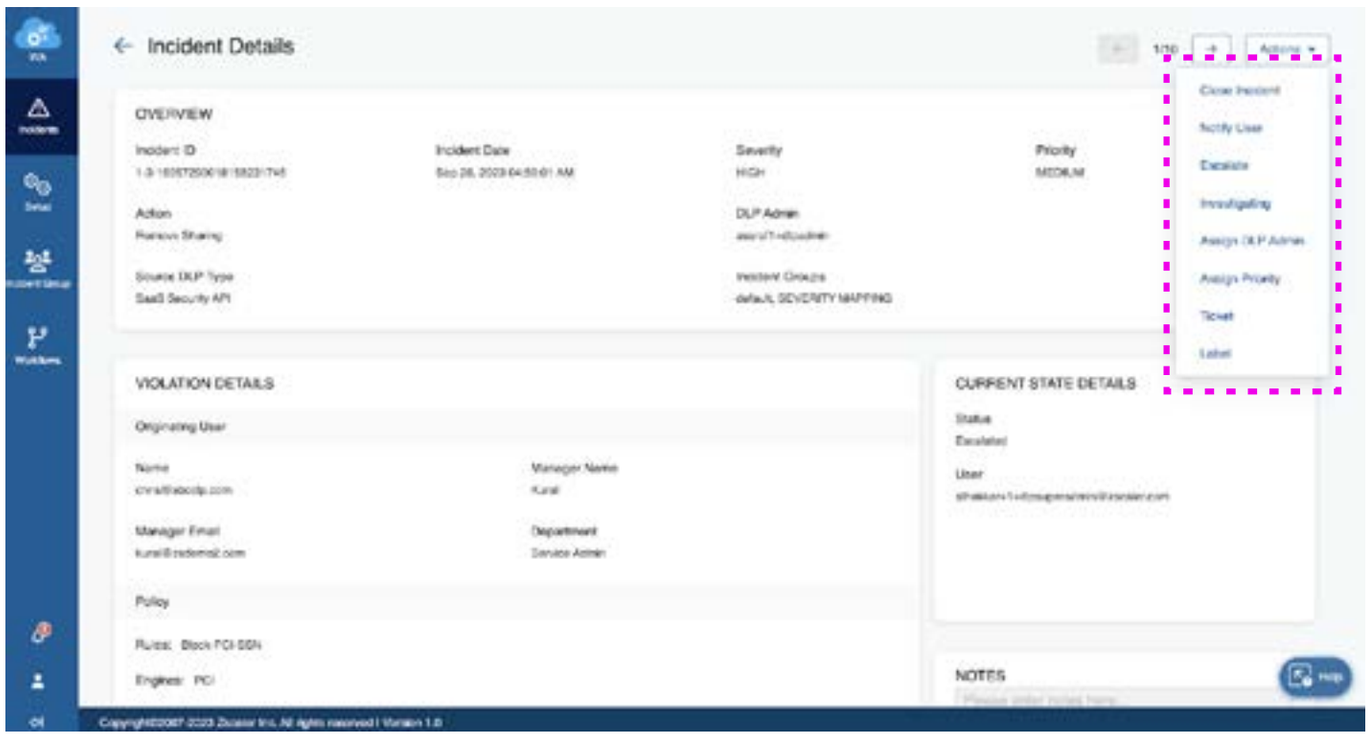
Al aprovechar la automatización del flujo de trabajo en DLP, las agencias pueden reducir significativamente los tiempos de resolución, reducir las cargas operativas en el SOC y obtener información útil sobre áreas de riesgo. Estos conocimientos se pueden utilizar para perfeccionar aún más las políticas o mejorar los programas de capacitación, garantizando que los usuarios estén mejor equipados para operar de forma segura y reduciendo al mismo tiempo la probabilidad de incidentes futuros.

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

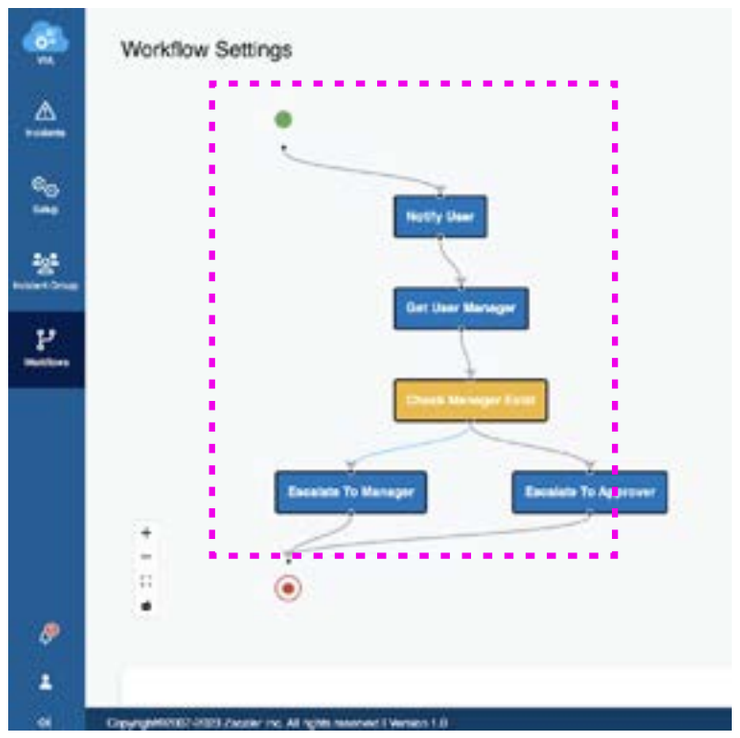
Automatización del flujo de trabajo
Justificar los incidentes al tiempo que se facilita la formación de los usuarios



Gestiona, asigna y escala incidentes fácilmente.



Definir rutinas para flujos de trabajo



5. Unir todo y utilizar un enfoque en capas

Los gobiernos estatales y locales están adoptando la IA generativa (GenAI) para lograr nuevas eficiencias y mejorar los servicios, pero hacerlo de forma segura es esencial. Con miles de herramientas de GenAI disponibles, junto con riesgos como la fuga de datos y el uso no autorizado, las agencias necesitan una estrategia clara que priorice la seguridad, integre los principios de Zero Trust y, al mismo tiempo, permita la productividad. Un enfoque en 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 las agencias a proteger datos confidenciales, agilizar las operaciones y capacitar a los usuarios para aprovechar de forma segura las aplicaciones GenAI, todo dentro de un marco escalable y manejable.

Implementar controles en capas

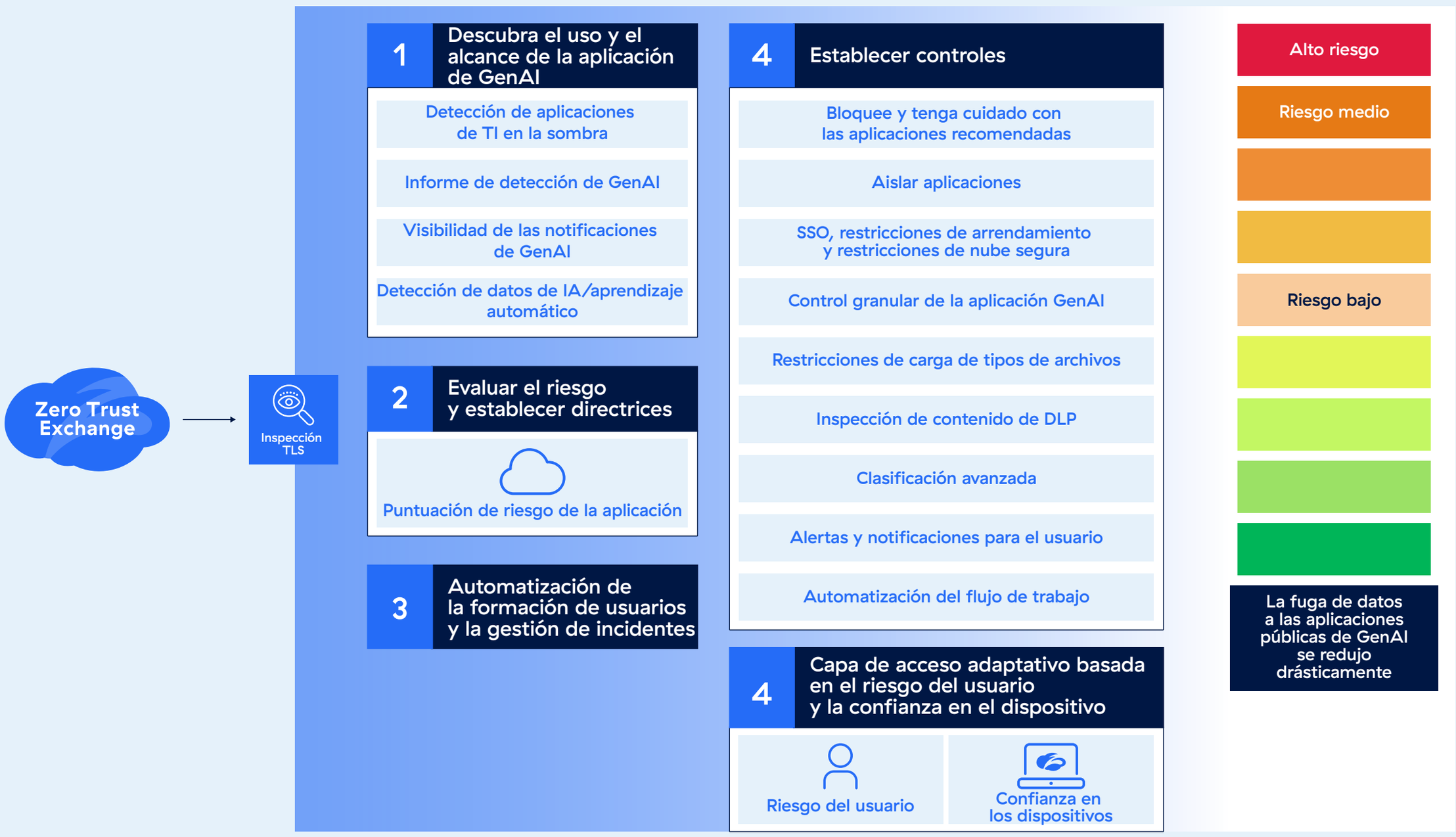
En esta sección, exploraremos cómo las agencias pueden reunir los diversos elementos de la adopción segura de GenAI utilizando un enfoque en capas. Con miles de herramientas de GenAI ya disponibles y nuevas lanzándose cada semana, administrar políticas e incidentes puede volverse rápidamente abrumador sin una estrategia bien pensada.

Un enfoque en 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 disminuye la cantidad de incidentes que los equipos de TI y seguridad deben abordar. Al adoptar este enfoque estructurado, las organizaciones pueden aprovechar de forma segura y eficaz el poder de GenAI y, al mismo tiempo, mantener la eficiencia operativa.

Como se mencionó anteriormente, herramientas como el descubrimiento de aplicaciones Shadow IT, los informes de detección de GenAI y la visibilidad de los avisos de GenAI ofrecen información valiosa sobre cómo deben evolucionar las políticas de IA y cómo pueden personalizarse los controles de seguridad para adaptarse a las necesidades cambiantes. Estos conocimientos forman la base de un enfoque práctico y en capas para gestionar aplicaciones GenAI.

Una forma útil de implementar este enfoque es categorizar las aplicaciones GenAI en tres categorías: alto riesgo, riesgo medio y riesgo bajo. 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. A las aplicaciones de bajo riesgo se les puede permitir acceso nativo, pero con restricciones centradas en el contenido específico o las acciones que los usuarios pueden realizar.

Enfoque en capas para proteger las aplicaciones de IA



Esta estructura permite a las agencias adoptar un enfoque Zero Trust para GenAI. Bajo este modelo, las aplicaciones desconocidas, recién lanzadas o no aprobadas se bloquean de forma predeterminada. Las aplicaciones aprobadas pero no sancionadas están aisladas con capas de seguridad adicionales, mientras que las aplicaciones totalmente sancionadas se benefician de una experiencia de usuario más fluida con protecciones personalizadas. Para que esto sea más fácil de implementar y gestionar, las agencias pueden utilizar herramientas como etiquetas de aplicación personalizadas y perfiles de riesgo. Estos permiten a los equipos de seguridad definir políticas preestablecidas que se aplican automáticamente a las aplicaciones en función del riesgo asignado. Con solo etiquetar una aplicación, se aplican las políticas adecuadas, lo que minimiza el esfuerzo administrativo y mantiene un control sólido.

Automatización de flujos de trabajo de incidentes

Otra capa crítica a considerar es la gestión de incidentes. Es esencial que las agencias reduzcan la cantidad de incidentes que el Centro de Operaciones de Seguridad (SOC) o los administradores de datos deben manejar manualmente. Las infracciones de gravedad media y baja, por ejemplo, deberían registrarse con fines de auditoría y cerrarse automáticamente sin requerir una intervención manual significativa. Sin embargo, dado que esto sigue representando infracciones de políticas, se debe notificar a los usuarios y solicitarles una justificación, una medida invaluable para reforzar la capacitación de los usuarios y fomentar la responsabilidad.

Con Zscaler, las políticas de inspección de contenido para GenAI permiten a las agencias definir el nivel de gravedad de las infracciones, que luego se pasan a las herramientas de automatización del flujo de trabajo. Esta función permite a los administradores diseñar flujos de trabajo adaptados a la gravedad de cada incidente. Se pueden usar atributos adicionales como la gravedad y otras características compartidas para categorizar incidentes en grupos, y estos grupos se pueden vincular a flujos de trabajo automatizados. Este enfoque simplifica la forma en que se procesan los incidentes, lo que garantiza que las infracciones se aborden adecuadamente y alivia significativamente la carga de los equipos del SOC.

Reflexiones finales

Las agencias gubernamentales deben estar a la vanguardia del aprovechamiento de las aplicaciones de IA generativa (GenAI) para transformar las operaciones, empoderar a los empleados y brindar un mejor servicio a los ciudadanos. Sin embargo, su adopción debe estar respaldada por una arquitectura de Zero Trust. Al garantizar que cada usuario, dispositivo e interacción esté verificado, supervisado y controlado, sin importar la ubicación o la aplicación, las agencias pueden proteger con confianza las iniciativas GenAI con una sólida protección de datos, una gobernanza clara y experiencias de usuario optimizadas en el centro de su estrategia.

Zscaler permite a las agencias gubernamentales adoptar las ventajas de productividad de GenAI con un enfoque seguro y en capas que simplifica la gobernanza, agiliza la implementación e incorpora seguridad sólida en cada interacción. Al establecer marcos de gobernanza de IA, automatizar el descubrimiento y la gestión de aplicaciones de GenAI, controlar el uso de instancias de aplicaciones de GenAI e implementar capacidades DLP avanzadas desde el principio, las agencias pueden reducir drásticamente los riesgos y ajustar sus estrategias de adopción con cargas mínimas para los equipos de TI y seguridad.

A medida que el panorama de GenAI continúa evolucionando, se alienta a los líderes de las agencias a adoptar un enfoque estratégico y gradual para su adopción. Comience por asegurar el acceso a las aplicaciones públicas de GenAI y desbloquee de forma segura una mayor productividad con la IA Agente (documento futuro). Por último, exploraremos cómo extender de forma segura las capacidades de GenAI a los servicios centrados en los ciudadanos, garantizando que los sistemas permanezcan seguros en cada paso. Con Zscaler, las agencias pueden implementar estas fases con confianza, acelerando la innovación y manteniendo los más altos estándares de seguridad y cumplimiento de datos.

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

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com/es**

zscaler™

Zero Trust Everywhere