Adoção segura da GenAI com zero trust:

uso seguro de aplicativos públicos de GenAI

DOCUMENTO TÉCNICO

Índice

Introdução

A inteligência artificial generativa (GenAI) está transformando a forma como os governos operam, permitindo-lhes melhorar a produtividade, simplificar processos e servir melhor os cidadãos. No entanto, para aproveitar o potencial transformador da GenAI e, ao mesmo tempo, mitigar seus riscos inerentes, as agências devem aplicar os princípios de zero trust. Esse paradigma garante que nenhuma entidade (humana ou máquina) seja considerada confiável por padrão, assegurando visibilidade contínua e verificação rigorosa em cada interação.

Este documento técnico é o primeiro da série "Adoção segura da GenAI com zero trust", uma estratégia abrangente concebida para apoiar as agências governamentais na utilização segura do ambiente de GenAI. A série inclui três fases:

- A fase 1, descrita neste documento, concentra-se na segurança dos aplicativos públicos de GenAI para mitigar riscos como vazamento de dados e uso não autorizado de IA ("IA paralela").
- A fase 2 explorará a adoção de ferramentas de IA agêntica para aumentar a produtividade dos funcionários de forma segura.
- A fase 3 se concentrará na implantação segura dos sistemas de GenAI para serviços aos cidadãos, garantindo que os sistemas e dados governamentais permaneçam protegidos.

Cada fase enfatiza uma abordagem proativa e multifacetada, equilibrando inovação com governança robusta e segurança.

Uso seguro da GenAI pública

Visão geral

Os governos estão cada vez mais conscientes do potencial transformador da inteligência artificial generativa (IAG) para as suas operações e para os serviços que prestam aos cidadãos. Essa tecnologia abre caminho para um aumento expressivo na produtividade e para a evolução dos serviços aos cidadãos por meio de diversas aplicações. Essas aplicações variam desde a compreensão do sentimento público e o fornecimento de chatbots com inteligência artificial para suporte aos cidadãos e à TI, até a facilitação da tradução de idiomas e a automatização de processos internos, como a elaboração de descrições de cargos, o resumo de reuniões e a criação de comunicados públicos.

Os primeiros órgãos governamentais a adotar essa prática já estão testemunhando melhorias na experiência e na satisfação dos funcionários. O surgimento de grandes modelos de linguagem (LLMs) de acesso público, como o ChatGPT, estimulou a experimentação em todo o setor público, à medida que as organizações buscam compreender e aproveitar as capacidades da IA. Esse amplo interesse ressalta as oportunidades de aprimorar a eficiência e a prestação de serviços por meio da integração dessas ferramentas avançadas de IA.

No entanto, a integração da GenAI, particularmente por meio de LLMs públicos e modelos de terceiros, introduz desafios de segurança consideráveis. O uso não autorizado de ferramentas de IA (“IA paralela”) pode expor dados sigilosos de cidadãos, registros comerciais ou propriedade intelectual. O risco é ainda maior em fluxos de trabalho que envolvem geração aumentada via recuperação (RAG) ou protocolo de contexto de modelo (MCP) e agentes de IA, podendo comprometer dados sigilosos e representar riscos à segurança nacional devido à possibilidade de agentes patrocinados por governos ou entidades maliciosas explorarem essas vulnerabilidades para espionagem, sabotagem ou paralização de infraestruturas críticas. Além disso, a GenAI apresenta uma ampla superfície de ataque que as medidas de segurança tradicionais, muitas vezes baseadas em controles binários restritivos ou que carecem de visibilidade abrangente em diferentes ambientes, não estão bem equipadas para gerenciar de forma eficaz.

Para aproveitar o potencial da GenAI, as agências devem adotar uma abordagem zero trust com segurança robusta, visibilidade e simplicidade de uso. As etapas a seguir descrevem um processo que as agências podem seguir para aproveitar a GenAI, mitigando proativamente os riscos de vazamento de dados e evitando sobrecarga indevida nas equipes de segurança:

1. Estabeleça estruturas e políticas de governança de IA
2. Integre estreitamente a experiência de usuário e o treinamento
3. Priorize a segurança e escolha a arquitetura correta
4. Implemente a proteção de dados desde o início
5. Utilize uma abordagem em camadas para proteção

Vamos analisar essas etapas em mais detalhes.

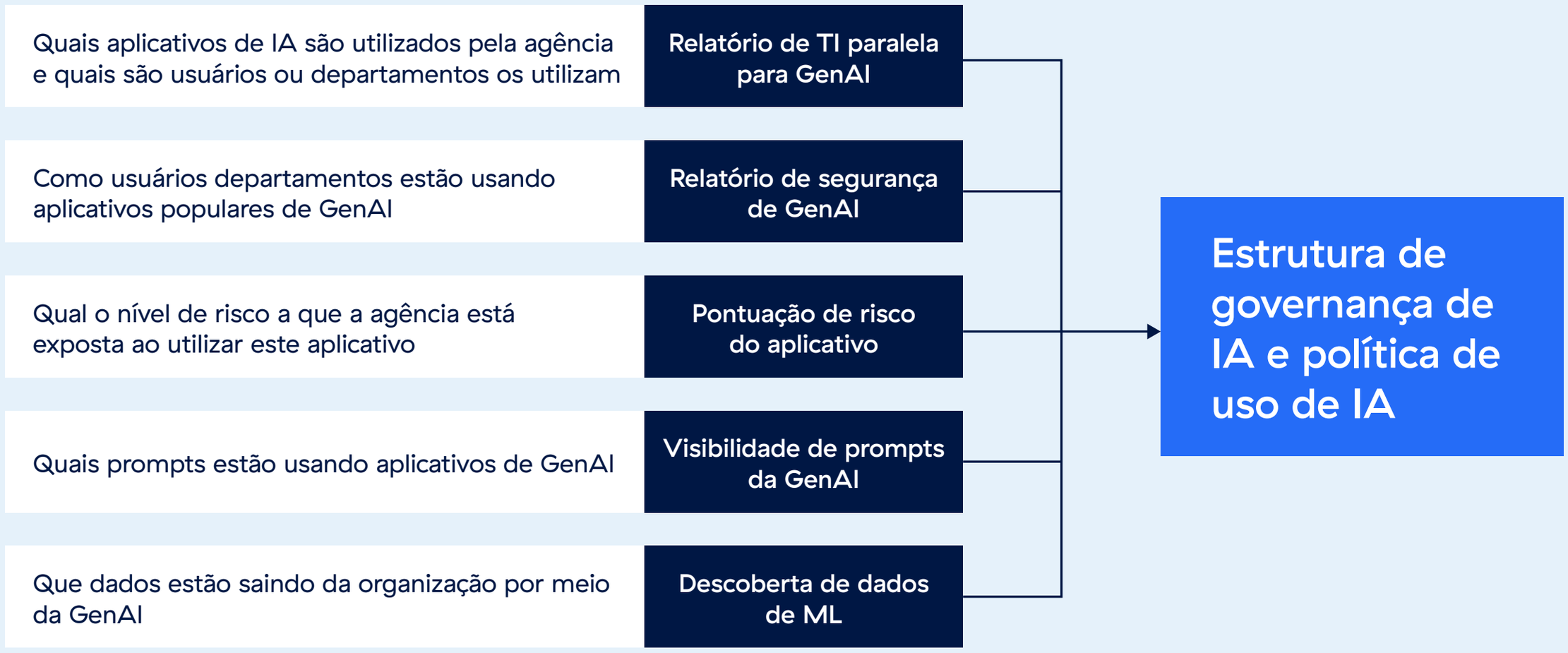
1. Estabeleça estruturas e políticas de governança de IA

Para aproveitar ao máximo os benefícios da GenAI, as agências devem implementar medidas de segurança robustas que abordem diretamente os riscos sem prejudicar a produtividade dos usuários. Esta seção explora como as agências podem adotar uma abordagem zero trust para aplicativos de GenAI, garantindo que os controles de segurança não impeçam uma experiência de usuário perfeita.

O desenvolvimento de estruturas e políticas de governança de IA é essencial para garantir a adoção da IA generativa em agências estatais. Isso geralmente envolve a criação de uma força-tarefa ou órgão de governança específico para supervisionar o desenvolvimento e a implementação de políticas. Por exemplo, a força-tarefa de GenAI do Alabama serve como modelo com sua abordagem colaborativa e de equipe multifuncional. As agências também devem aproveitar estruturas zero trust já estabelecidas, como o modelo de maturidade zero trust da CISA e o NIST 800-207, juntamente com estruturas de segurança específicas para IA, como o NIST AI Risk Management Framework (AI RMF), que enfatiza funções essenciais como governança, mapeamento, medição e gerenciamento, ou o TRISM da Gartner, para orientar seus esforços. Ao adotar uma força-tarefa focada e utilizar essas estruturas comprovadas, as agências podem acelerar a integração segura das tecnologias de GenAI em todos os departamentos.

Para auxiliar nesse processo, a Zscaler fornece insights que ajudam as agências a monitorar o uso de IA em seus ambientes, avaliar os riscos potenciais associados aos aplicativos de GenAI e identificar casos de vazamento de dados. A utilização de relatórios da Zscaler permite que as agências acessem dados essenciais sobre como as ferramentas de GenAI estão sendo usadas atualmente.

Pontos de dados fornecidos pela Zscaler para apoiar a criação de uma estrutura de governança de IA e uma política de uso de IA



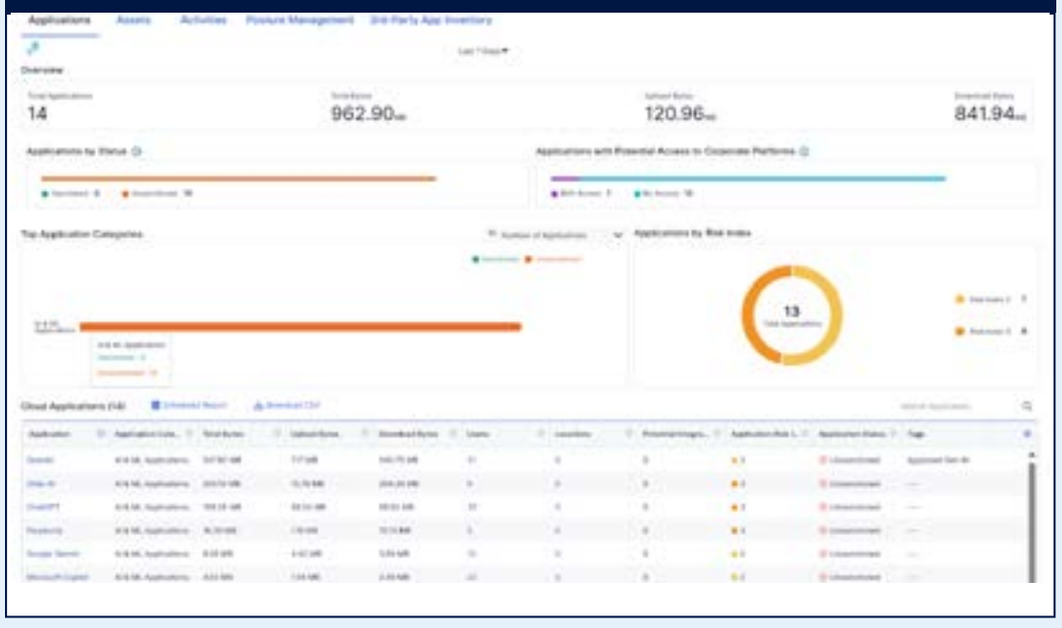
Entendendo o uso atual da IA

Compreender o uso atual da IA é um passo fundamental na criação de estruturas de governança. Ao analisar quais aplicativos de GenAI estão sendo utilizados, como estão sendo aplicados e os fatores de risco associados, as agências podem identificar onde as políticas são mais necessárias. Essa abordagem baseada em dados garante que a estrutura permaneça relevante, prática e adaptada para abordar com eficácia os desafios e oportunidades exclusivos da agência.

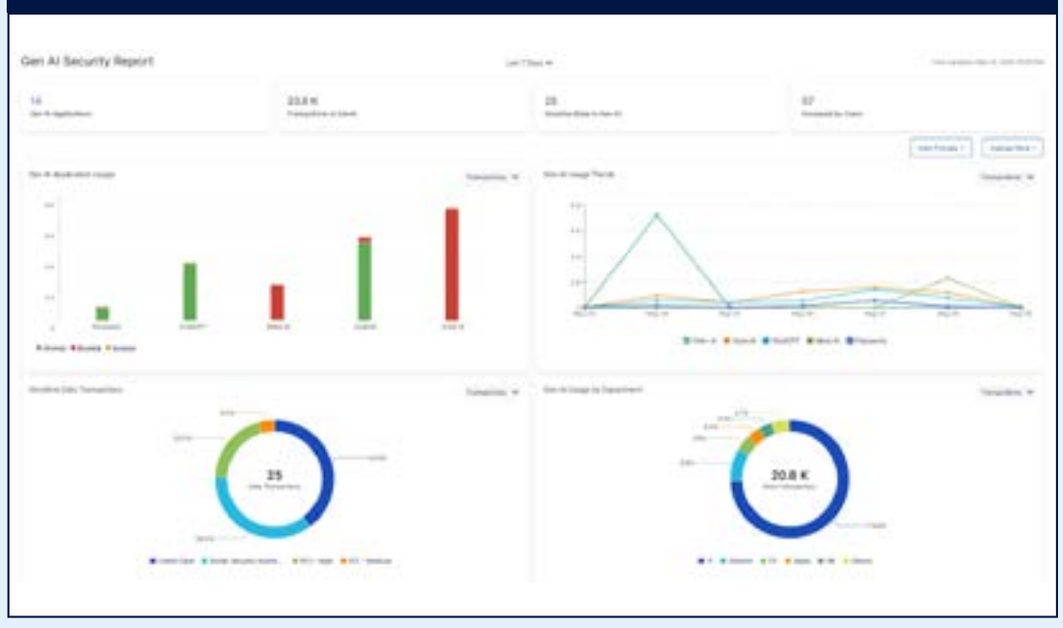
A Zscaler fornece relatórios detalhados sobre o uso de IA, oferecendo transparência sobre quais aplicativos de GenAI estão sendo usados em diferentes agências e a extensão desse uso. Essas informações podem ser segmentadas ainda mais para mostrar padrões de uso em departamentos ou subagências específicos, proporcionando às organizações uma visão mais clara do cenário de uso de IA.

Informações sobre o uso de IA paralela

Detecção de aplicativos de TI invisível para GenAI

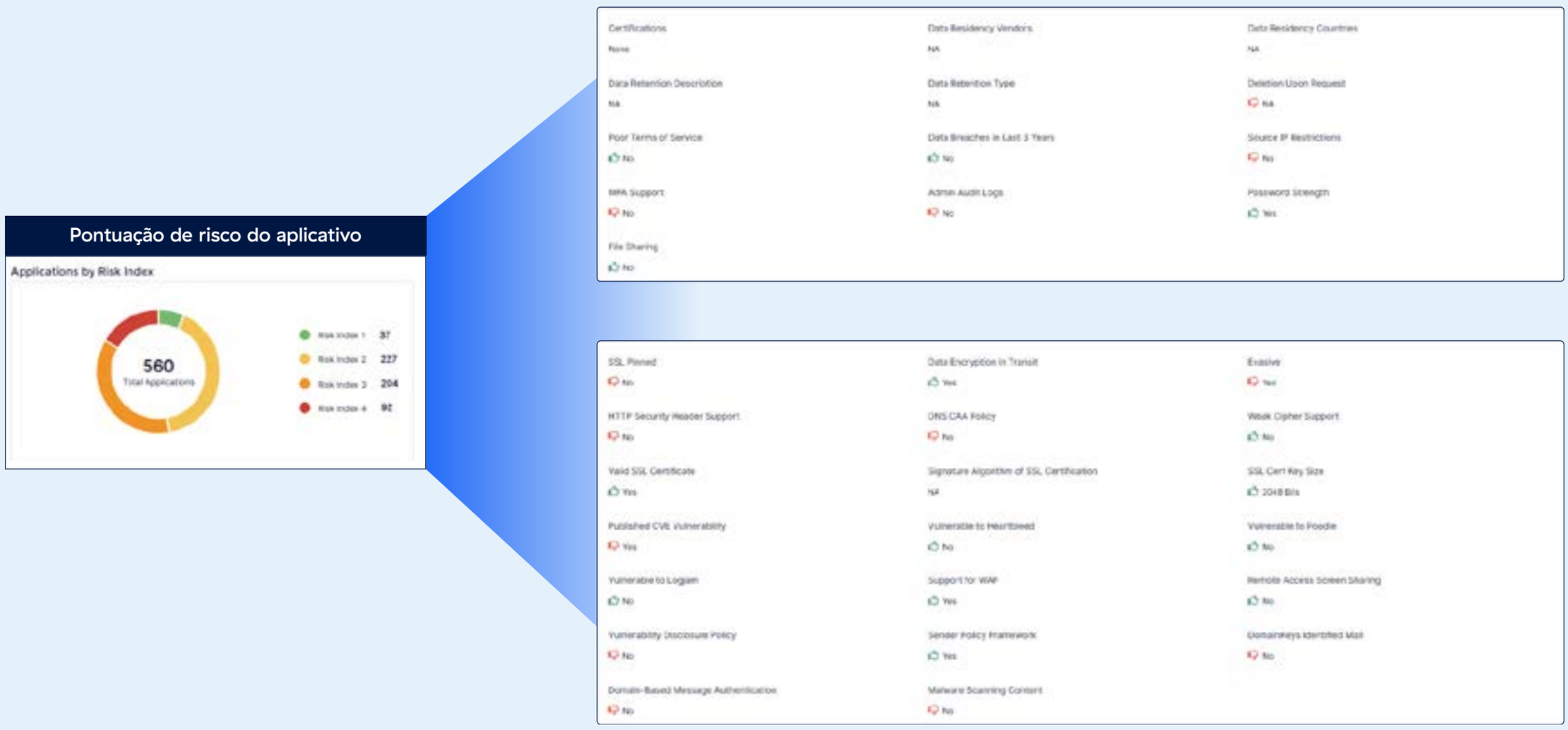


Relatório de segurança de GenAI



Com essa visibilidade, as agências ganham a capacidade de analisar mais profundamente os fatores de risco associados a esses aplicativos. A equipe ThreatLabz da Zscaler, em coordenação com serviços de inteligência sobre ameaças de terceiros, avalia esses riscos e atribui a eles pontuações agregadas que variam de 1 a 5, simplificando a análise de risco para os tomadores de decisão. As agências também têm a flexibilidade de personalizar essas pontuações com base em suas prioridades e requisitos específicos. As avaliações de risco podem incluir fatores-chave como vulnerabilidades de segurança ou questões de conformidade regulamentar, permitindo que os decisores políticos concentrem recursos nas áreas mais relevantes para a sua missão e necessidades de segurança. Alguns exemplos de fatores de risco são apresentados no relatório abaixo, como vulnerabilidades de segurança ou descumprimento de regulamentos, o que permite aos responsáveis pelas políticas da agência priorizar as áreas que são importantes para a respectiva agência.

Riscos associados ao uso de IA paralela

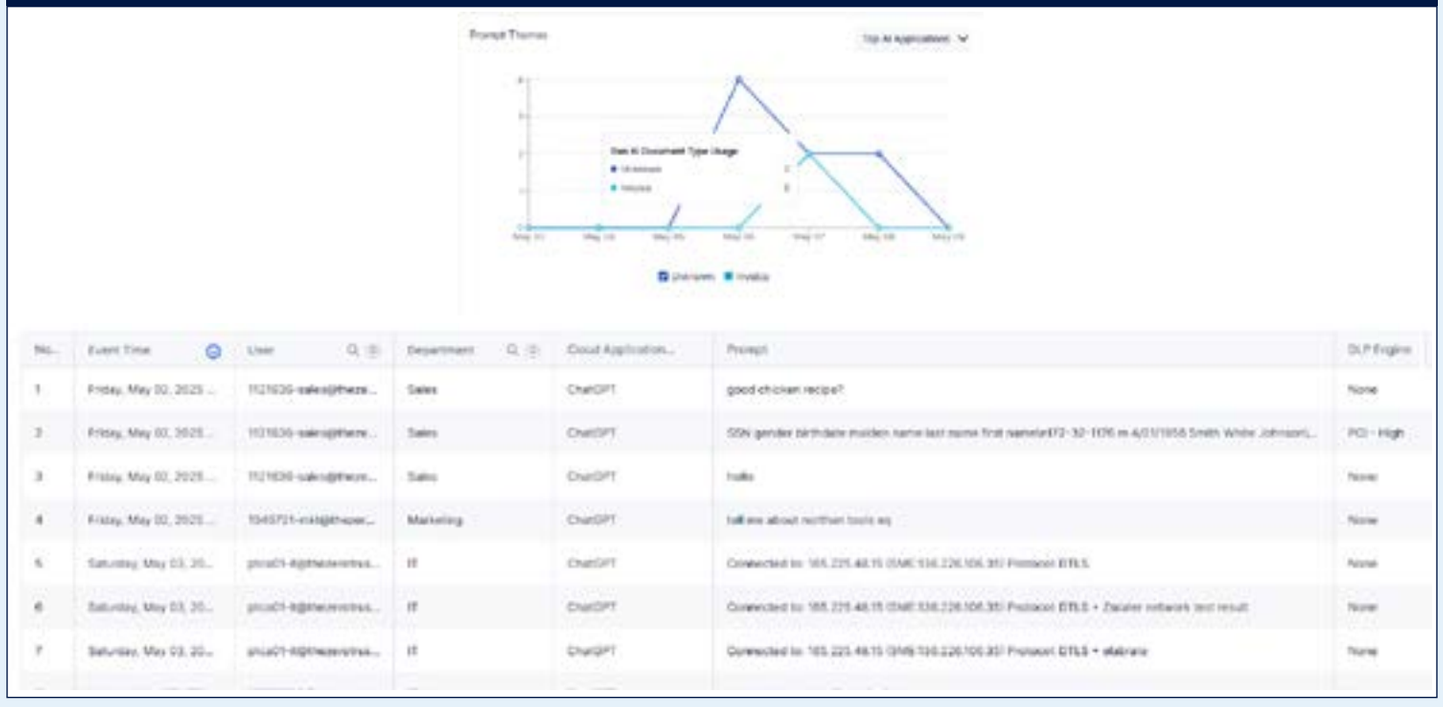


Análise detalhada das interações dos usuários com os aplicativos de GenAI

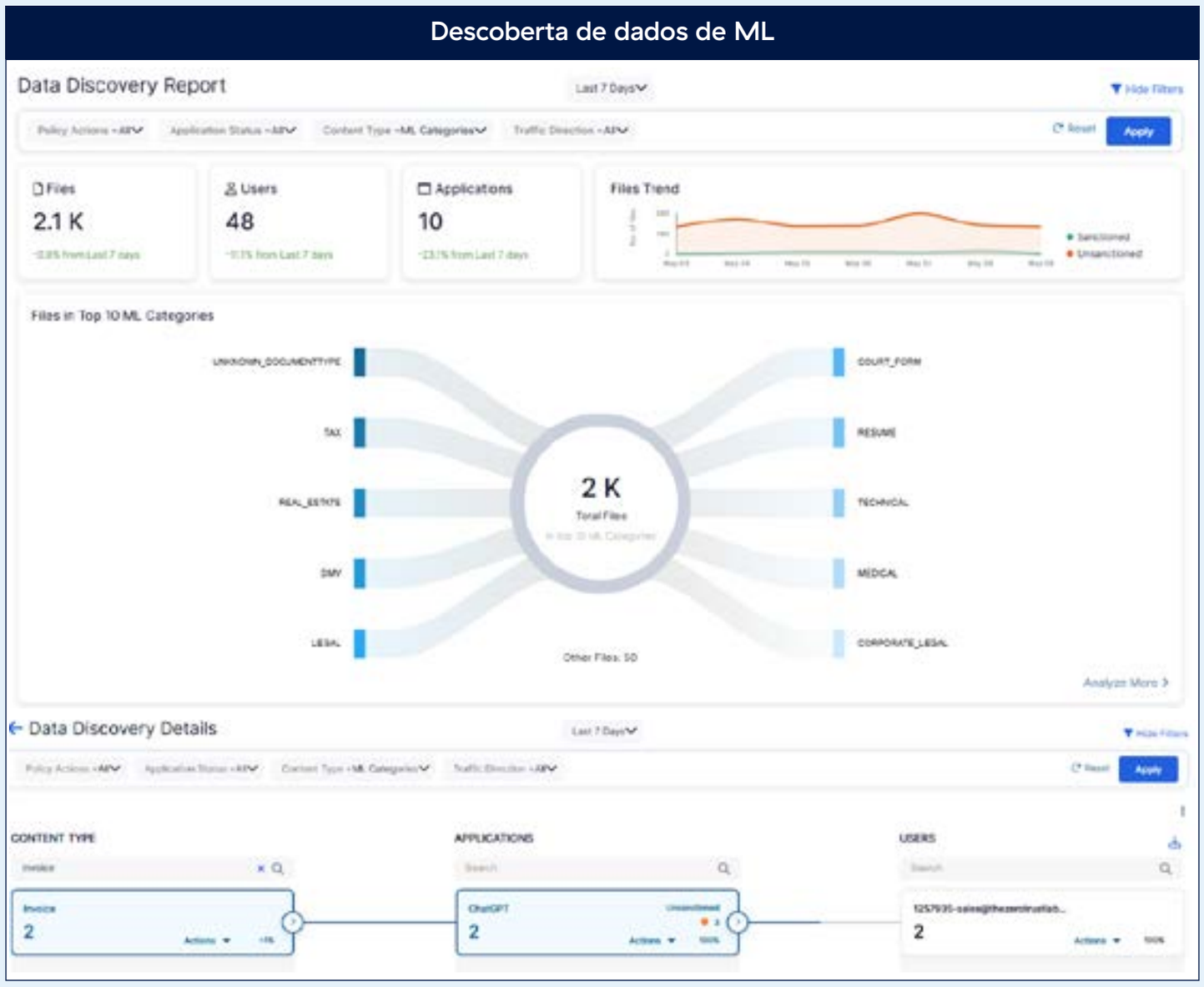
A Zscaler vai além da visibilidade em nível de aplicativo, fornecendo insights detalhados sobre cada transação, solicitação e interação de usuário em aplicativos de GenAI. Isso inclui dados detalhados sobre o que os usuários inserem não apenas por meio de transferências de arquivos, mas também por métodos como entradas de teclado, atividades da área de transferência e outras entradas compatíveis. Essas informações são inestimáveis para as agências, ajudando-as a entender melhor o tipo de dados que estão sendo compartilhados, aprimorar as políticas de segurança e garantir a conformidade com os padrões de governança. Além disso, esse nível de visibilidade é essencial para fins de auditoria e pode ser exportado facilmente para o SIEM da agência para rastreamento e análise abrangentes.

Relatório sobre o atual vazamento de dados fora da agência

Visibilidade de prompt da GenAI



Descoberta de dados de ML



Visibilidade de dados desconhecidos

A Zscaler aumenta ainda mais a visibilidade ao identificar dados que as agências podem não saber que estão vazando por meio de aplicativos de GenAI. Usando recursos baseados em IA/ML, o relatório ML Discovery da Zscaler vai além das regras tradicionais de DLP “somente de monitoramento” para detectar e classificar proativamente dados sigilosos compartilhados com ferramentas públicas de GenAI. Isso permite que os proprietários dos dados e os administradores de segurança identifiquem vazamentos de dados desconhecidos ou não reconhecidos e os resolvam antes que se tornem problemas críticos.

Essa visibilidade profunda dos dados permite que as agências identifiquem proativamente dados de alto risco que poderiam ser expostos a mecanismos de monitoramento de dados públicos. Ela também ajuda a estabelecer ou refinar a propriedade de informações sigilosas, desenvolver políticas de uso e implementar diretrizes personalizadas para proteger conjuntos de dados importantes.

Ao combinar informações sobre usuários, aplicativos, riscos de aplicativos, prompts e padrões de dados, a Zscaler auxilia na criação de políticas e procedimentos específicos que estejam alinhados aos objetivos organizacionais. Essas informações orientam a alocação de recursos e ajudam a definir funções e responsabilidades dentro da estrutura de governança zero trust, permitindo que as agências adotem uma abordagem com visão de futuro que equilibre a inovação com a definição de uma estratégia abrangente de mitigação de riscos.

2. Integre estreitamente a experiência de usuário e o treinamento

A experiência de usuário e o treinamento desempenham um papel central na adoção segura e bem-sucedida da inteligência artificial generativa (GenAI) em agências estatais. Para garantir uma adoção tranquila, é essencial que as medidas de segurança e o treinamento dos usuários sejam projetados de forma a permitir que os usuários permaneçam produtivos, oferecendo, ao mesmo tempo, forte proteção. A introdução de mais uma ferramenta ou aplicativo, especialmente aqueles que possam introduzir novas ferramentas complexas para os utilizadores aprenderem, deve ser evitada sempre que possível. Além disso, controles de segurança eficazes devem ser combinados com a educação contínua dos usuários para maximizar seu impacto. As plataformas devem integrar-se perfeitamente aos fluxos de trabalho e canais existentes, incorporando mecanismos de interação e feedback dos usuários. Isso ajudará as agências a se alinharem com estruturas como a AI Risk Management Framework (AI RMF) do NIST desde o início.

Aqui estão alguns recursos essenciais da plataforma que apoiam essa abordagem:

Acesso à GenAI descomplicado

O principal objetivo das ferramentas de IA generativa é liberar os usuários de tarefas repetitivas e permitir que eles se concentrem em trabalhos que se beneficiam do julgamento humano. As medidas de segurança da GenAI não devem interromper os fluxos de trabalho dos usuários. A Zscaler facilita isso eliminando a necessidade de usar softwares adicionais ou navegadores gerenciados. Por exemplo:

- **Zscaler Single Agent**
  O mesmo agente da Zscaler que garante o acesso seguro a aplicativos públicos e privados também gerencia os controles da GenAI, proporcionando acesso contínuo sem a necessidade de ferramentas adicionais.

- **De acesso seguro sem agente,**
  os usuários podem usar seu navegador nativo e seu fluxo de trabalho existente (por exemplo, acesso via portal de aplicativos do IdP) para acessar aplicativos de GenAI seguros sem precisar de um agente.

- **Controles de segurança flexíveis**
  Em vez de depender apenas das opções “permitir ou bloquear” para o uso da IA, a Zscaler oferece isolamento de navegador baseado na nuvem. Esse recurso redireciona os usuários que acessam aplicativos de GenAI para um ambiente de navegador isolado, hospedado na nuvem da Zscaler. Isso permite que os usuários mantenham uma experiência nativa do navegador, ao mesmo tempo que aplicam medidas de segurança avançadas, como impedir atividades da área de transferência, impressão ou uploads de arquivos. Esse design garante que as políticas de segurança sejam aplicadas sem interromper a experiência de usuário; tudo isso gerenciado por meio de uma plataforma unificada e um único agente da Zscaler para simplificar a administração.

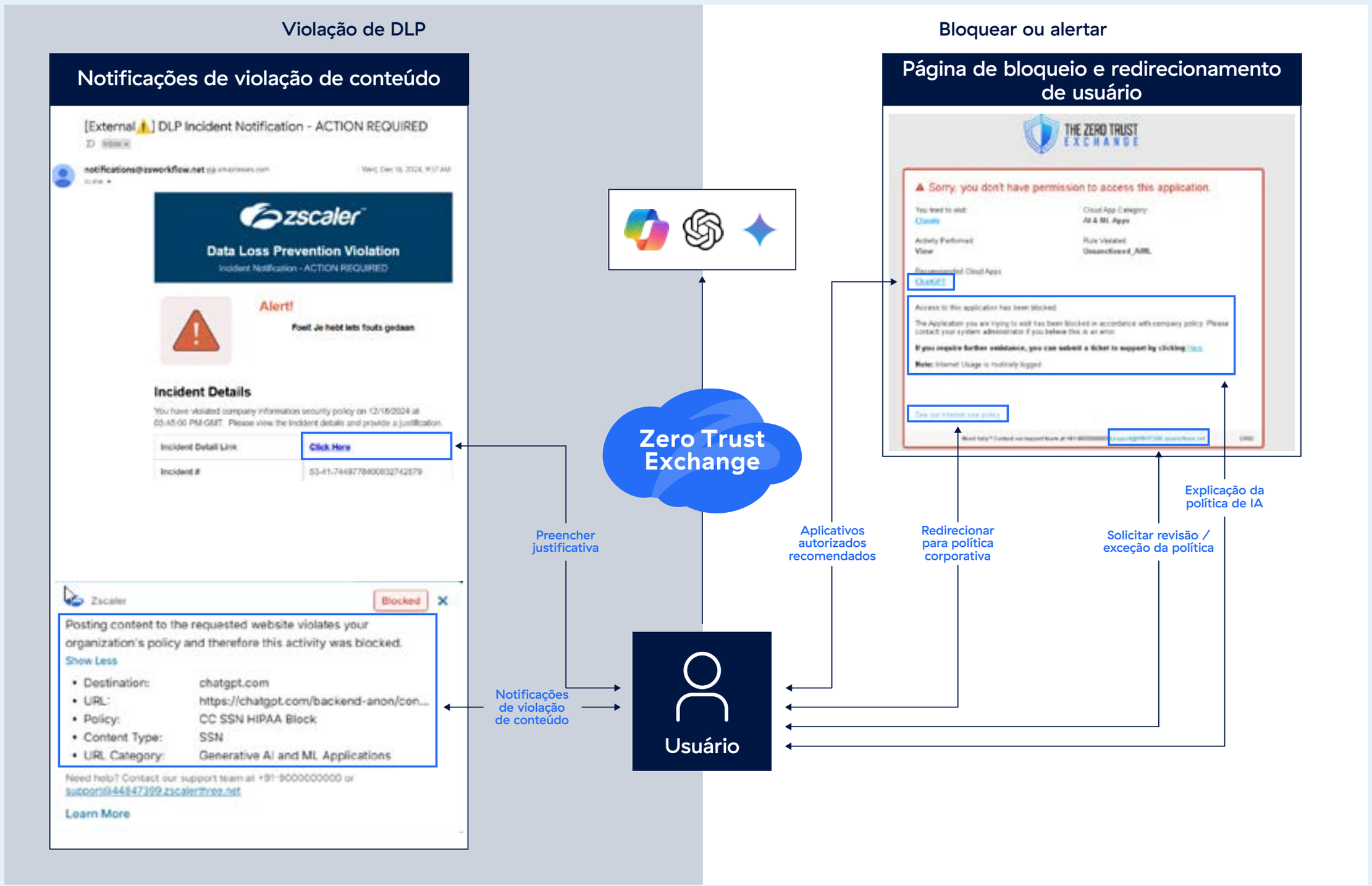
Esses controles podem ser implementados com impacto mínimo na infraestrutura ou nos dispositivos existentes, permitindo que as agências implementem políticas de segurança, preservando uma experiência de usuário perfeita e minimizando os esforços administrativos.

Treinamento e feedback de usuário integrados

A educação continuada sobre o uso seguro da IA generativa e suas violações é essencial, especialmente considerando a rápida evolução da GenAI. O treinamento deve ser frequente, contínuo e integrado diretamente ao fluxo de trabalho e às ferramentas nativas de usuário. A Zscaler oferece suporte a isso por meio de notificações dinâmicas: quando um recurso é bloqueado, isolado ou sinalizado por violações de conteúdo, os usuários recebem alertas personalizados. Por exemplo, se um aplicativo de GenAI não autorizado for bloqueado, a Zscaler sugere aplicativos equivalentes aprovados, ajudando a redirecionar o comportamento dos usuários e, ao mesmo tempo, mantendo a produtividade.
Em cenários de violação do uso de dados, a Zscaler se integra a ferramentas familiares como e-mail e Slack, facilitando que os usuários apresentem justificativas ou recebam feedback personalizado nas ferramentas que já utilizam.

Ao integrar o treinamento dos usuários aos fluxos de trabalho de segurança, as agências podem estabelecer uma base de governança sólida para os aplicativos de GenAI. Essa abordagem não apenas garante que os usuários entendam como interagir com a tecnologia de forma segura, mas também ajuda a criar uma estrutura dimensionável para lidar com incidentes relacionados à IA generativa e aprimorar as políticas de uso de IA em toda a organização.

Treinamento e feedback dos usuários com a Zscaler



3. Priorize a segurança e escolha a arquitetura correta

Com a expansão da superfície de ataque devido à crescente adoção de ferramentas de IA, é crucial que as organizações escolham uma plataforma que não apenas proteja contra ameaças baseadas em IA, mas também permita o uso seguro de aplicativos de GenAI, desenvolvidos em uma arquitetura zero trust e com autorização FedRAMP. A Zscaler oferece uma solução abrangente que combina segurança, usabilidade e conformidade para agências que adotam a GenAI.

As agências podem começar a aproveitar os recursos seguros de GenAI da Zscaler com alterações mínimas em sua infraestrutura existente. O tráfego pode ser encaminhado para a plataforma através do aplicativo da Zscaler, compatível com os principais sistemas operacionais, incluindo Windows, Mac, iOS, Android e Linux, ou por meio de um dispositivo da filial, ou simplesmente por um navegador para implantação sem agentes. Uma vez conectada, a Zscaler garante que os usuários sejam autenticados e autorizados antes de acessar quaisquer recursos na internet, incluindo aplicativos de GenAI. Atuando como intermediária, a Zscaler inspeciona todas as sessões de TLS estabelecidas com os aplicativos de IA generativa, fornecendo às agências visibilidade completa e controle granular sobre como os usuários interagem com essas ferramentas. Essa arquitetura permite que as agências forneçam informações detalhadas sobre como os usuários estão utilizando os aplicativos de GenAI, além de oferecer diversos controles de ponta do setor para proteger os dados das agências.

Inspeção de HTTPS e websocket seguro com a Zscaler

Controle de acesso

- Filtragem de URL
- Firewall de nuvem
- Controles granulares de aplicativos na nuvem
- Restrições de utilização
- Segurança DNS

Prevenção contra ameaças

- Proteção contra malware
- Cloud Sandbox
- Proteção avançada contra ameaças (IPS)
- Isolamento do navegador na nuvem

Proteção de dados

- DLP integrado
- EDM / IDM
- Controles de tipo de arquivo
- Controles de GenAI
- Isolamento do navegador na nuvem

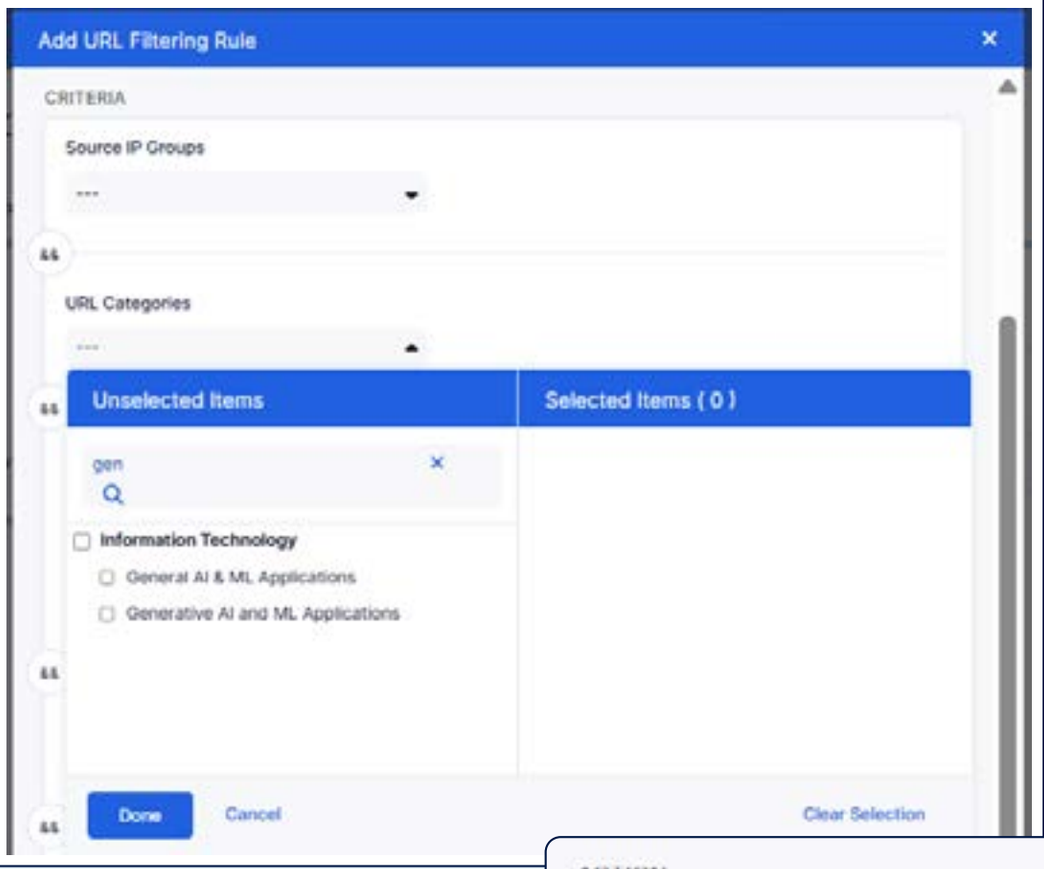
Automatizar a descoberta e o gerenciamento de aplicativos de GenAI

Com a inspeção de TLS implementada, as agências obtêm acesso ao conjunto completo de recursos da Zscaler, incluindo controle granular sobre GenAI e aplicativos de aprendizado de máquina. Uma das principais vantagens reside na categoria de aplicativos de IA e ML da Zscaler, selecionada pela equipe da ThreatLabz. Essa categoria abrange uma ampla gama de aplicativos de inteligência artificial, incluindo ferramentas populares como ChatGPT, Gemini, MetiAI, Claude e outras.

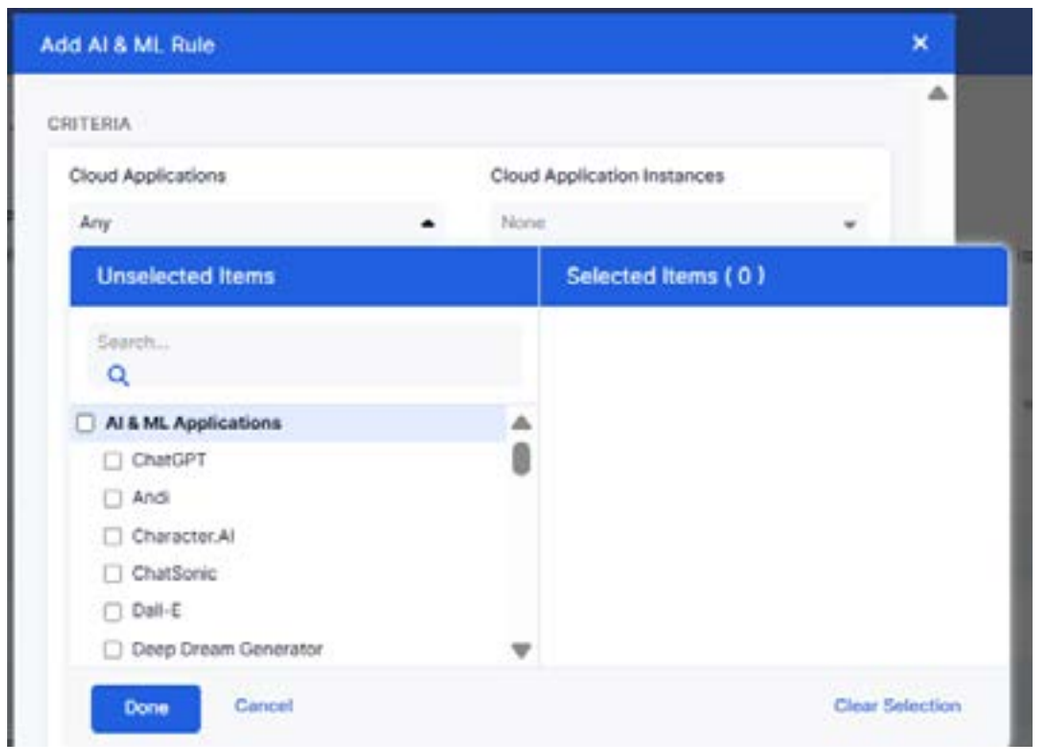
Ao utilizar essa categoria, as agências podem implementar políticas para bloquear, por padrão, aplicativos de GenAI desconhecidos ou não verificados, garantindo que apenas as ferramentas aprovadas estejam acessíveis. À medida que novos aplicativos surgem, eles são adicionados automaticamente a essas categorias, poupando às agências o esforço de descoberta e implantação manuais de atualizações. Além disso, as agências têm flexibilidade para expandir ou personalizar essa lista, adicionando domínios personalizados para melhor atender às suas necessidades específicas. A Zscaler também oferece categorias específicas, como “Aplicativos gerais de IA e ML” e “Aplicativos de IA generativa e ML”, que, quando combinadas com a lista mais abrangente de “Aplicativos de IA na nuvem”, oferecem uma cobertura significativa para reduzir os riscos de segurança que os aplicativos de IA generativa representam. Essa abordagem em camadas permite que as agências gerenciem com eficácia o acesso a centenas de aplicativos que são desenvolvidos e lançados a cada semana.

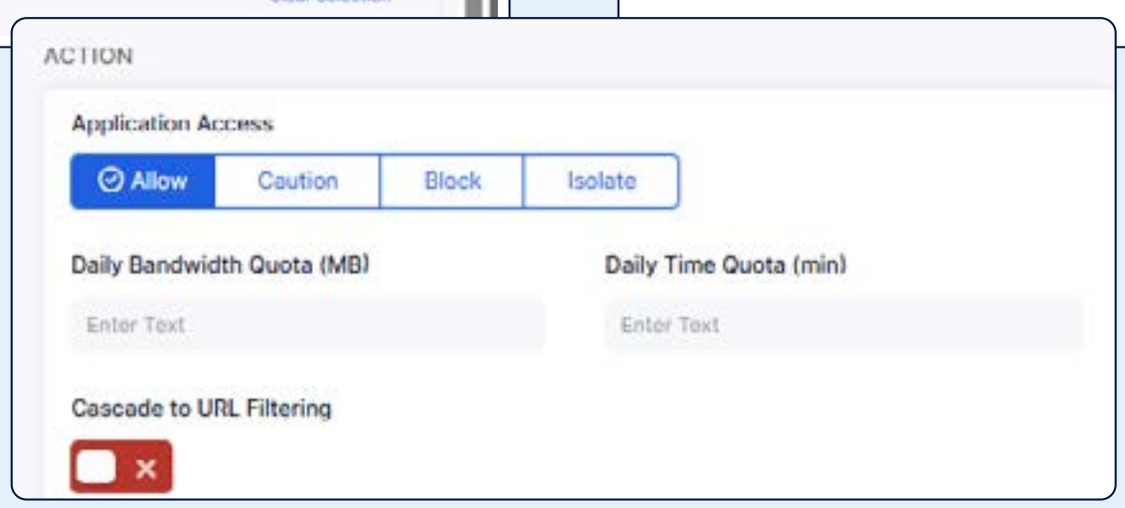
Seleção por categoria geral e aplicativo específico de IA

Categorias de URL para Wide Net



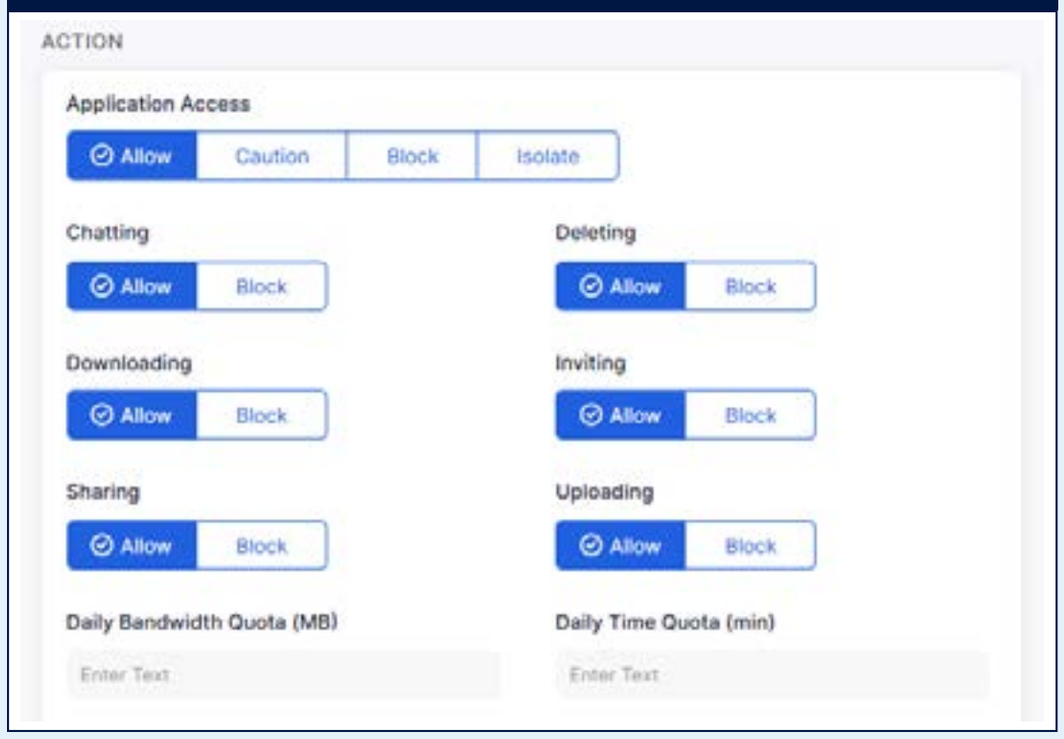
Aplicativo de GenAI para controles granulares



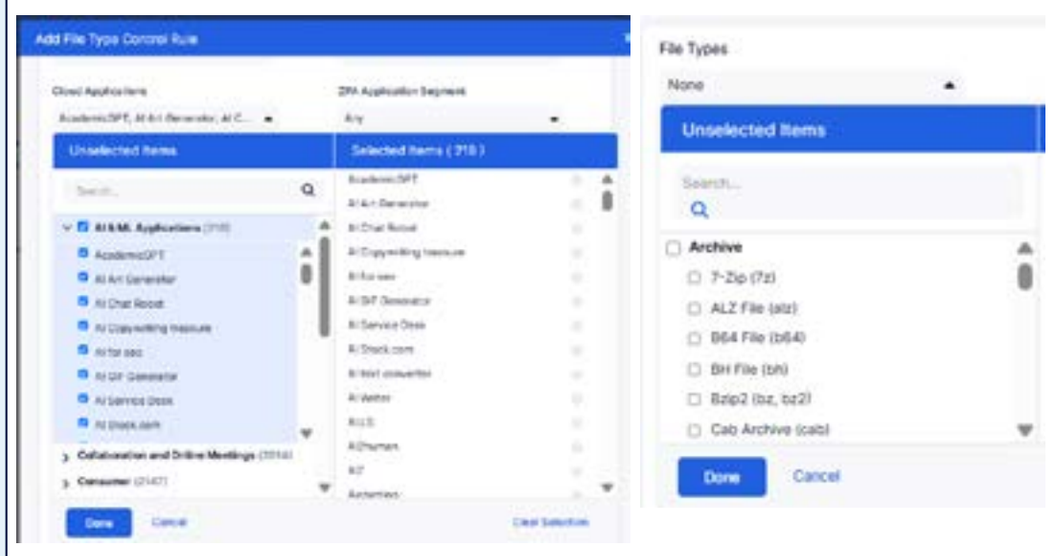


Controles granulares para aplicativos SaaS, web e de IA

Controles granulares de aplicativos de GenAI



Controles de upload de arquivos em aplicativos de GenAI



Permitir aplicativos autorizados por meio do controle de segurança de aplicativos SaaS

Além de manter uma lista abrangente de aplicativos de IA, a Zscaler oferece controles detalhados sobre como os usuários interagem com aplicativos de IA generativa. Esses controles são incrivelmente fáceis de aplicar, muito poderosos e consolidados em uma única plataforma. O lado esquerdo da imagem mostra alguns exemplos de controles granulares que podem ser aplicados; no caso, uma política de segurança do ChatGPT pode incluir controles como permitir o chat, mas bloquear o envio de arquivos ou restringir o compartilhamento de chats. As agências podem aplicar essas medidas para todo um departamento ou até mesmo em nível de usuário individual. Esses controles detalhados podem ser ainda mais refinados restringindo os tipos de arquivo que os usuários podem enviar para os aplicativos de GenAI, conforme mostrado à direita. Esse controle de arquivos também pode incluir a restrição do envio de documentos criptografados.

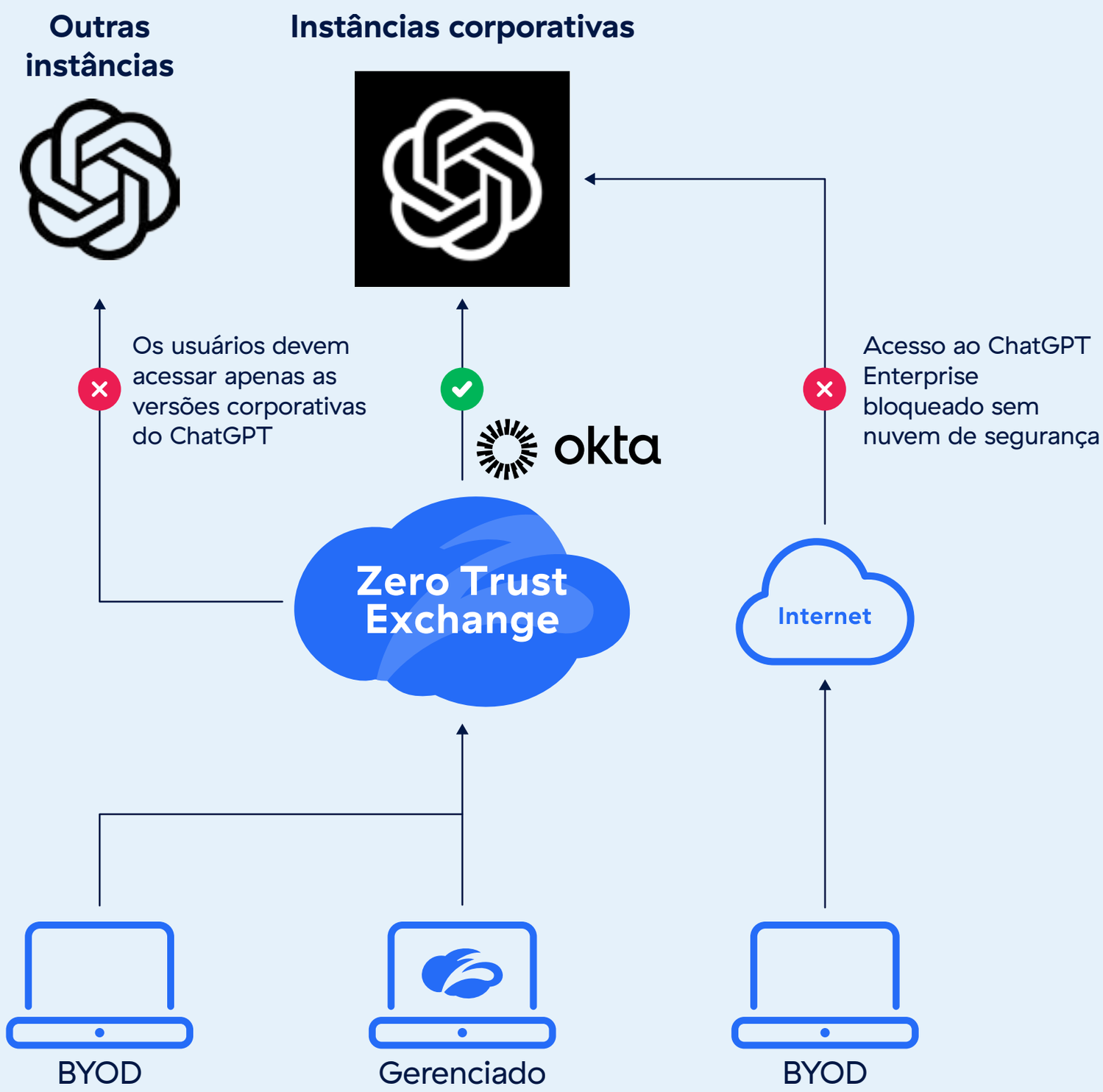
Restringir o acesso a instâncias corporativas de aplicativos de GenAI

As agências devem considerar seriamente o uso de versões corporativas dos aplicativos de GenAI para garantir maior segurança e controle. As versões corporativas, como o ChatGPT Enterprise, oferecem às agências total propriedade e controle sobre seus dados e conversas comerciais, sem que os dados corporativos contribuam para o treinamento do modelo. Essas soluções são compatíveis com o padrão SOC2 e fornecem criptografia tanto em trânsito quanto em repouso. Além disso, elas simplificam o gerenciamento de usuários com recursos como acesso baseado em equipes, verificação de domínio, autenticação única (SSO) e relatórios de uso, possibilitando uma implantação segura em larga escala.

As instâncias corporativas dos aplicativos de GenAI devem ser combinadas com SSO (Single Sign-On) para maximizar a segurança e fornecer às agências maior visibilidade e controle sobre o uso dos aplicativos. Com o SSO implementado, as agências podem aplicar políticas que bloqueiam o acesso a versões não corporativas dos aplicativos de IA generativa. Por exemplo, o controle de instâncias da Zscaler para o ChatGPT garante que apenas instâncias aprovadas possam acessar o sistema, enquanto as demais são automaticamente restritas. Além disso, as agências podem implementar controles na camada de gerenciamento de identidade e acesso (IAM), usando listas de permissão para garantir que as versões corporativas sejam a única instância de uso da GenAI e para garantir que o acesso ocorra em ambientes seguros, como a plataforma de nuvem da Zscaler. Para ampliar ainda mais o acesso seguro, as instâncias corporativas da GenAI também podem ser disponibilizadas para dispositivos não gerenciados ou pessoais usando o acesso de dispositivos sem agentes da Zscaler.

Uma abordagem simples de "permitir tudo ou bloquear tudo" é insuficiente no cenário atual da IA generativa. As agências devem adotar uma estratégia de segurança em camadas com controles granulares adaptados às diferentes interações dos aplicativos. Consolidar essas funcionalidades em uma plataforma unificada não apenas agiliza a implementação, mas também simplifica a adesão aos princípios fundamentais de zero trust, garantindo acesso de privilégio mínimo, visibilidade contínua e proteção abrangente para cada interação com a GenAI.

Controle de acesso a instâncias autorizadas de aplicativos de IA



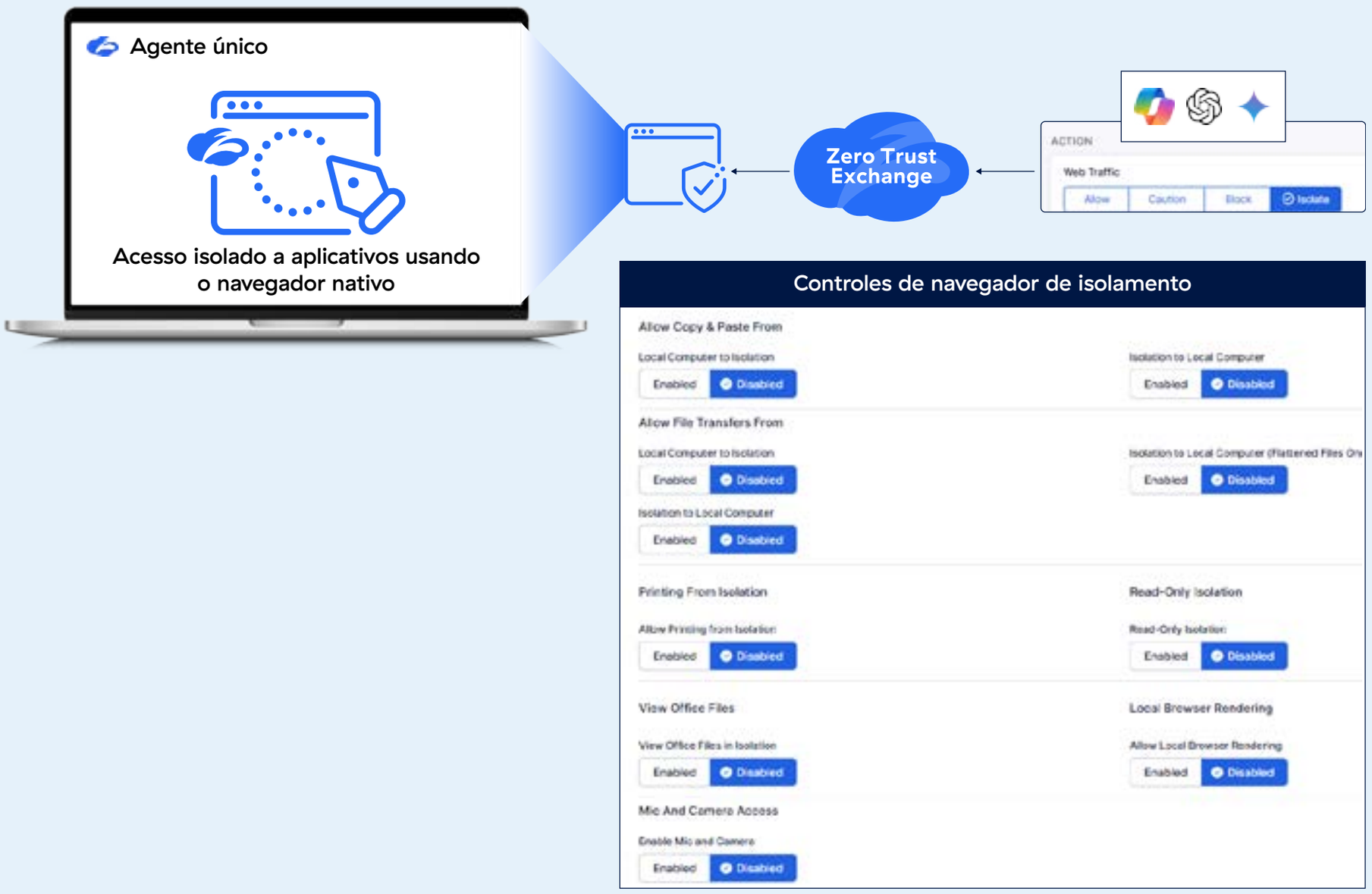
Reduza o risco de aplicativos de GenAI não autorizados

Quando for necessário acessar aplicativos de IA generativa que não sejam autorizados (ou seja, que não possuam licença corporativa e Single Sign-On (SSO)), esses aplicativos de GenAI devem ser tratados como de alto risco. Os dados carregados nesses aplicativos podem ser usados para treinar os modelos de GenAI, potencialmente expondo informações sigilosas. Para lidar com esse risco elevado, as agências devem implementar camadas adicionais de controles de segurança para garantir uma supervisão mais rigorosa das interações de dados.

A Zscaler oferece uma solução eficaz para gerenciar esse risco por meio do seu Zero Trust Browser. Essa ferramenta permite que as agências forneçam acesso seguro a aplicativos de GenAI não autorizados com controles avançados; por exemplo, limitar ações como transferência de arquivos, impressão e uso da área de transferência. Além disso, o Zero Trust Browser impede que os aplicativos de GenAI executem código diretamente no navegador dos usuários, renderizando as interações em páginas isoladas. Isso ajuda a proteger contra a coleta de impressões digitais, o rastreamento por cookies de terceiros e outras vulnerabilidades, permitindo que os usuários continuem usando o mesmo navegador implementado pela agência.

Essa abordagem pode ser implementada de duas maneiras: com o agente unificado da Zscaler ou usando um modelo sem agentes. Para dispositivos de propriedade da agência, recomenda-se uma implementação baseada em agentes para garantir que todo o tráfego seja roteado pela plataforma de aplicação de políticas da Zscaler. Em situações onde não é possível instalar um agente, a opção sem agentes da Zscaler oferece uma alternativa segura, garantindo acesso controlado aos aplicativos de GenAI sem comprometer a segurança.

Controles granulares para proteger aplicativos de IA isolados, equilibrando a experiência de usuário.



4. Implemente a proteção de dados desde o início

A falta de implementação de uma proteção de dados robusta desde o início da adoção da IA generativa pode resultar em violações de dados, descumprimento de regulamentações de privacidade e perda da confiança pública, comprometendo, em última análise, o sucesso dessas ferramentas. A natureza conversacional e amigável dos aplicativos públicos de IA generativa aumenta o risco de os usuários exporem involuntariamente dados governamentais sigilosos. Ações simples como copiar e colar informações ou carregar arquivos podem, sem uma supervisão cuidadosa, vazar detalhes confidenciais devido ao contexto ou à integração com outros sistemas. Isso destaca por que a incorporação de medidas robustas de proteção de dados deve ser uma parte essencial de qualquer estratégia pública de adoção da GenAI para governos estaduais e locais.

A Zscaler permite que as agências enfrentem esses riscos de frente com seus recursos avançados de prevenção contra perda de dados (DLP). Projetada para proteger informações sigilosas desde o início, a solução de DLP da Zscaler para IA generativa identifica e bloqueia o compartilhamento de dados confidenciais, seja por meio de um prompt, upload de arquivo ou uso indevido, antes que eles cheguem aos modelos públicos da GenAI. Essa abordagem proativa garante que as agências possam adotar a GenAI, protegendo informações sigilosas e mantendo a conformidade.

Acelerar a adoção da DLP

Iniciar uma jornada de proteção de dados pode parecer um desafio para muitas organizações, especialmente ao tentar equilibrar a necessidade de conceder acesso a ferramentas de GenAI com a implementação de medidas de segurança robustas. A Zscaler enfrenta esse desafio oferecendo uma plataforma simplificada, criada para dar suporte a equipes enxutas, permitindo a rápida adoção da IA generativa com controles eficazes de proteção de dados. Essa abordagem garante que as agências possam dimensionar sua estrutura de segurança de forma eficiente em diversos departamentos e bases de usuários.

Para agências que já possuem regras integradas aplicadas a outros destinos na internet, estender essas políticas aos aplicativos de GenAI é simples. A Zscaler também está integrando mecanismos de DLP e dicionários existentes, usados para outros canais, diretamente em aplicativos de IA e ML, reduzindo a redundância e acelerando a implementação. Se uma agência estiver começando do zero, a Zscaler fornece dicionários predefinidos que podem ser aplicados a aplicativos de GenAI com apenas alguns cliques para evitar o vazamento de dados sigilosos. Além disso, documentos ou conjuntos de dados conhecidos podem ser protegidos usando recursos de EDM/IDM, e a marcação da Microsoft Information Protection (MIP) pode proteger ainda mais os dados criptografados ou confidenciais contra exposição.

Para aprimorar ainda mais as políticas, os recursos de descoberta de aprendizado de máquina (ML) da Zscaler identificam informações sigilosas e vazamentos de dados anteriormente desconhecidos em aplicativos de GenAI, permitindo que as agências evoluam continuamente sua estratégia de proteção. Seja ajustando dicionários existentes ou criando regras de detecção personalizadas usando expressões regulares ou palavras-chave, as agências podem adaptá-las às suas necessidades. A Zscaler também se integra a soluções de backup de dados como a Rubrik, simplificando a identificação e a proteção de dados.

Implementação acelerada da DLP com a Zscaler

Implementar dia O

Dados específicos da agência com EDM e IDM

Dicionários predefinidos que devem ser usados por agências governamentais

- Números de roteamento bancário ABA
- Documento de finanças corporativas
- Documento jurídico corporativo
- Documento judicial
- Credenciais e segredos
- Cartões de crédito
- Informações sobre doenças
- Carteira de motorista (Estados Unidos)
- Informações sobre medicamentos
- Demonstrações financeiras
- Documento de imigração
- Documento de seguro
- Documento de fatura
- Documento jurídico
- Documento médico
- Informações médicas
- Documento imobiliário
- Números de segurança social (EUA)
- Documento fiscal
- Número de identificação fiscal (EUA)
- Documento do Departamento de Transportes e Veículos Motorizados
- Informações sobre tratamentos

Etiquetas de MIP / AP

Monitoramento contínuo e visibilidade

Identificar vazamentos de dados e aplicativos desconhecidos

Dados coletados de incidentes

Contribuições e feedback do usuário

Aprimorar e ajustar | Conforme necessário

Criar dicionário personalizado de expressões regulares / Palavra-chave

Palavras-chave simples e compostas com proximidade

Expandir EDM + IDM para soluções de backup de dados

A aplicação de políticas em tempo real e a visibilidade detalhada permitem que as equipes de TI protejam dados sigilosos sem complexidade adicional ou supervisão manual. Essa abordagem simplificada facilita a adoção rápida e confiante das ferramentas de GenAI, aproveitando seus benefícios de produtividade e, ao mesmo tempo, garantindo a conformidade e a confiança pública, em consonância com o princípio do zero trust: “Nunca confie, sempre verifique”.

Simplificar a governança da DLP

Um desafio comum na implementação da prevenção contra perda de dados (DLP), especialmente em grandes agências ou organizações de serviços compartilhados, é o volume de incidentes que as equipes de SOC e os proprietários dos dados precisam gerenciar. Esses incidentes podem variar desde a necessidade de acompanhamento por parte dos funcionários para justificar as ações, reforçar o treinamento dos usuários, lidar com exceções ou manter um registro de auditoria. Sem um sistema eficiente, isso pode rapidamente se tornar algo avassalador.

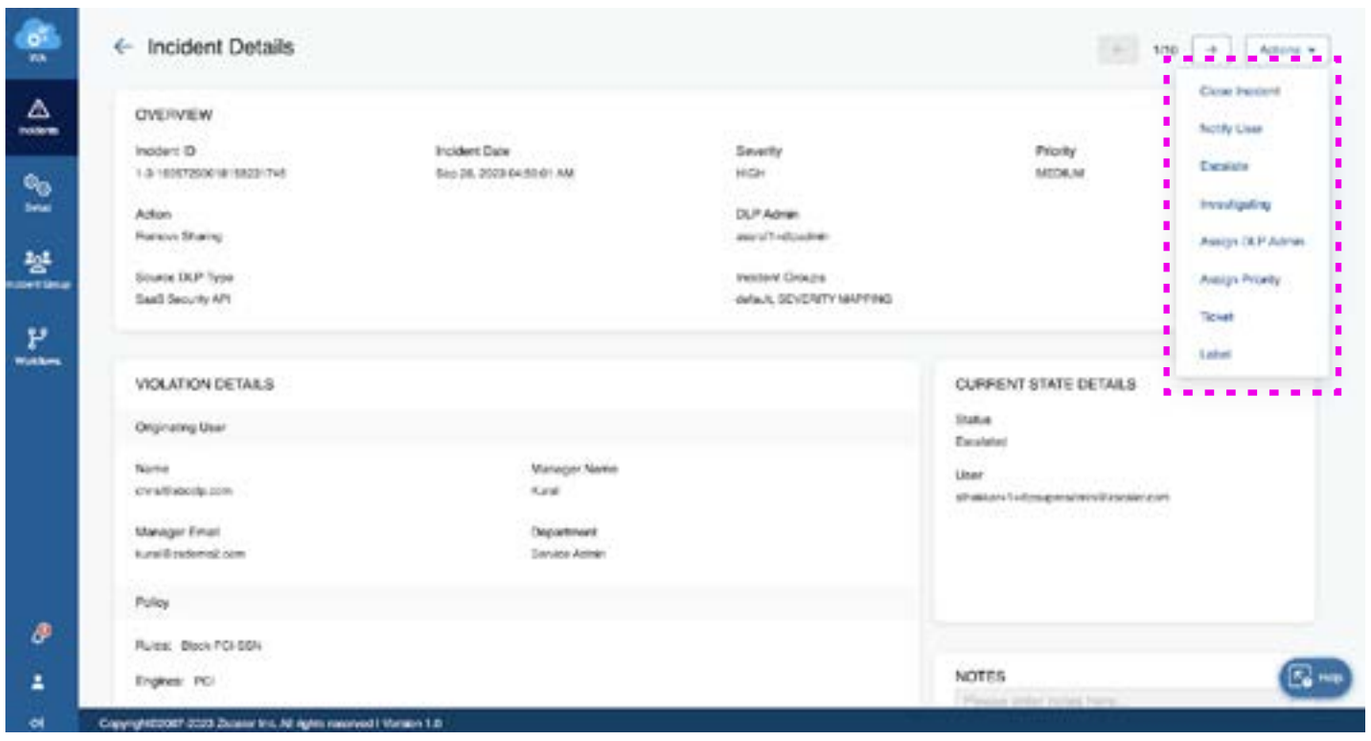
A automação do fluxo de trabalho simplifica esse processo, fornecendo uma solução centralizada para o gerenciamento de incidentes de proteção de dados relacionados a GenAI. Ela oferece uma visão completa de todos os incidentes em um só lugar, incluindo os metadados e detalhes das ações ou dados específicos que desencadearam a violação. Essa centralização permite que os administradores revisem, priorizem e corrijam incidentes rapidamente, conforme necessário.

Uma característica fundamental da automação do fluxo de trabalho é a sua capacidade de agrupar incidentes com base em características comuns e atribuir prioridades. Esses grupos podem então ser atribuídos a administradores específicos para oferecer uma resolução direcionada. A automação desempenha um papel importante nesse contexto, possibilitando fluxos de trabalho que notificam ou treinam os usuários finais envolvidos em incidentes, solicitam justificativas ou encaminham problemas para gerentes ou proprietários de dados para aprovação. Os fluxos de trabalho automatizados também podem acionar ações para solucionar incidentes sem intervenção manual.

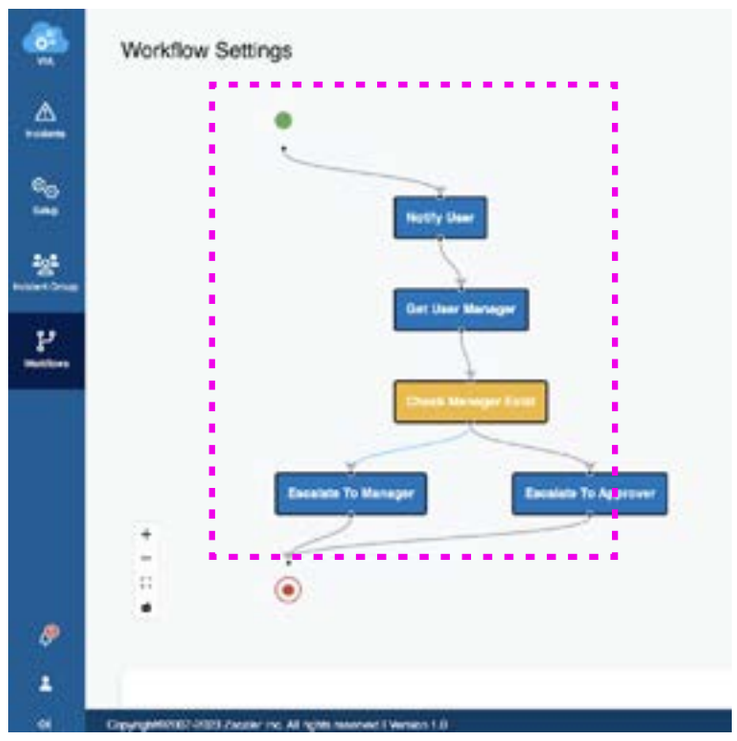
Ao aproveitar a automação do fluxo de trabalho na DLP, as agências podem reduzir significativamente os tempos de resolução, diminuir a carga operacional do SOC e obter insights práticos sobre áreas de risco. Essas informações podem ser usadas para aprimorar ainda mais as políticas ou melhorar os programas de treinamento, garantindo que os usuários estejam mais bem preparados para operar com segurança e reduzindo a probabilidade de incidentes futuros.

Otimize o gerenciamento de incidentes com gerenciamento de casos e treinamento de usuários

Gerencie, atribua e escale incidentes com facilidade



Defina rotinas para fluxos de trabalho



5. Reuna tudo e use uma abordagem em camadas

Governos estaduais e locais estão adotando a IA generativa (GenAI) para oferecer novas eficiências e melhorar os serviços, mas fazer isso com segurança é essencial. Com milhares de ferramentas de IA disponíveis, além de riscos como vazamento de dados e uso não autorizado, as agências precisam de uma estratégia clara que priorize a segurança, integre os princípios de zero trust e, ainda assim, permita a produtividade. Uma abordagem em camadas simplifica esse processo, agrupando aplicativos com base no risco, aplicando controles de segurança personalizados e automatizando o gerenciamento de incidentes para reduzir a pressão sobre as equipes de TI. Essa estratégia ajuda as agências a proteger dados sigilosos, otimizar operações e capacitar os usuários a aproveitar com segurança os aplicativos de GenAI, tudo dentro de uma estrutura dimensionável e gerenciável.

Implementar controles em camadas

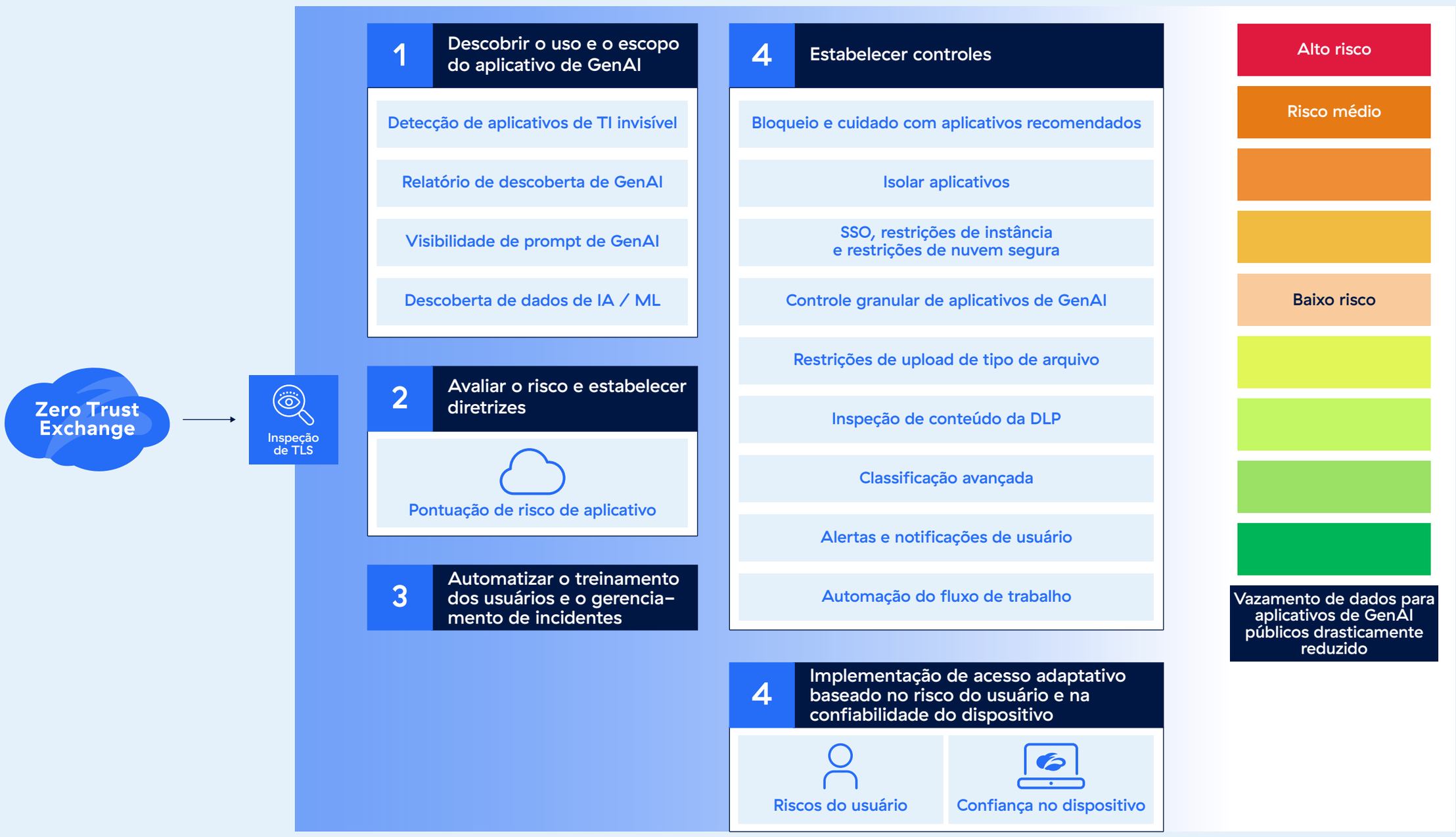
Nesta seção, exploraremos como as agências podem reunir os vários elementos da adoção segura da IA generativa usando uma abordagem em camadas. Com milhares de ferramentas de GenAI já disponíveis e novas sendo lançadas a cada semana, o gerenciamento de políticas e incidentes pode rapidamente se tornar algo avassalador sem uma estratégia bem planejada.

Uma abordagem em camadas simplifica esse processo, organizando o acesso e implementando controles de dados adaptados aos níveis de risco. Este método não apenas reduz a carga de trabalho dos administradores de segurança, como também minimiza significativamente os riscos de vazamento de dados e diminui o número de incidentes que as equipes de TI e segurança precisam resolver. Ao adotar essa abordagem estruturada, as organizações podem aproveitar o poder da GenAI de forma segura e eficaz, mantendo a eficiência operacional.

Conforme discutido anteriormente, ferramentas como a descoberta de aplicativos de TI invisível, os relatórios de descoberta de GenAI e a visibilidade de prompts da GenAI fornecem informações valiosas sobre como as políticas de IA devem evoluir e como os controles de segurança podem ser personalizados para atender às necessidades em constante mudança. Essas informações formam a base para uma abordagem prática e estruturada no gerenciamento de aplicativos de GenAI.

Uma forma útil de implementar essa abordagem é categorizar os aplicativos de GenAI em três grupos: risco alto, risco médio e risco baixo. Aplicativos de risco alto devem ser bloqueados completamente para evitar a exposição a vulnerabilidades desnecessárias. Aplicativos de risco médio podem ser acessados com controles de segurança reforçados, como isolamento do navegador e medidas de proteção de dados mais rigorosas. Aplicativos de risco baixo podem ter o acesso nativo permitido, mas com restrições focadas no conteúdo específico ou nas ações que os usuários podem realizar.

Abordagem em camadas para proteger aplicativos de IA



Essa estrutura permite que as agências adotem uma abordagem zero trust para a GenAI. Nesse modelo, aplicativos desconhecidos, recém-lançados ou não aprovados são bloqueados por padrão. Os aplicativos aprovados, mas não autorizados, são isolados com camadas de segurança adicionais, enquanto os aplicativos totalmente autorizados se beneficiam de uma experiência de usuário mais integrada, com proteções personalizadas. Para facilitar a implementação e o gerenciamento, as agências podem usar ferramentas como etiquetas de aplicativos personalizadas e perfis de risco. Essas ferramentas permitem que as equipes de segurança definam políticas predefinidas que se aplicam automaticamente aos aplicativos com base no risco atribuído a eles. Ao simplesmente rotular um aplicativo, as políticas apropriadas são aplicadas, minimizando o esforço administrativo e mantendo um controle robusto.

Automatizar fluxos de trabalho de incidentes

Outro fator crítico a ser considerado é o gerenciamento de incidentes. É essencial que as agências reduzam o número de incidentes que o Centro de Operações de Segurança (SOC) ou os administradores de dados precisam assimilar manualmente. Violações de gravidade média e baixa, por exemplo, devem ser registradas para fins de auditoria e encerradas automaticamente, sem necessidade de intervenção manual significativa. No entanto, como essas infrações ainda representam violações de políticas, os usuários devem ser notificados e questionados sobre a justificativa; uma medida essencial para reforçar o treinamento dos usuários e promover a responsabilização.

Com a Zscaler, as políticas de inspeção de conteúdo para GenAI permitem que as agências definam o nível de gravidade das violações, que são então repassadas para ferramentas de automação de fluxo de trabalho. Essa funcionalidade permite que os administradores criem fluxos de trabalho personalizados de acordo com a gravidade de cada incidente. Atributos adicionais, como gravidade e outras características compartilhadas, podem ser usados para categorizar incidentes em grupos, e esses grupos podem ser vinculados a fluxos de trabalho automatizados. Essa abordagem simplifica o processamento de incidentes, garantindo que as violações sejam tratadas adequadamente e, ao mesmo tempo, aliviando significativamente a carga de trabalho das equipes do SOC.

Considerações finais

As agências governamentais precisam estar na vanguarda para aproveitar os aplicativos de IA generativa (GenAI) para transformar operações, capacitar funcionários e melhor servir os cidadãos. No entanto, a sua adoção deve ser sustentada por uma arquitetura zero trust. Ao garantir que cada usuário, dispositivo e interação seja verificado, monitorado e controlado (independentemente da localização ou aplicativo), as agências podem proteger com confiança as iniciativas de IA generativa, tendo como pilares de sua estratégia uma proteção de dados robusta, governança clara e experiências de usuário otimizadas.

A Zscaler permite que as agências governamentais aproveitem os benefícios de produtividade da GenAI com uma abordagem segura e em camadas que simplifica a governança, agiliza a implementação e incorpora segurança robusta em cada interação. Ao estabelecer estruturas de governança de IA, automatizar a descoberta e o gerenciamento de aplicativos de GenAI, controlar o uso de instâncias de aplicativos de GenAI e implementar recursos avançados de DLP desde o início, as agências podem reduzir drasticamente os riscos e dimensionar suas estratégias de adoção com o mínimo de sobrecarga para as equipes de TI e segurança.

À medida que o cenário da GenAI continua a evoluir, os líderes das agências são incentivados a adotar uma abordagem estratégica e em fases para a sua implementação. Comece garantindo o acesso a aplicativos públicos de IA generativa, e desbloqueie produtividade com segurança com a IA agêntica (documento futuro). Por fim, exploraremos como estender com segurança os recursos da GenAI para serviços centrados no cidadão, garantindo que os sistemas permaneçam seguros em todas as etapas. Com a Zscaler, as agências podem implementar essas fases com confiança, acelerando a inovação e, ao mesmo tempo, mantendo os mais altos padrões de segurança e conformidade de dados.

Entre em contato com sua equipe de conta da Zscaler ou fale conosco para agendar um workshop específico para a sua organização.

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

zscaler™

Zero Trust Everywhere