Adozione sicura della GenAI con lo zero trust:

Utilizzo sicuro delle applicazioni di GenAI pubbliche

©2025 Zscaler, Inc. Tutti i diritti riservati.

WHITE PAPER

Indice

©2025 Zscaler, Inc. Tutti i diritti riservati.

Introduzione

L’IA generativa (GenAI) sta rivoluzionando il modo di operare dei governi, consentendogli di migliorare la produttività, semplificare i processi e servire al meglio i cittadini. Ma per sfruttare il potenziale trasformativo della GenAI, e mitigarne al contempo i rischi intrinseci che può comportare, gli enti pubblici devono applicare i principi dello zero trust. Questo paradigma garantisce che nessuna entità, umana o meccanica, venga considerata attendibile per impostazione predefinita, assicurando una visibilità continua e una verifica rigorosa di ogni interazione.

Questo white paper è il primo della serie “Adozione sicura della GenAI con lo zero trust”, che offre una strategia completa progettata per supportare gli enti governativi nell’affrontare in sicurezza il panorama della GenAI. La serie comprende tre fasi:

- La 1° fase, che viene delineata in questo documento, si concentra sulla protezione delle applicazioni di GenAI pubbliche, per affrontare rischi come la fuga dei dati e l’utilizzo non autorizzato dell’IA (la cosiddetta “shadow AI”, o “IA ombra”).

- La 2° fase esplorerà l’adozione degli strumenti di IA agentica per incrementare la produttività dei dipendenti in modo sicuro.

- La 3° fase si concentrerà sull’implementazione sicura dei sistemi di GenAI per i servizi ai cittadini, per garantire la protezione dei sistemi e dei dati governativi.

Ogni fase enfatizza un approccio proattivo e multilivello per bilanciare l’innovazione con una governance e una sicurezza ben strutturate.

©2025 Zscaler, Inc. Tutti i diritti riservati.

Utilizzo sicuro della GenAI pubblica

Panoramica

I governi sono sempre più consapevoli del potenziale trasformativo dell'intelligenza artificiale generativa (GenAI) per le loro operazioni e i servizi che forniscono ai cittadini. Questa tecnologia offre la possibilità di ottenere significativi guadagni in termini di produttività e di far evolvere i servizi ai cittadini in diversi ambiti. Questi ultimi vanno dalla comprensione dell'opinione pubblica e dalla fornitura di chatbot basati sull'IA per l'assistenza ai cittadini e all'IT, alla facilitazione della traduzione linguistica e all'automazione dei processi interni, come scrivere le descrizioni delle offerte di lavoro, riassumere le riunioni e creare annunci pubblici.

Coloro che hanno adottato per primi questa dirompente tecnologia all'interno della pubblica amministrazione stanno già notando miglioramenti nell'esperienza e nella soddisfazione dei dipendenti. L'emergere di modelli linguistici di grandi dimensioni (LLM) accessibili al pubblico, come ChatGPT, ha stimolato la sperimentazione nel settore pubblico, perché le organizzazioni cercano di comprendere e sfruttare le capacità dell'IA. Questo interesse diffuso sottolinea le opportunità di migliorare l'efficienza e l'erogazione dei servizi attraverso l'integrazione di questi strumenti avanzati di IA.

L'integrazione della GenAI, in particolare attraverso LLM pubblici e modelli di terze parti, introduce però anche delle criticità in termini di sicurezza. L'uso non autorizzato di strumenti di IA ("shadow AI") può esporre i dati sensibili dei cittadini, le documentazioni aziendali o la proprietà intellettuale. Il rischio è ulteriormente amplificato dai flussi di lavoro che coinvolgono il protocollo RAG (Retrieval Augmented Generation) o MCP (Model Content Protocol) e gli agenti di IA, compromettendo potenzialmente i dati sensibili e ponendo rischi per la sicurezza nazionale che derivano dalla possibilità che utenti malintenzionati con il supporto di Stati nazionali o entità malevole sfruttino queste vulnerabilità per attività quali lo spionaggio, il sabotaggio o l'interruzione delle infrastrutture critiche. Inoltre, la GenAI presenta una superficie di attacco molto estesa che le misure di sicurezza tradizionali, che spesso si basano su controlli binari restrittivi o non offrono una visibilità completa sui diversi ambienti, non sono in grado di gestire in modo efficace.

Per sfruttare il potenziale della GenAI, gli enti pubblici dovrebbero adottare un approccio zero trust che offra massimi livelli di sicurezza, visibilità e semplicità d'uso. I seguenti passaggi delineano un processo che gli enti pubblici possono adottare per sfruttare la GenAI, mitigando proattivamente i rischi di fuga dei dati ed evitando un carico di lavoro eccessivo sui team di sicurezza:

1. Definire quadri di rifermento e policy per la governance dell'IA
2. Integrare strettamente l'esperienza utente e la formazione
3. Scegliere l'architettura giusta e dare la priorità alla sicurezza
4. Implementare la protezione dei dati fin dal principio
5. Utilizzare un approccio multilivello alla protezione

Analizziamo questi passaggi più nel dettaglio.

©2025 Zscaler, Inc. Tutti i diritti riservati.

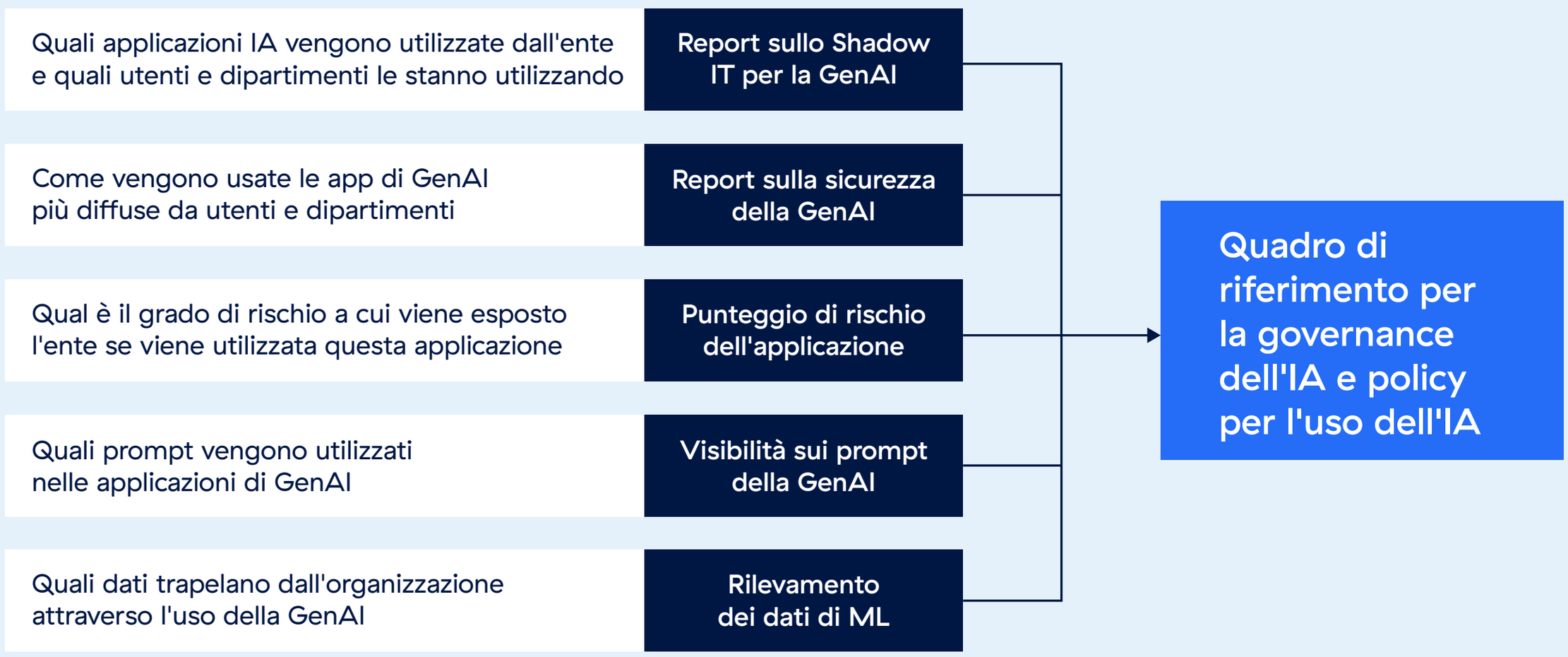
1. Definire quadri di rifermento e policy per la governance dell'IA

Per sfruttare appieno i vantaggi della GenAI, gli enti pubblici devono implementare misure di sicurezza ber strutturate, che affrontino direttamente i rischi senza ostacolare la produttività degli utenti. Questa sezione esplora come gli enti pubblici possono adottare un approccio zero trust per le applicazioni di GenAI, garantendo al contempo che i controlli di sicurezza non ostacolino la fluidità dell'esperienza utente.

Lo sviluppo di quadri di riferimento e policy per la governance dell'IA è essenziale per garantire l'adozione della GenAI all'interno degli enti statali. Ciò spesso comporta la creazione di una task force o di un organo di governance dedicato per supervisionare lo sviluppo e l'attuazione delle policy. Ad esempio, l'Alabama GenAI Task Force funge da modello con il suo approccio collaborativo e interfunzionale. Per guidare il proprio impegno in tal senso, gli enti pubblici dovrebbero inoltre sfruttare framework zero trust consolidati, come il modello di maturità zero trust della CISA e lo standard NIST 800–207, insieme a framework di sicurezza specifici per l'IA come l'AI Risk Management Framework (AI RMF) del NIST, che pone l'accento sulle funzioni fondamentali come la governance, la mappatura, la misurazione e la gestione, o il TRISM di Gartner. Adottando una task force dedicata e utilizzando questi framework collaudati, gli enti pubblici possono accelerare l'integrazione sicura delle tecnologie di GenAI tra i vari dipartimenti.

Per supportare questo processo, Zscaler fornisce approfondimenti utili che aiutano gli enti pubblici a monitorare l'utilizzo dell'IA nei loro ambienti, a valutare i potenziali rischi legati alle applicazioni di GenAI e a identificare i casi che possono comportare la fuga di dati. Sfruttando i report di Zscaler, gli enti pubblici possono accedere a informazioni essenziali sulle attuali modalità di utilizzo degli strumenti di GenAI.

I punti dati forniti da Zscaler per supportare la creazione di un quadro di riferimento per la governance dell'IA e di una policy di utilizzo dell'IA



©2025 Zscaler, Inc. Tutti i diritti riservati.

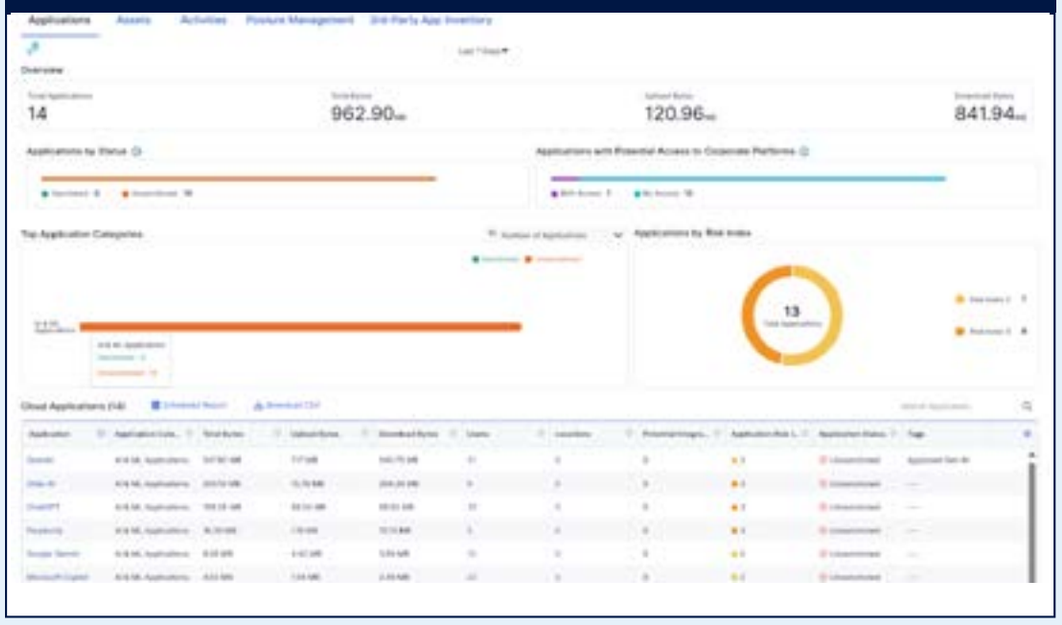
Comprendere l’utilizzo attuale dell’IA

Comprendere l’utilizzo attuale dell’IA è un passaggio fondamentale per la creazione di quadri di rifermento per la governance. Analizzando quali applicazioni di GenAI vengono utilizzate, come vengono impiegate e i fattori di rischio associati, gli enti pubblici possono identificare dove sono maggiormente necessarie delle policy. Questo approccio basato sui dati garantisce che il quadro di rifermento rimanga pertinente, attuabile e personalizzato per affrontare in modo efficace le sfide e le opportunità specifiche di un dato ente.

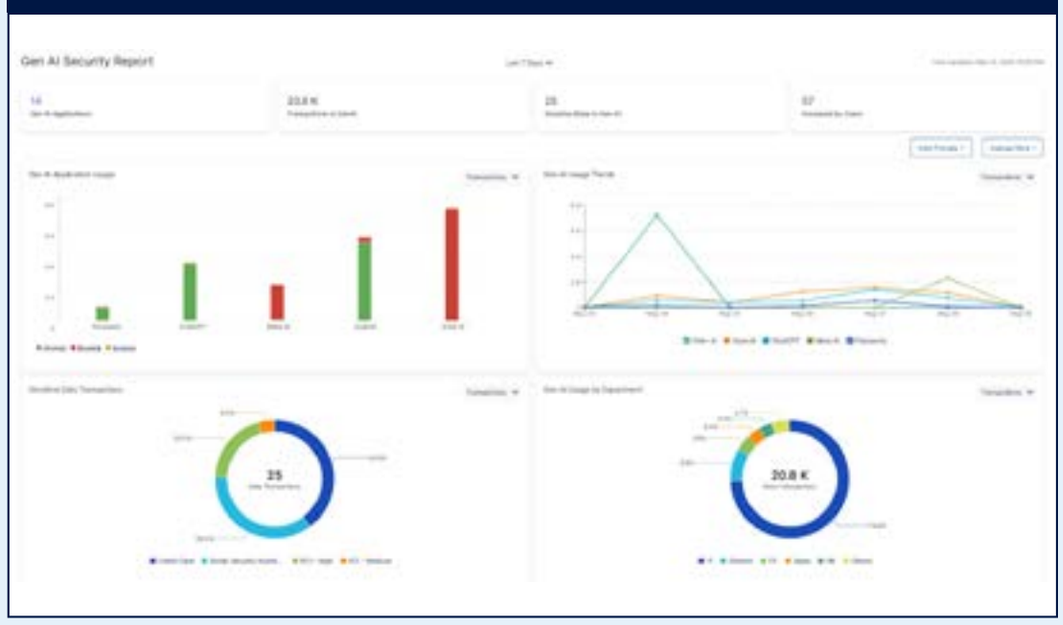
Zscaler fornisce report dettagliati sull’uso dell’IA che indicano in modo trasparente quali sono le applicazioni di GenAI utilizzate dagli enti pubblici e la portata del relativo utilizzo. Queste approfondimenti utili possono essere ulteriormente segmentati per mostrare i modelli di utilizzo all’interno di dipartimenti specifici o sezioni distaccate, offrendo alle organizzazioni una visione più chiara del proprio modello di utilizzo dell’IA.

Approfondimenti sull’utilizzo della shadow AI

Rilevamento delle app Shadow IT per la GenAI



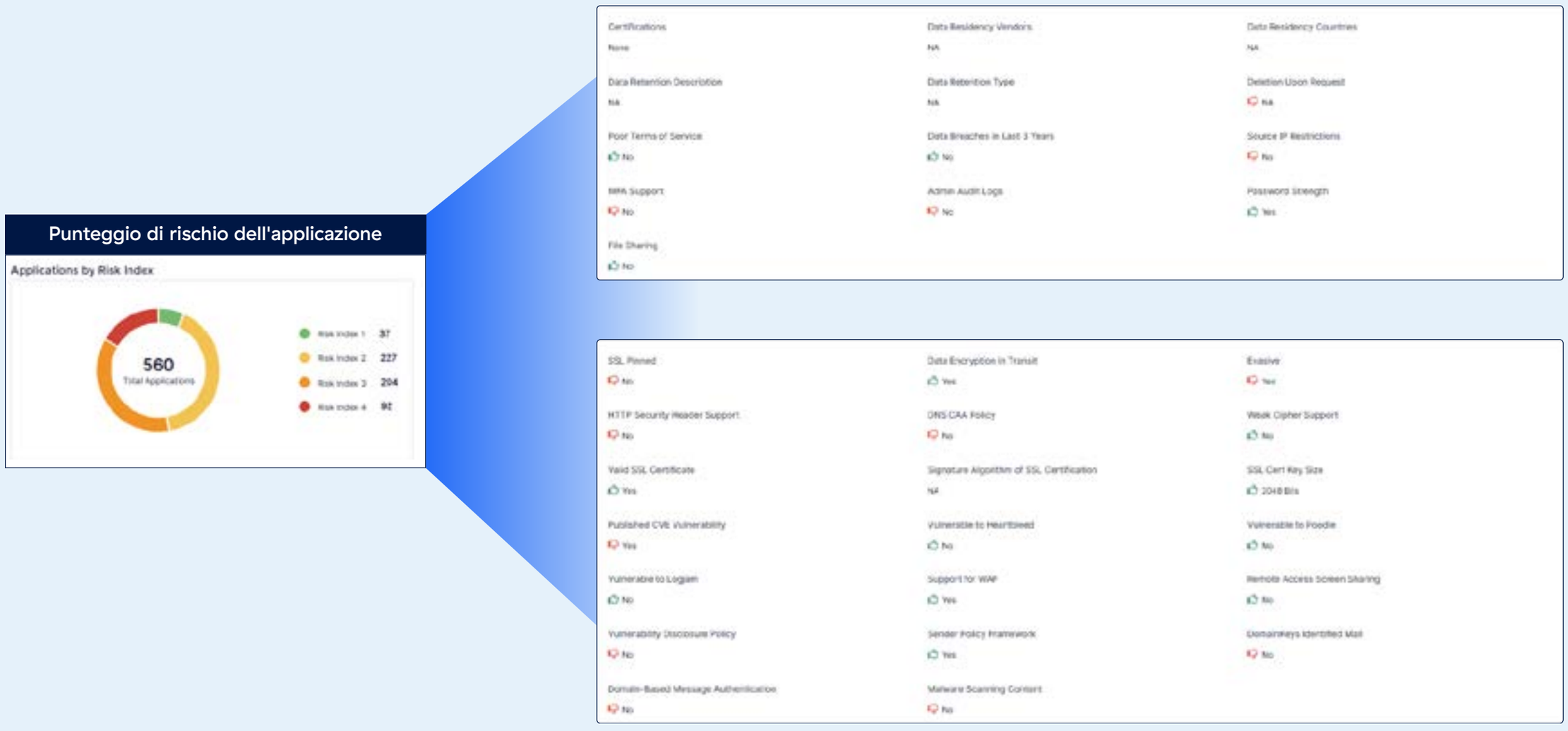
Report sulla sicurezza della GenAI



Grazie a questa visibilità, gli enti pubblici hanno la possibilità di analizzare più a fondo i fattori di rischio associati a queste applicazioni. Il team ThreatLabz di Zscaler, in coordinamento con l’intelligence sulle minacce di terze parti, valuta questi rischi e assegna dei punteggi aggregati che vanno da 1 a 5, semplificando l’analisi del rischio per i responsabili decisionali. Gli enti pubblici godono inoltre della flessibilità di personalizzare tali punteggi in base alle proprie priorità ed esigenze specifiche. Le valutazioni del rischio possono includere fattori chiave quali le vulnerabilità della sicurezza o i problemi correlati alla conformità alle normative, consentendo agli organi decisionali di concentrare le proprie risorse sulle aree più rilevanti per la loro missione e le loro esigenze di sicurezza. Più avanti nel report sono riportati alcuni esempi di fattori di rischio, come le vulnerabilità della sicurezza o la mancanza di conformità alle normative, che consentono agli organismi decisionali dell’ente di dare la priorità alle aree interne più determinanti.

©2025 Zscaler, Inc. Tutti i diritti riservati.

Rischio associato all’utilizzo della shadow AI



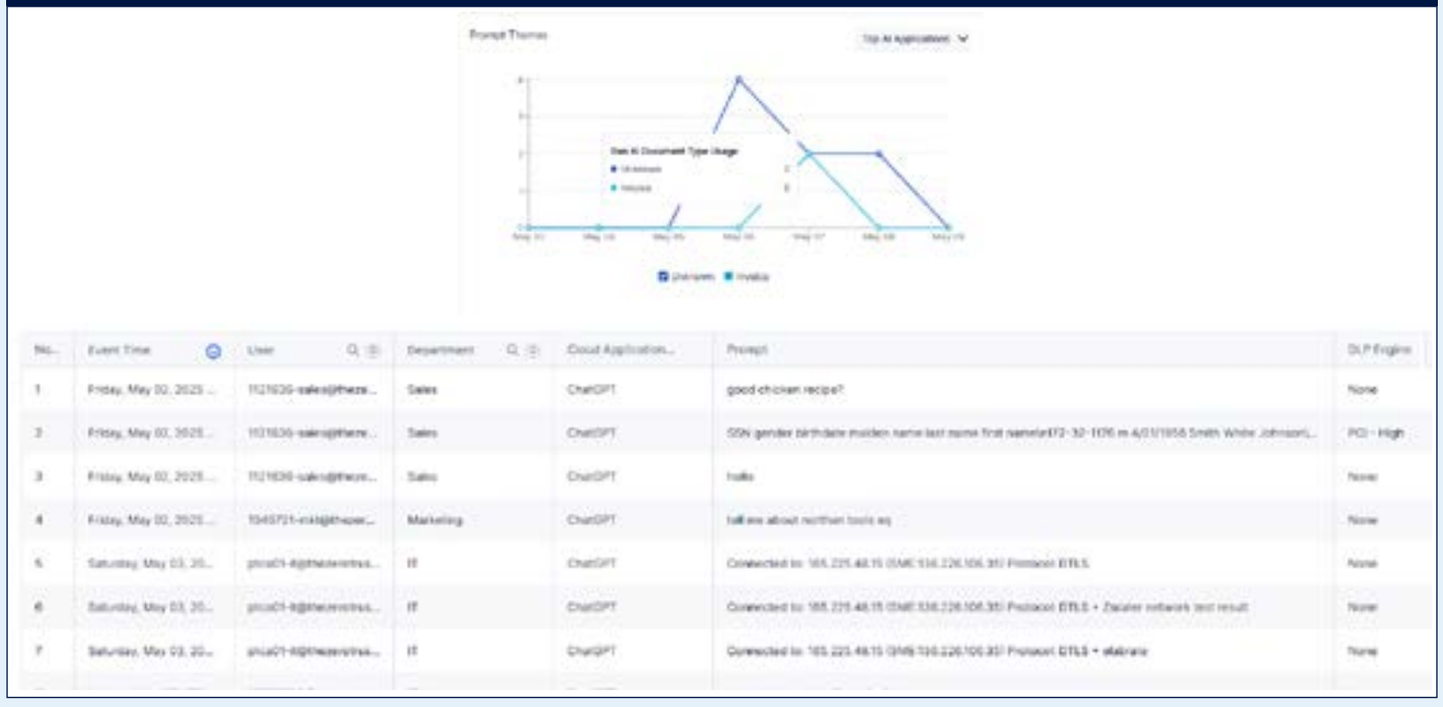
Approfondimenti dettagliati sulle interazioni degli utenti con le applicazioni di GenAI

Zscaler va oltre la visibilità a livello di applicazione, fornendo informazioni dettagliate su ogni transazione, richiesta e interazione dell’utente all’interno delle applicazioni di GenAI. Ciò include dati dettagliati su ciò che gli utenti inseriscono non solo tramite i trasferimenti di file, ma anche mediante metodi quali immissioni da tastiera, attività negli appunti e altri input supportati. Queste informazioni sono preziose per gli enti pubblici, poiché li aiutano a comprendere meglio il tipo di dati che vengono condivisi, a perfezionare le policy di sicurezza e a garantire la conformità agli standard di governance. Inoltre, un tale grado di visibilità è essenziale ai fini dell’audit e può essere esportato senza problemi nel sistema SIEM dell’ente per un monitoraggio e un’analisi più completi.

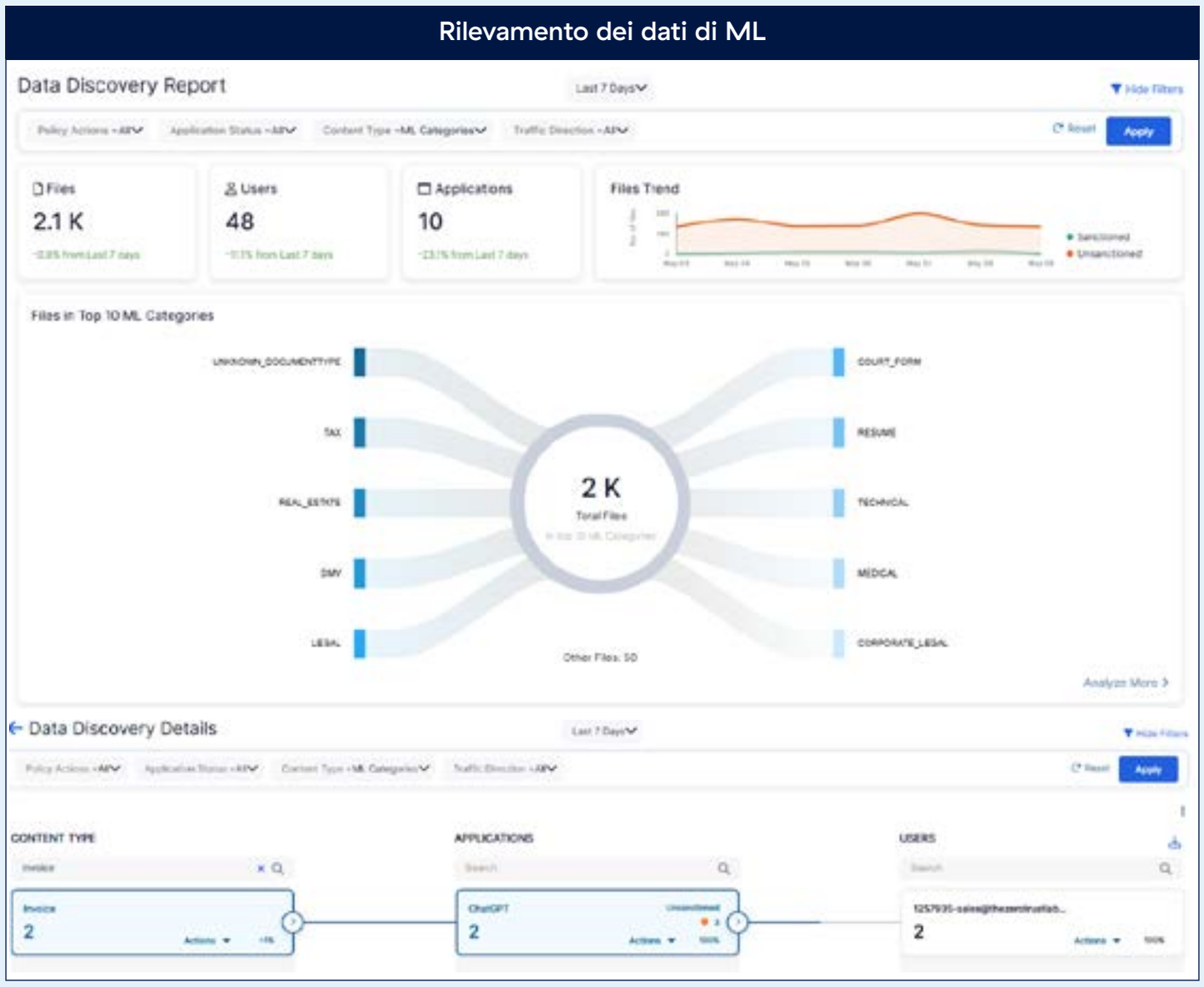
©2025 Zscaler, Inc. Tutti i diritti riservati.

Segnalazione delle fughe di dati in corso al di fuori dell’ente

Visibilità sui prompt della GenAI



Rilevamento dei dati di ML



Visibilità sui dati sconosciuti

Zscaler accresce ulteriormente la visibilità identificando i dati che trapelano attraverso le applicazioni di GenAI all’insaputa degli enti pubblici stessi. Utilizzando funzionalità alimentate da IA ed ML, il report ML Discovery di Zscaler va oltre le tradizionali regole di“solo monitoraggio” della DLP per rilevare e classificare in modo proattivo i dati sensibili condivisi con gli strumenti di GenAI pubblici. Ciò consente ai proprietari dei dati e agli amministratori della sicurezza di individuare le fughe di dati sconosciute o non riconosciute e di affrontarle prima che si trasformino in problemi critici.

©2025 Zscaler, Inc. Tutti i diritti riservati.

Questa visibilità avanzata sui dati consente agli enti pubblici di identificare in modo proattivo i dati ad alto rischio che potrebbero essere esposti agli LLM pubblici. Aiuta inoltre a stabilire o perfezionare la proprietà delle informazioni sensibili, a sviluppare policy di utilizzo e a implementare linee guida personalizzate per proteggere i set di dati chiave.

Combinando informazioni su utenti, applicazioni, rischi associati alle applicazioni, prompt e modelli di dati, Zscaler supporta la creazione di policy e procedure specifiche in linea con gli obiettivi dell'organizzazione. Queste informazioni guidano l'allocazione delle risorse e aiutano a definire i ruoli e le responsabilità all'interno del quadro di riferimento per la governance zero trust, consentendo agli enti pubblici di adottare un approccio lungimirante, che bilanci l'innovazione con la definizione di una strategia completa per la mitigazione del rischio.

2. Integrare strettamente l'esperienza utente e la formazione

L'esperienza utente e la formazione svolgono un ruolo centrale nell'adozione sicura e disuccesso dell'IA generativa (GenAI) all'interno degli enti pubblici statali. Per garantire un'adozione senza intoppi, è essenziale che le misure di sicurezza e la formazione degli utenti siano progettate in modo da consentirgli di rimanere produttivi, offrendo comunque una protezione efficace. Quando è possibile, si dovrebbe evitare di introdurre un altro strumento o un'altra applicazione, in particolare quelli che potrebbero rivelarsi particolarmente complessi da usare per gli utenti. Inoltre, per massimizzarne l'impatto, i controlli di sicurezza efficaci devono essere abbinati a una formazione continua degli utenti. Le piattaforme dovrebbero integrarsi in modo ottimale con i flussi di lavoro e i canali esistenti, incorporando al contempo meccanismi di interazione e feedback da parte degli utenti. Ciò aiuterà gli enti pubblici ad allinearsi fin dal principio a quadri normativi come l'AI Risk Management Framework (AI RMF) del NIST.

Ecco alcune delle funzionalità chiave della piattaforma che supportano questo approccio:

Un accesso ottimale alla GenAI

L'obiettivo principale degli strumenti di GenAI è liberare gli utenti da compiti ripetitivi per consentirgli di concentrarsi sulle attività che traggono vantaggio dal giudizio umano. Le misure di sicurezza per la GenAI non devono quindi interrompere i flussi di lavoro degli utenti. Zscaler rende tutto questo molto più semplice, eliminando la necessità di ricorrere a software aggiuntivi o browser gestiti. Per esempio:

- **Un unico agente di Zscaler**
  Lo stesso agente Zscaler che garantisce un accesso sicuro alle applicazioni pubbliche e private gestisce anche i controlli della GenAI, garantendo un accesso, fluido senza dover ricorrere a strumenti aggiuntivi.

- **Accesso sicuro agentless**
  Gli utenti possono utilizzare il proprio browser nativo e il proprio flusso di lavoro esistente (ad esempio il riquadro del portale dell'app IDP) per accedere alle applicazioni di GenAI protette senza il bisogno di un agente.

©2025 Zscaler, Inc. Tutti i diritti riservati.

- **Controlli di sicurezza flessibili**
  Invece di affidarsi solo alle opzioni “consenti o blocca” per l’utilizzo dell’IA, Zscaler offre l’isolamento del browser con base cloud. Questa funzionalità reindirizza gli utenti che accedono alle applicazioni di GenAI a un ambiente browser isolato, ospitato nel cloud di Zscaler. Ciò consente agli utenti di mantenere un’esperienza ottimale di navigazione, sebbene al contempo vengano applicate misure di sicurezza avanzate, come la prevenzione dell’attività degli appunti, della stampa o del caricamento di file. Questo approccio garantisce che le policy di sicurezza vengano applicate senza ledere l’esperienza utente, e il tutto viene gestito tramite una piattaforma unificata e un unico agente di Zscaler per semplificare l’amministrazione.

Questi controlli possono essere implementati con un impatto minimo sull’infrastruttura o sugli endpoint esistenti, consentendo agli enti pubblici di implementare le proprie policy di sicurezza, preservando al contempo un’esperienza utente fluida e riducendo al minimo le operazioni amministrative.

Un agente universale per supportare l’accesso nativo e isolato

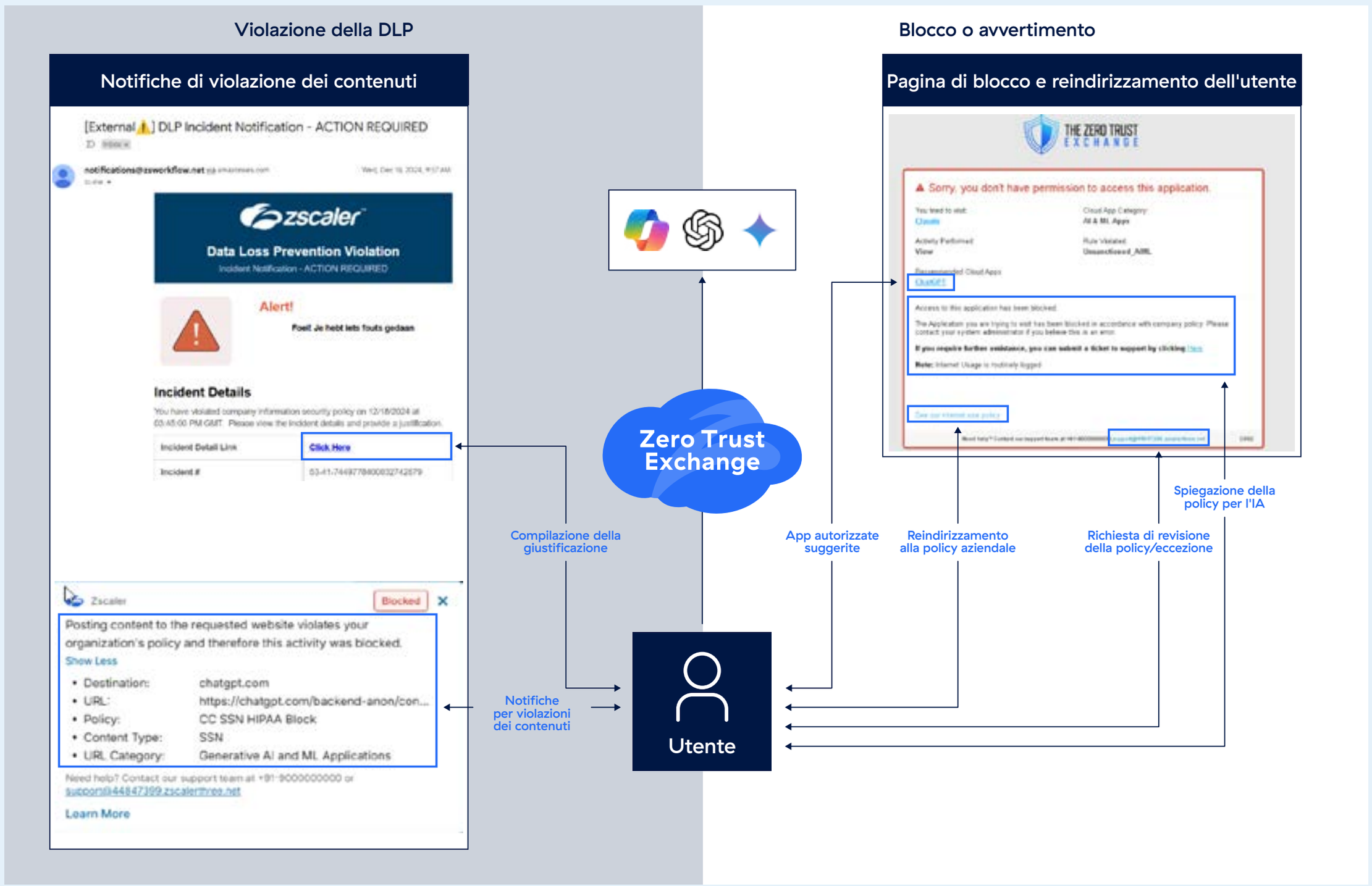
©2025 Zscaler, Inc. Tutti i diritti riservati.

Formazione e feedback integrati per gli utenti

Una formazione continua sull’uso sicuro e sulle violazioni correlate alla GenAI è essenziale, soprattutto data la rapida evoluzione di questa tecnologia. La formazione deve essere periodica, continua e integrata direttamente nel flusso di lavoro e negli strumenti nativi dell’utente. Zscaler supporta questa funzionalità tramite notifiche dinamiche, ovvero quando una risorsa viene bloccata, isolata o segnalata per delle violazioni nel contenuto, gli utenti ricevono delle allerte personalizzate. Ad esempio, se un’applicazione di GenAI non autorizzata viene bloccata, Zscaler suggerisce le soluzioni analoghe che sono invece approvate, contribuendo a reindirizzare il comportamento degli utenti, preservando al contempo la produttività. Negli scenari in cui avviene una violazione correlata all’utilizzo dei dati, Zscaler si integra in strumenti molto diffusi, come le e-mail e Slack, per consentire agli utenti di fornire le eventuali giustificazioni in modo più semplice o facilitare la ricezione di feedback personalizzati, che vengono integrati in strumenti già ampiamente in uso.

Integrando la formazione degli utenti nei flussi di lavoro di sicurezza, gli enti pubblici possono gettare solide basi di governance per le applicazioni di GenAI. Questo approccio non solo garantisce che gli utenti comprendano come interagire in modo sicuro con questa tecnologia, ma aiuta anche a creare un quadro di riferimento scalabile per gestire gli incidenti correlati alla GenAI e perfezionare le policy di utilizzo dell’IA in tutta l’organizzazione.

Formazione e feedback degli utenti con Zscaler



©2025 Zscaler, Inc. Tutti i diritti riservati.

3. Dare la priorità alla sicurezza e scegliere l'architettura giusta

Data l'espansione della superficie di attacco, dovuta all'adozione diffusa degli strumenti IA, è fondamentale per le organizzazioni scegliere una piattaforma che non solo protegga dalle minacce basate sull'IA, ma che consenta anche l'uso sicuro delle applicazioni di GenAI, si basi su un'architettura zero trust e disponga dell'autorizzazione FedRAMP. Zscaler offre una soluzione completa che unisce sicurezza, usabilità e conformità per gli enti pubblici che adottano la GenAI.

Gli enti pubblici possono iniziare a sfruttare le funzionalità di GenAI sicure di Zscaler, apportando modifiche minimali alla loro infrastruttura esistente. Il traffico può essere inoltrato alla piattaforma tramite l'app Zscaler, che è compatibile con i principali sistemi operativi, tra cui Windows, Mac, iOS, Android e Linux, oppure tramite un dispositivo dedicato per la filiale o semplicemente un browser per la distribuzione agentless.

Una volta eseguita la connessione, Zscaler garantisce che gli utenti vengano autenticati e autorizzati prima che possano accedere a una qualsiasi risorsa su Internet, comprese le applicazioni di GenAI. Agendo da proxy, Zscaler ispeziona tutte le sessioni TLS stabilite con le applicazioni di GenAI, offrendo agli enti pubblici una visibilità completa e un controllo granulare sul modo in cui gli utenti interagiscono con questi strumenti. Questa architettura consente agli enti pubblici di disporre di informazioni approfondite su come gli utenti utilizzano le applicazioni di GenAI e di implementare molteplici controlli all'avanguardia nel settore per proteggere i propri dati.

Ispezione HTTPS e websocket sicura con Zscaler

Controllo di accesso

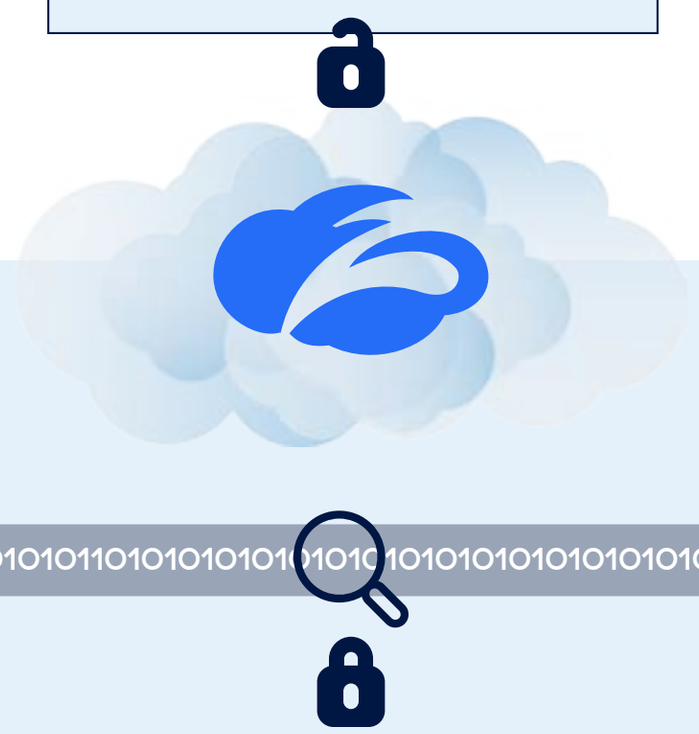
- Filtro URL
- Firewall cloud
- Controlli granulari delle app cloud
- Restrizioni della tenancy
- Sicurezza DNS

Prevenzione delle minacce

- Protezione da malware
- Cloud Sandbox
- Protezione dalle minacce avanzate
- Cloud Browser Isolation

Protezione dei dati

- DLP in linea
- EDM / IDM
- Controlli del tipo di file
- Controlli della GenAI
- Cloud Browser Isolation



©2025 Zscaler, Inc. Tutti i diritti riservati.

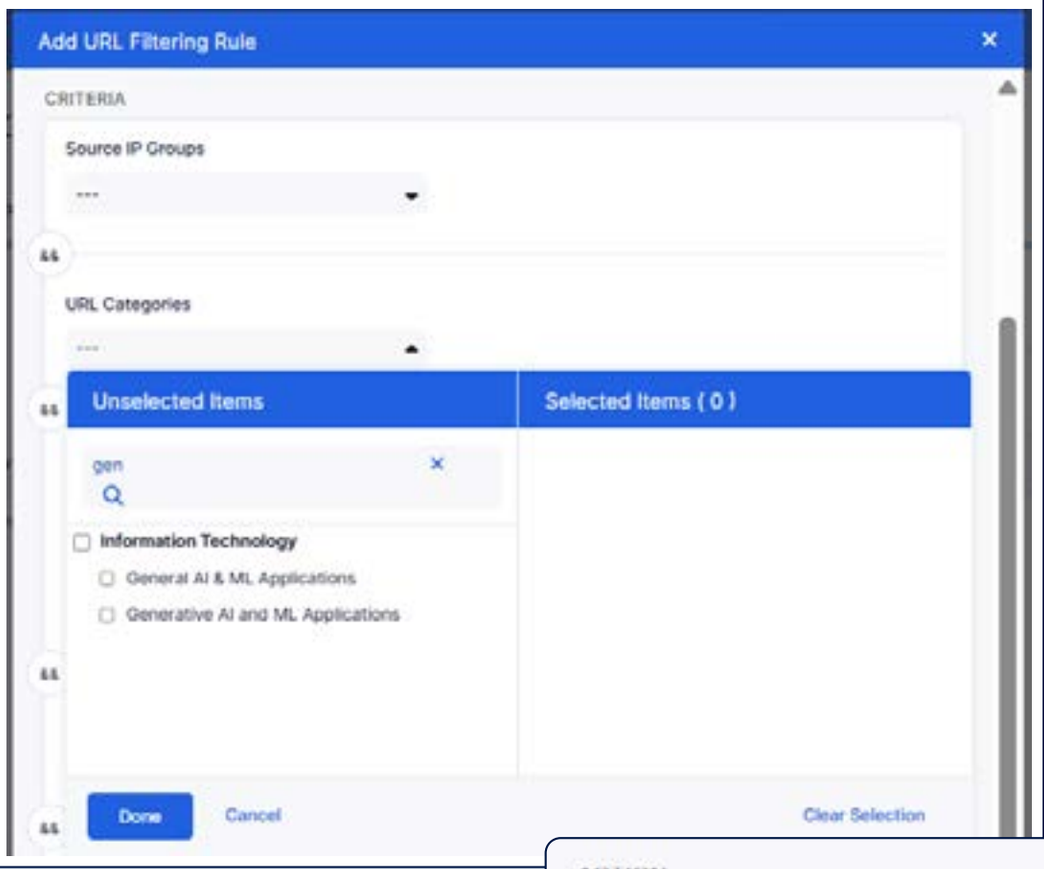
Automatizzare il rilevamento e la gestione delle applicazioni di GenAI

Grazie all’ispezione TLS, gli enti pubblici hanno accesso all’intera gamma di funzionalità di Zscaler, incluso il controllo granulare sulle applicazioni di GenAI e di machine learning. Un vantaggio chiave risiede nelle applicazioni di IA ed ML di Zscaler, curate dal team ThreatLabz. Questa categoria comprende un’ampia gamma di applicazioni di IA, tra cui strumenti popolari come ChatGPT, Gemini, MetiAI, Claude e altri ancora.

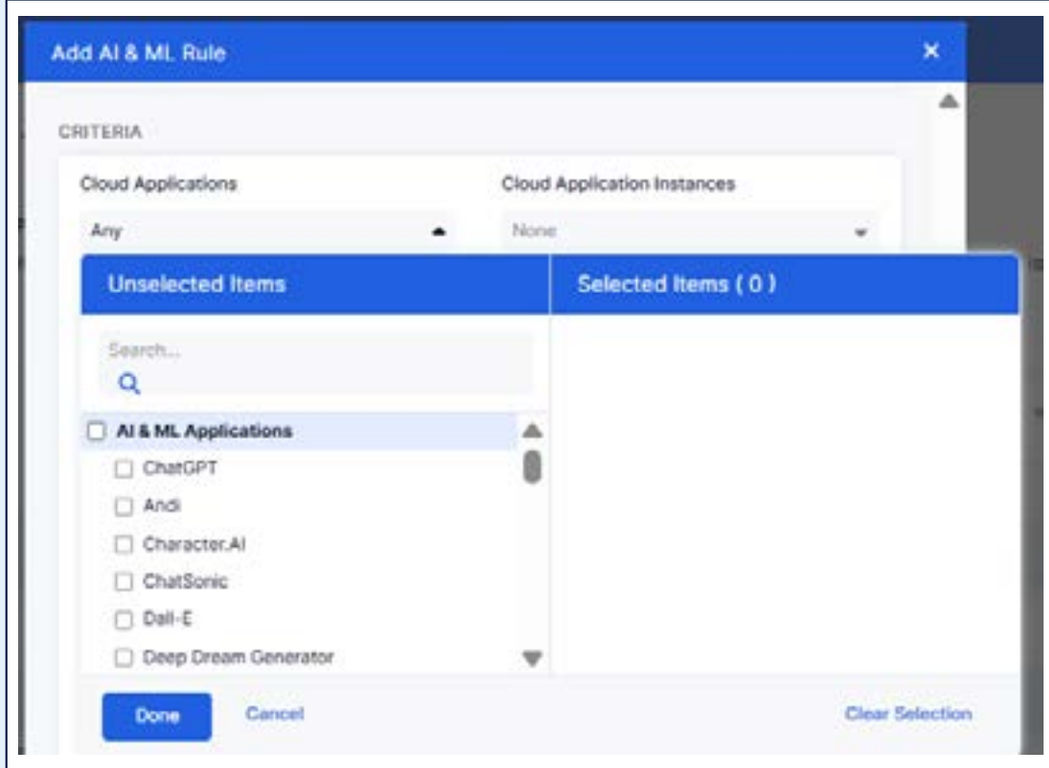
Utilizzando questa categoria, gli enti pubblici possono applicare delle policy per bloccare per impostazione predefinita le applicazioni di GenAI sconosciute o non verificate, garantendo l’accesso solo agli strumenti approvati. Man mano che emergono nuove applicazioni, queste vengono aggiunte automaticamente a queste categorie, risparmiando agli enti pubblici lo sforzo di dover individuare e inviare manualmente gli eventuali aggiornamenti. Inoltre, gli enti godono della flessibilità di poter ampliare o personalizzare questo elenco, aggiungendo domini personalizzati per adattarli al meglio alle loro esigenze specifiche. Zscaler fornisce inoltre delle categorie dedicate, come “Applicazioni generiche di IA ed ML” e “Applicazioni di IA generativa ed ML”, che, se abbinate all’elenco più ampio “Applicazioni di IA sul cloud”, offrono una copertura molto più estesa, per ridurre i rischi per la sicurezza posti dalle applicazioni di GenAI. Questo approccio multilivello consente agli enti pubblici di gestire in modo efficace l’accesso a centinaia di applicazioni che vengono sviluppate e rilasciate ogni settimana.

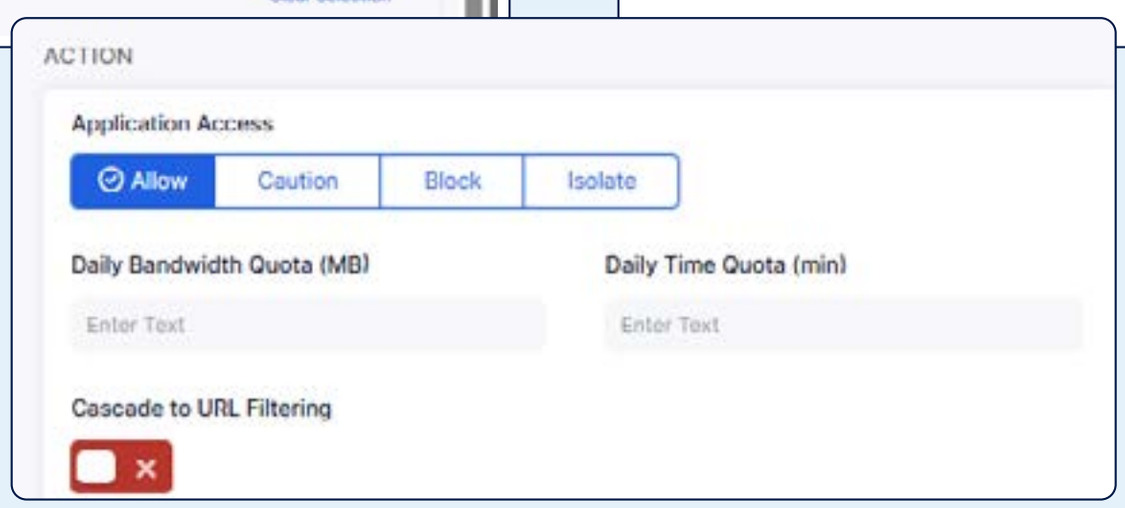
Ampia selezione di categorie e applicazioni specifiche di IA

Categorie di URL per la copertura estesa



Applicazione della GenAI per controlli granulari

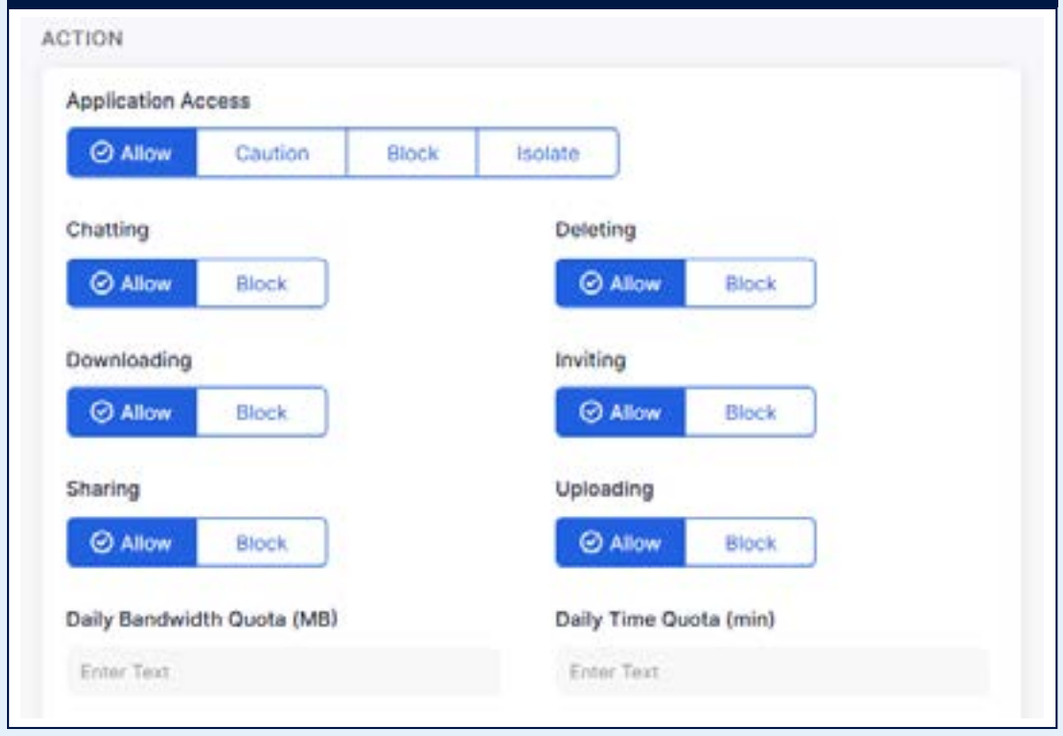




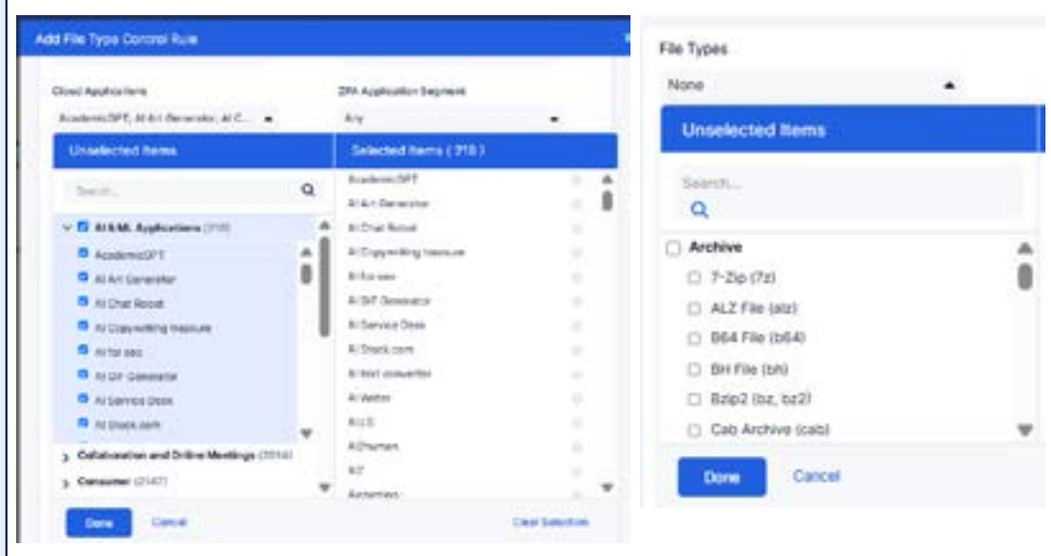
©2025 Zscaler, Inc. Tutti i diritti riservati.

Controlli granulari per SaaS, web e applicazioni di IA

Controlli granulari delle applicazioni di GenAI



Controlli sul caricamento dei file nelle applicazioni di GenAI



Consentire l’uso delle app autorizzate tramite il controllo di sicurezza delle applicazioni SaaS

Oltre a gestire un elenco completo di applicazioni di IA, Zscaler fornisce controlli granulari su come gli utenti interagiranno con le applicazioni di GenAI. Si tratta di controlli incredibilmente semplici da applicare, molto potenti e consolidati in un’unica piattaforma. Il lato sinistro dell’immagine mostra alcuni esempi dei controlli granulari che possono essere applicati, nel caso in cui una policy di sicurezza per chatGPT possa includere controlli granulari come consentire la chat, ma bloccare il caricamento dei file o limitare la condivisione delle chat. Gli enti pubblici possono applicarli a livello di reparto o addirittura a livello di singolo utente. Tali controlli granulari possono essere ulteriormente perfezionati limitando i tipi di file che gli utenti possono caricare nelle applicazioni di GenAI, come mostrato a destra. Questo controllo sui file può includere inoltre la limitazione del caricamento di documenti criptati.

Limitare l’accesso alle istanze aziendali delle applicazioni di GenAI

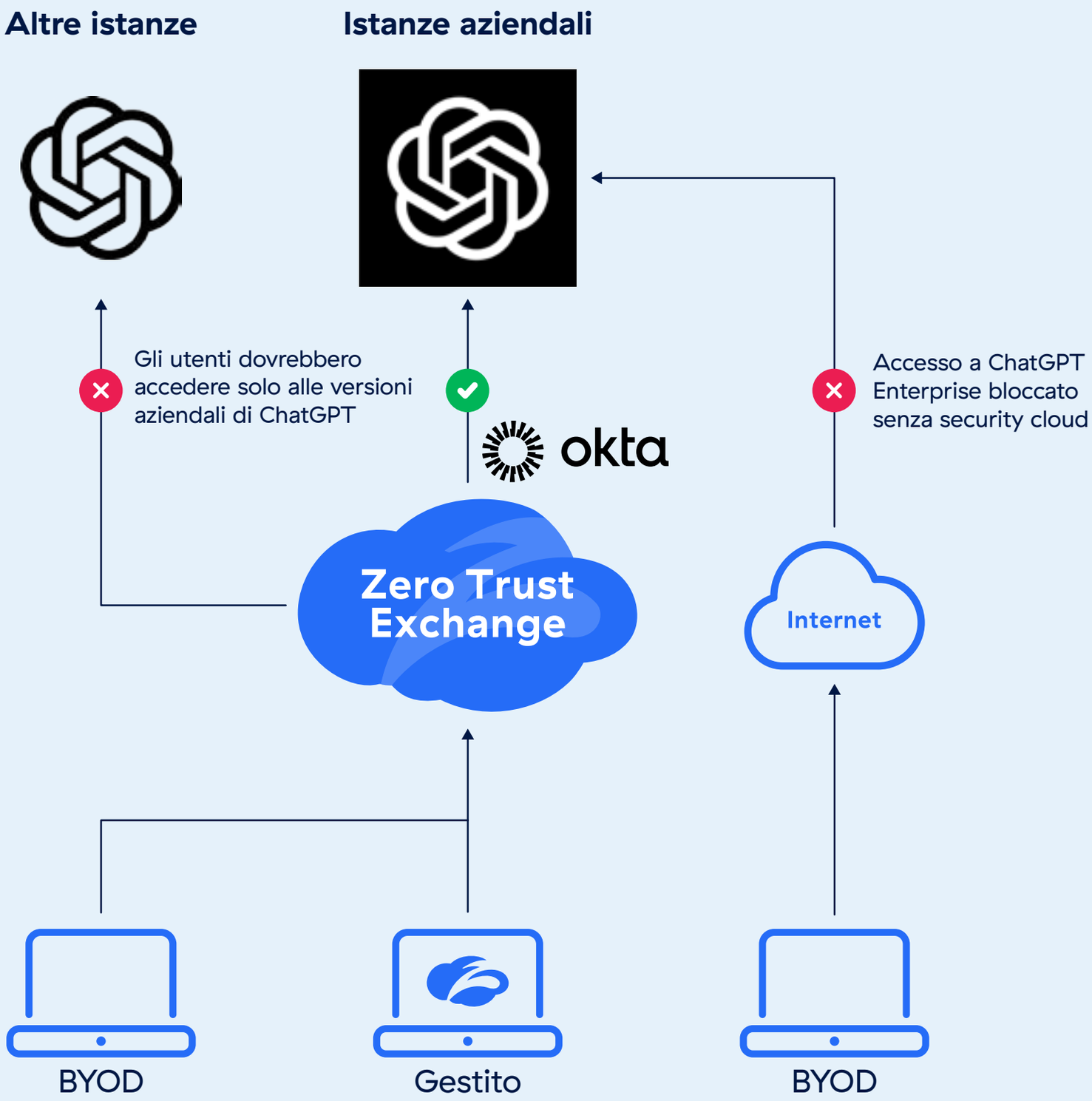
Gli enti pubblici dovrebbero considerare di utilizzare le versioni per le aziende delle applicazioni di GenAI, per garantire una maggiore sicurezza e controllo. Le versioni Enterprise, come ChatGPT Enterprise, offrono agli enti pubblici la piena proprietà e il controllo dei propri dati e delle conversazioni, per evitare che i dati aziendali contribuiscano all’addestramento del modello. Queste soluzioni sono conformi allo standard SOC2 e forniscono la crittografia sia per i dati in transito che inattivi. Inoltre, semplificano la gestione degli utenti con funzionalità quali l’accesso per team, la verifica del dominio, il Single Sign-On (SSO) e le informazioni sull’utilizzo, consentendo una distribuzione sicura su larga scala.

©2025 Zscaler, Inc. Tutti i diritti riservati.

Le istanze aziendali delle applicazioni di GenAI dovrebbero essere abbinate all’SSO per massimizzare la sicurezza e fornire agli enti pubblici visibilità e controllo maggiori sull’utilizzo delle applicazioni. Grazie all’SSO, gli enti pubblici possono applicare policy che bloccano l’accesso alle versioni non aziendali delle applicazioni di GenAI. Ad esempio, il controllo della tenancy di Zscaler per ChatGPT garantisce che solo i tenant approvati possano accedere, mentre gli altri vengono limitati in automatico. Inoltre, gli enti pubblici possono implementare controlli a livello di IAM (Identity and Access Management) utilizzando una whitelist per garantire che le versioni aziendali siano l’unica istanza di utilizzo di GenAI e che l’accesso avvenga tramite ambienti sicuri, come la piattaforma cloud di Zscaler. Per estendere ulteriormente l’accesso sicuro, le istanze di GenAI aziendali possono essere rese disponibili anche ai dispositivi non gestiti o personali (BYOD), utilizzando l’accesso BYOD agentless di Zscaler.

Un approccio semplice, basato su regole come “consenti tutto o blocca tutto”, non è più efficace in un mondo dominato dalla GenAI. Gli enti pubblici devono adottare una strategia di sicurezza multilivello con controlli granulari adattati alle diverse interazioni delle applicazioni. Consolidare queste funzionalità in una piattaforma unificata non solo semplifica l’implementazione, ma favorisce anche l’adesione ai principi cardine dello zero trust, garantendo un accesso con privilegi minimi, una visibilità continua e una protezione completa di ogni interazione con la GenAI.

Controllo dell’accesso alle istanze autorizzate delle applicazioni di IA



©2025 Zscaler, Inc. Tutti i diritti riservati.

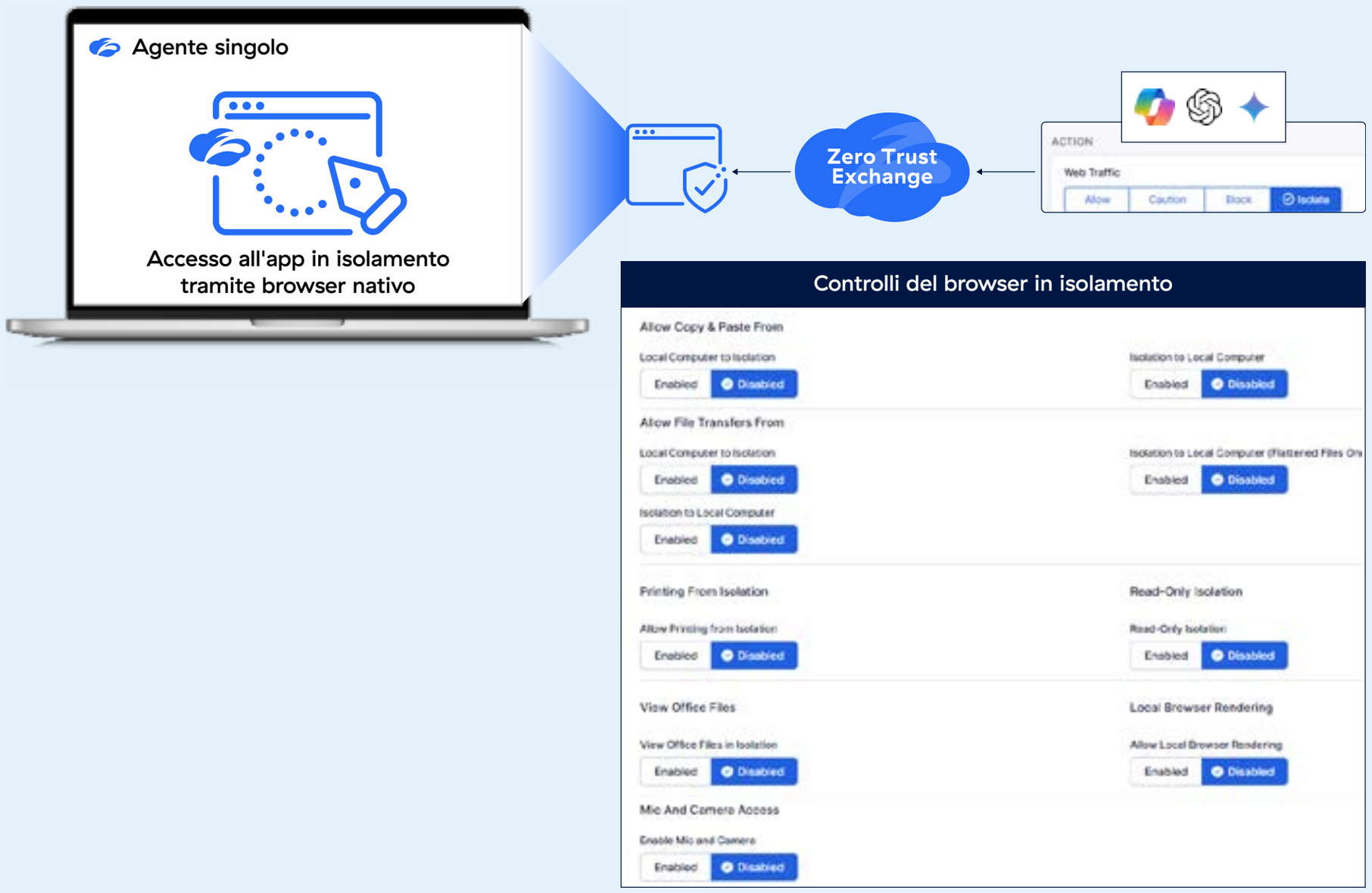
Ridurre il rischio associato alle applicazioni di GenAI non autorizzate

Quando è necessario concedere l'accesso alle applicazioni di GenAI non autorizzate (prive di licenza aziendale e SSO), tali app devono essere considerate ad alto rischio. I dati caricati su tali applicazioni potrebbero essere utilizzati per addestrare i modelli di GenAI, esponendo potenzialmente le informazioni sensibili. Per far fronte a questo rischio critico, gli enti pubblici devono implementare ulteriori livelli di controlli di sicurezza per garantire una supervisione più rigorosa delle interazioni che interessano i dati.

Zscaler offre una soluzione efficace per gestire questo rischio tramite il suo Zero Trust Browser. Questo strumento consente agli enti pubblici di fornire un accesso sicuro alle applicazioni di GenAI non autorizzate con controlli avanzati, come la limitazione di azioni quali i trasferimenti di file, la stampa e l'utilizzo degli appunti. Inoltre, Zero Trust Browser impedisce alle applicazioni di GenAI di eseguire il codice direttamente sul browser dell'utente, effettuando invece il rendering delle interazioni su pagine isolate. Ciò contribuisce a proteggere dalle impronte digitali, dal tracciamento dei cookie di terze parti e da altre vulnerabilità, consentendo al contempo agli utenti di continuare a utilizzare lo stesso browser distribuito dall'ente.

Questo approccio può essere implementato in due modi: con Zscaler Unified Agent oppure utilizzando un modello agentless. Per i dispositivi di proprietà dell'ente, si consiglia una distribuzione basata su agente per garantire che tutto il traffico venga instradato tramite la piattaforma di applicazione di Zscaler. Nei contesti in cui non è possibile installare un agente, l'opzione agentless di Zscaler offre un'alternativa sicura, garantendo un accesso controllato alle applicazioni di GenAI, senza compromettere la sicurezza.

Controlli granulari per proteggere le applicazioni di IA isolate bilanciando l'esperienza utente



©2025 Zscaler, Inc. Tutti i diritti riservati.

4. Implementare la protezione dei dati fin dal principio

La mancata implementazione di una solida strategia di protezione dei dati fin da quando si inizia ad adottare la GenAI può comportare violazioni dei dati, violazioni delle normative sulla privacy e una perdita di fiducia da parte del pubblico, compromettendo in definitiva il successo di questi stessi strumenti. La natura conversazionale e intuitiva delle applicazioni pubbliche di GenAI accresce il rischio che gli utenti espongano involontariamente dei dati governativi sensibili. Se non vengono attentamente supervisionate, delle semplici azioni come copiare e incollare informazioni o caricare file possono far trapelare informazioni riservate per via del contesto o dell'integrazione con altri sistemi. Ciò evidenzia perché l'integrazione di solide misure di protezione dati dovrebbe essere una parte fondamentale di qualsiasi strategia pubblica di adozione della GenAI per gli enti statali e locali.

Zscaler consente agli enti pubblici di affrontare efficacemente questi rischi, grazie alle sue funzionalità avanzate di prevenzione della perdita dei dati (Data Loss Prevention, DLP). Progettata per proteggere le informazioni sensibili fin dal principio, la soluzione di DLP di Zscaler per la GenAI identifica e blocca la condivisione dei dati riservati, che sia tramite prompt, caricamento di file o uso improprio, prima che possano raggiungere i modelli di GenAI pubblici. Questo approccio proattivo garantisce che gli enti pubblici possano adottare la GenAI salvaguardando al contempo le informazioni sensibili e preservando la conformità.

Accelerare l'adozione della DLP

Per molte organizzazioni, intraprendere un percorso di protezione dati può sembrare un'impresa ardua, soprattutto quando si tratta di bilanciare la necessità di concedere l'accesso agli strumenti di GenAI con l'implementazione di solide misure di sicurezza. Zscaler affronta questa sfida offrendo una piattaforma semplificata, pensata per supportare team snelli e consentire un'adozione rapida della GenAI con efficaci controlli di protezione dati. Questo approccio garantisce che gli enti pubblici possano adattare in modo efficiente il proprio quadro di riferimento per la sicurezza a diversi dipartimenti e basi di utenti.

Per gli enti pubblici che hanno già applicato regole inline ad altre destinazioni su Internet, estendere tali policy alle applicazioni di GenAI risulterà molto semplice. Zscaler integra inoltre i motori di DLP e i dizionari esistenti utilizzati per altri canali direttamente nelle applicazioni di IA ed ML, riducendo la ridondanza e accelerando la distribuzione. Se un ente parte invece da zero, Zscaler fornisce dizionari predefiniti che possono essere implementati nelle applicazioni di GenAI in pochi clic, per impedire la fuga dei dati sensibili. Inoltre, i documenti o i set di dati noti possono essere protetti utilizzando le funzionalità di EDM/IDM, mentre i tag di Microsoft Information Protection (MIP) possono fornire un ulteriore grado di protezione dall'esposizione per i dati criptati o classificati.

Per perfezionare ulteriormente le policy, le funzionalità di rilevamento supportate dal machine learning (ML) di Zscaler identificano le informazioni sensibili e le fughe di dati precedentemente sconosciute all'interno delle applicazioni di GenAI, consentendo agli enti pubblici di far evolvere costantemente la propria strategia di protezione. Gli enti possono inoltre adattare i dizionari esistenti in base alle proprie esigenze, sia perfezionandoli, sia creando regole di rilevamento personalizzate utilizzando espressioni regolari o parole chiave. Zscaler si integra infine con le soluzioni di backup dei dati come Rubrik, semplificando l'identificazione e la protezione dei dati.

©2025 Zscaler, Inc. Tutti i diritti riservati.

Accelerare l'implementazione della DLP con Zscaler

Giorno O di implementazione

Dati specifici dell'ente con EDM e IDM

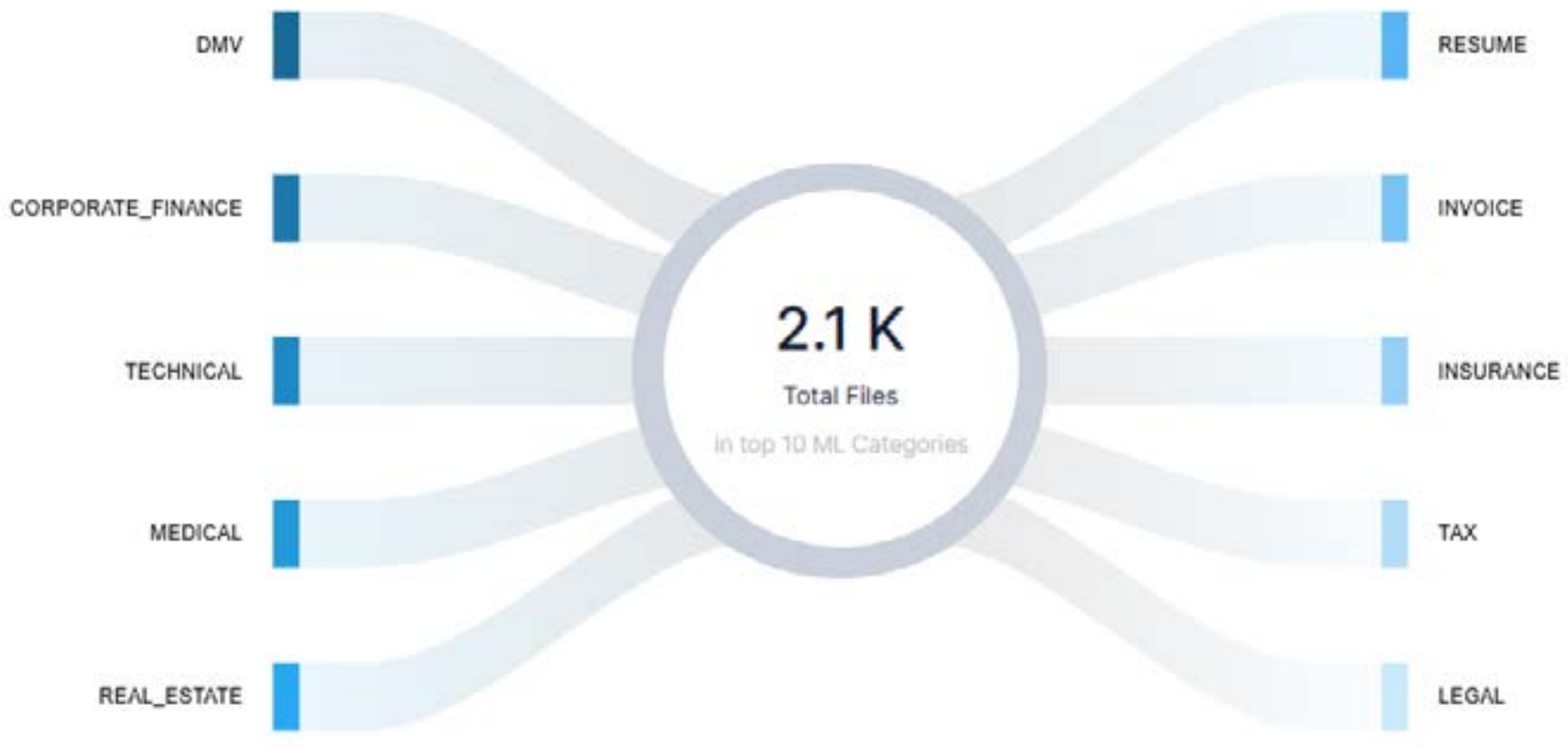
Dizionari predefiniti che dovrebbero essere utilizzati dagli enti governativi

- Numeri di instradamento bancario (ABA)
- Documento finanziario aziendale
- Documento legale aziendale
- Documento giudiziario
- Credenziali e dati riservati
- Carte di credito
- Informazioni su malattie
- Patente di guida (Stati Uniti)
- Informazioni sui farmaci
- Relazioni finanziarie
- Documento di immigrazione
- Documento assicurativo
- Fattura
- Documento legale
- Documento medico
- Informazioni mediche
- Documento immobiliare
- Numeri di previdenza sociale (Stati Uniti)
- Documento fiscale
- Numero di identificazione fiscale (Stati Uniti)
- Documento del Dipartimento dei Trasporti o della Motorizzazione (Stati Uniti)
- Informazioni sui trattamenti sanitari

Etichette MIP/AP

Monitoraggio e visibilità continui

Identificazione di fughe di dati e app sconosciute



Dati acquisiti dagli incidenti

Input e feedback degli utenti

Ottimizzazione e adattamento | Secondo necessità

Creazione di un dizionario personalizzato con regex/parole chiave

Parole chiave composte da una o più parole con prossimità

Estensione di EDM + IDM alle soluzioni di backup dei dati

©2025 Zscaler, Inc. Tutti i diritti riservati.

L'applicazione delle policy in tempo reale e la visibilità granulare consentono ai team IT di proteggere i dati sensibili senza aggravare la complessità o necessitare della supervisione manuale. Questo approccio semplificato facilita l'adozione rapida e sicura degli strumenti di GenAI, per sfruttarne i vantaggi in termini di produttività, garantendo al contempo la conformità e la fiducia del pubblico, in linea con il principio dello zero trust del "fidarsi mai, verificare sempre".

Semplificare la governance della DLP

Una sfida comune legata all'implementazione della prevenzione della perdita dei dati (DLP), soprattutto negli enti pubblici più grandi o nelle organizzazioni con servizi condivisi, è data dal volume di incidenti che i team del SOC e i proprietari dei dati devono gestire. Questi incidenti possono variare dalla richiesta di follow-up da parte dei dipendenti per giustificare un comportamento, al rafforzamento della formazione degli utenti, alla gestione delle eccezioni o al mantenimento di un audit trail. Senza un sistema efficiente, questo scenario può diventare rapidamente ingestibile.

Workflow Automation semplifica questo processo offrendo una soluzione centralizzata per la gestione degli incidenti di protezione dati correlati alla GenAI. Fornisce una panoramica completa di tutti gli incidenti in un unico posto, inclusi i metadati e i dettagli delle azioni o dei dati specifici che hanno innescato la violazione. Questa centralizzazione consente agli amministratori di esaminare, stabilire le priorità e risolvere rapidamente gli incidenti, secondo le necessità.

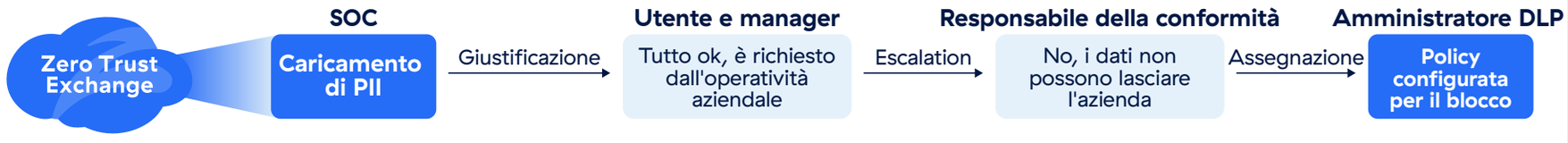
Una caratteristica fondamentale di Workflow Automation è la sua capacità di raggruppare gli incidenti in base a caratteristiche condivise e di definire le priorità. Tali gruppi possono quindi essere assegnati ad amministratori specifici per una risoluzione più mirata. In questo caso, l'automazione svolge un ruolo molto significativo, favorendo flussi di lavoro che notificano o istruiscono gli utenti finali coinvolti negli incidenti, richiedono giustificazioni sul comportamento o inoltrano i problemi ai responsabili o ai proprietari dei dati per l'approvazione. I flussi di lavoro automatizzati possono inoltre attivare delle azioni per porre rimedio agli incidenti, senza necessitare di interventi manuali.

Sfruttando Workflow Automation nella DLP, gli enti pubblici possono ridurre drasticamente i tempi di risoluzione, alleggerire il carico operativo sul SOC e ottenere informazioni utili sulle aree di rischio. Queste informazioni possono essere utilizzate per perfezionare ulteriormente le policy o potenziare i programmi formativi, garantendo che gli utenti siano attrezzati al meglio per operare in modo sicuro, riducendo al contempo la probabilità di incorrere in incidenti futuri.

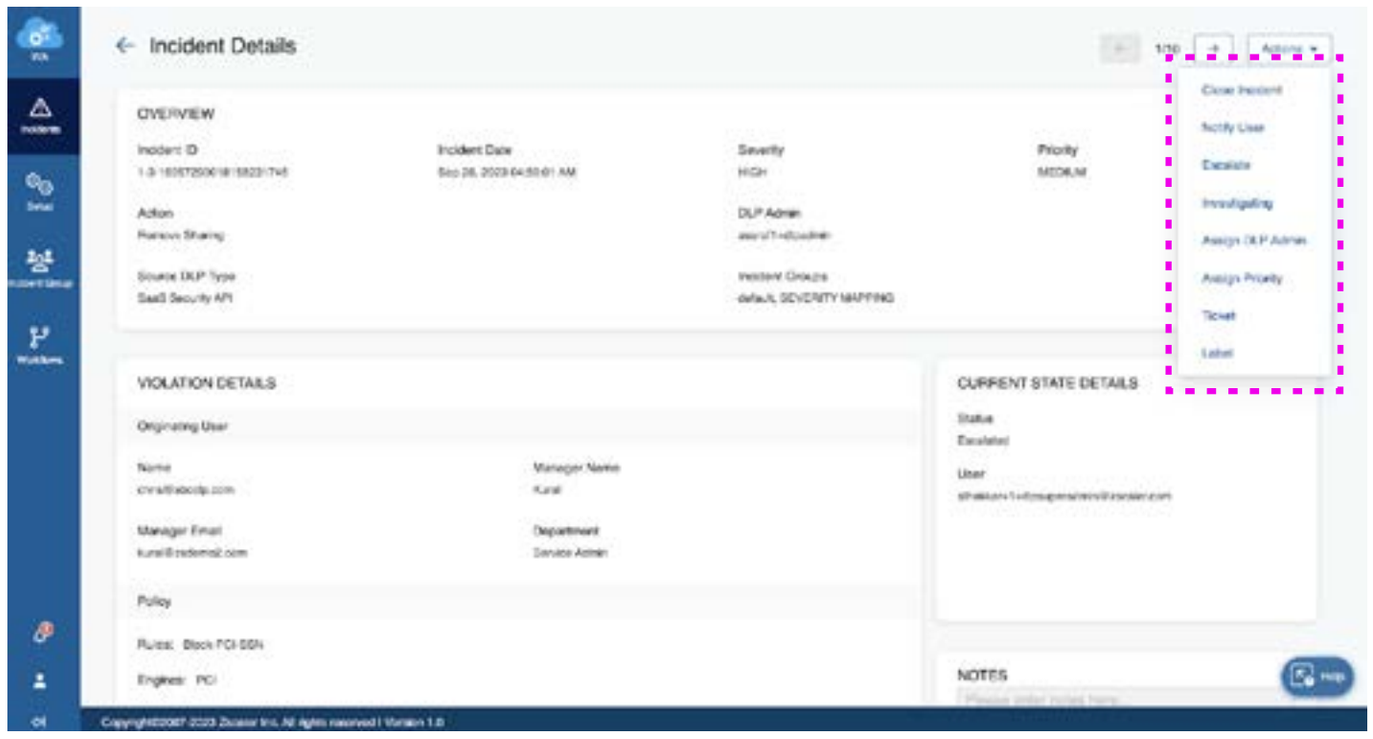
©2025 Zscaler, Inc. Tutti i diritti riservati.

Semplificare la gestione degli incidenti con la gestione dei casi e il coaching degli utenti

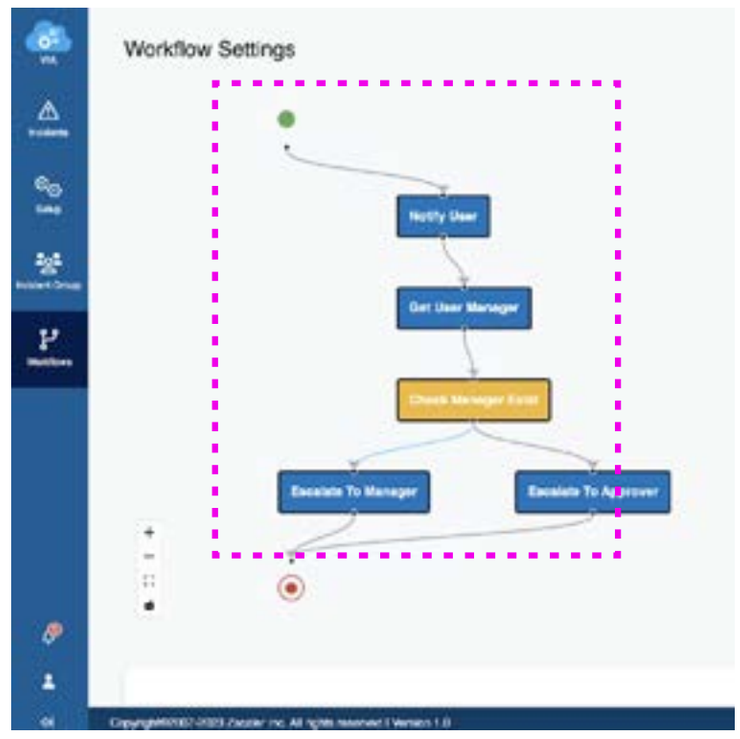
Automazione dei flussi di lavoro
Possibilità di giustificare gli incidenti abilitando al contempo il coaching degli utenti



Gestione, assegnazione ed escalation rapide degli incidenti



Definizione di routine per i flussi di lavoro



5. Consolidare l’ambiente e utilizzare un approccio multilivello

Gli enti statali e locali stanno adottando l’IA generativa (GenAI) per sfruttare nuove efficienze e migliorare i servizi, ma è fondamentale farlo in modo sicuro. Con migliaia di strumenti di GenAI disponibili, insieme a rischi quali la fuga dei dati e l’uso non autorizzato, gli enti pubblici necessitano di una strategia ben definita, che dia la priorità alla sicurezza, integri i principi dello zero trust e favorisca comunque la produttività. Un approccio multilivello semplifica questo processo raggruppando le applicazioni in base al rischio, applicando controlli di sicurezza personalizzati e automatizzando la gestione degli incidenti per ridurre la pressione sui team IT. Questa strategia aiuta gli enti pubblici a proteggere i dati sensibili, semplificare le operazioni e consentire agli utenti di sfruttare in modo sicuro le applicazioni di GenAI, il tutto all’interno di un quadro di riferimento scalabile e gestibile.

Implementare controlli multilivello

In questa sezione esploreremo come possono procedere gli enti pubblici per unire i vari punti e ottenere un’adozione sicura della GenAI utilizzando un approccio multilivello. Con migliaia di strumenti di GenAI già disponibili e nuovi strumenti che vengono lanciati ogni settimana, la gestione delle policy e degli incidenti può rapidamente trasformarsi in un’impresa ardua, senza una strategia ben ponderata.

©2025 Zscaler, Inc. Tutti i diritti riservati.

Un approccio multilivello semplifica questo processo organizzando l’accesso e implementando controlli dei dati personalizzati in base ai livelli di rischio. Questo metodo non solo riduce il carico di lavoro degli amministratori della sicurezza, ma riduce anche significativamente i rischi associati alla perdita dei dati e il numero di incidenti che i team IT e di sicurezza devono gestire. Adottando questo approccio strutturato, le organizzazioni possono sfruttare in modo sicuro ed efficace la potenza della GenAI, preservando al contempo l’efficienza operativa.

Come discusso in precedenza, strumenti come il rilevamento delle app dello Shadow IT, i report sul rilevamento della GenAI e la visibilità sui prompt della GenAI forniscono informazioni preziose su come dovrebbero evolversi le policy di IA e su come i controlli di sicurezza possono essere personalizzati per soddisfare delle esigenze in continua evoluzione. Questi approfondimenti utili costituiscono la base per un approccio pratico e multilivello alla gestione delle applicazioni di GenAI.

Un modo utile per implementare questo modello è quello di classificare le applicazioni di GenAI in tre categorie: ad alto rischio, a medio rischio e a basso rischio. Le applicazioni ad alto rischio dovrebbero essere bloccate integralmente, per evitare l’esposizione a vulnerabilità inutili. Alle applicazioni a medio rischio può essere concesso l’accesso con controlli di sicurezza più rigorosi, come l’isolamento del browser e misure di protezione dati più stringenti. Alle applicazioni a basso rischio può essere consentito l’accesso nativo, ma con restrizioni incentrate sui contenuti specifici o sulle azioni che gli utenti possono intraprendere.

Approccio multilivello per la protezione delle applicazioni di IA

©2025 Zscaler, Inc. Tutti i diritti riservati.

Questa struttura consente agli enti pubblici di adottare un approccio zero trust per la GenAI. Con questo modello, le applicazioni sconosciute, appena uscite o non approvate vengono bloccate per impostazione predefinita. Le applicazioni approvate, ma non autorizzate, vengono isolate con livelli di sicurezza aggiuntivi, mentre le applicazioni integralmente autorizzate beneficiano di un’esperienza utente più fluida con misure di sicurezza personalizzate. Per semplificare l’implementazione e la gestione, gli enti pubblici possono utilizzare strumenti come delle etichette personalizzate per le applicazioni e profili di rischio. Tali strumenti consentono ai team di sicurezza di definire policy predefinite che vengono applicate in automatico alle applicazioni in base al rischio assegnato. Le policy appropriate vengo applicate sulla base dell’etichetta assegnata all’applicazione, riducendo al minimo il carico di lavoro amministrativo, mantenendo al contempo un controllo efficace.

Come automatizzare i flussi di lavoro degli incidenti

Un altro aspetto critico da considerare è la gestione degli incidenti. È essenziale che gli enti pubblici riducano il numero di incidenti che il SOC (Security Operations Center, o centro delle operazioni di sicurezza) o gli amministratori dei dati devono gestire manualmente. Ad esempio, le violazioni di media e bassa gravità dovrebbero essere registrate a fini di controllo e chiuse automaticamente, senza richiedere un intervento manuale significativo. Tuttavia, poiché si tratta comunque di violazioni delle policy, gli utenti dovrebbero essere avvisati e andrebbe richiesta una giustificazione del comportamento assunto, un passaggio prezioso per rafforzare la formazione degli utenti e promuovere la responsabilità.

Con Zscaler, le policy di ispezione dei contenuti per la GenAI consentono agli enti pubblici di definire il livello di gravità delle violazioni, che vengono quindi trasmesse agli strumenti di automazione dei flussi di lavoro. Questa funzionalità consente agli amministratori di progettare flussi di lavoro personalizzati in base alla gravità di ciascun incidente. Ulteriori attributi, come appunto la gravità e altre caratteristiche condivise, possono essere utilizzati per categorizzare gli incidenti in gruppi, e questi gruppi possono essere a loro volta collegati a flussi di lavoro automatizzati. Questo approccio semplifica il processo di gestione degli incidenti, garantendo che le violazioni vengano affrontate in modo appropriato e riducendo notevolmente il carico di lavoro dei team del SOC.

©2025 Zscaler, Inc. Tutti i diritti riservati.

Riflessioni conclusive

Gli enti governativi devono essere in prima linea nello sfruttamento delle applicazioni di IA generativa (GenAI) per rivoluzionare le operazioni, responsabilizzare i dipendenti e servire al meglio i cittadini. L'adozione di questa tecnologia deve essere però supportata da un'architettura zero trust. Garantendo che ogni utente, dispositivo e interazione vengano verificati, monitorati e controllati, indipendentemente dalla relativa posizione o dall'applicazione utilizzata, gli enti pubblici possono proteggere l'uso della GenAI attraverso una solida protezione dati, una governance ben articolata ed esperienze utente ottimizzate al centro della loro strategia.

Zscaler consente agli enti governativi di sfruttare i vantaggi in termini di produttività della GenAI con un approccio sicuro e multilivello che semplifica la governance, ottimizza la distribuzione e integra una solida sicurezza in ogni interazione. Grazie alla definizione di quadri di riferimento per la governance dell'IA, all'automazione del rilevamento e della gestione delle applicazioni di GenAI, al controllo dell'uso delle istanze delle applicazioni di GenAI e all'implementazione di funzionalità di DLP avanzate fin dal principio, gli enti pubblici possono ridurre drasticamente i rischi e ampliare le proprie strategie di adozione con un carico di lavoro minimo per i team IT e di sicurezza.

Data l'evoluzione continua della GenAI, i responsabili degli enti pubblici sono incoraggiati ad adottare un approccio strategico e graduale all'adozione di questa tecnologa dirompente, che inizia proteggendo l'accesso alle applicazioni di genAI pubbliche, per sfruttare in modo sicuro la maggiore produttività offerta dall'IA agentica (tema che verrà trattato in futuro). Infine, un altro aspetto importante da esplorare è come estendere in modo sicuro le funzionalità della GenAI ai servizi incentrati sul cittadino, garantendo che i sistemi rimangano sicuri in ogni momento. Con Zscaler, gli enti pubblici possono implementare queste fasi in sicurezza, accelerando l'innovazione e mantenendo al contempo i più elevati standard di sicurezza e conformità dei dati.

Contatta il team del tuo account o contattaci per fissare un workshop su misura per la tua organizzazione.

Informazioni su Zscaler
Zscaler (NASDAQ: ZS) accelera la trasformazione digitale in modo che i clienti possano essere più agili, efficienti, resilienti e sicuri. La piattaforma Zscaler Zero Trust Exchange™ protegge migliaia di clienti dagli attacchi informatici e dalla perdita dei dati, collegando in modo sicuro utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in oltre 150 data center a livello globale, Zero Trust Exchange™, basata sul framework SSE, è la più grande piattaforma di cloud security inline del mondo. Per saperne di più, visita **zscaler.com/it** oppure seguici su X (precedentemente Twitter) **@zscaler**.

© 2025 Zscaler, Inc. Tutti i diritti riservati. Zscaler™ e gli altri marchi commerciali presenti su **zscaler.com/it/legal/trademarks** sono (I) marchi commerciali o marchi di servizio registrati o (II) marchi commerciali o marchi di servizio di Zscaler, Inc. negli Stati Uniti e/o in altri Paesi. Tutti gli altri marchi commerciali sono di proprietà dei rispettivi titolari.

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

zscaler™

Zero Trust Everywhere