

Zscaler Risk360™

Un potente framework per la quantificazione e la visualizzazione del rischio per correggere i rischi legati alla sicurezza informatica

PANORAMICA SULLA SOLUZIONE

©2025 Zscaler, Inc. Tutti i diritti riservati.

Zscaler Risk360: il framework per la quantificazione e la visualizzazione del rischio

Risk360 è un potente framework di quantificazione e visualizzazione del rischio per aiutare le organizzazioni a correggere i rischi legati alla sicurezza informatica. Il suo sistema elabora i dati reali dell'azienda provenienti dall'ambiente di Zscaler e dalle ricerche sulla sicurezza condotte da ThreatLabz per generare un dettagliato profilo di rischio.

Zscaler Risk360 impiega oltre 100 fattori all'interno dell'ambiente di security del cliente, per aiutare a comprendere le stime sulle perdite finanziarie, i principali fattori di rischio informatico, i flussi di lavoro investigativi consigliati, i trend e i confronti con altre realtà analoghe. Inoltre, consente di esportare slide chiare da mostrare al consiglio di CISO. Questo modello copre i quattro aspetti di un attacco, ossia la superficie di attacco esterna, la compromissione, la propagazione laterale e la perdita dei dati, e tutte le entità presenti nell'ambiente aziendale, come gli asset, le applicazioni e gli utenti.

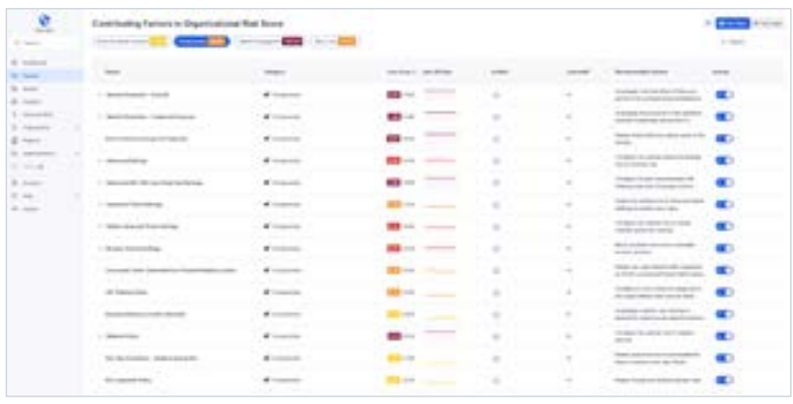
SUPERFICIE DI ATTACCO ESTERNA

Zscaler Risk360 esamina un'ampia gamma di variabili rilevabili pubblicamente, come i server esposti e gli ASN, per determinare le risorse cloud sensibili. Questo report fornisce una visione olistica di tutte le risorse aperte alla rete Internet, e consente di ottenere una vista completa della superficie di attacco esterna che risulta potenzialmente vulnerabile ed esposta.



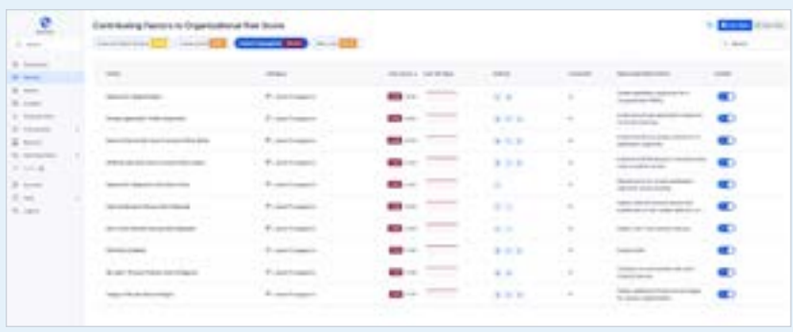
RISCHIO DI COMPROMISSIONE

Zscaler Risk360 analizza un'estesa varietà di eventi, configurazioni di sicurezza e attributi dei flussi di traffico per calcolare le probabilità di subire una compromissione. Ciò consente agli amministratori di comprendere il rischio di subire attacchi attraverso file dannosi, esposizione a paziente zero e utenti che mostrano segni di infezione.



MOVIMENTO LATERALE

Zscaler Risk360 prende in considerazione le configurazioni e le metriche legate all'accesso privato per calcolare il rischio di propagazione laterale. Questo consente di valutare le policy di segmentazione per evitare che gli aggressori informatici si spostino più in profondità nella rete.



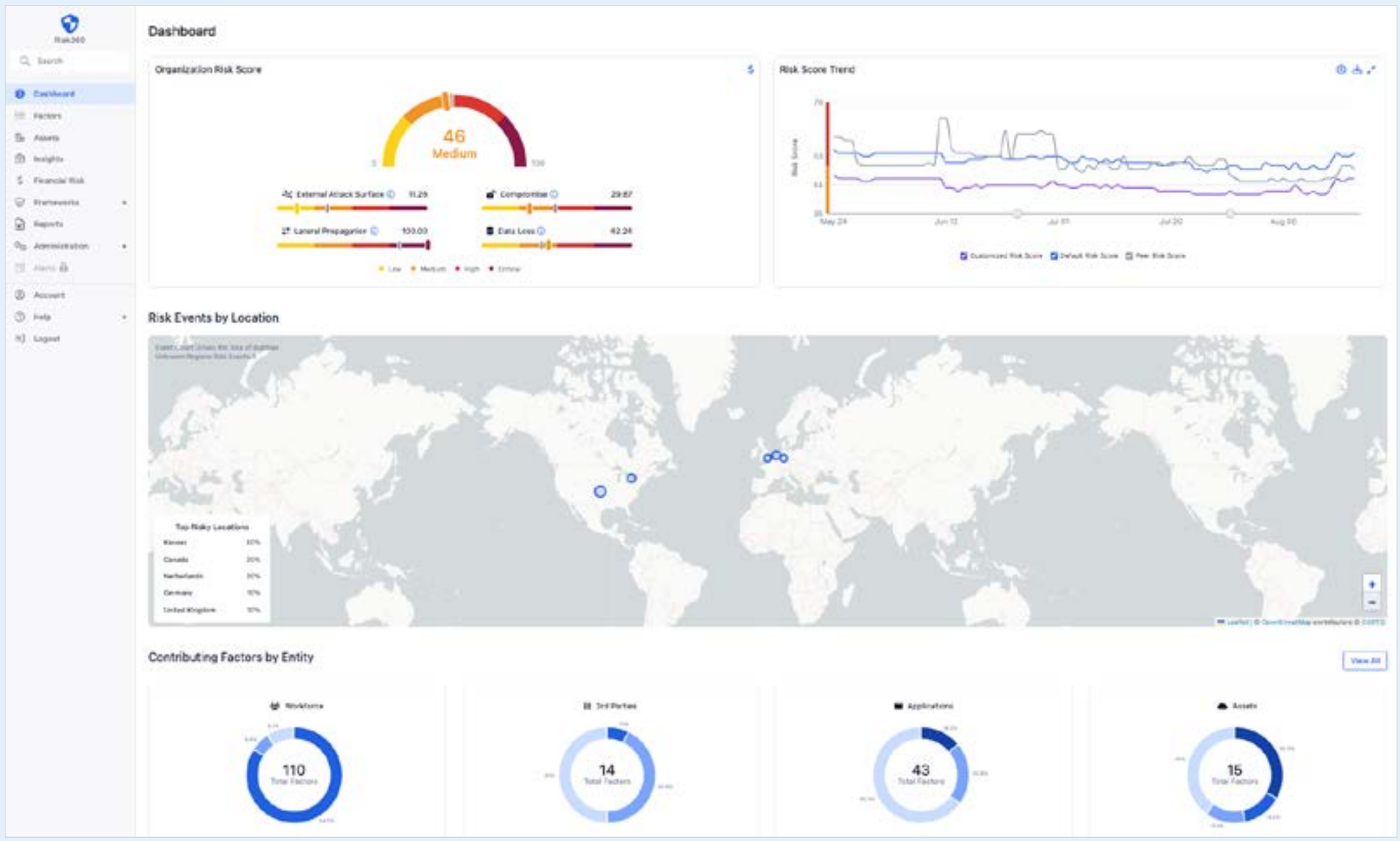
PERDITA DI DATI

Gli attributi dei dati sensibili vengono raccolti per verificare se i dati possono fuoriuscire dall'ambiente del cliente. L'analisi e la visione completa sulla potenziale perdita di dati è indispensabile per impedirne la violazione e la compromissione.



©2025 Zscaler, Inc. Tutti i diritti riservati.

Scopri il profilo di rischio, le tendenze e i principali fattori che contribuiscono alla tua organizzazione con informazioni fruibili



Come funziona?

1 ACCESSO

Molti clienti Zscaler possono sfruttare Zscaler Risk360 fin da subito.

2 RACCOLTA DATI

Elabora i dati provenienti da diverse fonti Zscaler per offrire una panoramica completa e basata sui dati del rischio.

3 MITIGA IL RISCHIO

Filtra, approfondisci e individua i fattori di rischio per agire e correggere le problematiche più critiche che alimentano il rischio informatico.

4 ANALISI FINANZIARIA

Stime di perdita finanziaria basate su dati e ricerca, mappate sullo Zscaler score della tua azienda.

©2025 Zscaler, Inc. Tutti i diritti riservati.

Il valore di Zscaler Risk360

Quantificazione del rischio

Zscaler Risk360 sviluppa un punteggio di rischio per ciascuna delle quattro fasi di una violazione, visualizzandolo per tutte le entità d'uso come forza lavoro, terze parti, applicazioni e asset. Il framework di rischio si basa su centinaia di segnali derivati da anni di ricerca sulla sicurezza condotta dagli esperti di Zscaler ThreatLabz. Poiché Zscaler Zero Trust Exchange opera in linea, la piattaforma ha una capacità unica di identificare con sicurezza i fattori di rischio. Tutto ciò risulta estremamente utile per l'allocazione dei budget di sicurezza informatica, le strategie di investimento e di mitigazione. I team di sicurezza possono sfruttare i punteggi di Zscaler Risk360 per costruire un business case a supporto di tutte le decisioni di investimento in sicurezza.

Visualizzazione e report intuitivi

Zscaler Risk360 offre visualizzazioni e report intuitivi per fornire ai leader una panoramica sintetica di alto livello. I responsabili e gli operatori possono anche filtrare e analizzare più a fondo i principali fattori di rischio dell'organizzazione per prendere decisioni di sicurezza più informate. Zscaler Risk360 consente di esportare facilmente slide riassuntive da presentare al consiglio di amministrazione, illustrando il rischio informatico, le principali evidenze e l'esposizione finanziaria stimata. I team di sicurezza possono concentrarsi sull'impatto strategico per l'azienda e automatizzare il processo di reporting.

Approfondimenti attuabili per la correzione

Il framework di remediation delle priorità di rischio all'interno di Zscaler Risk360 consente ai clienti di intervenire sulle policy per aggiornarle o modificarle. Include inoltre flussi di lavoro investigativi guidati che permettono di approfondire e analizzare problemi specifici. Ad esempio, identificare utenti specifici che caricano dati sensibili. I clienti possono monitorare periodicamente il punteggio di rischio per comprendere meglio la propria postura di sicurezza.

I vantaggi di Zscaler Risk360

- Visione accurata dell'esposizione al rischio nelle quattro fasi dell'attacco
- Consolida il punteggio di rischio da più fonti per un'analisi completa del rischio informatico
- Analisi dei principali fattori di rischio informatico dell'organizzazione e valutazione degli elementi che vi contribuiscono
- Informazioni concrete, con flussi di lavoro guidati per indagare e risolvere i problemi più critici
- Miglioramento dei report e delle linee guida per CXO e consiglio di amministrazione, in modo da supportare la gestione, la strategia, la governance e la conformità in relazione al rischio informatico e alla copertura assicurativa

©2025 Zscaler, Inc. Tutti i diritti riservati.

Casi d’uso

Quantificazione e visualizzazione del rischio informatico nell’intera organizzazione

Zscaler Risk360 sfrutta motori automatizzati che acquisiscono dati reali da fonti interne (Zscaler Zero Trust Exchange). Il punteggio di rischio dell’organizzazione è indicato su una scala da 0 a 100 (dove 100 rappresenta il livello critico) e consente anche il confronto con i peer di settore per analizzare benchmark e trend nel tempo e valutare i miglioramenti nella postura di sicurezza. Poiché molte organizzazioni stanno intraprendendo un percorso Zero Trust, Zscaler Risk360 aiuta anche a visualizzare il punteggio del loro percorso Zero Trust.

Rimedio basata sull’esposizione dei dati

Grazie ai flussi di lavoro investigativi guidati e agli approfondimenti con raccomandazioni attuabili, i clienti possono intervenire rapidamente dopo aver compreso il punteggio di rischio. Questo strumento aiuta a creare un elenco prioritario di problemi che possono essere analizzati e approfonditi tramite il workflow investigativo.

Impatto finanziario dell’esposizione al rischio informatico

I clienti possono stimare l’impatto finanziario del rischio della propria organizzazione grazie alla quantificazione delle perdite.

Reportistica, mappatura del rischio e orientamento

Risk360 offre report dettagliati preconfigurati, come i nostri CISO Board Reports che riassumono la postura di rischio informatico per i dirigenti, e una valutazione della maturità della sicurezza informatica basata su AI per mostrare il percorso Zero Trust dell’azienda e le aree di rischio più significative.

L’adozione di Zscaler Risk360

Molti clienti di Zscaler possono conoscere il punteggio di rischio della propria organizzazione in modo semplice e veloce sfruttando strumenti e raccomandazioni reali. Questo framework di visualizzazione consente a CISO e CIO di valutare il rischio informatico e l’esposizione finanziaria, confrontando inoltre il punteggio con quello di altre realtà analoghe e ottenendo suggerimenti sui flussi di lavoro da adottare per migliorarlo. I reparti che hanno accesso a questo report sono in grado di suddividere i dati in base al tipo di rischio, all’entità (utenti, applicazioni, asset) e alla posizione. Il report consente di ordinare l’elenco degli utenti in base al rischio e mostra le applicazioni (sia SaaS che private e combinate) e gli asset con valutazioni di rischio individuali e specifiche.

Zscaler offre inoltre la possibilità di monitorare il punteggio di rischio nel corso del tempo per vedere l’effetto delle azioni intraprese in base all’esposizione e ai consigli ricevuti.

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 **www.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