Solution Brief

Zscaler Risk360™

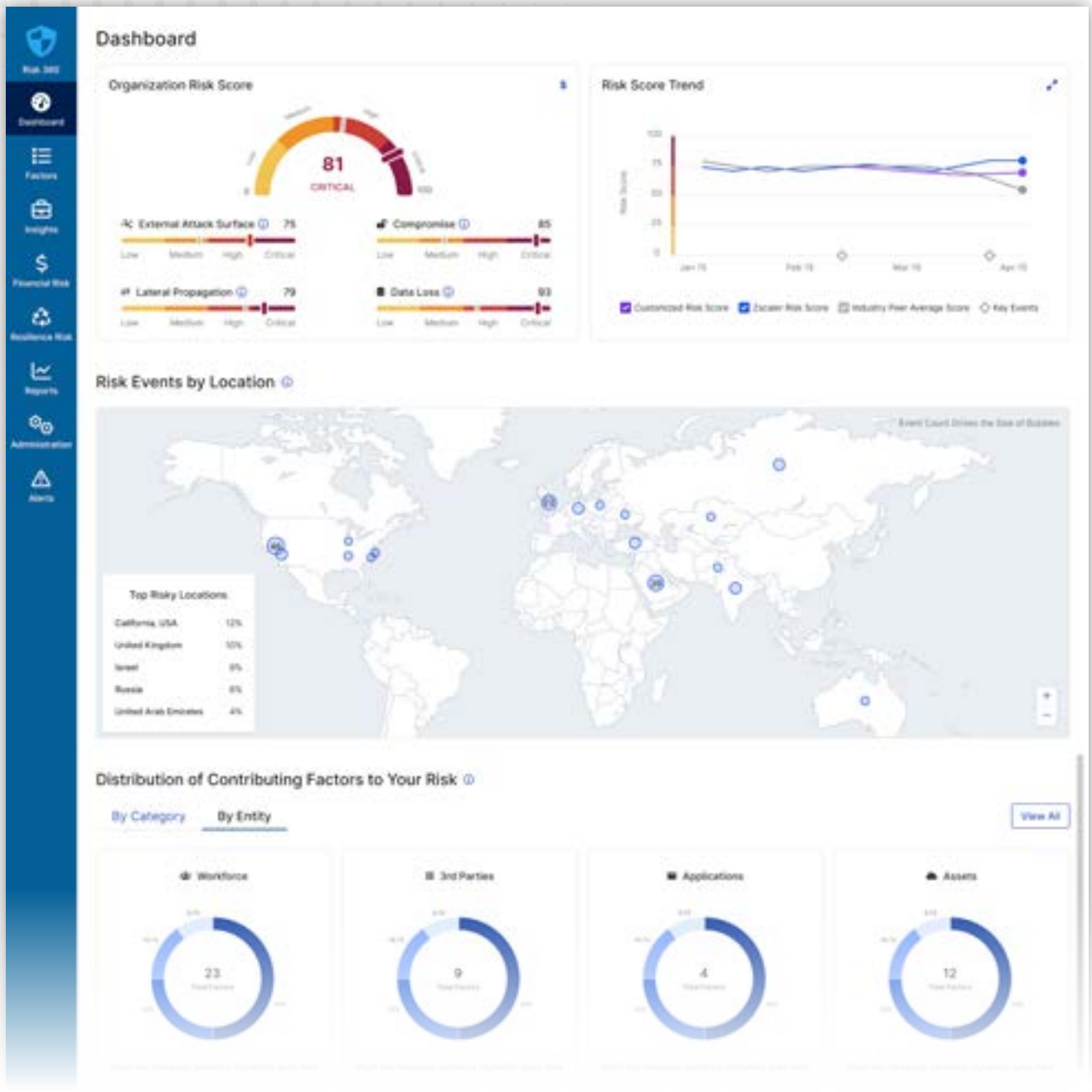
Un potente framework per la quantificazione e la visualizzazione del rischio per correggere i rischi legati alla sicurezza informatica

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

Risk360 è un potente framework di quantificazione e visualizzazione del rischio per la correzione dei rischi legati alla sicurezza informatica. Il suo sistema elabora dati reali provenienti da fonti esterne, dall'ambiente di Zscaler e dalle ricerche sulla sicurezza condotte da ThreatLabz al fine di generare un dettagliato profilo di rischio.

Zscaler Risk360 impiega oltre 100 fattori all'interno dell'ambiente di sicurezza 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 diapositive chiare da mostrare al consiglio di CISO. Questo modello copre i quattro elementi di un attacco, ossia la superficie di attacco esterna, la compromissione, la propagazione laterale e la perdita di dati, con tutte le entità dell'ambiente aziendale, compresi risorse, applicazioni, utenti e terze parti.

Superficie di attacco esterna	Zscaler Risk360 esamina un'ampia gamma di variabili rilevabili pubblicamente, come i server esposti e gli ASN, per determinare quali sono 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 una 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 dei dati	Gli attributi dei dati sensibili vengono raccolti per verificare l'eventualità che i dati possano 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.	



Come funziona?

1. **Accesso**
   Tutti i clienti di Zscaler possono usare da subito Zscaler Risk360.

2. **Elaborazione dei dati**
   Elabora le informazioni provenienti da diverse fonti di Zscaler e da fonti esterne per fornire una panoramica sul rischio basata sui dati.

3. **Mitigazione del rischio**
   Per filtrare, approfondire e individuare i fattori di rischio e intervenire per porre rimedio alle questioni più critiche che determinano il rischio informatico.

4. **Analisi finanziaria**
   Per ottenere stime sulle perdite finanziarie basate su dati e ricerche di settore e mappate secondo il punteggio di rischio di Zscaler.

Il valore di Zscaler Risk360

Quantificazione del rischio
Zscaler Risk360 definisce un punteggio di rischio per ciascuna delle quattro fasi di una violazione, che viene visualizzato per tutte le entità che intervengono nel processo di utilizzo, come la forza lavoro, le terze parti, le applicazioni e le risorse. Questo framework di rischio è supportato da centinaia di segnali corroborati da diversi anni di ricerche sulla sicurezza condotte dagli esperti di Zscaler ThreatLabz. Inoltre, dato che Zscaler Zero Trust Exchange si colloca inline, ha la capacità di identificare con estrema sicurezza i fattori di rischio. Oltre a utilizzare i dati di Zscaler Zero Trust Exchange, Zscaler Risk360 utilizza inoltre quelli provenienti da fonti terze, come l'EDR, per fornire un punteggio di rischio affidabile. Tutto questo è utile per l'allocazione del budget destinato alla sicurezza informatica e per definire gli investimenti e le strategie di mitigazione. I team responsabili della sicurezza possono sfruttare i punteggi di Zscaler Risk360 per creare un business case che supporti le decisioni relative agli investimenti in questo ambito.

Funzionalità intuitive di visualizzazione e report
Zscaler Risk360 offre funzionalità intuitive di visualizzazione e report che consentono di realizzare analisi ad ampio spettro da presentare alla dirigenza. I leader e gli operatori hanno inoltre la possibilità di filtrare ed esaminare i principali fattori di rischio informatico dell'organizzazione per eseguire analisi più approfondite e prendere le giuste decisioni in materia di sicurezza. I clienti hanno invece la possibilità di analizzare le stime sull'esposizione finanziaria e di vedere le raccomandazioni per la relativa risoluzione. Oltre a tutto questo, Zscaler Risk360 consente di esportare diapositive riepilogative che possono essere inserite nelle presentazioni rivolte al consiglio di amministrazione per illustrare il rischio informatico, i risultati più significativi e l'esposizione finanziaria stimata. In questo modo, i team responsabili della sicurezza possono concentrarsi sulla generazione di un maggiore impatto sul business e automatizzare il processo di reportistica.

I vantaggi di Zscaler Risk360

- Visione accurata dell'esposizione al rischio nelle quattro fasi dell'attacco
- Punteggio di rischio consolidato 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
- Report sulla quantificazione delle perdite finanziarie con i risultati del metodo Monte Carlo
- Mappature della sicurezza rispetto ai framework di rischio per la sicurezza: MITRE Attack e NISF CSF

Informazioni a supporto delle azioni correttive
Il framework per la correzione dei rischi prioritari all'interno di Zscaler Risk360 consente ai clienti di intervenire sulle policy per aggiornarle o modificarle. Include inoltre flussi di lavoro investigativi guidati che consentono di approfondire le indagini su problemi specifici, come ad esempio l'identificazione di particolari utenti che caricano dati sensibili. I clienti sono in grado di monitorare periodicamente il punteggio di rischio per conoscere nel dettaglio lo stato del proprio profilo.

Casi d'uso

Quantificazione e visualizzazione del rischio informatico per l'intera organizzazione
Zscaler Risk360 sfrutta motori automatizzati che elaborano dati reali provenienti da fonti interne (Zscaler Zero Trust Exchange) ed esterne (terze parti). Il punteggio di rischio dell'organizzazione viene indicato su una scala da 0 a 100 (dove 100 rappresenta la gravità massima) e consente inoltre il confronto con altre realtà analoghe del settore, per comprendere i benchmark e le tendenze nel corso del tempo e seguire il miglioramento del profilo di sicurezza. Zscaler Risk360 supporta inoltre il crescente numero di organizzazioni che hanno scelto di intraprendere un percorso zero trust, consentendo loro di visualizzare il punteggio relativo a tale percorso.

Correzione dell'esposizione basata sui dati
Grazie a flussi di lavoro investigativi guidati e informazioni concrete a supporto delle azioni correttive, dopo aver compreso il proprio punteggio di rischio i clienti possono agire eseguendo una bonifica rapida. Questo strumento aiuta a creare un elenco di problemi prioritari che possono essere analizzati attraverso flussi di lavoro investigativi per approfondire e analizzare problemi specifici.

Impatto finanziario dell'esposizione al rischio informatico
I clienti possono stimare l'impatto finanziario del rischio a cui è sottoposta la propria organizzazione quantificando le perdite finanziarie. Questi report sull'esposizione finanziaria includono la modellazione Monte Carlo, che indica un intervallo di potenziali risultati finanziari.

Report, mappatura dei rischi e linee guida
Risk360 offre report dettagliati e pronti all'uso, come i nostri report per il consiglio di CISO, che riassumono i profili di rischio informatico per i dirigenti, e la nostra valutazione della maturità della sicurezza informatica basata sull'IA, per mostrare il percorso zero trust dell'azienda e le principali aree di rischio. Offre inoltre le mappature dei controlli rispetto ai framework di rischio per la sicurezza, come MITRE Attack e NIST CSF, e supporta i report sulla conformità in ottemperanza all'articolo 106 del regolamento S-K della SEC.

L'adozione di Zscaler Risk360

Tutti i clienti di Zscaler possono conoscere il punteggio di rischio della propria organizzazione in modo semplice e veloce grazie a strumenti e raccomandazioni reali. Questo framework di visualizzazione consente a CISO e CIO di valutare il rischio informatico e l'esposizione finanziaria confrontando 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, terze parti, applicazioni, risorse) 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), le terze parti e le risorse 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.

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