Scheda tecnica

Zscaler Sandbox

Il primo motore al mondo per il rilevamento, la prevenzione e la quarantena dei malware basato sull'IA

Zscaler Sandbox previene le infezioni da paziente zero e impedisce alle minacce avanzate persistenti di accedere alla rete.

Nel mondo mobile e cloud-first di oggi, gli utenti accedono ai file anche in movimento, direttamente da Internet e dalle applicazioni SaaS. Sono lontani i tempi in cui si avviavano i client di posta elettronica dall'ufficio aziendale e gli utenti erano circondati da svariati livelli di sicurezza. Le difese incentrate sulla rete non vanno di pari passo con il miglioramento della semplicità d'uso, e le organizzazioni si ritrovano con una superficie di attacco sempre più estesa in un momento storico in cui gli attacchi sono più subdoli e gli aggressori sfruttano a proprio vantaggio i punti ciechi negli stack di soluzioni di sicurezza legacy.

Nel tentativo di proteggere i dati personali e aziendali sensibili, oggi quasi tutto il traffico Internet viene cifrato. Tuttavia, se da un lato questo ha scoraggiato alcuni utenti malintenzionati, la crittografia ha in realtà creato un falso senso di sicurezza. Le sandbox legacy basate su un'architettura passthrough non dispongono della dovuta visibilità e consentono inavvertitamente ai file dannosi di passare inosservati nel traffico cifrato, senza passare per un'ispezione approfondita o una quarantena. Implementare dispositivi per la decifrazione SSL può aiutare, ma come avviene con la maggior parte delle soluzioni hardware, questi strumenti non sono scalabili e non fanno altro che aumentare il numero di dispositivi (e i relativi costi amministrativi). Di conseguenza, le infezioni da paziente zero continuano a contagiare le reti, lasciando i team IT

I vantaggi di Zscaler Sandbox

- **Motore di prevenzione dei malware basato sull'IA**
  Identifica, metti in quarantena e previeni le minacce sconosciute o sospette inline in modo intelligente utilizzando modelli avanzati di IA/ML, senza dover riscansionare i file benigni.
- **Ispezione completa inline per rilevare gli attacchi nascosti**
  Esponi e previeni le minacce elusive e i malware nascosti nel traffico cifrato sui protocolli di trasferimento di file e web, senza latenza e senza limitazioni nella capacità.
- **Prevenzione uniforme e condivisa a livello globale**
  Ottieni una protezione automatica dalle minacce precedentemente sconosciute grazie all'intelligence integrata condivisa tra tutti gli utenti in tempo reale.
- **Miglioramento dei flussi di lavoro del SOC grazie all'intelligence sulle minacce**
  Accelera le attività di indagine e risposta condividendo le informazioni sul comportamento dei malware, l'intelligence sulle minacce e i report avanzati grazie ad API solide.
- **Niente più dispositivi fisici e software costosi**
  Effettua la distribuzione in pochi secondi, senza hardware da acquistare o software da gestire: ti basta configurare e implementare una policy della sandbox per poter sfruttarne immediatamente il valore aggiunto.
- **Protezione fornita tramite il cloud con presenza all'edge a livello globale**
  Ottieni una sicurezza e un'esperienza utente completamente integrate e senza pari con Zscaler Internet Access™, parte della piattaforma Zscaler Zero Trust Exchange™.

e di sicurezza alle prese con il difficile compito di bloccare il movimento laterale e l'esfiltrazione dei dati, che avrebbero dovuto essere scongiurati fin dall'inizio.

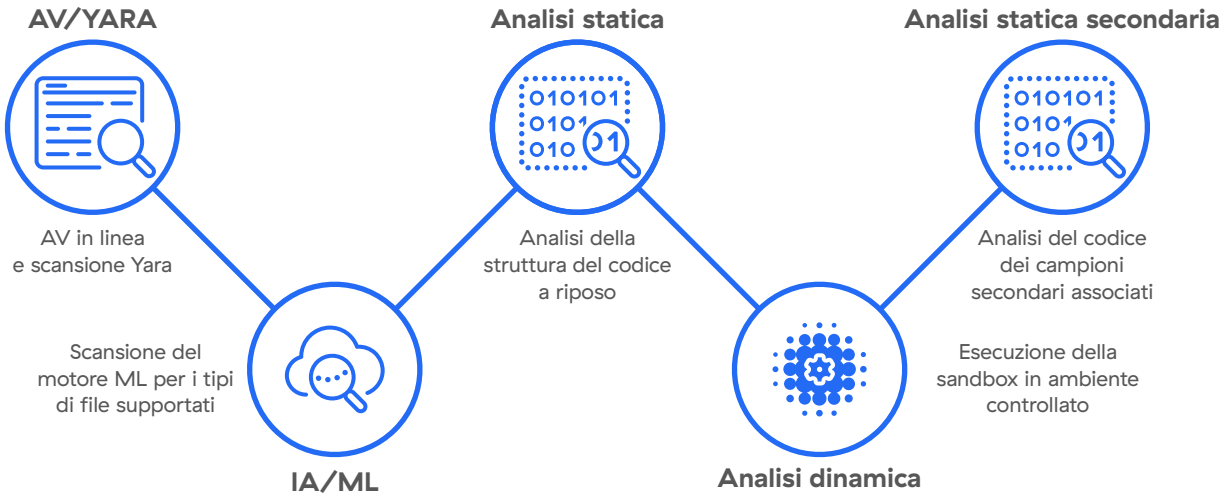
Zscaler Sandbox

Le sandbox hanno una funzione fondamentale in uno stack di soluzioni di sicurezza, in quanto forniscono le misure preventive contro l'esecuzione di codici e file dannosi. A differenza delle sandbox fuori banda, che proteggono solo dopo il verificarsi di una compromissione iniziale, Zscaler Sandbox è una soluzione creata appositamente per individuare e fermare le minacce moderne ed elusive che sfruttano le tecniche di elusione e i punti deboli delle sandbox tradizionali.

Il primo motore per la prevenzione dei malware alimentato dall'IA al mondo, Zscaler Sandbox si fonda su un'architettura nativa del cloud e proxy, ed è in grado di rilevare, prevenire e mettere in quarantena in modo automatico e intelligente minacce sconosciute e file sospetti inline. L'ispezione illimitata e senza latenza di tutti i protocolli di trasferimento file (FTP) e web, inclusi SSL e TLS, consente alla sandbox cloud-gen di eseguire un'analisi dinamica approfondita e in tempo reale, per garantire che nessun file sconosciuto raggiunga l'utente e impedire quindi il download dei file dannosi.

Il file sconosciuto o sospetto viene prima inviato a un motore di analisi di pre-filtraggio, che ne controlla il contenuto rispetto a oltre 40 feed di minacce, firme di antivirus, regole YARA e modelli IA/ML per emettere un verdetto rapido, bloccando le minacce analoghe note. Dopo il triage iniziale, il file viene quindi sottoposto a una robusta analisi statica, dinamica e secondaria, che include l'esecuzione del file in un ambiente controllato e isolato per raggiungere un verdetto con informazioni utilizzabili immediatamente. Il passaggio finale è la post-elaborazione, che aggiorna il database delle minacce di Zscaler e l'applicazione delle policy del cliente.

Con i verdetti basati sull'IA, i file benigni vengono consegnati istantaneamente, mentre quelli dannosi vengono bloccati per tutti gli utenti di Zscaler a livello globale, per una protezione condivisa che sfrutta il cloud. Questo consente di bloccare le infezioni da paziente zero e le minacce emergenti per tutti gli utenti, indipendentemente dal dispositivo o dalla posizione.



I vantaggi della sandbox cloud-gen

Oltre a mettere in quarantena i file sospetti inline, eseguire analisi basate sull'IA in tempo reale ed emettere verdetti istantanei senza ritardi, i report avanzati e dettagliati di Zscaler Sandbox possono portare il sandboxing dall'ultima linea al primo passaggio della difesa, in un'azione basata sull'intelligence. Usufruendo di informazioni comportamentali sui malware reali che prendono di mira la tua organizzazione, puoi arricchire i flussi di lavoro SecOps e rafforzare le difese in tutto lo stack di soluzioni di sicurezza.

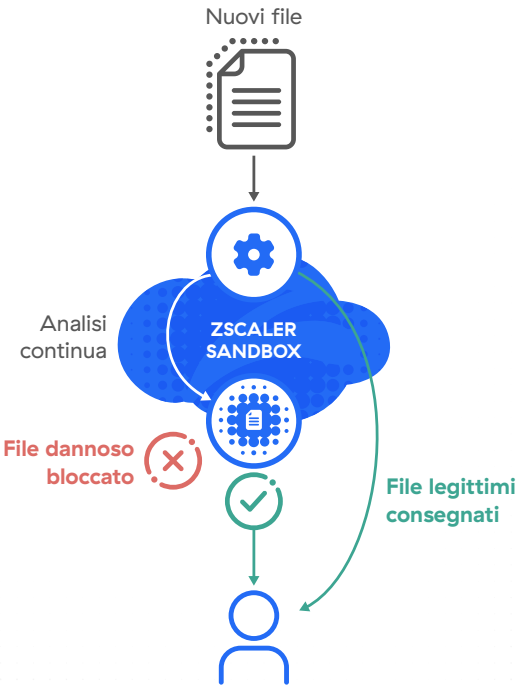
Blocca in modo intelligente le minacce emergenti e le infezioni da paziente zero Gli aggressori fanno uso di crittografia e app cloud attendibili per sferrare attacchi elusivi. Un recente report di ThreatLabZ ha infatti osservato la distribuzione di malware da Google Drive, AWS e OneDrive. La capacità di scansionare i file su web ed FTP, in particolare il traffico cifrato, garantisce la massima visibilità e impedisce agli aggressori di accedere alla rete.

Prima che un dipendente scarichi e apra accidentalmente un nuovo documento Office dannoso (Maldocs) con una macro nascosta, entra in azione la funzione di quarantena inline basata sull'IA di Zscaler Sandbox. Se l'analisi approfondita del file restituisce un rating alto sulla minaccia, il file viene bloccato per quel dipendente e non risulterà accessibile nemmeno agli altri utenti di Zscaler. I verdetti istantanei sui file senza necessità di nuove scansioni prevengono l'interruzione della produttività dei dipendenti, mentre le azioni automatiche per la messa in quarantena e il blocco dei file sconosciuti o dannosi prevengono l'arrivo di una raffica di ticket all'assistenza IT.

Dopo una rapida distribuzione di Zscaler Sandbox, che ha richiesto solo venti minuti, il team IT e di sicurezza di un cliente è stato in grado di consegnare in modo sicuro e immediato il 91% dei file benigni agli utenti dopo aver ricevuto un verdetto basato sull'IA. È stato deciso che i rimanenti file sconosciuti avrebbero subito un ulteriore analisi dinamica e approfondita; si è scoperto che il 5% di questi file conteneva malware o aveva intenti dannosi. I file vengono bloccati per gli utenti interessati, e per tutti gli utenti e i dispositivi di Zscaler a livello globale, indipendentemente dalla posizione, per una protezione condivisa e uniforme.

La quarantena basata sull'IA blocca i malware sconosciuti

Protezione inline con consegna istantanea dei file benigni, difesa da paziente zero e controlli granulari delle policy



Migliora i flussi di lavoro del SOC con metriche utili sui malware e MITRE ATT&CK
Dopo l'analisi approfondita dei file e la detonazione sicura del malware sconosciuto, la sandbox genera in automatico un report di analisi. L'ambiente controllato e isolato della sandbox acquisisce le schermate di analisi e fornisce agli analisti informazioni su eventuali tecniche di elusione basate su polimorfismo e offuscamento, sul comportamento delle callback e altre azioni. Questo report descrive nel dettaglio il ciclo di vita dell'attacco e la kill chain degli eventi, il comportamento del malware e l'intento del payload ricollegandoli al framework MITRE ATT&CK.

Rendendo utilizzabili i risultati contestuali della sandbox grazie al framework ATT&CK, i team IT e di sicurezza possono condividere informazioni dettagliate con l'intero stack di soluzioni di sicurezza. In questo modo, la sandbox cloud-gen non è solo l'ultima linea di difesa contro i malware, ma diventa il primo passaggio per il rilevamento, accelerando l'indagine e la risposta e supportando al contempo la caccia alle minacce.

Gestione semplificata delle policy con controlli granulari
Trattandosi di un prodotto distribuito attraverso il cloud, non è necessario acquistare o configurare hardware, né ci saranno software da gestire; questo consente di ridurre la complessità e le risorse. Dato che non sarà più necessario essere sul posto per configurare e connettere i dispositivi, Zscaler Sandbox consente di essere operativi sin da subito, con una semplice configurazione in due passaggi: **criteri** e **azione**. A tutto ciò si aggiunge il fatto che le policy sono facili da gestire, configurare e implementare. In pochi semplici clic, gli amministratori sono in grado di implementare le policy, come l'ordine delle regole e altre policy che seguono utenti o gruppi di utenti indipendentemente dalla loro ubicazione.

La sandbox cloud-gen consente inoltre di migliorare l'analisi dei file statici e dinamici con il rilevamento automatico delle impronte digitali JA3 e di configurare liste di blocco degli hash personalizzate e regole YARA per implementare controlli più granulari. Inoltre, le policy di blocco basate sul punteggio possono intervenire sui file greyware e adware fastidiosi o sospetti, che in genere non superano la soglia di punteggio per essere considerati minacce.

Basata su una piattaforma zero trust nativa del cloud, Zscaler Sandbox è una funzionalità completamente integrata di Zscaler Internet Access e parte di Zscaler Zero Trust Exchange. La sua esclusiva architettura basata su proxy protegge gli utenti inline sin dall'inizio, indirizzando il traffico allo stack di soluzioni di sicurezza sul cloud più grande del settore, per applicare protezioni avanzate e intelligenti a ogni utente, indipendentemente dalla posizione o dalla rete. Ottieni una difesa globale condivisa basata sugli aggiornamenti in tempo reale provenienti da 300 bilioni di segnali giornalieri sulle minacce e combinata con la protezione cloud e il principio dei privilegi minimi dell'approccio zero trust.

Advanced Sandbox e Standard Sandbox a confronto

	Standard Sandbox	Advanced Sandbox	
Edizioni di ZIA	Professional Edition Business Edition	Transformation Edition ELA Edition	**Advanced Sandbox può essere un componente aggiuntivo di ZIA Professional e Business Edition**
File supportati	.exe, .dll	.exe, .dll, .scr, .ocx, .sys, .class, .jar, .pdf, .swf, .doc(x), .xls(x), .ppt(x), .apk, .zip, .rar, .7z, .bz, .bz2, .tar, .tgz, .gtar, .rtf, .ps1, .hta, .vbs, file script negli zip	
Quarantena basata sull'IA	—	✓	
Policy granulari	—	✓	
Report	—	✓	
API	—	✓	

Principali funzionalità cloud-gen

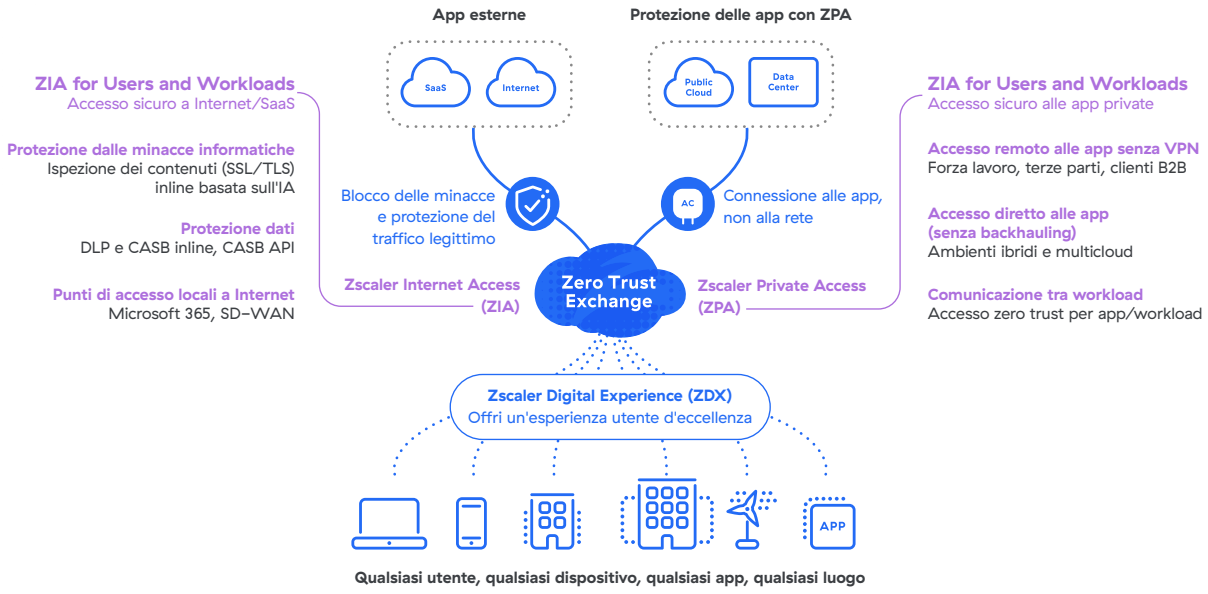
Motore di analisi di pre-filtraggio	AV, liste di blocco degli hash, regole YARA, rilevamenti automatizzati delle impronte digitali JA3 e modelli ML/IA
Analisi statica, dinamica e secondaria	Analisi statica e analisi dinamica, inclusa l'analisi del codice e l'analisi secondaria del payload
File supportati	.exe, .dll, .scr, .ocx, .sys, .class, .jar, .pdf, .swf, .doc(x), .xls(x), .ppt(x), .apk, .zip, .rar, .7z, .bz, .bz2, .tar, .tgz, .gtar, .rtf, .ps1, .hta, .vbs, file script negli zip
Ispezione SSL	Capacità illimitata di ispezione SSL/TLS
Conservazione dei file	Zscaler Cloud Sandbox funziona esclusivamente in memoria. I file vengono privati delle informazioni di identificazione durante l'analisi. Una volta completata l'analisi, i file legittimi vengono eliminati dalla memoria, mentre i file dannosi vengono cifrati e archiviati a tempo indeterminato, e le informazioni vengono condivise con tutti gli utenti di Zscaler per offrire una protezione continua.
Sistemi operativi supportati	Windows XP, Windows 10, Android
Protocolli supportati	HTTP, HTTPS, FTP, FTP su HTTP
File al giorno	Illimitati
Dimensione massima del file	20 MB per Windows e 50 MB per Android
Metodo di distribuzione	Nativo del cloud
Integrazione dell'intelligence sulle minacce	Oltre 40 feed di intelligence sulle minacce dei partner di sicurezza
Gestione e report	Report completi che includono: comportamento e intento del malware, indicatori di compromissione (IOC), file rilasciati, PCAP
Analisi forense	Esempio iniziale, carichi utili secondari, PCAP
Supporto API	Solido supporto delle API, recupero dei report tramite API in formato JSON
Policy granulari	Policy facili da utilizzare e configurare per utenti, posizioni, gruppi di posizioni, tipi di file, gruppi di utenti, dipartimenti, categorie di URL e protocolli
Certificazioni di privacy e conformità	Ottemperanza a rigorosi standard globali commerciali e governativi relativi a rischio, privacy e conformità
Normative di settore e sulla privacy dei dati	Conformità alle normative sulla privacy dei dati specifiche del settore e dei singoli Paesi

Zscaler Sandbox è completamente integrata in Zscaler Internet Access™ e fa parte della piattaforma olistica Zero Trust Exchange

Zscaler Zero Trust Exchange consente connessioni veloci e sicure e permette ai dipendenti di lavorare da qualsiasi luogo utilizzando Internet come rete aziendale. Sulla base del principio dello zero trust, fondato sull'accesso a privilegi minimi, offre una sicurezza completa utilizzando l'identità basata sul contesto e l'applicazione delle policy.

Ecco come Zscaler fornisce una sicurezza zero trust a utenti, workload e IIoT/OT

Distribuzione in poche settimane per migliorare la protezione informatica e l'esperienza utente



Gartner

Zscaler è stata nominata leader nel MQ di Gartner per il Security Service Edge, posizionandosi al vertice per capacità di esecuzione (categoria Ability to Execute).

Scopri di più →

zscaler™ | Experience your world, secured.™

Informazioni su Zscaler
Zscaler (NASDAQ: ZS) accelera la trasformazione digitale, in modo che i clienti possano essere più agili, efficienti, resilienti e sicuri. Zscaler Zero Trust Exchange protegge migliaia di clienti dagli attacchi informatici e dalla perdita dei dati grazie alla connessione sicura di utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in più di 150 data center nel mondo, Zero Trust Exchange, basata sul framework SASE, è la più grande piattaforma di cloud security inline del mondo. Scopri di più su **zscaler.it** o seguici su X (precedentemente Twitter) sull'account **@zscaler**.

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