E-BOOK

Guida all'acquisto degli strumenti per prevenire le minacce

Trova la soluzione migliore per la protezione dalle minacce, alimentata dall'AI, per fermare gli attacchi basati sui file.

Contenuti

Ripensare la sicurezza per l'attuale panorama di minacce

La sicurezza basata solo sul perimetro è troppo pericolosa per il mondo digitale di oggi

Il passaggio al lavoro flessibile e alle applicazioni ospitate sul cloud ha cambiato le modalità con cui gli utenti accedono alle risorse aziendali. I dipendenti utilizzano dispositivi non gestiti su reti non protette, come il Wi-Fi pubblico, per rimanere produttivi da remoto o mentre sono in viaggio, rendendo di fatto Internet la nuova rete aziendale. Questa espansione dei punti di accesso rende il vecchio approccio di tipo "castle-and-moat" alla sicurezza inadeguato per proteggere utenti, applicazioni e dati. Affidarsi esclusivamente alle difese perimetrali è rischioso, in quanto i controlli incentrati sulla rete vengono aggirati per ottenere l'accesso diretto a Internet, spesso dando priorità alla facilità d'uso rispetto alla sicurezza.

Gli attacchi informatici di nuova generazione riescono a eludere con estrema facilità i controlli di sicurezza legacy. È giunto il momento di avvicinare la sicurezza agli utenti e di passare dalla protezione del perimetro alla protezione degli utenti, dei workload e dell'OT/IOT.

Gli aggressori approfittano della corsa al cloud

I team addetti alla sicurezza si trovano quindi tra l'incudine e il martello: hanno fatto del loro meglio per adattare i controlli di sicurezza legacy al mondo mobile e cloud di oggi, ma l'inefficacia di questi strumenti ha finito per favorire gli aggressori. Le organizzazioni faticano a proteggere più edge di rete, e di conseguenza le porte vengono inavvertitamente lasciate aperte ai malware, come dimostrato dai risultati delle ricerche di Zscaler ThreatLabz:

- **L'86%** delle minacce viene trasmesso tramite i canali cifrati, e i malware che rappresentano il 78% di questi attacchi.[1]
- Gli attacchi ransomware sono aumentati del **40%** su base annua.[2]
- I payload osservati in Zscaler Sandbox sono aumentati del **58%**.[2]

Questa rapida evoluzione delle minacce digitali, aggravata dall'espansione della superficie di attacco sul cloud, non fa che rimarcare la necessità che i team di sicurezza riconsiderino le proprie strategie e rafforzino le difese per rispondere ai rischi informatici moderni.

1. Report del 2023 di Zscaler ThreatLabz sugli attacchi cifrati
2. Report del 2023 di Zscaler ThreatLabz sui ransomware

È necessario evolversi per proteggersi dai malware O-day

Gli aggressori hanno due vantaggi importanti: la **velocità** e la **proliferazione**. Gli sviluppatori di malware creano minacce molto più velocemente di quanto i difensori non riescano a definirle, e usano l'intelligenza artificiale per creare varianti in grado di eludere le misure di sicurezza convenzionali e i metodi di rilevamento.

Il phishing con allegati o link dannosi rimane attualmente il meccanismo di consegna più comune. L'uso diffuso del traffico cifrato complica ulteriormente le strategie di difesa. Le minacce moderne si nascondono spesso nel traffico cifrato, e questo sottolinea l'importanza di ispezionare tutto il traffico web e non web, per evitare di far entrare inconsapevolmente malware sulla rete.

Le sandbox hanno una funzione fondamentale in uno stack di soluzioni di sicurezza, e rappresentano una misura preventiva contro l'esecuzione di codice e file dannosi. Sono concepite per costituire una difesa efficace contro gli attacchi sconosciuti basati su file, che hanno l'obiettivo di eludere l'EDR e le altre scansioni che vanno alla ricerca di malware noti. Sfortunatamente, molte sandbox vengono distribuite fuori banda e si basano sull'inoltro di campioni di malware da parte di NGFW, prodotti di sicurezza cloud o agenti sugli endpoint.

Per questo motivo, spesso il rilevamento avviene dopo che il malware è stato scaricato sul dispositivo dell'utente; questo accade perché non vengono rispettati i principi delle zero trust, e il paziente zero può così essere infettato dal malware o il ransomware. Inoltre, molte sandbox non impiegano l'analisi su larga scala basata su AI ed ML per rilevare e mettere in quarantena automaticamente le minacce sconosciute e i file sospetti, un aspetto importante per fornire una difesa inline da paziente zero senza che si verifichino interruzioni della produttività.

I sistemi di prevenzione delle intrusioni (IPS) e gli antivirus basati sulle firme non sono in grado di prevenire da soli le minacce O-day e polimorfiche.

I requisiti di una sandbox cloud

Finora gli aggressori hanno avuto la meglio perché hanno saputo sfruttare a loro vantaggio l'architettura mutevole dell'ambiente cloud.

Scegliere la sandbox cloud giusta è fondamentale per prevenire le infezioni da paziente zero e bloccare le minacce avanzate persistenti impedendo loro di accedere alla rete.

La sezione seguente ha lo scopo di aiutarti a comprendere i requisiti specifici da prendere in considerazione per la scelta di una sandbox cloud.

Decifrazione e ispezione su larga scala

Quella della crittografia è considerata una strategia molto promettente per garantire la sicurezza, in quanto consente di proteggere le comunicazioni private e le informazioni sensibili. Purtroppo, anche i criminali informatici sfruttano il traffico cifrato per nascondere i loro payload dannosi.

La decifrazione e l'ispezione del traffico sono processi che richiedono un'elaborazione intensiva; queste operazioni possono trasformare anche i dispositivi sandbox ad alte prestazioni in veri e propri ostacoli che interrompono le attività e generano una latenza inaccettabile.

Quando si valuta una soluzione di sandboxing moderna, è importante capire quali sono i fornitori in grado di offrire operazioni di decifrazione e ispezione illimitate e prive di latenza.

Le minacce tramite HTTPS sono cresciute del 24,3% su base annua, contando 30 miliardi di attacchi cifrati nel 2023.[3]

La checklist prima dell'acquisto:

- ☐ La decifrazione del traffico SSL non deve richiedere hardware aggiuntivo o l'installazione di macchine virtuali (VM)
- ☐ La soluzione deve ispezionare e analizzare i seguenti tipi di file senza latenza o limitazioni di capacità:

EXE	DOC(X)	TAR
DLL	XLS(X)	TGZ
SCR	PPT(X)	GTAR
OCX	APK	RTF
SYS	ZIP	PS1
CLASS	RAR	HTA
JAR	7Z	VBS
PDF	BZ	Script nei file ZIP
SWF	BZ2	

3. Report del 2023 di ThreatLabZ sugli attacchi cifrati

La checklist prima dell'acquisto:

- ☐ Applicazione immediata delle policy per tutti gli utenti con la stessa protezione, sia all'interno che all'esterno della rete aziendale
- ☐ Regole e funzionalità avanzate per la messa in quarantena di tutti i file provenienti da destinazioni sospette
- ☐ Gestione centralizzata delle policy che consente un controllo granulare sulle operazioni di sandboxing, comprese le autorizzazioni in base al tipo di file e i blocchi automatizzati dalle destinazioni sospette

Gestione centralizzata delle policy e delle regole

Evita la gestione impropria delle regole e la configurazione manuale delle sandbox per ogni gateway con la gestione delle policy e le regole centralizzate fornite attraverso il cloud. Prendi in considerazione soluzioni con policy adattive e dinamiche che seguono i principi zero trust delineati dalla pubblicazione del **NIST 800-207**. Con policy di accesso e sicurezza basate sul contesto, che include fattori come il ruolo e la posizione dell'utente, il profilo di sicurezza del dispositivo e i dati che vengono richiesti, lo zero trust riduce al minimo la superficie di attacco. Le soluzioni fornite attraverso il cloud offrono ulteriori vantaggi, che possono consentirti di bloccare le minacce per tutti gli utenti dell'organizzazione. Questo significa niente più ispezioni successive sui file (come ispezioni fuori banda e protezioni applicate quando ormai è troppo tardi) per una sicurezza più sincronizzata. Un aspetto fondamentale delle policy per le sandbox è che offrano la flessibilità per supportare il business, con regole granulari per diversi set di utenti, posizioni, categorie di URL o azioni. I controlli granulari ti consentono di allineare le policy con la tolleranza al rischio e le aspettative prestazionali della tua organizzazione.

Allineamento delle policy alla tolleranza al rischio e alle aspettative prestazionali

Una soluzione sandbox cloud deve controllare i rischi ed eseguire policy conformi all e esigenze specifiche dell'organizzazione. Come primo passo, determina se l'azienda ha:

- **Bassa tolleranza per i file dannosi:** per le organizzazioni avverse al rischio, è possibile scegliere la quarantena come primo intervento per i file sconosciuti o sospetti. Questo garantirà l'assenza di infezioni da paziente zero, perché la sandbox analizzerà il file prima che possa essere scaricato.
- **Bassa tolleranza per la quarantena dei file:** per le organizzazioni tolleranti al rischio e che desiderano evitare ritardi e interruzioni, è possibile scegliere la quarantena e l'isolamento come primo intervento. Questa azione integra la sandbox con le capacità di isolamento del browser sul cloud, fornendo agli utenti un accesso immediato a un PDF di sola lettura senza contenuti attivi mentre la sandbox analizza i file potenzialmente dannosi in background.

Indipendentemente dalle esigenze specifiche, le policy devono essere facili da applicare a tutti gli utenti, i gruppi, i reparti, le sedi e i gruppi di sedi attraverso un'unica piattaforma.

Analisi intelligente e intelligence sulle minacce

Gli aggressori notoriamente riutilizzano gli attacchi che vanno a buon fine, ed è quindi essenziale condividere le protezioni con la community della sicurezza per fermare rapidamente le minacce sul nascere. Le sandbox sul cloud svolgono un ruolo importante in questo, catturando dati di telemetria e condividendo l'intelligence sulle minacce appena identificate con feed e informazioni per la community della sicurezza.

Motore di prevenzione dei malware alimentato dall'AI

Le sandbox distribuite sul cloud sono in grado di gestire modelli di AI/ML a elevata intensità di calcolo, per garantire una protezione di livello superiore.

Cerca una sandbox in grado di identificare, mettere in quarantena e prevenire inline le minacce sconosciute o sospette utilizzando funzionalità avanzate basate su AI/ML, senza la necessità di ulteriori analisi:

- **Verdetti immediati sui file:** comprendendo istantaneamente quali file sono potenzialmente dannosi, gli utenti non devono attendere un verdetto.
- **Prevenzione contro le minacce O-day:** è difficile crederci, ma non tutte le sandbox prevengono le infezioni da paziente zero mettendo in quarantena le minacce sconosciute prima di consentirne il download.

Flussi di lavoro SOC che impiegano l'intelligence sulle minacce

Gli analisti possono necessitare di molte ore di lavoro al giorno per ricercare una singola minaccia. Affidati a una sandbox sul cloud che riduca questo onere e acceleri le indagini e la risposta, condividendo approfondimenti comportamentali e l'intelligence sulle minacce relativi ai payload dannosi. I team di sicurezza dovrebbero essere in grado di supportare le indagini con analisi dirette dei file nelle sandbox tramite l'inoltro attraverso API fuori banda. Assicurati che i feed sulle minacce si integrino con i tuoi strumenti di sicurezza esistenti; questi dovrebbero includere il contesto aggiornato sugli URL segnalati, gli indicatori di compromissione (IoC) estratti e le tattiche, tecniche e procedure (TTP) in base a framework di sicurezza informatica come MITRE ATT&CK®.

La checklist prima dell'acquisto:

- ☐ Funzionalità di quarantena basate sull'intelligenza artificiale che impiegano AI ed ML per fornire un verdetto immediato sui file e fermare le minacce senza richiedere l'analisi dei file
- ☐ Contributo autonomo alle pratiche di protezione giornaliera dalle minacce condiviso tra utenti e reti, indipendentemente dalla posizione
- ☐ Integrazione dei feed sulle minacce con gli strumenti di sicurezza esistenti
- ☐ Inoltro programmato tramite API dei file nelle sandbox fuori banda, con coda separata per i file inviati tramite API

Assicurati di scegliere una sandbox che non fornisca semplicemente un punteggio sulle minacce, ma che sia in grado di delineare le tecniche elusive utilizzate, ad esempio:

- Ritardo di esecuzione del codice per evitare il rilevamento da parte della sandbox
- Acquisizione e visualizzazione del traffico che si muove attraverso la rete
- Apertura di porte per consentire la connettività da remoto
- Tentativo di movimento laterale per individuare gli obiettivi di maggior valore
- Tentativo di consentire il controllo da remoto

Reportistica

Le soluzioni di sicurezza con funzionalità di solo se le informazioni riportate possono essere sfruttate a proprio vantaggio. La reportistica delle sandbox sul cloud dovrebbe:

- Comprendere l'intero ciclo di vita dell'attacco dannoso
- Essere semplice da usare e facile da consultare
- Essere facile da integrare
- Essere disponibile attraverso un'interfaccia di programmazione delle applicazioni (API), in modo da poter essere correlata ai log esistenti
- Fare parte di una piattaforma più ampia, che supporti anche la reportistica sulla conformità

Miglioramento del SOC con il framework MITRE ATT&CK

Quando si valutano le funzionalità di reportistica, è fondamentale che l'intelligence della sandbox possa essere mappata sulla base del **framework MITRE ATT&CK.** Grazie a questa funzione, i team SOC possono impiegare le informazioni ottenute per creare tattiche di difesa da applicare in altre parti dello stack di soluzioni di sicurezza. In questo modo, la sandbox diventa parte integrante dei flussi di lavoro delle operazioni di sicurezza.

A seconda della dimestichezza dell'azienda con questo framework, i report possono essere utilizzati in diversi modi:

- Ridurre le operazioni di classificazione utilizzando la tassonomia fornita
- Visualizzare le tecniche stealth che potrebbero riuscire a eludere la soluzione di rilevazione e risposta degli endpoint (EDR) adottata
- Confrontare e contrastare altri controlli
- Concentrarsi sulle TTP più comuni messe in atto contro l'organizzazione, invece di prevenire inutilmente ogni tipo di tattica e tecnica
- Eseguire un report di reverse engineering

Domande da porre prima dell'acquisto

Per aiutarti durante il processo decisionale, ecco un riepilogo delle domande principali da porre e il motivo per cui dovresti porle:

La sandbox può consentire anche una sola infezione iniziale da paziente zero?

Le sandbox che consentono un'infezione iniziale da paziente zero mentre un file viene analizzato non sono in grado di preservare la sicurezza dell'organizzazione.

La soluzione copre tutti gli utenti e i loro dispositivi, indipendentemente dalla posizione?

I tuoi utenti potrebbero accedere alle risorse aziendali quando sono in movimento, dai propri dispositivi o tramite reti non protette. È fondamentale proteggere tutti i dispositivi che sono essenziali per lo svolgimento del lavoro.[4]

La soluzione effettua il rilevamento inline o richiede l'inoltro dei file fuori banda?

Le soluzioni che funzionano inline possono identificare le minacce e bloccarle direttamente, senza dover fare affidamento sui flussi di rete degli NGFW o implicare il software di EDR degli endpoint.

La sandbox esamina il traffico di tutti i protocolli HTTP, HTTPS, FTP e FTP su HTTP? Ci sono delle limitazioni?

È importante esaminare il traffico per riuscire a smascherare le minacce nascoste. Una sandbox distribuita sul cloud potrebbe essere la soluzione migliore per ispezionare tutto il traffico senza latenza.

È conforme alle leggi e alle normative pertinenti, inclusi i requisiti sullo zero trust?

Le normative sulla conformità possono avere requisiti rigorosi su come il sandboxing debba essere gestito e su questioni correlate all'archiviazione e alla privacy. Trovare una soluzione che operi solo in memoria e rimuova le informazioni di identificazione personale, durante l'analisi, ti aiuta a soddisfare questi requisiti. Inoltre, considera le soluzioni che aderiscono ai principi delle zero trust, come stabilito dagli standard globali NIST 800-207 e usa tali standard come guida per ridurre le superfici di attacco e proteggere i dati.

Con quali altri moduli di sicurezza funziona la sandbox?

I prodotti singoli e isolati non sono in grado di fornire una protezione completa dalle minacce avanzate persistenti (APT). È invece necessario un approccio multilivello di prevenzione, mitigazione, rilevamento e risposta alle minacce. La sandbox rappresenta un livello essenziale e, come tale, deve funzionare in modo efficiente con altre soluzioni e moduli.

4. us.samsung.com/SamsungUS/samsungbusiness/short-form/maximizing-mobile-value-2022/Maximizing_Mobile_Value_2022-Final.pdf

Zscaler Cloud Sandbox e Advanced Threat Protection

È tempo di usare una vera sandbox inline e nativa del cloud

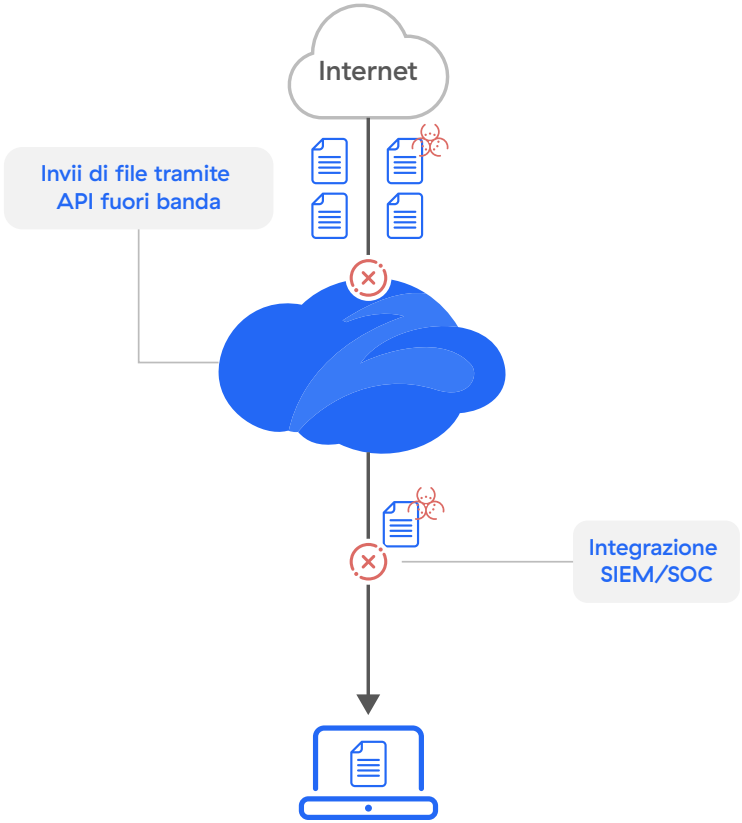
Le organizzazioni sono alle prese con superfici di attacco sempre più estese, e gli aggressori sfruttano le lacune negli stack di soluzioni di sicurezza legacy; per questo motivo, è giunto il momento di scegliere una vera sandbox inline e nativa del cloud. Zscaler Cloud Sandbox è una soluzione creata appositamente per catturare e bloccare le minacce moderne e garantire al contempo la protezione contro i malware O-day per tutti gli utenti e in ogni luogo.

Zscaler Cloud Sandbox si fonda su un'architettura nativa del cloud e proxy, ed è il primo motore di prevenzione dei malware alimentato dall'AI al mondo, in grado di rilevare, prevenire e mettere in quarantena in modo automatico e intelligente le minacce sconosciute e i file sospetti inline. L'ispezione illimitata e senza latenza di tutti i protocolli di trasferimento di file (FTP) e web, inclusi SSL e TLS, consente alla sandbox cloud 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 valore aggiunto della soluzione Zscaler Sandbox AI: è addestrata con oltre 500 milioni di campioni, con aggiornamenti di sicurezza in tempo reale provenienti da 300 bilioni di segnali giornalieri.

La quarantena basata sull'AI blocca i malware sconosciuti

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



Riduzione di complessità e costi

- Facile da distribuire, senza hardware o software da gestire
- Eliminazione dei prodotti ridondanti e isolati
- Eliminazione del backhauling del traffico Internet su MPLS o VPN

Protezione immediata e adattiva di tutti gli utenti e le sedi

- Definizione globale delle policy tramite un'unica console centralizzata
- Applicazione immediata delle policy aggiornate
- Identificazione delle minacce una sola volta e blocco immediato per proteggere tutti i clienti

Rilevamento delle minacce nascoste

- Blocco delle infezioni da paziente zero provenienti da minacce note ed emergenti con la quarantena basata sull'AI
- Upload dei file per l'analisi (portale filecheck)

Una piattaforma integrata fornita come servizio

- Filtraggio preliminare di tutte le minacce dannose note tramite antivirus, liste di blocco degli hash, regole YARA per la classificazione dei malware, rilevamento automatico delle impronte digitali JA3 e modelli di ML/AI
- I feed del CIF (Collective Intelligence Framework) consentono a Zscaler di integrarsi con oltre 60 feed sulle minacce che si aggiungono al feed di Zscaler, il quale sfrutta miliardi di transazioni all'interno del suo bacino di clienti
- Una protezione multilivello che abbina una sandbox cloud a una soluzione EDR consente di migliorare l'efficacia della sicurezza e mitigare l'accesso iniziale, l'esecuzione e le tattiche persistenti

Uno studio di Economic Validation condotto da ESG ha rilevato che Zscaler Zero Trust Exchange ha generato una riduzione del 90% delle apparecchiature di sicurezza.[5]

- Analisi statica, dinamica e secondaria, che include l'analisi del codice e dei payload secondari
- Ispezione SSL illimitata e senza latenza
- Protezione del traffico in entrata e in uscita
- Migliora le indagini di sicurezza e le azioni di risposta grazie a una ricca documentazione forense sull'inoltro dei file tramite API, che include utenti, origine della posizione, tattiche elusive e altro

Zscaler Cloud Sandbox™ è una funzionalità completamente integrata in Zscaler Internet Access™ e che fa parte di Zero Trust Exchange™.

Per maggiori informazioni, visita
zscaler.com/it/technology/cloud-sandbox

5. info.zscaler.com/resources-industry-report-esg-economic-validation

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 di dati, collegando in modo sicuro utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in oltre 150 data center nel mondo, Zero Trust Exchange, basata sul framework SASE, è la piattaforma di cloud security inline più grande del mondo. Per saperne di più, visita il sito **www.zscaler.com/it**.

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