La soluzione per la compliance, il log management e la sicurezza di dati e sistemi aziendali

CONTENUTI

INTRODUZIONE

L'obiettivo di qualsiasi attacco informatico è l'esfiltrazione di dati. Incorporando la tecnologia Anti Data Exfiltration (ADX) di BoxSec nel proprio piano di sicurezza informatica garantisce che non ci sia nulla da guadagnare per l'hacker. Senza esfiltrazione di dati non vi è violazione, ransomware o estorsione. Quando i criminali informatici non possono appropriarsi di dati, passano al bersaglio successivo.

Il ransomware è una delle più grandi minacce che tutte le organizzazioni a livello globale stanno affontando, e gli attacchi stanno diventando più frequenti e più sofisticati. I criminali informatici stanno costantemente sviluppando nuove tattiche e strumenti per abbattere le barriere di difesa tradizionali come firewall, antivirus, DLP, XDR ed EDR. Gli Hacker sono sempre più concentrati sull'estorsione, come confermato dalla ricerca del 2022 che ha rilevato che l'89% degli attacchi ransomware include l'esfiltrazione di dati.

La nuova generazione di tecnologia ADX di BoxSec fornisce un nuovo approccio nella lotta contro gli attacchi informatici. Scopri di più in questa guida interattiva progettata per aiutarti a vendere BoxSec e condividere i concetti chiave di ADX con i tuoi clienti e partner.

Chi è CerebroSec

CerebroSec, ideatore di BoxSec, è stata fondata nel 2019, per affrontare le nuove minacce alla sicurezza informatica da parte di ransomware. Le tecnologie esistenti sono inefficaci nel fermare il ransomware e non si concentrano sul problema chiave che porta alla perdita e l'esfiltrazione di dati.

BoxSec e' pioniere di una nuova categoria chiamata Anti Data Exfiltration (ADX) creando una tecnologia all'avanguardia per il mercato globale. La tecnologia "end-point" di BoxSec funziona su dispositivi mobili e desktop, fornendo protezione contro le minacce alla sicurezza globale come ransomware, spyware, malware, phishing, raccolta di dati e profiling non autorizzati.

ACQUIRENTI CHIAVE

In media ci sono più di 7 persone coinvolte nelle decisioni di acquisto di nuove soluzioni nella maggior parte delle organizzazioni, la maggior parte delle quali non sono in realtà addetti alla sicurezza. Si possono includere infrastruttura e operation, networking, ufficio acquisti, architetto/ingegnere cloud, software developer.

I generalisti IT svolgono un ruolo chiave nelle decisioni di acquisto. Altri ruoli coinvolti nel processo decisionale potrebbero includere project manager, compliance e architetti. E' importante comprendere le avversita' giornaliere, non solo dell'organizzazione stessa, ma quali problemi o sfide devono affrontare questi decisori nelle loro aree specialistiche e come BoxSec può aiutare a superare questi ostacoli.

Focalizzati su quelli che sono i recquisiti e i bisogni chiave: solo perché non corrispondono ai nostri acquirenti chiave non significa che non facciano parte di un team decisionale. Nelle organizzazioni più ampie, i dirigenti potrebbero non impegnarsi nel processo di acquisto di nuove tecnologie fino a quando i compiti di base non saranno stati completati dai membri di competenza.

Interagisci con acquirenti reali e forniscici feedback per comprendere meglio il bisogno dell'utente finale.

CISO

Dimensione azienda:
Ampia o Multinazionale

Team:
Guida oltre 20 professionisti IT/sicurezza

Responsabile di:
Protezione dei dati, delle risorse e dei programmi aziendali. Aspetti di gestione del rischio del ruolo.

Conoscenza della sicurezza informatica:
Elevato livello di conoscenza del settore e degli strumenti disponibili. Si tiene aggiornato con le novità del settore, le tendenze e le nuove soluzioni del mercato.

Strumenti di sicurezza informatica attuali:
MDR o XDR o altri strumenti tradizionali. Sofisticata suite di strumenti. Personale dedicato esclusivamente alla cybersecurity. Soluzioni tradizionali come Firewall e Antivirus (McAfee, Norton, Kaspersky ecc.). Potrebbe semplicemente utilizzare le difese gia' integrate nei sistemi . (il 70% delle piccole imprese non sono preparate ad affrontare un attacco informatico)

Marchi in uso:
Crowdstrike, SentinelOne o altri grandi brands

Bilancio:
Sostanziale – una ventina di strumenti in uso (il 22% utilizza più di trentuno strumenti)

Livello decisionale:
Fa rapporto al CIO o consiglio di amministrazione (il 90% dei CISO riporta direttamente al proprio consiglio di amministrazione)

Obiettivi:

- Fornire all'organizzazione gli strumenti per prevenire in modo efficiente un attacco informatico (l'89% ritiene di poter chiaramente determinare le giuste soluzioni per le esigenze aziendali)
- Gestione del rischio e caccia alle minacce per garantire l'assenza di vulnerabilità
- Ridurre i punti di contatto manuali per limitare i fattori di stress
- Adottare nuove tecnologie (il 50% fa fatica ad adottare nuove tecnologie a causa di problemi di integrazione o problemi legati all'infrastruttura legacy)

Avversita':

- Gestire la sicurezza di un gran numero di dispositivi, app e programmi
- La copertura del personale è in genere dal lunedì al venerdì
- Livello di abilità del personale (il 32% non adotta nuove tecnologie a causa della mancanza di abilità nel team)
- Dati di diversi livelli di sensibilità da proteggere in modo appropriato
- Dipendenti in varie sedi o che lavorano da remoto
- Fornitori con propri piani di sicurezza informatica: devono essere monitorati e verificati.
- Stress – lavoro ad alta pressione! (Il 41% ha lasciato o è stato licenziato dopo un attacco informatico, con solo il 44% che si diverte a fare il "protettore")
- Aspettative vs budget (il 75% ha dichiarato il pieno allineamento tra le aspettative del Consiglio di amministrazione su cio' che ci si puo' aspettare in base alle soluzioni in utilizzo)
- Costi/budget (il 22% lascerebbe il ruolo per mancanza di budget per le nuove tecnologie. 22% ha riferito che garantire un budget aggiuntivo era una delle loro maggiori priorità entro i primi sei mesi d'impiego)
- Tenersi aggiornati con le nuove tecnologie (il 52% ha ammesso di avere difficoltà a stare al passo con i nuovi framework. Il 54% non è in grado di tenere il passo con le nuove informazioni sulle ultime soluzioni per la sicurezza informatica)

Esigenze:

- Processi automatizzati per limitare i punti di contatto e l'intervento umano per garantire la protezione durante le ore non lavorative e nei giorni festivi
- Monitoraggio centralizzato di tutti i dispositivi sulla rete e delle eventuali minacce e vulnerabilita'
- Soluzione per coprire i lavoratori remoti e le connessioni non sicure, ad esempio: aeroporti, hotel, conferenze
- Sul dispositivo: sempre protetto e non solo quando è all'interno del network aziendale
- Soluzione scalabile: facile aggiunta o rimozione di dispositivi a costi ragionevoli
- Gestione dei trend: sapere da dove potrerebbero provenire le minacce e come ridurne l'efficacia
- Tutti i tentativi di minaccia informatica bloccati – tentativi di phishing ecc.
- Una soluzione che fornisce servizi aggiuntivi e consulenza/guida
- Individuare le vulnerabilità nella propria rete

Cosa vogliono sentirsi dire:

- Promuovere un approccio unico per risolvere i loro problemi
- Comprendere i loro obiettivi, budget e livello di influenza
- Conoscere la loro azienda e settore: strumenti utilizzati, panorama informatico e problemi
- Promuovere scalabilità, convenienza economica e servizi aggiuntivi
- Cosa possiamo fare per rendere la loro vita più semplice? Automazione, Enterprise Console, un nuovo punto di vista sul come affrontare il problema
- Funziona con gli attuali strumenti di sicurezza informatica
- POV – provare per credere prima di investire tempo e denaro
- Configurazione semplice, gestione semplice, libera larghezza di banda dei dipendenti

Altri punti:

- Ai CISO piace conoscere il prodotto prima della demo
  - Ricerca effettuata da un membro dello staff
- Utilizzare le connessioni in rete principalmente per il passaparola o per la nuova adozione della tecnologia
  - Può essere difficile convincerlo a diventare un "early adopter"
  - Ama leggere casi di studio e storie di successo come loro
  - Cerca la convalidita' da altri CISO e analisti.

CEO/PROPRIETARIO

Dimensione azienda:
SME/SMB (il 43% di tutti gli attacchi informatici prende di mira le piccole imprese)

Squadra:
Risorse IT o di sicurezza informatica interne scarse o assenti (il 52% non dispone di esperti di sicurezza IT interni)

Responsabile di:
Operazioni generali e risorse per il business

Conoscenza della sicurezza informatica:
Dipende, ma generalmente ha una conoscenza limitata e non oltre la terminologia di base

Strumenti di sicurezza informatica attuali:
Strumenti limitati possibilmente antivirus, firewall o altri approcci tradizionali. Può avere strumenti EDR o XDR su piccola scala. Può esternalizzare a MSP/MSSP. Ha bisogno di una soluzione completa. (il 70% delle piccole imprese non è preparato ad affrontare un attacco informatico)

Marchi in uso:
Budget ridotto per la sicurezza informatica, a volte legato al budget IT

Bilancio:
Alto – può rispondere a un consiglio nominato o agli investitori

Livello decisionale:
Alto – potrebbe fare rapporto ad un consiglio di amministrazione o investitori.

- **Obiettivi:**
- Crescita aziendale
- Strategie chiare per i progetti
- Attenzione ai clienti
- Mantenere buoni rapporti con i clienti/fornitori attuali
- Nuove opportunità per investimenti da terzi

Avversita':

- Decisori chiave per la maggior parte, se non per tutti, gli aspetti dell'azienda
- Vincoli di bilancio
- Risorse limitate da dedicare all'adozione di nuove tecnologie
- Gestione di terzi (Servizi esterni)
- Sensibilita' dati
- Gestione di dipendenti in smart working
- Assicurazione Cybersecurity (All'inizio del 2022, il 91% di SMB non aveva nessun tipo di polizza assicurativa)
- Necessita di dati sul ROI per progetti o nuove tecnologie

Esigenze:

- I prodotti per la sicurezza della rete devono essere centralizzati, facilli da usare e gestire.
- Allineamento al budget
- La soluzione deve essere scalabile
- Se le mansioni IT sono affidate a terzi, serve che la soluzione sia compatibile con il workflow del service provider
- Una soluzione per rafforzare le difese tradizionali (firewall, antivirus)
- Attività automatizzate: nessuna risorsa di personale o molto tempo dedicato a tale soluzione
- Difese sufficienti per consentire migliori opzioni di polizza assicurative (se lo si desidera)
- Supporto

Cosa vogliono sentirsi dire:

- Comprendere la loro azienda, i loro budget e il loro settore
- Promuovere il supporto non solo per la soluzione, ma anche per il nostro servizio vCISO
- Rendi la loro vita più facile/una cosa in meno di cui preoccuparsi: automazione, percentuali di successo, ecc
- Facile da configurare e utilizzare: limita il tempo impiegato e la manodopera/risorse necessarie per iniziare
- Funziona bene con altri servizi di sicurezza informatica tradizionali: ulteriore livello di protezione
- Assicurazione sulla sicurezza informatica approvata
- Potrebbe pensare di avere tutto ciò di cui ha bisogno con l'attuale suite di difesa

IT MANAGERS

Dimensione azienda:
Impresa di medie dimensioni

Squadra:
Dipendenti sotto di lui/lei ma non necessariamente ruoli specifici di sicurezza informatica. Conterrà personale di supporto IT.

Responsabile di:
Tutte le funzionalità e i programmi IT in tutta l'azienda, inclusi hardware, software, reti, cloud e sicurezza informatica. I membri del team forniranno supporto IT ai dipendenti.

Conoscenza della sicurezza informatica:
Conoscenza completa della sicurezza informatica e degli strumenti che possono essere utilizzati per prevenire gli incidenti. Conoscenze approfondite specifiche limitate.

Strumenti di sicurezza informatica attuali:
EDR e XDR. Può ancora utilizzare alcuni strumenti più tradizionali in aziende di piccole dimensioni.

Bilancio:
Budget IT nel suo insieme, non specificamente suddiviso per la sicurezza informatica

Livello decisionale:
Basso: sarà probabilmente inferiore nella linea di segnalazione rispetto ai CISO e potrebbe riferire al CIO o al CTO. Tuttavia, l'80% delle organizzazioni afferma che l'IT è coinvolto nella valutazione e nell'approvazione degli acquisti di sicurezza.

Obiettivi:

- Approccio innovativo all'infrastruttura IT e operazioni semplificate
- Identificare le opportunità per migliorare l'efficienza e supportare al meglio l'azienda
- Soddisfare le esigenze, comprese le esigenze di supporto, dell'organizzazione e dei dipendenti al suo interno.
- Sfruttare le nuove tecnologie per migliorare le operazioni tecniche
- Costruire solide relazioni con fornitori.

Avversita':

- Conformità a legalità e regolamenti
- Varie responsabilità – nessun focus dedicato
- Vincoli di budget – risorse costose
- Costante necessità di fornire soluzioni innovative
- Responsabile di un team con ruoli diversi
- problemi ricorrenti basati sulla tecnologia

Esigenze:

- Supporto sulle nuove tecnologie – ne hanno troppe per poter sapere tutto
- Semplice e facile da usare
- Reports e gestione centralizzate
- Threat hunting e visibilita' delle vulnerabilità
- Copertura 24/7

Cosa vogliono sentirsi dire:

- Comprendere la loro azienda, i budget e l'industria
- Promuovere il supporto non solo per la soluzione, ma anche per il nostro servizio vCISO
- Automazione e processi di sicurezza informatica semplificati
- Facile da configurare e utilizzare: limita il tempo impiegato e la manodopera/risorse necessarie per iniziare
- Funziona bene con altri servizi di sicurezza informatica tradizionali: ulteriore livello di protezione
- Assicurazione sulla sicurezza informatica approvata
- Funzionalità di ricerca delle minacce e report sulle tendenze

PROPRIETARI DI PICCOLE IMPRESE

Dimensione azienda:
Piccole imprese (il 43% di tutti gli attacchi informatici prende di mira le piccole imprese)

Squadra:
Meno di 20 dipendenti su tutta l'organizzazione. Probabilmente nessuno staff IT dedicato. (il 52% non dispone di esperti interni di sicurezza informatica)

Responsabile di:
Controllo completo sul business. Può rispondere agli investitori. Responsabile delle decisioni per tutte le funzionalità e le risorse operative

Conoscenza della sicurezza informatica:
Poca o nessuna conoscenza specifica della sicurezza informatica.

Strumenti di sicurezza informatica attuali:
Soluzioni tradizionali come Firewall e Antivirus (McAfee, Norton, Kaspersky ecc.).
Potrebbe semplicemente utilizzare le difese gia' integrate nei sistemi.
(il 70% delle piccole imprese non sono preparate ad affrontare un'attacco informatico)

Bilancio:
Budget limitato per IT e sicurezza informatica. Non vede necessariamente la sicurezza informatica come una priorità per l'azienda. (il 51% afferma di non stanziare alcun budget per la sicurezza informatica)

Livello decisionale:
Alto – decisore per l'intera azienda

Obiettivi:

- Crescita aziendale
- Strategie chiare per i progetti
- Attenzione ai clienti
- Mantenere buoni rapporti con i clienti/fornitori attuali
- Nuove opportunità per investimenti da terzi

Avversita':

- Molta responsabilità – difficile concentrarsi
- Vincoli di bilancio
- Piccola forza lavoro che lavora da casa?
- Dovrebbero esternalizzare alcuni aspetti del business? Troppo costoso? Un'altra cosa da gestire?

Esigenze:

- Una soluzione che può "fare tutto"
- Supporto ed a volte consigli per rimediare ad un problema
- Automazione 24/7

Cosa vogliono sentirsi dire:

- Comprendere la loro azienda, i loro budget e il loro settore
- Promuovere il supporto non solo per la soluzione, ma anche per il nostro servizio vCISO
- Rendi la loro vita più facile/una cosa in meno di cui preoccuparsi: automazione, percentuali di successo, ecc
- Facile da configurare e utilizzare: limita il tempo impiegato e la manodopera/risorse necessarie per iniziare
- Funziona bene con altri servizi di sicurezza informatica tradizionali: ulteriore livello di protezione
- Assicurazione sulla sicurezza informatica approvata

DIFFERENZE CHIAVE

1 BoxSec ha creato una nuova categoria

L'Anti Data Exfiltration (ADX) di BoxSec fornisce un nuovo paradigma nella lotta contro ransomware e attacchi informatici. Invece di concentrarsi sulla difesa, come il 99% degli altri prodotti, BoxSec si concentra su ciò che conta davvero, i dati stessi.

2 BoxSec utilizza "Network filtering" in tempo reale

La tecnologia ADX di BoxSec filtra il traffico di rete in tempo reale e opera sul livello 3 del modello OSI (modello concettuale ISO). Utilizzando avanzati algoritmi basati sull'intelligenza artificiale, può fermare gli attacchi informatici e impedire l'esfiltrazione di dati da un dispositivo, proteggendo segreti commerciali, proprietà intellettuale, informazioni di identificazione personale (PII), furto di dati ed estorsione.

3 BoxSec fornisce protezione sul dispositivo per ogni dispositivo

BoxSec protegge tutti i dispositivi e tutte le piattaforme. Il sistema fornisce la gestione completa di tutti i dispositivi nel Cloud con un'unica installazione dell'agente su ciascun dispositivo. BoxSec è completamente orchestrato in base alla progettazione, senza costi di gestione o configurazioni complesse, richiede meno dell'1% di sovraccarico della CPU e funziona 24 ore su 24, 7 giorni su 7.

4 BoxSec si concentra sulla prevenzione piuttosto che sulla difesa

La sofisticatezza degli attacchi odierni ha reso le soluzioni di sicurezza esistenti obsolete.
Le tecnologie di prima generazione come Antivirus che utilizzano le tradizionali "fingerprint technologies" non funzionano più.
Allo stesso modo, le tecnologie di seconda generazione come EDR e XDR si concentrano su approcci difensivi che, sebbene migliori, non riescono comunque a prevenire gli attacchi e fanno molto affidamento sui reparti IT per identificare e rispondere a minaccie.
BoxSec blocca l'attacco in tempo reale dando la priorità alla sicurezza dei dati e all'esfiltrazione dei dati dal dispositivo per eliminare direttamente ogni tentativo di estorsione. Anziche' permettere l'infezione di un sistema, BoxSec si concentra sulla prevenzione dell'attacco in primo luogo, proteggendo la privacy dei dati aziendali e rafforzando la conformità normativa.

5 BoxSec fornisce protezione ransomware di terza generazione

La tecnologia ADX di BoxSec blocca con successo il 99% dei ransomware, eliminando efficacemente violazioni dei dati, estorsioni e multe normative.

6 BoxSec fornisce protezione 24 ore su 24, 7 giorni su 7

Anziché dover allocare risorse per monitorare e rispondere agli allarmi, BoxSec fornisce una protezione completamente automatizzata 24 ore su 24, 7 giorni su 7 per prevenire gli attacchi informatici, incluso il ransomware, in tempo reale.

ADX VS

ADX VS EDR

Le soluzioni EDR e XDR forniscono la necessaria protezione degli endpoint, nonché il rilevamento, l'indagine e la risposta alle minacce utilizzando l'intelligence sulle minacce e l'analisi dei dati. CrowdStrike e Sentinel One sono alcuni degli strumenti e competitor più referenziati che incontriamo attualmente sul campo.

I Pro	I Contro	BoxSec la soluzione
Proteggiti da attacchi frequenti e altamente distruttivi	Gli EDR basati sull'intelligenza artificiale non sono sempre in grado di fornire soluzioni persistenti e proteggibili per il rilevamento delle minacce al 100%.	BoxSec utilizza l'analisi comportamentale per identificare e bloccare attività sospette prima che inizi l'attacco
Rileva le minacce sfuggenti e rivelane l'intera portata e le origini		Le minacce vengono bloccate prima che diventino dannose. La nostra scheda di ricerca delle minacce mostra i dati necessari per indagare su un evento tra cui origini, posizioni, ricerche inverse IP e feed da fonti interne ed esterne
Risponde immediatamente per prevenire costose interruzioni dell'attività	Non tutte le risposte sono automatizzate, quindi sono necessari input e risposte umane.	BoxSec blocca le minacce in base alle regole del dispositivo, il che significa che l'azione è automatica ed eseguita dall'agente sul dispositivo. Nessun intervento umano richiesto.
Controlli centralizzati automatizzati e semplici	Alcune soluzioni EDR non possono facilitare la protezione e la reportistica multipiattaforma e richiedono "una spinta" per installare gli aggiornamenti	La nostra tecnologia può funzionare sulla maggior parte delle piattaforme e tutti i report sono disponibili dalla nostra Enterprise Console. I nostri aggiornamenti vengono completati automaticamente tramite l'agente sul dispositivo.
	L'EDR tradizionale richiede personale specializzato	Grazie alla natura automatizzata della tecnologia BoxSec, la soluzione non richiede personale specializzato per monitorare o reagire a minacce o attacchi, eliminando la necessità di risorse dedicate. La nostra Enterprise Console fornisce una visione centralizzata e facile da usare di ciò che accade su tutti i dispositivi aziendali.
	Può essere scarsamente attrezzato per prevenire l'esfiltrazione di dati a causa di errori dei dipendenti e furto di credenziali: richiede l'intervento umano	La funzione principale di BoxSec è prevenire l'esfiltrazione dei dati e lo fa monitorando il traffico in uscita e limitando i dati che lasciano il dispositivo in circostanze specifiche e sospette.
	La maggior parte degli EDR sono basati sul cloud	BoxSec offre protezione sul dispositivo stesso e non necessita di mandare traffico di rete a un server o in cloud per l'analisi di un'evento

ADX VS DLP

La prevenzione della perdita di dati (DLP) è uno degli approcci più popolari per mantenere i dati sensibili al sicuro per le organizzazioni. Trattandosi di un approccio tradizionale, può avere difficoltà ad accogliere i cambiamenti organizzativi e le esigenze della forza lavoro moderna.

ADX si basa sulla tecnologia alla base della DLP, rendendola più rilevante per la forza lavoro odierna e le minacce alla sicurezza.

I Pro	I Contro	BoxSec la soluzione
Proteggiti da attacchi frequenti e altamente distruttivi	Il rigoroso insieme di Policy e' progettato per limitare la capacita' di autenti non-autorizzati di compromettere i dati – Le Policy sono complesse e richiedono cospicue risorse per modificarne i contenuti	La tecnologia di BoxSec è facile da adattare, modificando facilmente regole e policy quando necessario.
Rileva minaccie elusive e ne rilvela le origini	Non discrimina tra gli utenti, quindi non è in grado di rilevare differenze tra comportamenti dannosi, manipolazione sociale o errori involontari.	Invece di un dizionario di firme di attacco, la tecnologia ADX utilizza l'analisi comportamentale per identificare comportamenti insoliti incentrati sull'utente. ADX esamina tutti i tipi di attacco ed è in grado di identificare e bloccare qualsiasi tentativo non autorizzato di esfiltrare qualsiasi tipo di informazione da un utente/dispositivo.
	Le soluzioni DLP tradizionali sono costose da gestire e utilizzare, richiedono enormi risorse di elaborazione e monitoraggio e gestione costanti. Funziona ai margini della rete come un firewall. Nell'ambiente di lavoro remoto di oggi questo ha un uso limitato e non fornisce alcuna protezione a questi lavoratori.	La tecnologia ADX di BoxSec è un approccio "imposta e lascia" alle difese. Non richiede monitoraggio o gestione costante poiché identifica le minacce e le blocca in tempo reale. La console Enterprise consente di visualizzare tutte le minacce in un unico posto e può aiutare a identificare le tendenze degli attacchi e le vulnerabilità all'interno dei tuoi dispositivi e delle tue reti. Modifiche o nuovi utenti/sistemi possono essere gestiti facilmente con ADX poiché è scalabile e richiede solo l'aggiunta di una licenza sul dispositivo dell'utente finale. Quando si modificano le regole, come ad esempio l'inserimento nella whitelist di determinati siti Web, il semplice processo può essere eseguito sulla console Enterprise da utenti autorizzati. ADX ha un ingombro notevolmente inferiore rispetto a DLP, esaminando il traffico in entrata e in uscita senza utilizzare una grande quantità di potenza di calcolo o memoria. Gli utenti di BoxSec commentano inoltre che la loro connessione è 2 volte più veloce a causa del blocco degli annunci indesiderati mentre sono online.
	La DLP rompe la catena della sicurezza, richiedendo un'introspezione diretta e agendo da intermediario. Ciò rompe la fiducia tra la fonte e la destinazione.	ADX non richiede un "intermediario". Grazie all'identificazione e al blocco automatico delle minacce, non vi è alcuna interruzione in nessuna fase del processo difensivo.Solo gli utenti privilegiati e gli account autorizzati possono inviare informazioni all'esterno della rete.

ADX VS ANTIVIRUS

L'antivirus è progettato per rilevare e rimuovere virus e altri tipi di software dannosi dal tuo dispositivo. Alcuni sostengono che, date le nuove tecnologie, l'antivirus non sia più uno strumento necessario.

I Pro	I Contro	BoxSec la soluzione
Protegge da virus e spyware. Dispone di protezione web, protezione antispam e firewall	Alcuni software antivirus non sono in grado di difendersi dalle minacce sofisticate e hanno difficoltà una volta che l'attacco inizia nella rete. Si basa sulla protezione delle impronte digitali che è inefficace con gli attuali attacchi polimorfici (impronta digitale che cambia costantemente)	BoxSec protegge da tutti i tipi di minacce informatiche senza utilizzare le impronte digitali. Utilizzando la profilazione comportamentale, continua a funzionare una volta che la rete è stata infiltrata. La tecnologia ADX garantisce che nessun dato venga esfiltrato dal tuo dispositivo da hacker.
Conveniente: alcuni sono completamente gratuiti e altri hanno abbonamenti minimi	Gli abbonamenti economici o gratuiti non forniscono una protezione completa: alcune funzionalità potrebbero essere limitate alle versioni premium	BoxSec è conveniente e tutte le versioni del nostro prodotto forniscono una protezione completa. Il nostro modello di abbonamento consente alle organizzazioni di scalare facilmente quando necessario.
	Può utilizzare molta memoria e risorse del disco rigido, il che può rallentare notevolmente la velocità complessiva del dispositivo	L'agente BoxSec e' molto leggero e consuma meno dell1% della CPU di un dispositivo. Anche le attivita' online sono significatamente piu' veloci.
	Se sono presenti buchi di sicurezza o vulnerabilità, un virus può aggirare il software antivirus. Se il software non e' aggiornato può essere inefficace. Le nuove minacce richiedono molto tempo da parte del fornitore per reagire.	Gli aggiornamenti di BoxSec vengono eseguiti automaticamente in modo da avere sempre la versione più recente. Ogni 2 settimane vengono inoltre rilasciate nuove regole per affrontare nuove vulnerabilità e tecniche di hacheraggio.
	Assistenza clienti assente o limitata	La tecnologia di BoxSecx è molto intuitiva, rendendola molto semplice da usare, navigare e configurare. Il nostro team di supporto è sempre a disposizione per rispondere a qualsiasi domanda dei clienti tramite e-mail o chat.

DOMANDE FREQUENTI

Cos'è l'ADX?

ADX è una tecnica utilizzata per impedire che dati non autorizzati lascino un dispositivo. Prendendo di mira più parti della "kill chain", ADX blocca efficacemente l'attivazione e la diffusione degli attacchi informatici. Poiché gli attacchi informatici, in particolare il ransomware, si concentrano sul furto di dati a scopo di estorsione, questa è diventata una soluzione importante per contrastare i moderni attacchi polimorfici che non possono essere fermati dalle soluzioni antivirus tradizionali.

Come funziona ADX?

ADX funziona esaminando i dati in uscita sui dispositivi endpoint. Ciò rende l'utilizzo di risorse CPU nettamente inferiori rispetto ad altre soluzioni, come firewall o DLP, che esaminano il traffico in entrata e in uscita ai margini della rete. Le soluzioni ADX sono abbastanza leggere da poter essere eseguite su dispositivi mobili e non è necessario che funzionino sulla rete aziendale.
Le soluzioni ADX utilizzano analisi comportamentale per identificare comportamenti insoliti incentrati sull'utente. ADX limita la possibilità per gli utenti, inclusi gli utenti con privilegi e gli amministratori, di inviare dati sensibili all'esterno della rete

Che ruolo gioca ADX in una strategia di sicurezza informatica?

L'obiettivo di qualsiasi attacco informatico è l'esfiltrazioen di dati. L'aggiunta di una soluzione ADX ad una strategia di sicurezza informatica garantisce che non ci sia nulla da guadagnare per un utente malintenzionato. Senza esfiltrazione di dati non vi è violazione, riscatto o estorsione. Quando i criminali informatici non possono appropriarsi di dati, passano al bersaglio successivo

Cosa lo rende un approccio diverso?

Sappiamo che qualsiasi criminale informatico intento ad infiltrarsi in un dispositivo o in una rete alla fine troverà un modo per entrare, indipendentemente dalle soluzioni di difesa perimetrale in atto. ADX guarda al problema in un modo nuovo. Supponendo che i malintenzionati entreranno nella rete, si concentra sull'impedire loro di uscire con i dati di un'organizzazione. Nessuna esfiltrazione di dati significa che nessun attacco informatico e' riuscito nell'intento.

Cos'è il modulo Threat Hunting?

L'esclusivo modulo "Threat Hunting" fornisce informazioni sulle minacce per tutte le aziende, dove in precedenza solo le organizzazioni con determinati budget e team di esperti erano in grado di beneficiare di questo tipo di informazioni. Questo modulo porta il "Threat Intelligence" ad un nuovo livello fornendo approfondimenti dettagliati su ciascuna minaccia identificata, consentendo ai team di competenza di stare al passo con i criminali informatici. Con approfondimenti come l' impatto del "crowdsourcing", il livello di fiducia e la classificazione MITRE, le capacità di "Threat Hunting" sono in grado di identificare falsi positivi, indagare sulle origini delle minacce e fornire analisi dei rischi.

Che cos'è il modulo di monitoraggio delle violazioni?

Il modulo di monitoraggio dei "Breach" consente ad un'organizzazione di monitorare la propria esposizione sul Dark Web con una regolare scansione del dominio. Con oltre 10 miliardi di account esposti sul Dark Web, BoxSec ti assicura di essere avvisato in tempo reale quando si è verificata una violazione. Il modulo consente inoltre il benchmarking con i colleghi del settore e la facile generazione di report.

Quali problemi risolve BoxSec?

BoxSec fornisce la privacy dei dati del dispositivo, la sicurezza dei dati e la prevenzione di ransomware. La tecnologia ADX previene ransomware, spyware, malware, phishing, raccolta e profilazione non autorizzate dei dati e mitiga i rischi associati a violazioni dei dati e minacce interne. BoxSec elimina efficacemente il rischio di estorsione che è di norma per tutti coloro che diventano vittime di ransomware.

In che modo BoxSec è diverso da DLP?

BoxSecx fornisce la privacy dei dati del dispositivo, la sicurezza dei dati e la prevenzione di ransomware. La tecnologia ADX previene ransomware, spyware, malware, phishing, raccolta e profilazione non autorizzate dei dati e mitiga i rischi associati a violazioni dei dati e minacce interne. BoxSec elimina efficacemente il rischio di estorsione che è di norma per tutti coloro che diventano vittime di ransomware.

Per un confronto più dettagliato, dai un'occhiata alla sezione ADX vs DLP.

Quali prodotti BoxSec potrebbe aiutarmi a sostituire?

BoxSec può sostituire qualsiasi prodotto AV ed EDR.

Quali minacce informatiche previene BoxSec?

La tecnologia di BoxSec previene ransomware, spyware, malware, phishing, raccolta e profilazione non autorizzate dei dati e mitiga i rischi associati a violazioni dei dati e minacce interne.