Perché BlackFog è diverso

Che cos'è ADX

ADX è una tecnica utilizzata per impedire ai dati, non autorizzati, di lasciare un dispositivo. Mirando a più parti della catena decisionale, ADX blocca efficacemente l'attivazione e la diffusione di attacchi informatici. Il ransomware si concentra sul furto di dati per estorsione ed ADX è diventato importante per contrastare i moderni attacchi polimorfici, che non possono essere fermati dalle tradizionali soluzioni antivirus.

Come funziona ADX?

ADX funziona sulla base dello studio dei dati in uscita dagli endpoint. Ciò gli conferisce un ingombro notevolmente inferiore rispetto ad altre soluzioni, come i firewall o DLP, che esaminano il traffico in entrata ed in uscita ai margini della rete. Invece di confrontare il traffico con un dizionario di firme di attacco, la soluzione ADX utilizza l'analisi comportamentale, per identificare comportamenti insoliti incentrati sull'utente. ADX limita la possibilità per gli utenti – inclusi utenti e amministratori privilegiati – di inviare dati sensibili al di fuori della rete.

Quale ruolo svolge ADX in una strategia di sicurezza informatica?

L'obiettivo di qualsiasi attacco informatico è il furto di dati. L'aggiunta della soluzione ADX ad una strategia di sicurezza, garantisce che non vi sia nulla da guadagnare per un malintenzionato. Senza l'esfiltrazione dei dati non vi è alcuna violazione, nessun riscatto e nessuna estorsione. Quando i criminali informatici non possono rubare i dati, passano al target successivo.

Cosa lo rende un approccio diverso?

Sappiamo che qualsiasi criminale informatico intenzionato a infiltrarsi in un dispositivo o in una rete, alla fine troverà un modo per entrare, indipendentemente dalle soluzioni di difesa

perimetrale in atto. ADX esamina il problema in un modo nuovo. Partendo dal presupposto che i cattivi attori entreranno nella rete, si concentra sulla prevenzione della loro uscita con i dati di un'organizzazione. Nessuna esfiltrazione di dati significa nessun attacco informatico di successo.

Quali problemi risolve BlackFog?

BlackFog fornisce la privacy dei dati, sicurezza dei dati e prevenzione del ransomware. La tecnologia ADX di BlackFog previene ransomware, spyware, malware, phishing, raccolta e profilazione di dati non autorizzati e mitiga i rischi associati a violazioni dei dati e minacce interne. BlackFog elimina efficacemente la minaccia di estorsioni, che è diventata la norma per attacchi ransomware di successo.

Quali prodotti potrebbe aiutarmi a sostituire BlackFog?

BlackFog può sostituire qualsiasi prodotto AV ed EDR. Può anche lavorare a fianco delle soluzioni esistenti per fornire un ulteriore livello di protezione.

Prevenzione e protezione

Qual è il modulo di prevenzione alle minacce di BlackFog?

BlackFog è l'unico prodotto che fornisce informazioni sulle minacce, senza distinzione di grandezza aziendale, non necessita di grandi budget per implementare la tecnologia e fornisce un team di esperti per beneficiare dell'intelligence sulle minacce. BlackFog porta l'intelligence delle minacce a un nuovo livello, fornendo approfondimenti dettagliati su ciascuna minaccia identificata, consentendo alle organizzazioni di stare al passo con i criminali informatici, man mano che il panorama delle minacce si evolve. La capacità di caccia alle minacce di BlackFog permette di identificare falsi positivi, indagare sulle origini delle minacce e fornire analisi dei rischi.

Qual è il modulo di monitoraggio della violazione?

Il modulo Breach Monitoring di BlackFog consente ad un'organizzazione di monitorare la propria esposizione sul Dark Web con una normale scansione del dominio. Con oltre 10 miliardi di account esposti sul Dark Web, BlackFog ti assicura di essere avvisato in tempo reale quando si è verificata una violazione. Il modulo consente inoltre il benchmarking rispetto ad altri prodotti del settore ed una facile generazione di report.

In che modo BlackFog è diverso da un DLP?

Data Loss Prevention (DLP) è uno degli approcci legacy più popolari, per mantenere i dati sensibili sicuri. E' un approccio di rete tradizionale sviluppato negli '90, ma oggi fa fatica a soddisfare le esigenze di sicurezza. ADX si basa sulla tecnologia alla base di DLP, rendendolo più performante contro le minacce alla sicurezza. A differenza del DLP classico, che richiede una serie rigorosa di politiche, difficili da implementare e modificare, BlackFog è facile da implementare e completamente automatizzato.

Quali minacce informatiche previene BlackFog?

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

BlackFog mi proteggerà dal ransomware?

Assolutamente! Il 100% dei clienti BlackFog non ha subito un attacco ransomware con esfiltrazione dei dati. Vale anche la pena ricordare che BlackFog scopre regolarmente le minacce ransomware nella prima fase, sin dall'inizio dei movimenti laterali, anche in presenza di più soluzioni di sicurezza informatica.

Anti Data Exfiltration (ADX): Beyond Antivirus ed EDR

BlackFog va oltre le tecnologie di prima e seconda generazione come Antivirus ed EDR / XDR e si concentra sull'esfiltrazione di dati (ADX), proteggendo in definitiva le organizzazioni dall'estorsione e garantendo la sua risorsa più preziosa, i dati. Invece di impegnare i reparti IT nel monitoraggio e risposta agli eventi, BlackFog, tramite i suoi partner MSP, offre una protezione completamente automatizzata 24 ore su 24, 7 giorni su 7, per prevenire gli attacchi informatici in tempo reale, in modo che il cliente si possa concentrare su ciò che fa meglio.

Domande comuni

Non ho mai sentito parlare di BlackFog o ADX, come posso fidarmi della tecnologia?

BlackFog è un prodotto commercializzato dal 2015 ed è il leader ADX, una nuova categoria, per la tecnologia che blocca l'esfiltrazione dei dati. BlackFog è stato approvato da analisti del software e ha ricevuto diversi premi per la sua tecnologia unica che anticipa le prossime generazioni di soluzioni di sicurezza informatica. Centinaia di clienti, in tutti i settori, si fidano di BlackFog per proteggere i propri dati e prevenire attacchi informatici.

https://www.blackfog.com/gdpr-statement/

https://privacy.blackfog.com/wp-content/uploads/2024/02/VPAT25INT_November2023_v2.pdf

https://www.blackfog.com/data-processing-agreement/

In che modo ADX interagisce con l'approccio zero trust?

ADX è stato specificamente progettato per essere una soluzione “ zero trust”, in quanto impedisce qualsiasi codice che tenta di esfiltrare i dati senza autorizzata. BlackFog convalida efficacemente un'architettura a zero trust assicurando che ogni applicazione stia facendo esattamente ciò che dice che dovrebbe. In un mondo ideale questo non sarebbe necessario, ma il codice latente può attivarsi in qualsiasi momento come abbiamo visto più volte.

Penso che la nostra tecnologia firewall e antivirus sia sufficiente per proteggerci

Le tecnologie basate sulla difesa non sono efficaci nel prevenire i diversi tipi di attacchi che vediamo oggi. Se un criminale informatico vuole davvero infiltrarsi in un dispositivo o in una rete, avrà successo. Prevenire la fuoriuscita, dei criminali informatici, con i tuoi dati è fondamentale per prevenire un attacco informatico.

Il mio EDR / XDR mi protegge già dal ransomware

Con l'89% degli attacchi ransomware che esfiltrano i dati, è necessario assicurarsi di disporre di uno strumento che prevenga l'esfiltrazione dei dati attraverso le varie tipologie di attacco. Quando leggi che le svariate società subiscono attacchi ransomware regolarmente, è chiaro che molti di questi strumenti non stanno bloccando con successo gli attacchi. La prevenzione dell'esfiltrazione dei dati offre un ulteriore livello di protezione che è diventato una tecnologia ‘che si deve avere ’.