SOPHOS
Security made simple.

Intercept X

Rilevamento antimalware con tecnologie di deep learning, prevenzione degli exploit, antiransomware, Root Cause Analysis e Sophos Clean

Sophos Intercept X applica la tecnica giusta al momento giusto per bloccare le minacce sconosciute e negare l'accesso agli autori degli attacchi. Può essere aggiunta all'attuale protezione antivirus, oppure eseguita con Sophos Endpoint Protection per una protezione next-gen completa dello stack.

Caratteristiche principali

- Modelli predisposti per il deep learning, in grado di rilevare i nuovi tipi di malware
- Prevenzione degli exploit, per bloccare le tecniche che gli autori degli attacchi adoperano per controllare software vulnerabili
- Attacchi informatici Sistemi di mitigazione, per prevenire la persistenza sui computer
- La Root cause analysis consente di visualizzare le azioni effettuate dal malware e individuarne la provenienza
- Sophos Clean rimuove il malware ed eventuali residui rimasti
- Potenziamento dell'attuale investimento nelle soluzioni antivirus

Impostare la sicurezza Endpoint Next-Gen

I giorni in cui si effettuava la semplice scansione dei file sono ormai lontani. L'obiettivo deve essere ora cercare di impedire alle minacce di raggiungere i dispositivi, bloccarle prima che possano eseguirsi, rilevarne la presenza se riescono a bypassare le misure di prevenzione, e non solo rimuovere il malware, bensì analizzarlo e invertirne gli effetti.Sophos Intercept X si serve di livelli multipli di tecnologie compatibili con la soluzione antivirus già in uso, che permettono di raggiungere massimi livelli di protezione next-gen completa dello stack.

Rilevamento antimalware con tecnologie di deep learning

Predisposta dai SophosLabs con reti neurali di deep learning, Intercept X rileva file di malware nuovi e inediti con la massima accuratezza, senza dover ricorrere alle signature. Spesso i metodi alternativi di machine learning richiedono l'intervento di scienziati che identifichino gli attributi da rilevare. Pertanto, il modello che ne risulta è limitato dall'efficacia della selezione degli attributi e dai dati di preparazione forniti. Il deep learning utilizzato in Intercept X identifica gli attributi importanti ed è in grado di distinguere autonomamente tra file di malware e file benevoli. Questo sistema, in combinazione con un vasto set di dati impostati dai SophosLabs, garantisce la creazione di una linea di delimitazione efficace per le decisioni relative alla natura dei file. Questo modello predisposto ha dimensioni inferiori ai 20MB e richiede aggiornamenti poco frequenti. Nel cloud, i SophosLabs continuano ad aggiornare il modello, monitorandone l'efficacia attraverso l'utilizzo di campioni di malware nuovi e precedentemente inediti.

Protezione dei software più vulnerabili

Le vulnerabilità emergono a una velocità allarmante. Rappresentano difetti presenti nel software e i vendor devono applicare patch per eliminarle. D'altro canto, le nuove tecniche di exploit compaiono in media solo due volte l'anno e vengono utilizzate dagli autori degli attacchi ripetutamente, man mano che si scoprono nuove vulnerabilità. La prevenzione degli exploit blocca queste tecniche, impedendo agli autori degli attacchi di approfittare delle vulnerabilità prima che ricevano una patch.

Rilevamento efficace del ransomware

La tecnologia CryptoGuard rileva la cifratura spontanea dei dati a scopo malevolo, al fine di bloccare sul nascere gli attacchi di ransomware. Anche se dovessero essere file o processi attendibili a venire compromessi o utilizzati in maniera impropria, CryptoGuard bloccherà e ne ripristinerà il corretto funzionamento senza alcuna interazione da parte degli utenti o del personale di supporto IT. CryptoGuard agisce in maniera silenziosa a livello di file system, tenendo traccia dei computer remoti e dei processi locali che cercano di modificare documenti e altri file.

Root Cause Analysis

Il processo di identificazione, isolamento e rimozione del malware risolve i problemi più immediati. Ma sapete davvero tutto ciò che ha fatto il malware prima della sua rimozione, o come sia riuscito a infiltrarsi nel sistema? La Root Cause Analysis mostra tutti gli eventi che hanno portato al rilevamento del malware. In questo modo potrete capire quali sono stati i file, i processi e le chiavi di registro colpiti dal malware, e ciò vi consentirà di attivare la disinfezione avanzata del sistema per riportare tutto allo stato originale.

Maggiore semplicità di gestione e distribuzione

Gestire la sicurezza da Sophos Central significa non dover più installare o distribuire server per poter proteggere gli endpoint. Sophos Central offre policy predefinite e configurazioni consigliate, per garantire la massima protezione sin dal primo istante.

La protezione in quattro passaggi

1. Visitare sophos.it/intercept-x per cominciare una prova gratuita.
2. Creare un account da amministratore in Sophos Central.
3. Scaricare e installare l'agente di Intercept X.
4. Gestire la protezione con Sophos Central.

Specifiche tecniche

Sophos Intercept X supporta Windows 7 e versioni successive, a 32 e a 64 bit. Può essere eseguita insieme a Sophos Endpoint Protection Standard o Advanced, se gestita da Sophos Central. In alternativa, può essere utilizzata con altri prodotti endpoint e antivirus, per aggiungere funzionalità di rilevamento antimalware con deep learning, antiexploit, antiransomware, root cause analysis e Sophos Clean.

	Funzionalità	
PREVENZIONE DEGLI EXPLOIT	Implementazione della Data Execution Prevention (DEP)	✓
	Uso obbligatorio della Address Space Layout Randomization (ASLR)	✓
	ASLR dal basso verso l'alto	✓
	Null Page (protezione contro Null Dereference)	✓
	Heap Spray Allocation	✓
	Dynamic Heap Spray	✓
	Stack Pivot	✓
	Stack Exec (MemProt)	✓
	Misure di mitigazione ROP basate su stack (chiamante)	✓
	Misure di mitigazione ROP basate sui rami (assistite da hardware)	✓
	Protezione strutturata contro la sovrascrittura del gestore eccezioni (Structured Exception Handler Overwrite Protection, SEHOP)	✓
	Filtraggio importazione della tabella indirizzi (Import Address Table Filtering, IAF)	✓
	Load Library	✓
	Reflective DLL Injection	✓
	Shellcode	✓
	VBScript God Mode	✓
	Wow64	✓
	Syscall	✓
	Hollow Process	✓
	DLL Hijacking	✓
	Squiblydoo Applocker Bypass	✓
	Protezione APC (Double Pulsar / AtomBombing)	✓
	Privilege escalation dei processi	✓
MITIGAZIONE DEGLI ATTACCHI	Protezione contro il furto di credenziali	✓
	Code Cave Mitigation	✓
	Protezione contro gli attacchi man-in-the-browser (Safe Browsing)	✓
	Malicious Traffic Detection (Rilevamento del traffico malevolo)	✓
	Rilevamento shell Meterpreter	✓

	Funzionalità	
ANTIRANSOMWARE	Protezione antiransomware per i file (CryptoGuard)	✓
	Recupero automatico dei file (CryptoGuard)	✓
	Protezione del disco e del record di avvio (WipeGuard)	✓
LOCKDOWN DELLE APPLICAZIONI	Browser web (incluso HTA)	✓
	Plugin dei browser web	✓
	Java	✓
	Applicazioni multimediali	✓
	Applicazioni Office	✓
DEEP LEARNING	Rilevamento antimalware con tecnologie di deep learning	✓
	Blocco delle applicazioni potenzialmente indesiderate (PUA) con deep learning	✓
	Eliminazione dei falsi positivi	✓
	Live Protection	✓
RISPOSTA INVESTIGAZIONE RIMOZIONE	Root Cause Analysis	✓
	Sophos Clean	✓
	Synchronized Security Heartbeat	✓
DISTRIBUZIONE	Esecuzione possibile come agente standalone	✓
	Esecuzione possibile insieme ad antivirus già esistente	✓
	Esecuzione possibile come componente di un agente Sophos Endpoint già esistente	✓
	Windows 7	✓
	Windows 8	✓
	Windows 8.1	✓
	Windows 10	✓
	macOS*	✓

* Funzionalità supportate: CryptoGuard, Malicious Traffic Detection, Synchronized Security Heartbeat, Root Cause Analysis

Utilizzate già Sophos Endpoint Protection con Enterprise Console per le vostre attività di gestione? Potete gestire gli endpoint con Sophos Central e attivare Intercept X per l'installazione automatica.

Effettuate subito una prova gratuita

Registratevi per una prova gratuita di 30 giorni su: sophos.it/intercept-x.

Vendite per l'Italia:
Tel: (+39) 02 94 75 98 00
E-mail: sales@sophos.it

10/09/2017-DS-IT (MP)

SOPHOS

SOPHOS

Intercept X Advanced for Server with EDR

La miglior protezione per i server

Sophos Intercept X for Server protegge gli ambienti server in cloud, on-premise o ibridi contro le più recenti minacce malware, garantendo una visibilità senza precedenti sulla struttura informatica dell'organizzazione e un controllo completo sui processi eseguiti sui server.

Funzionalità principali

- Protezione antimalware basata sulla tecnologia Deep Learning
- Protezione contro active adversary, exploit e ransomware
- Il sistema di rilevamento e risposta alle minacce endpoint (Endpoint Detection and Response, EDR) garantisce una visibilità completa sull'intero ambiente
- Rilevamento e protezione di: istanze di AWS EC2, bucket S3 e carichi di lavoro di Microsoft Azure
- Protezione delle configurazioni dei server, per prevenire le modifiche non autorizzate

Protezione all-in-one per i server

Intercept X for Server garantisce una protezione che ha ricevuto valutazioni estremamente positive da parte degli esperti di settore: offre una combinazione ottimale di funzionalità appositamente studiate per i server, garantendolivelli di difesa in profondità a 360 gradi. Blocca anche il malware inedito, stronca il ransomware sul nascere, previene le tecniche di exploit più pericolose e impedisce agli hacker di agire.

Nel cloud, consente di individuare e proteggere le istanze di Amazon AWS EC2 e i workload di Microsoft Azure; inoltre, permette di implementare policy omogenee a gruppi di auto scaling e virtual machine (VM). Distribuzione e impostazione sono semplici e veloci, grazie agli script di estensione per VM e ai modelli di CloudFormation.

Automatizzazione del rilevamento e della risposta alle minacce

Intercept X for Server offre il massimo livello di visibilità sui server. Permette di identificare le minacce più elusive, di visualizzare e controllare le applicazioni in esecuzione e di rispondere automaticamente agli incidenti.

Il sistema di rilevamento e risposta alle minacce endpoint (Endpoint Detection and Response, EDR) garantisce la massima visibilità sull'intera struttura informatica dell'organizzazione, per consentire agli amministratori di individuare proattivamente gli attacchi più insidiosi, di comprendere meglio la portata e l'impatto degli incidenti di sicurezza, nonché di compilare report sullo stato di sicurezza dell'azienda, anche con scarso preavviso.

Utilizzando Intercept X for Server e Sophos XG Firewall insieme e in maniera coordinata, è possibile isolare i server compromessi e impedire alle minacce di diffondersi lateralmente. La minaccia viene rimossa automaticamente e gli amministratori ottengono una visibilità del 100% sulle app in esecuzione sui server. Infine, vengono bloccate le comunicazioni verso l'esterno delle app.

Pieno controllo sui server

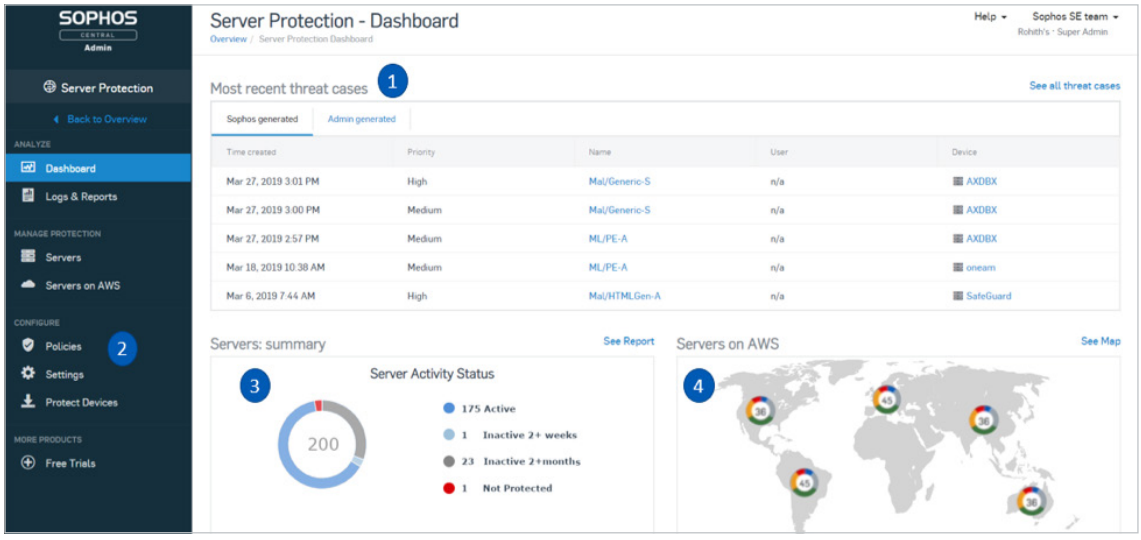
I server sono la risorsa più importante dell'organizzazione. Intercept X for Server permette di controllare gli elementi che possono essere eseguiti nei sistemi, per garantire massima sicurezza e protezione per le configurazioni dei server.

Le policy di protezione contro le minacce e di controllo su applicazioni, periferiche e web sono facili e veloci da creare e possono essere applicate a tutte le distribuzioni con pochissimi clic. Le policy possono anche essere configurate individualmente per i server che le richiedono.

Il Lockdown dei server protegge le configurazioni dei server con un unico clic, impedendo le modifiche non autorizzate e facendo in modo che possano essere eseguite solamente le app approvate dall'amministratore, tutto senza periodi di inattività dei server.

Maggiore semplicità di gestione e distribuzione

Sophos Central semplifica la gestione dei server. La gestione delle policy, gli alert e la reportistica sono tutti disponibili dalla stessa schermata. Sophos Central offre anche policy predefinite e configurazioni consigliate, per garantire la massima protezione sin dal primo istante. Inoltre, la policy relativa alla licenza e l'agent che viene distribuito sono gli stessi per tutti i tipi di deployment: fisici, virtuali, in cloud e misti.



1. Visualizzazione immediata dei casi più recenti, della loro priorità, del tipo di malware e del server interessato*
2. Accesso rapido alle policy dei server, alle impostazioni e alle opzioni di distribuzione
3. Identificazione dei server in stato protetto, non protetto oppure off-line
4. Rilevamento delle istanze di AWS in esecuzione e della regione in cui sono situate

**EDR permette ulteriori approfondimenti sui casi di minacce, sfruttando i più recenti dati di intelligence sul malware, forniti direttamente dai SophosLabs*

Cominciare è facile

1. Visitare sophos.it/server per avviare una prova gratuita
2. Creare un account Sophos Central Admin
3. Scaricare e installare l'agente di Intercept X for Server
4. Gestire la protezione da Sophos Central

Effettuate subito una prova gratuita

Registratevi per ricevere una prova gratuita di 30 giorni su: sophos.it/server.

Vendite per l'Italia:
Tel: (+39) 02 94 75 98 00
E-mail: sales@sophos.it

05/08/2019 DS-ITA (PS)

SOPHOS