

Intercept X for Server

Sia che si trovino nel cloud o on premise, le applicazioni critiche e i dati essenziali per la vostra organizzazione devono essere protetti. Intercept X for Server offre un approccio completo di difesa in profondità, grazie a funzionalità quali: rilevamento del malware con deep learning, prevenzione degli exploit, tecnologie antiransomware, whitelisting delle applicazioni, protezione contro gli active adversary e root cause analysis.

Caratteristiche principali

- ▶ Individuazione e protezione dei carichi di lavoro su Microsoft Azure e Amazon Web Services
- ▶ Protezione antiransomware sui server, inclusa la protezione contro gli attacchi remoti provenienti da endpoint non autorizzati
- ▶ Whitelisting delle applicazioni, con Server Lockdown
- ▶ Blocco delle tecniche avanzate di hacking e degli exploit
- ▶ Root cause analysis, per informazioni dettagliate sul percorso di infezione e sulla causa che ha scatenato gli attacchi
- ▶ La Synchronized Security abilita la condivisione tra i prodotti Sophos delle informazioni sulle minacce, sullo stato di integrità dei sistemi e sulla sicurezza
- ▶ Gestione semplificata con Sophos Central
- ▶ Protezione contro le minacce per i sistemi Windows e Linux

Protezione efficace e realizzata appositamente per i server

Intercept X for Server può contare su una vasta gamma di sistemi di protezione per il blocco di attacchi del giorno zero, exploit e tentativi di hacking. Queste opzioni di sicurezza impediscono agli attacchi di raggiungere i server e li rilevano prima della loro esecuzione. Se tuttavia gli attacchi dovessero comunque riuscire a eludere le difese, le funzionalità di sicurezza li bloccano ed effettuano una disinfezione profonda dei sistemi. Il modello di intelligenza artificiale viene aggiornato costantemente ed è addestrato per individuare gli attributi sospetti dei codici potenzialmente malevoli sui server. Inoltre, sono anche presenti funzionalità appositamente realizzate per i server, quali Server Lockdown e Cloud Workload Discovery (individuazione dei carichi di lavoro nel cloud), che garantiscono la sicurezza delle configurazioni dei server.

Intercept X for Server individua e protegge i carichi di lavoro nel cloud, inclusi quelli su Microsoft Azure e Amazon Web Services. Intercept X for Server connette Sophos Central con AWS e Azure e offre così una conferma visiva dello stato di protezione dei server, semplificando la gestione grazie alla visualizzazione delle informazioni più pertinenti in Sophos Central.

Blocco del ransomware che attacca i server

CryptoGuard difende i sistemi dal ransomware, agendo a livello del file system per rilevare e intercettare la cifratura indesiderata dei file, sia che essa avvenga sul server o su un endpoint remoto connesso al server. Anche WipeGuard agisce in maniera analoga, per proteggere dalla cifratura malevola il record di avvio principale.

Sophos Intercept X for Server isola il server con un unico clic, inserendo le applicazioni legittime in una whitelist, per proteggere i server e mantenerli in uno stato sicuro, impedendo l'esecuzione di applicazioni non autorizzate. Sophos effettua automaticamente la scansione del sistema, creando un inventario (whitelist) di applicazioni note per essere legittime, senza bisogno di creare regole manualmente. Sophos stabilisce un legame inscindibile tra le applicazioni e i relativi file, come per esempio i file dll, i file di dati e gli script.

Blocco degli attacchi: negazione dell'accesso ai server per gli hacker

Le vulnerabilità insorgono velocemente e applicare le patch ai server senza interferire con le attività degli utenti può essere un problema. Gli attacchi che sfruttano gli exploit possono avere effetti devastanti e spesso non vengono rilevati dalle tradizionali tecnologie di protezione per i server. Intercept X for Server è progettata per impedire anche agli hacker più ostinati di sfruttare le tecniche di exploit basate sul furto di credenziali. Sia che i tentativi rimangano nascosti e persistenti o che utilizzino movimenti laterali, Intercept X è appositamente realizzata per bloccarli.

Root Cause Analysis

Intercept X for Server include anche tecnologie di rilevamento e risposta, che garantiscono agli amministratori una visibilità completa sui metodi utilizzati dagli attacchi per infiltrarsi nella rete, indicandone anche i movimenti e gli elementi infettati. Inoltre, offre consigli pratici su come procedere dopo la disinfezione. Intercept X for Server offre tutto questo senza bisogno di un altro agente o un'altra console di gestione.

Synchronized Security

La Synchronized Security è un sistema di sicurezza di primissima categoria che permette alle difese informatiche di coordinarsi, proprio come fanno gli attacchi che le minacciano. Questa soluzione offre la combinazione ideale tra una piattaforma di sicurezza estremamente intuitiva e prodotti pluripremiati che agiscono in perfetta sincronia per bloccare le minacce più avanzate e offrire una protezione di livelli inediti.

Caratteristiche principali di Intercept X for Server

PIATTAFORME			
	Server Windows	✓	
	Linux ¹	✓	
	Cloud pubblico (Microsoft Azure e Amazon AWS)	✓	
PREVENZIONE	RIDUZIONE DELLA SUPERFICIE DI ATTACCO		
		Whitelisting delle applicazioni (Server Lockdown)	✓
		Web Security	✓
		Controllo di Windows Firewall	✓
		Download Reputation	✓
		Controllo web (blocco degli URL)	✓
		Controllo periferiche (ad es. USB)	✓
		Controllo applicazioni	✓
	PRIMA DELL'ESECUZIONE NEI DISPOSITIVI		
		Rilevamento antimalware con tecnologie di deep learning	✓
		indipendente dalle firme	✓
		Scansione antimalware dei file	✓
		Live Protection	✓
		Analisi del comportamento in pre-esecuzione (HIPS)	✓
	Scansione esterna per le VM (ESXi e Hyper-V) ²	✓	
	Rilevamento delle applicazioni potenzialmente indesiderate (PUA)	✓	
	Data Loss Prevention (prevenzione della perdita di dati)	✓	

Semplicità di gestione con Sophos Central

Gestire la sicurezza da Sophos Central significa non avere più bisogno di installare server per poter proteggere i sistemi. Sophos Central offre accesso immediato, senza bisogno di impostare server di console. Sophos Central include policy di sicurezza per server che sono subito pronti per l'uso e consente di gestire anche altri prodotti Sophos, inclusi: Sophos Intercept X, Mobile, Wireless, Email e Web. Tutto da un unico riquadro trasparente.

RILEVAMENTO	BLOCCO DELLE MINACCE IN ESECUZIONE	Mitigazioni di hacker/active adversary	✓
		Protezione antiransomware dei file [CryptoGuard], con rilevamento degli attacchi al server da parte di endpoint connessi in remoto	✓
		Protezione del disco e del record di avvio [WipeGuard]	✓
		Rilevamento del traffico malevolo	✓
RISPOSTA	INVESTIGAZIONE E RIMOZIONE	Rimozione automatica del malware Sophos Clean	✓
		Root Cause Analysis	✓
GESTIONE	APPLICAZIONI	Gestione dei criteri server	✓
		Cache degli aggiornamenti e relay dei messaggi	✓
		Esclusioni automatiche alla scansione	✓
		Controllo sincronizzato delle applicazioni ⁴	✓
	VISIBILITÀ	Individuazione e protezione dei carichi di lavoro Azure	✓
		Individuazione e protezione dei carichi di lavoro AWS	✓
		Mappa di AWS, visualizzazione di aree geografiche multiple	✓
		Synchronized Security con Security Heartbeat™ (Migliore protezione contro le minacce, identificazione positiva dell'origine e isolamento automatico) ⁴	✓
		Windows Remote Desktop Services (visibilità utenti)	✓
		Gestione basata sul cloud, per eliminare il bisogno di installare e mantenere un server on-premise a parte e per gestire la protezione dei server da un'unica console, insieme alla sicurezza di endpoint, dispositivi mobili, e-mail e wireless	✓
SOPHOS CENTRAL	Multi-factor authentication	✓	
	Amministrazione basata sui ruoli	✓	

1 Tutte le funzionalità sono disponibili su Windows; funzionalità selezionate sono disponibili su Linux

2 Vedere la Guida alle licenze di Sophos for Virtual Environments, distribuzione dell'agente ultra-leggero

3 Per i server Windows gestiti da Sophos Enterprise Console, CryptoGuard è

disponibile con la licenza add-on Endpoint Exploit Prevention (EXP)

4 Se utilizzata insieme a Sophos XG Firewall



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

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

