SOPHOS
Security made simple.

Server Application Whitelisting

Advanced Server Protection completa e semplice

Di **Tsailing Merrem**, Senior Product Marketing Manager

È fondamentale cercare di neutralizzare gli attacchi ai server aziendali, sempre più frequenti e sofisticati, implementando soluzioni di sicurezza potenti ed efficaci. La vera sfida è trovare una soluzione in grado di garantire il giusto livello di protezione, senza alcun impatto sulle performance e con costi di installazione e gestione ridotti. Le soluzioni di Application Whitelisting impediscono alle minacce avanzate o sconosciute di raggiungere i server aziendali, ma sono particolarmente complesse e molto costose. Sophos porta tutta la potenza dell'Application Whitelisting negli ambienti aziendali tramite la tecnologia in-the-cloud, fornendo così la soluzione perfetta per proteggere in modo efficace i server e tutti i dati confidenziali in essi contenuti.

La sfida di proteggere in modo efficace i server aziendali

Il volume e il valore dei dati archiviati nei server aziendali li ha resi il bersaglio principale degli attacchi di malware diretti e del cosiddetto "giorno zero". Al momento una delle principali priorità di tutte le organizzazioni è proteggere l'integrità dei server e dei dati confidenziali in essi contenuti. Finora l'unica alternativa a disposizione delle aziende è stata quella di estendere le soluzioni di protezione per endpoint anche ai server. Le soluzioni di protezione specificamente progettate per endpoint non riescono tuttavia a fare le dovute distinzioni fra server e computer endpoint, per questo è necessario effettuare operazioni di configurazione e ottimizzazione estremamente complesse.

Le soluzioni di Application Whitelisting sono un investimento sempre più diffuso nelle aziende, in quanto rappresentano la modalità più efficace per proteggere i server da minacce sconosciute. Il Whitelisting consente alle organizzazioni di proteggere il sistema operativo del server e le applicazioni in esso installate tramite regole di tipo default-deny, invece che utilizzare regole known-bad (ovvero default-allow). In questo modo viene garantita una protezione proattiva e senza firma contro tutte le minacce, sia note che sconosciute, oltre a consentire l'esecuzione solo di applicazioni autorizzate dal dipartimento IT aziendale.

Le soluzioni di Application Whitelisting convenzionali richiedono però costi di gestione sostanziosi, non solo durante le fasi di distribuzione iniziali, ma anche durante le operazioni di manutenzione e di cambio di gestione. Le aziende di medie dimensioni, con competenze informatiche ridotte, dispongono di risorse limitate che rendono difficile l'adozione di queste soluzioni o la collaborazione con servizi di consulenza solitamente molto costosi.

Sophos Application Whitelisting—Server Protection semplice ed efficace

Sophos Cloud Server Protection offre l'unica soluzione di Server Application Whitelisting ideale per le aziende di medie dimensioni o dall'approccio pragmatico. Garantisce protezione efficace, performance ottimizzate, installazione veloce e gestione semplice. È inoltre l'unica soluzione di Application Whitelisting completamente integrata alle funzionalità anti-malware e HIPS (Host-based Intrusion Prevention System) dei server; è in grado, di garantire livelli di protezione senza precedenti contro attacchi noti e del "giorno zero", fra cui attacchi di tipo in-memory, DLL injection e basati su script.

Si tratta dell'unica funzionalità di server lockdown semplice da utilizzare, in grado di avviare automaticamente la scansione del server alla ricerca di malware mentre si effettua il fingerprinting delle applicazioni (identificazione tramite impronte digitali), per poi stabilire la baseline (linea guida) relativa al whitelist delle applicazioni e quindi eseguire il lockdown del server. Una volta in modalità lockdown, è impossibile sostituire o apportare modifiche utilizzando i file delle applicazioni baseline. La Sophos ServerAuthority riconosce, però, le applicazioni server ed adatta le sue configurazioni in modo da abilitare automaticamente tutte le modifiche valutate affidabili. Riesce inoltre ad impostare esclusioni relative alle scansioni antivirus in completa autonomia, garantendo performance di livelli elevatissimi. Questa funzionalità consente di eliminare procedure manuali lunghe e laboriose di configurazione o impostazione delle regole. Il motore di protezione di Sophos, sensibile al contesto (context-aware), monitora costantemente il sistema con l'obiettivo di prevenire attacchi basati sui contenuti.

PANORAMICA

Sophos Application Whitelisting, unito a software anti-malware e HIPS all'avanguardia, garantisce protezione per server senza precedenti, con delivery e manutenzione estremamente semplici.

ELEMENTI CHIAVE

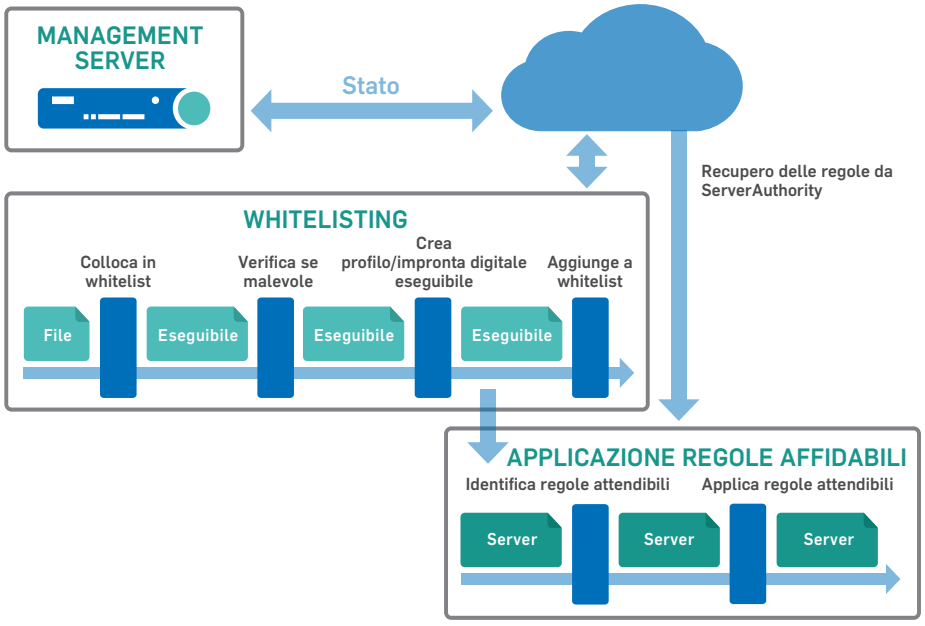
- Server Lockdown attivo con un solo clic
- Impostazione automatica di regole affidabili per adattarsi agli ambienti server
- Integrazione con software anti-malware e HIPS per una protezione efficace contro attacchi basati sui contenuti o del giorno zero
- Esclusioni dalla scansione antivirus automatizzate per potenziare le performance
- Protezione e gestione basata sul cloud

Server Application Whitelisting

L'Application Whitelisting di Sophos va ben oltre il whitelisting di DLL e script. Sophos ServerAuthority effettua il lockdown automatico di tutti i collegamenti fra applicazioni e relativi file, come per esempio fra DLL e file script, per proteggere il sistema da attacchi basati sulla memoria. Queste operazioni vengono effettuate senza richiedere nessuna regola personalizzata, evitando così potenziali errori di configurazione.

Questa soluzione è stata progettata con l'obiettivo di massimizzare le performance delle applicazioni server. Fornisce avvisi e report personalizzabili, accessibili ovunque ci si trovi tramite la console integrata di Sophos Cloud. L'interfaccia di gestione consente agli amministratori server di avere una "visuale completa" di tutti i server, delle applicazioni e dello stato di protezione.

Ecco come opera il Sophos Application Whitelisting



Server Lockdown attivo con un solo clic

Il Sophos Application Whitelisting consente di attivare, in modo estremamente semplice, la funzionalità di Server Lockdown. Non sarà più necessario impostare server fisici o configurazioni delle policy, creare inventari delle applicazioni o scrivere regole relative alle modifiche delle modalità di gestione. Tutte queste operazioni richiederebbero un lavoro di giorni ed in alcuni casi, addirittura di mesi; ora potranno invece essere completate in modo estremamente veloce e semplice. Basterà infatti un solo clic per dare avvio alla scansione completa del sistema alla ricerca di malware, alla creazione dei cataloghi delle applicazioni, oltre che all'affermazione di relazioni affidabili fra applicazioni, updater e file di sistema.

Impostazione automatica di regole con ServerAuthority

Sophos Server Protection si adatta dinamicamente agli ambienti server tramite Sophos ServerAuthority. Riesce a identificare le applicazioni incluse nelle whitelist a cui applica le regole di attendibilità, a garanzia che tali applicazioni vengano aggiornate solo ed esclusivamente da fonti considerate affidabili. Questa procedura non solo protegge in modo efficace l'integrità delle applicazioni, ma verifica anche che siano sempre aggiornate e che dispongano di tutte le patch.

Sophos ServerAuthority gestisce un elenco delle applicazioni server più diffuse, come per esempio Domain Controller, Exchange Server o SharePoint, e applica automaticamente le esclusioni antivirus consigliate in modo tale da escludere file e directory che possono avere ripercussioni negative su performance o stabilità.

Sicurezza integrata

L'integrazione fra Sophos Application Whitelisting e Sophos Server Antivirus garantisce che i server siano sempre sicuri, utilizzando entrambe queste tecnologie per contrastare le minacce più recenti. Questa soluzione sfrutta la tecnologia Live Protection che offre collegamenti basati sul cloud con i SophosLabs per effettuare ricerche in tempo reale sulle minacce.

Advanced Protection specifica per server

Sophos Server Protection distingue nettamente fra policy per utenti e per server. Le policy per server predefinite sono state ottimizzate con l'obiettivo di garantire il giusto equilibrio fra performance e protezione dei sistemi operativi dei server. Le policy possono essere applicate a server singoli, a gruppi definiti in Active Directory, manualmente nella console o a tutto l'ambiente.

Conclusione

Al giorno d'oggi la necessità e la difficoltà di riuscire a garantire protezione efficace per i server aziendali contro gli attacchi del giorno zero stanno crescendo esponenzialmente. Sophos Application Whitelisting ha vinto questa sfida, offrendo una soluzione di protezione per server efficace e semplice da utilizzare unica nel settore. Questa soluzione include Server Lockdown attivo in un solo clic, Sophos ServerAuthority in grado di autorizzare automaticamente gli aggiornamenti provenienti da fonti affidabili, oltre che software anti-malware e HIPS integrati. Ciò consente alle aziende di medie dimensioni o dall'approccio pragmatico di disporre di una soluzione, specificamente progettata per server, estremamente facile da utilizzare e gestire, dalle performance ottimizzate, oltre che sempre efficace.

Sophos Cloud Server Protection

Per maggiori info, visitate Sophos.it/Servers

Vendite per Italia:
Tel: (+39) 02 911 808
E-mail: sales@sophos.it

06.15NOLA.wpit

SOPHOS