

Sophos per Microsoft SharePoint

Sophos per Microsoft SharePoint fornisce un'efficace protezione in tempo reale dei dati aziendali all'interno di un ambiente collaborativo e il blocco di virus, spyware, adware, di file sospetti e di applicazioni potenzialmente indesiderate (PUA). Inoltre, Sophos per Microsoft SharePoint utilizza sofisticate funzionalità di filtraggio dei contenuti per impedire la diffusione non autorizzata di informazioni sensibili.

Protezione da minacce multiple in un unico prodotto

- Il nostro motore di rilevamento delle minacce fornisce protezione dei dati sensibili dell'azienda contro virus, worm, Trojan, spyware, adware, file sospetti e applicazioni potenzialmente indesiderate (PUA).
- Il nostro software utilizza un sistema di Host Intrusion Prevention (HIPS) per bloccare le minacce del giorno zero. Il rilevamento pre-esecuzione in tempo reale identifica malware sconosciuto, file e comportamenti sospetti.
- Un sofisticato motore di ricerca dei criteri di filtraggio dei contenuti blocca la distribuzione di contenuto improprio o sensibile, basandosi sul nome dei file, sul tipo dei file o su frasi e parole chiave contenute all'interno di un file.
- Il gestore quarantena integrato e di facile utilizzo permette l'autorizzazione, la cancellazione o la rimozione di malware, applicazioni potenzialmente indesiderate, file sospetti e contenuti controllati.

Gestione semplificata e automatizzata

- Sophos per Microsoft SharePoint fornisce un'intuitiva console di gestione basata sul Web. Il pannello di controllo in tempo reale, la personalizzazione dei criteri di ricerca, l'efficace gestione della quarantena e i relativi report semplificano la protezione dell'ambiente collaborativo.
- La scansione del contenuto effettuabile al momento dell'accesso, pianificata e su richiesta, garantisce la protezione automatica e ottimale di tutti i file contro le minacce più recenti, riducendo al minimo il sovraccarico di lavoro e assicurando facilità d'uso da parte dell'utente.
- Le funzionalità di creazione di report personalizzabili forniscono un'analisi immediata dell'attività delle minacce, informazioni sul filtraggio dei contenuti e sullo stato della quarantena. La creazione di dettagliati log consultabili fornisce funzionalità di analisi approfondite.



Vantaggi fondamentali

- » Protegge i dati aziendali contro virus, spyware, adware, file sospetti e applicazioni potenzialmente indesiderate
- » Ferma automaticamente il malware sconosciuto grazie alla tecnologia di protezione Behavioral Genotype®, che analizza il comportamento del codice prima che venga eseguito
- » Identifica malware sconosciuto, file e comportamenti sospetti grazie a tecnologie incorporate di prevenzione delle intrusioni prima dell'esecuzione
- » Controlla la distribuzione di contenuto improprio o sensibile mediante sofisticati controlli dei criteri di filtraggio del contenuto
- » Semplifica l'amministrazione tramite la console di gestione remota semplificata
- » Le pratiche funzionalità di creazione di report forniscono un'analisi immediata dell'attività delle minacce, informazioni sul filtraggio dei contenuti e sullo stato della quarantena
- » La creazione di dettagliati log consultabili fornisce funzionalità di analisi approfondite
- » Include un Gestore quarantena integrato per l'eliminazione, la rimozione o l'autorizzazione dei file
- » Si aggiorna automaticamente con la protezione più recente rilasciata dai SophosLabs™, la rete mondiale Sophos di centri per l'analisi delle minacce informatiche
- » Eseguire la scansione al momento dell'accesso, su richiesta e al momento della pianificazione, consentendo la massima protezione e flessibilità
- » Include il supporto tecnico e l'assistenza personalizzata 24 ore su 24, 365 giorni l'anno, per tutta la durata della licenza

Protezione preventiva più rapida ed efficace grazie a tecnologie innovative

- La tecnologia Genotype® di rilevazione dei virus blocca preventivamente le famiglie di virus, anche prima che siano disponibili firme digitali specifiche.
- La tecnologia HIPS di Sophos sfrutta il motore antivirus per identificare i programmi sospetti prima che vengano eseguiti per rilevare malware potenziale.
- La protezione Behavioral Genotype® esegue la scansione alla ricerca di comportamenti sospetti in modo da fornire protezione proattiva contro il malware del giorno zero. Svolge il compito fondamentale di rilevare nuove minacce prima dell'inizio dell'esecuzione del codice.
- Il set di regole comportamentali Sophos viene costantemente confrontato con un'ampia libreria di applicazioni legittime, in modo da assicurare un rilevamento accurato.
- Il motore di scansione blocca le applicazioni potenzialmente indesiderate (PUA) che sono considerate potenzialmente malevole, contenenti adware o che consumano risorse (come ad esempio utilità, barre degli strumenti e altre applicazioni non autorizzate).
- Gli aggiornamenti Sophos sono di piccole dimensioni e vengono rilasciati ogni cinque minuti – un vantaggio per le aziende che desiderano una protezione veloce con un impatto ridotto sulle risorse di rete.

Il filtraggio dei contenuti e la prevenzione della perdita dei dati semplificano la conformità

- Impedire la perdita di dati e garantire l'utilizzo proattivo della propria infrastruttura mediante l'applicazione di criteri sofisticati atti a controllare un'ampia varietà di tipi di file (compresi i file eseguibili, multimediali e di archivio) nonché dati sensibili come i file binari, il codice sorgente, i database, l'elenco di contatti e i file XML.
- Eliminare i tipi di file che si mascherano grazie alla tecnologia anti-spoofing che consente di rilevare la vera estensione dei file (es, rinominando un file MP3 in DOC).
- Semplificare la conformità alle policy aziendali mediante criteri di gestione dei contenuti, basati su parole chiavi definite dall'amministratore o espressioni regolari contenuti nei più diffusi tipi di file per il controllo e la distribuzione di informazioni sensibili o riservate.
- Proteggere gli utenti contro l'esposizione a linguaggio offensivo utilizzando come paragone un elenco già incluso di parole/frasi offensive.
- Mettere in quarantena, bloccare e/o sostituire le violazioni dei file con testo segnaposto.

Supporto affidabile da parte degli esperti

- Gli analisti di SophosLabs e la nostra rete globale di centri di analisi delle minacce forniscono una protezione rapida e proattiva contro le minacce conosciute e sconosciute.
- Tecnologia all'avanguardia, vigilanza sulle minacce emergenti a livello globale e competenza a 360 gradi in materia di sicurezza informatica sono i punti di forza di SophosLabs. Con l'attività di ricerca 24 ore su 24, 7 giorni su 7, Sophos reagisce rapidamente in qualsiasi situazione, aiutando la vostra azienda a proteggersi da minacce alla sicurezza sempre più complesse.
- L'assistenza clienti è compresa come componente standard in ogni licenza.
- I nostri tecnici forniscono assistenza personalizzata, sia per e-mail che telefonicamente; in alternativa potete consultare la nostra knowledgebase nel sito web.

Requisiti di sistema

Piattaforme SharePoint supportate

- » Windows SharePoint Services 3.0 (SP1)
- » Microsoft Office SharePoint Server 2007 (SP1)

Piattaforme server supportate

- » Windows Server 2003/R2 (SP2+), 32 bit e 64 bit
- » Windows Small Business Server 2003/R2 (SP2+), 32 bit
- » Windows Server 2008, 32 bit e 64 bit

Piattaforme del database supportate

- » Microsoft SQL Server 2008
- » Microsoft SQL Server 2005

Requisiti hardware

- » 1 GB di spazio su disco
- » 1 GB di memoria (si consigliano 2 GB)
- » CPU da 1,5 GHz (si consigliano 2 GHz)

Per provare Sophos per Microsoft SharePoint visitate il sito www.sophos.it/products