SOPHOS

Cybersecurity made simple.

Sophos Sandstorm

La protezione next-gen contro le advanced threat diventa semplice

Sophos Sandstorm sfrutta tecnologie di sandboxing in cloud di ultima generazione per offrire alla vostra azienda il livello di sicurezza aggiuntivo di cui ha bisogno per difendersi da ransomware e attacchi mirati.

È l'unica sandbox di rete basata su analisi di Deep Learning che garantisce un rilevamento più efficace. Si integra con Sophos XG Firewall, Sophos UTM, Sophos Web Appliance, Sophos Email Appliance e Sophos Email su Sophos Central, senza bisogno di altro hardware.

E in più offre un ottimo rapporto qualità-prezzo. Vi dona tutti i vantaggi di una protezione di classe enterprise, ma senza i costi solitamente associati a questa categoria.

Caratteristiche principali

- Facile integrazione con la vostra soluzione di sicurezza Sophos.
- Pronto all'azione nel giro di pochi minuti
- Protezione contro ransomware, APT, malware sconosciuto, PUA e attacchi mirati
- Intelligence sulle minacce pratica e utile
- Analisi di Deep Learning
- Report dettagliati e basati sui singoli incidenti

Protezione avanzata contro gli attacchi mirati

Difesa della rete contro ransomware e malware sconosciuti che agiscono prelevando i dati in maniera illecita. La presenza di una potente tecnologia di sandboxing di ultima generazione in cloud e basata su analisi di Deep Learning si traduce in ottime capacità di rilevamento, blocco e risposta per APT e minacce del giorno zero, tutto con la massima efficacia e rapidità.

Con noi è tutto più semplice

Sophos Sandstorm è completamente integrato alla vostra soluzione di sicurezza Sophos. Basta aggiornare la subscription, applicare il criterio Sandstorm, e siete immediatamente protetti contro gli attacchi mirati. Sarete pronti all'azione nel giro di pochi minuti.

Blocco delle minacce più elusive, che tendono a sfuggire alle altre soluzioni

Rilevamento di ransomware e minacce sconosciute, appositamente realizzate per eludere le appliance di sandboxing di prima generazione. Il nostro approccio basato sull'emulazione del sistema completo garantisce il più elevato livello di visibilità nel comportamento del malware sconosciuto, rilevando gli attacchi malevoli che tendono a sfuggire alle altre soluzioni.

Reportistica dettagliata

Risposta accelerata alle minacce avanzate, con semplici analisi delle violazioni basate sui singoli incidenti. Forniamo intelligence sulle APT in ordine di priorità, correlando i dati raccolti. Questo approccio elimina le informazioni superflue e aiuta a risparmiare tempo prezioso.

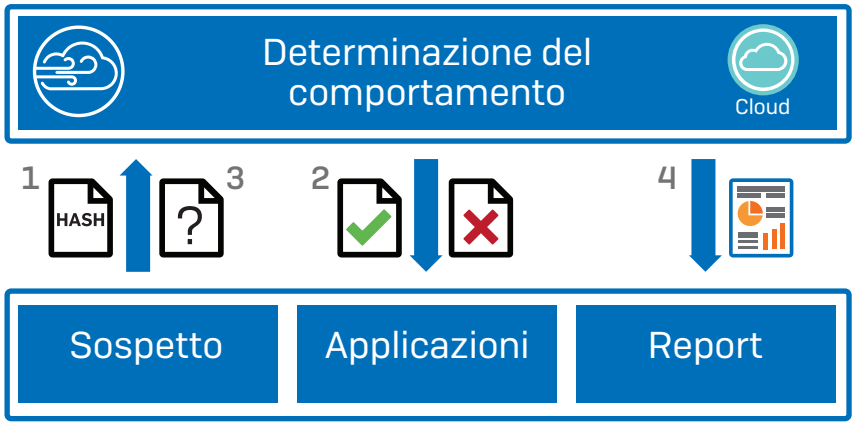
Performance rapidissima

La vostra soluzione di sicurezza Sophos pre-filtra accuratamente il traffico, in modo tale da inviare a Sandstorm solamente i file sospetti, garantendo quindi livelli minimi di latenza e impatto sull'utente.

Le funzionalità di Sophos Sandstorm

- Integrazione completa con la dashboard della soluzione di sicurezza Sophos
- Ispezione dei file eseguibili e dei documenti che includono contenuti eseguibili
  - File eseguibili di Windows (inclusi .exe, .com e .dll)
  - Documenti Word (inclusi .doc, .docx, docm e .rtf)
  - Documenti PDF
  - Archivi contenenti i tipi di file sopraelencati (ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet)
  - Supporto di più di 20 tipi di file
- L'analisi dinamica del malware con tecnologie di Deep Learning esegue i file in ambienti reali
- Report dettagliati sui file malevoli e funzionalità di rilascio dei file dalla dashboard
  - Tempo medio di analisi inferiore ai 120 secondi
  - Criteri utente e di gruppo con opzioni flessibili per tipo di file, esclusioni e azioni al momento dell'analisi
  - Supporto dei link per il download unico

Come funziona



1. La soluzione di sicurezza Sophos effettua la scansione dei file secondo tutti i tradizionali controlli di sicurezza (ad es. firme antimalware, URL malevoli, ecc). Se è eseguibile o ha contenuti eseguibili, e non è stato scaricato da un sito web sicuro, il file viene considerato sospetto. La soluzione di sicurezza Sophos invia l'hash del file sospetto a Sophos Sandstorm, per stabilire se sia già stato analizzato in precedenza.
2. Se l'hash del file è già stato analizzato, Sophos Sandstorm passa i dati di intelligence sulle minacce alla soluzione di sicurezza Sophos. A questo punto il file viene o inviato al dispositivo dell'utente, oppure bloccato, a seconda delle informazioni fornite da Sophos Sandstorm.
3. Se l'hash risulta essere inedito, una copia del file sospetto viene inviata a Sophos Sandstorm. Qui, il file viene detonato, e il suo comportamento attentamente monitorato. Una volta svolta l'analisi completa, Sophos Sandstorm passa i dati di intelligence sulle minacce alla soluzione di sicurezza Sophos. A questo punto il file viene nuovamente inviato al dispositivo dell'utente, oppure bloccato, a seconda delle informazioni fornite da Sophos Sandstorm.
4. La soluzione di sicurezza Sophos adopera i dati di intelligence dettagliati forniti da Sophos Sandstorm per creare report estremamente dettagliati di ciascun caso di minaccia.

Effettuate subito una prova gratuita

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

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

03/01/2019 DSIT (PC)

SOPHOS