SOPHOS
Security made simple.

La Synchronized Security:

Un sistema di difesa di alto livello in grado di rispondere agli attacchi più sofisticati

Oggi come oggi, la strategia di sicurezza di molte organizzazioni prevede l'installazione di livelli multipli dei più disparati prodotti di sicurezza su reti ed endpoint: firewall basati su host e reti, strumenti di controllo dei contenuti o di analisi del malware, sistemi di gestione degli eventi e molto altro ancora. Lo scopo di questa strategia di "difesa in profondità" è aiutare a proteggere i sistemi contro minacce note ed emergenti, basandosi sul concetto che, in un punto o in un altro della catena di attacco, uno di questi prodotti dovrebbe essere in grado di neutralizzare un eventuale attacco malevolo.

Sebbene nel loro piccolo i singoli prodotti siano in grado di svolgere al meglio la loro funzione, questa strategia "compartimentalizzata" presenta dei gravi svantaggi. Tanto per cominciare, spesso questi prodotti agiscono in maniera isolata e indipendente gli uni dagli altri, per cui non condividono informazioni in maniera rapida o utile. Di conseguenza, già a un livello di base, sono presenti evidenti opportunità di migliorare la sicurezza, se si consente a firewall ed endpoint di condividere reciprocamente dati contestuali a livello di rete e processi, per isolare e neutralizzare le infezioni.

In secondo luogo, più è profonda e vasta la strategia di difesa in profondità di un'organizzazione, più diventa difficile da gestire. Da ciò derivano costi aggiuntivi per arruolare personale che si occupi manualmente della correlazione degli avvisi, della gestione di interfacce utente multiple e del monitoraggio degli eventi. Inoltre, tutto questo influisce anche sulla performance, per via della presenza di un gran numero di agenti software che si contendono le risorse di sistema.

In terzo luogo, sebbene siano stati sviluppati sistemi di gestione delle informazioni e degli eventi di sicurezza (Security Information and Event Management, SIEM) per cercare di colmare le lacune comunicative tra i vari prodotti indipendenti, la loro funzione è semplicemente quella di raccogliere i dati e presentarli in maniera razionale in un'unica vista. La loro capacità di estrarre informazioni pratiche è generalmente bassa, risulta nel conseguimento di dati obsoleti, e richiede l'analisi da parte di personale tecnico altamente qualificato.

Per una rappresentazione metaforica della situazione attuale, si immagini di aver collocato guardie di sicurezza sia all'interno che all'esterno del proprio edificio, ma di non averle dotate di ricetrasmittenti per comunicare tra di loro. Alle guardie viene invece imposto di inviare qualsiasi messaggio a un sistema centrale in maniera unidirezionale, il che significa che c'è bisogno di un'altra persona che rimanga costantemente all'erta nel caso in cui trovasse informazioni che possono essere utili a una delle guardie; in tale evenienza, queste informazioni dovrebbero essere consegnate a mano alle guardie. Si immagini ora che vi sia più di un edificio, con diverse guardie situate al suo esterno per difendere il perimetro, e con una guardia in ciascuna stanza interna; si immagini quindi che tutte queste guardie inviino dati al sistema centrale di cui sopra: un sistema che non è in grado di riconoscere in maniera coerente la guardia che invia ciascun messaggio.
Si aggiunga al mix una valanga costante di intrusi che cercano di superare questa difesa discontinua utilizzando nuove tecniche innovative e sempre più insidiose.

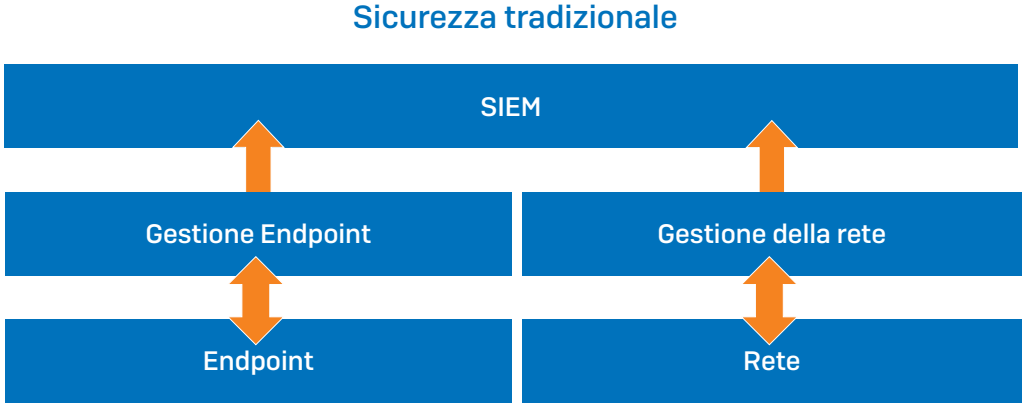


Figura 1: Le soluzioni tradizionali cercano di correlare e trovare un senso nei dati ricevuti, esigendo personale e competenze tecniche già carenti

Strategie di difesa del passato contro attacchi del presente

Sebbene all'inizio gli attacchi informatici fossero nati per lo più da un misto di curiosità e desiderio di causare scompiglio, gli attacchi di oggi sono molto più sofisticati e coordinati che mai. Gli attacchi hanno origine in motivazioni quali denaro, segretezza e cause politiche, e vengono sferrati da gruppo organizzati di cybercrimine, intere nazioni e hacktivisti. Gli autori sottomettono gli utenti finali alla loro volontà, per mezzo di attacchi di phishing realizzati con la massima attenzione ai particolari per raggiungere obiettivi quali furto dei dati e privilege escalation. Individuano bug nei software con la stessa rapidità con cui vengono applicate patch per le vulnerabilità. Si infiltrano nelle reti utilizzando malware a livello di memoria, per poi spostarsi lateralmente in un batter d'occhio, lasciandosi dietro una scia di sistemi infettati.

Con un settore della sicurezza che fatica a tenere il passo, oggi come oggi i criminali informatici si trovano in una posizione di vantaggio, grazie alla presenza di reti di comunicazioni alternative, alla condivisione di tecniche e codice, alle valute anonime e al malware metamorfico intelligente, nonché grazie alle reti a cui appartengono dispositivi precedentemente infettati. Esistono persino servizi di attacco sofisticati basati sul malware con funzionalità complete, che possono essere utilizzati da chiunque (in altre parole app store per il cybercrimine), con tanto di opzioni di ripartizione degli utili, che permettono agli autori di codice malevolo di ricevere parte dei profitti ogni volta che un attacco genera un guadagno.

74%
Percentuale di violazioni dei dati che passano inosservate per più di 6 mesi.

Nel frattempo gli utenti finali ricorrono sempre più alla memorizzazione dei dati nel cloud pubblico, caricano sempre più frequentemente risorse aziendali sui dispositivi personali, e richiedono di poter svolgere il proprio lavoro all'esterno del perimetro di rete aziendale: da casa, da un altro quartiere della città, o dalla parte opposta del mondo.

Il trovarsi alle prese con le minacce attualmente in circolazione ha causato problemi pressoché insormontabili a tutte le organizzazioni, anche quelle più importanti e con maggiore lungimiranza. Gli attacchi sono sempre più complessi e coordinati, mentre i prodotti che dovrebbero difendere i sistemi spesso agiscono in maniera isolata. La superficie di attacco continua a espandersi e gli utenti finali adoperano smartphone, applicazioni cloud e dispositivi portatili diversi, mentre il budget dedicato ai reparti informatici non riesce a tenere il passo con necessità sempre più pressanti. Secondo il Ponemon Institute, il 74% delle violazioni dei dati passa inosservato per più di sei mesi, mentre ESG Group segnala che il 46% delle organizzazioni ritiene di avere una carenza critica di competenze di cybersecurity.

46%
Percentuale di organizzazioni alle prese con una carenza critica di competenze di cybersecurity.

La Synchronized Security: una soluzione semplice a un problema complesso

Per la prima volta, le soluzioni di protezione della rete e degli endpoint possono agire come un unico sistema di sicurezza integrato che include prodotti di primissima classe in grado di utilizzare la stessa interfaccia e condividere in maniera bidirezionale informazioni utili in tempo reale, abilitando così un sistema di risposta automatica alle minacce.

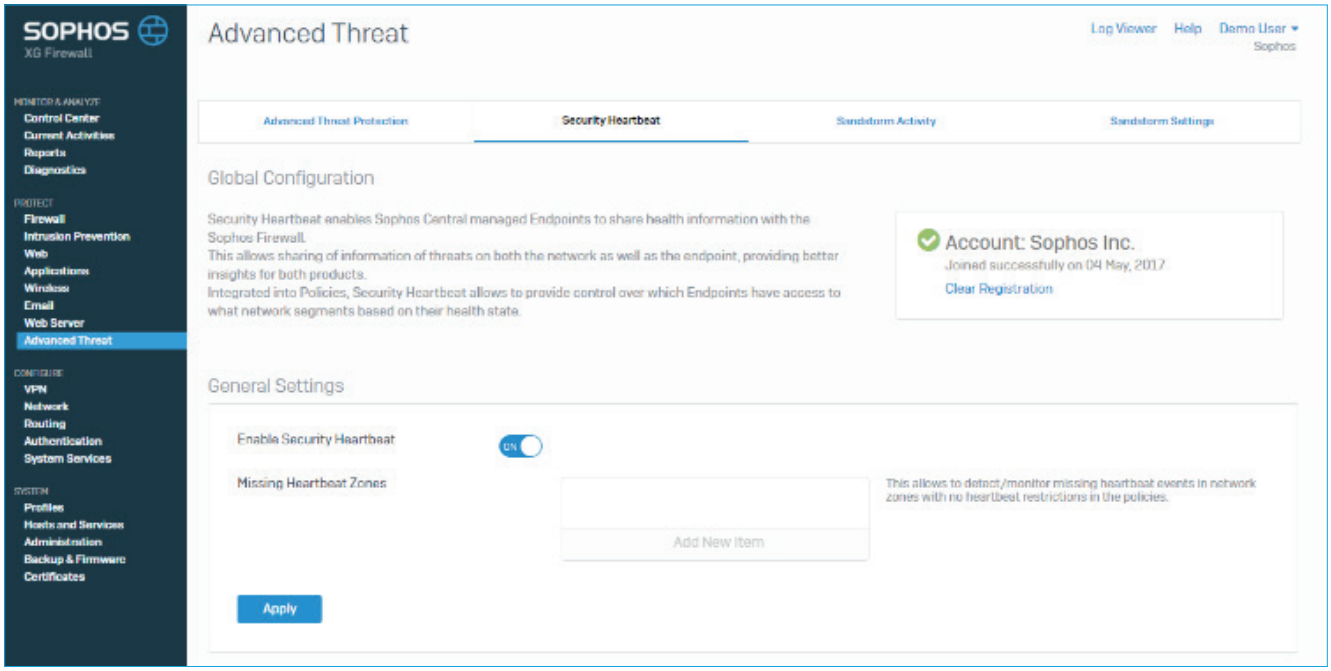
Figura 2: La Synchronized Security semplifica e unifica comunicazione e gestione

Una gestione più semplice facilita l'impostazione e l'amministrazione dell'intera struttura, senza richiedere ulteriori sistemi di analisi e gestione degli eventi; inoltre, l'automazione dei processi di rilevamento, isolamento e correzione consente di neutralizzare gli attacchi nel giro di pochi secondi, anziché ore o giorni. È una protezione di qualità superiore, che implica anche notevoli risparmi di tempo e denaro.

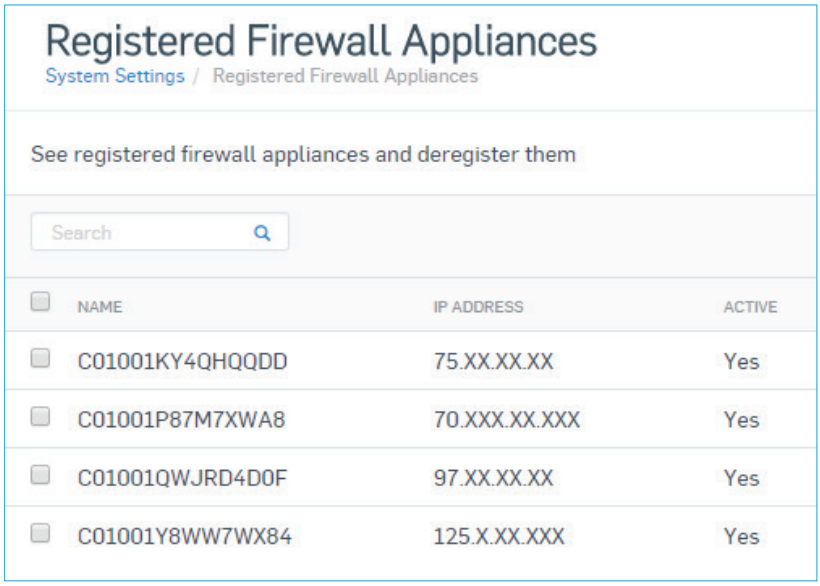
	Synchronized Security	Sicurezza tradizionale
Intelligence	Condivisa	Isolata
Correlazione	Automatizzata	Manuale e parzialmente automatizzata
Individuazione delle minacce sconosciute	Assistita dal contesto	Non assistita
Risposta in caso di incidenti	Altamente mirata	Imprecisa
Esigenza di investire in prodotti e personale aggiuntivi	Nessuna	Notevole
Gestione	Semplice e unificata	Complessa e compartimentalizzata

Tabella 1: Caratteristiche della Synchronized Security e della sicurezza tradizionale a confronto

La comunicazione tra firewall ed endpoint viene agevolata da Sophos Security Heartbeat: una funzionalità facile da installare che crea un canale sicuro e bidirezionale, controllato dalla console di gestione nel cloud di Sophos Central.



Per il setup basta semplicemente immettere le proprie credenziali di amministratore di Sophos Central nella sezione dell'interfaccia di Sophos XG Firewall dedicata a Security Heartbeat. Una volta completata questa operazione, il firewall diventa visibile in Sophos Central, tutti i computer gestiti con Sophos Central cominciano a inviare dati di connessione heartbeat ai firewall connessi, e tutti i firewall connessi restituiscono un heartbeat ai computer.



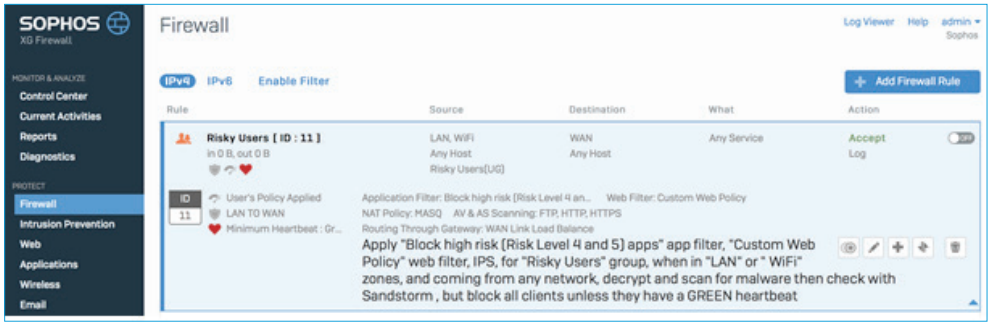
I computer si connettono automaticamente al firewall più vicino, mentre i firewall verificano le richieste di connessione in entrata provenienti dai computer, in modo tale da garantirne la protezione tramite Sophos Central. A loro volta, anche i computer convalidano il firewall, confrontandone le informazioni di sicurezza con quelle disponibili da Sophos Central. Tutto avviene automaticamente: nessun bisogno di regole, configurazioni o aggiornamenti complessi.

La Synchronized Security in azione: le basi

Il widget Sophos Security Heartbeat nella dashboard di XG Firewall

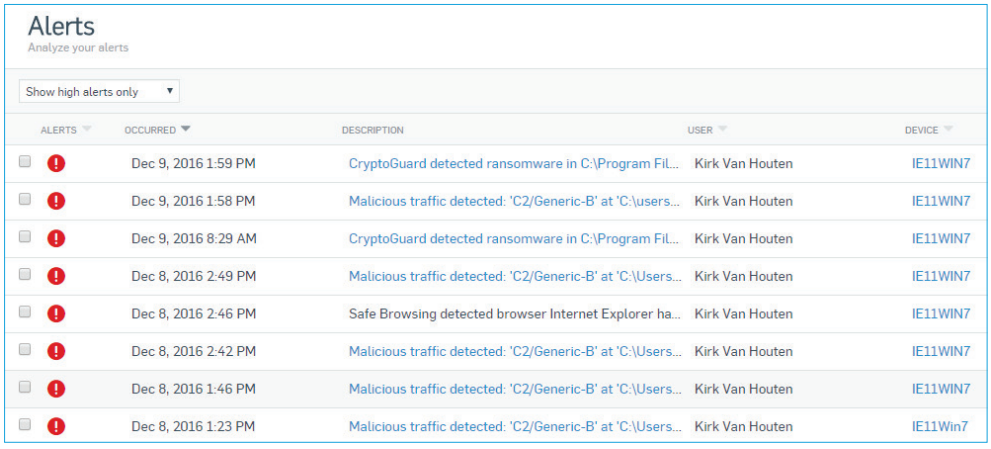
Una volta stabilita la connessione tra firewall e client endpoint, gli endpoint cominciano a inviare al firewall le informazioni relative al proprio stato di integrità del sistema tramite Sophos Central. Sulla dashboard di XG Firewall, il widget Sophos Security Heartbeat indica lo stato di integrità di tutti gli endpoint gestiti da Sophos Central. Se uno qualsiasi dei sistemi dovesse eseguire applicazioni indesiderate o infette, viene indicato in giallo o in rosso. Gli indicatori in rosso segnalano problemi che devono essere risolti immediatamente, mentre quelli in giallo significano rischio ma non urgenza.

È possibile creare regole firewall che agiscano in base ai cambiamenti dello stato di sicurezza. È ad esempio possibile consentire ai computer con stato giallo di accedere a internet, ma impedire a questi computer di visitare siti che possono contenere informazioni aziendali di natura sensibile, come Salesforce o Dropbox. In presenza di uno stato rosso, è possibile vietare completamente l'accesso a internet ed eventualmente, se in possesso di una licenza in corso di validità del nostro prodotto di cifratura dei file SafeGuard, revocare le chiavi di cifratura dei file fino a quando non venga ripristinato uno stato verde sui computer interessati. A questo punto verrebbe automaticamente ripristinato l'accesso a internet, e si procederebbe a riemettere le chiavi di cifratura.



Regola firewall nell'interfaccia di XG Firewall che impedisce agli utenti a rischio di accedere alla rete a meno che non presentino uno stato sicuro

Sophos XG Firewall è anche in grado di rilevare un endpoint precedentemente integro che dovesse cominciare a generare traffico di rete senza inviare un heartbeat. Tale comportamento potrebbe indicare che la protezione antimalware dell'endpoint è stata manomessa o disattivata da un intruso. In casi come questo, l'endpoint verrebbe isolato dal resto della rete fino a quando non sia possibile effettuarne la disinfezione, e fino al ripristino del relativo heartbeat.
Grazie al Security Heartbeat, i computer infetti vengono chiaramente identificati sia nell'interfaccia di XG Firewall che in quella di Sophos Central Admin. Vengono condivise tutte le informazioni relative a nome del computer, utente che vi ha effettuato l'accesso e nome del processo che ha generato l'avviso, riducendo enormemente il tempo da trascorrere nei processi di investigazione, rilevamento e riparazione dei danni delle minacce. In un tradizionale ambiente di protezione compartimentalizzata, questo processo potrebbe richiedere ore o giorni di lavoro manuale, visto che il responsabile dispone solamente dell'indirizzo di rete IP temporaneo.



Pagina degli avvisi che mostra avvisi in rosso in Sophos Central Admin

Synchronized Security significa server più sicuri

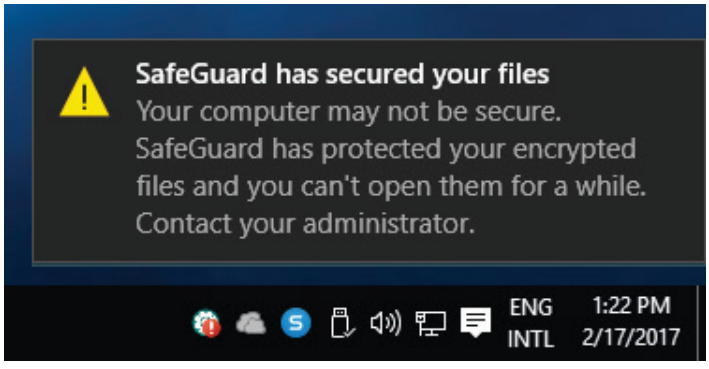
Quasi sempre i server contengono i dati più importanti delle organizzazioni; di conseguenza rappresentano un obiettivo molto ambito per gli autori del malware. Naturalmente è importante proteggere i server contro gli attacchi diretti, ma occorre anche respingere lateralmente le minacce provenienti dai computer degli utenti finali che sono connessi ai server.

In caso di attacco, Sophos Server Protection può segnalare a XG Firewall un cambiamento dello stato di integrità, e a questo punto il firewall può isolare il server sia da internet che dagli altri computer della rete, per prevenire il furto dei dati e il potenziale diffondersi di un'infezione. Note come Destination Heartbeat (heartbeat di destinazione), le connessioni in entrata inviate al server vengono respinte dal firewall, e il server viene nascosto anche agli altri dispositivi della rete. Una volta risolto il problema, l'accesso alla rete e la visibilità del server possono essere ripristinati automaticamente.

Con la comunicazione bidirezionale tra firewall, server ed endpoint, Sophos Synchronized Security garantisce una coordinazione immediata per sventare anche gli attacchi più sofisticati. Inoltre, l'identificazione e l'isolamento automatico dei server in base al relativo Sophos Security Heartbeat significa un minore investimento di tempo in attività di risposta agli incidenti. Utilizzato in combinazione con la normale implementazione del criterio Heartbeat, può isolare in maniera efficace e completa un sistema compromesso, sia per quanto riguarda il traffico in entrata che in uscita.

Una nuova prescrizione: Synchronized Encryption

Cifrare i file è un processo a cui vengono tradizionalmente associati difficoltà di impostazione per gli amministratori e problemi d'uso per gli utenti finali. Tuttavia, Sophos SafeGuard Encryption adotta un approccio innovativo alla strategia di protezione delle organizzazioni: tutti i file vengono cifrati per impostazione predefinita, e successivamente vengono convalidati per la decifratura in base all'utente, all'applicazione e allo stato di sicurezza del dispositivo. Solamente le applicazioni ritenute sicure vengono autorizzate a visualizzare i dati cifrati, il che significa che il malware non può accedere ai dati di natura sensibile. L'intero processo è invisibile agli occhi dell'utente finale. I contenuti vengono cifrati subito dopo la loro creazione, e rimangono cifrati quando sono condivisi all'interno dell'organizzazione o caricati sul cloud; esiste anche l'opzione di proteggere i file con password attraverso un solo clic, se si desidera effettuarne la condivisione all'esterno dell'azienda.



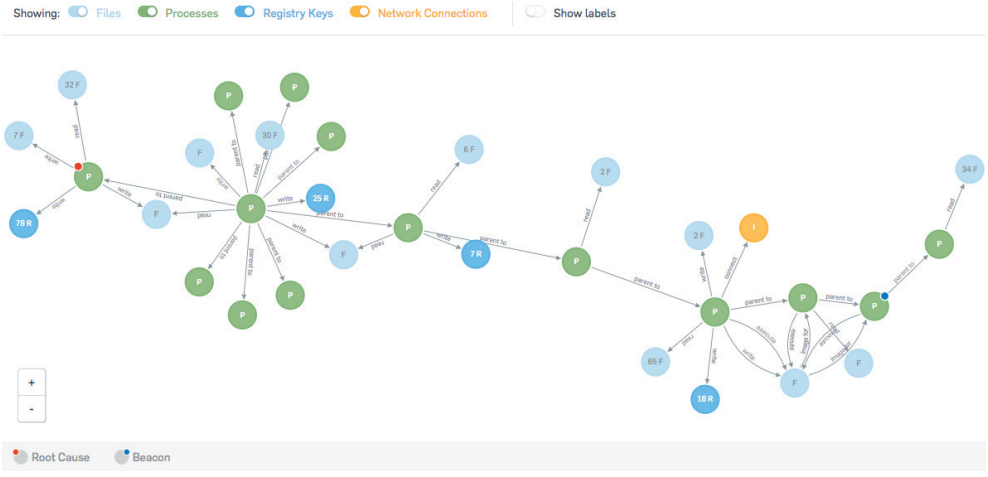
Messaggio che indica che SafeGuard ha revocato le chiavi di cifratura dei file durante un attacco

Anche Sophos SafeGuard Encryption è compatibile con la Synchronized Security. Se un endpoint protetto con tecnologie Sophos comunica a XG Firewall di essere stato attaccato, il firewall non si limita soltanto a isolare l'endpoint dalla rete, ma rimuove anche le chiavi di cifratura dei file di SafeGuard dal computer infetto. In questo modo, anche se i dati dovessero essere rubati, rimangono inutilizzabili da parte degli autori dell'attacco. Una volta ripristinato a uno stato sicuro, l'endpoint viene autorizzato a tornare nella rete, e si procede alla riemissione delle sue chiavi di cifratura. L'intero processo (da isolamento a rimozione e ripristino) avviene automaticamente e nel giro di pochi secondi, anziché ore o giorni, come probabilmente avverrebbe in caso di attacco a un sistema di difesa discontinuo, composto da prodottisingoli.

Risalire alla radice di un attacco

Naturalmente, sebbene i processi di isolamento, correzione e ripristino offerti dalla Synchronized Security e dalla comunicazione bidirezionale del Security Heartbeat rappresentino una svolta nel settore della sicurezza informatica, è importantissimo disporre anche di opzioni semplici e chiare di analisi degli attacchi passati, per rafforzare le difese contro eventuali attacchi futuri.

La funzionalità di root cause analysis presente in Sophos Intercept X offre una visualizzazione dettagliata e approfondita del percorso di infezione di un attacco, con tanto di informazioni relative ai file, ai processi e alle chiavi di registro infetti, nonché consigli pratici e prescrittivi per la correzione dei problemi.

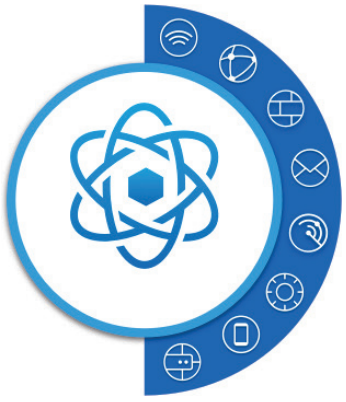


La scheda Visualizza della funzionalità di root cause analysis in Sophos Intercept X

Consente di scoprire come abbia fatto il malware a infiltrarsi nei sistemi e quali azioni abbia svolto prima di essere stato bloccato e rimosso; inoltre, verifica che sia stato completamente rimosso e implementa le misure necessarie per evitare che attacchi simili si ripetano in futuro.

La Synchronized Security è semplicemente una sicurezza migliore

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 alto livello, con opzioni di risposta automatica agli incidenti e analisi approfondita e controllo in tempo reale.



A differenza delle soluzioni di sicurezza che utilizzano i più disparati prodotti considerati singolarmente, diventando sempre più complesse man mano che si aggiungono ulteriori livelli di protezione, con Sophos è l'opposto: più soluzioni vengono implementate, maggiori sono i vantaggi della Synchronized Security.

Maggiori informazioni e prova gratuita: www.sophos.it/synchronized

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

05/2017 WP-NA (NP)

SOPHOS