SOPHOS

Security made simple.

Intercept X

Nowe rozwiązanie anty exploit, anty ransomware i źródłowej analizy problemu

Sophos Intercept X dodaje nową generację technologii bezsygnaturowych do istniejących rozwiązań bezpieczeństwa urządzeń końcowych, zapewniając ich kompletną ochronę.

Najważniejsze informacje

- Ochrona przed zagrożeniami dnia zerowego typu exploit
- Technologia CryptoGuard ochrony przed zagrożeniami ransomware
- Analiza źródeł problemów
- Trwałe usuwanie szkodliwego oprogramowania za pomocą Sophos Clean
- Wzmocnienie istniejącej infrastruktury antywirusowej

Nowa generacja ochrony urządzeń końcowych

Zwykłe skanowanie plików dziś już nie wystarcza. Teraz najważniejszym celem jest zapobieganie aby zagrożenia nie dotarły do urządzeń, zatrzymanie ich zanim zostaną uruchomione, wykrycie ich jeśli ominęły już metody prewencyjne i nie tylko usunięcie szkodliwego oprogramowania typu malware ale także analiza i cofnięcie wszystkich szkód jakie poczyniło ono na urządzeniach końcowych.
Sophos Intercept X używa wielu technologii pozwalających na stworzenie dopasowanego do różnych wymagań rozwiązania bezpieczeństwa urządzeń końcowych.

Ochrona podatnego na zagrożenia oprogramowania

Technologia anty exploit zatrzymuje zagrożenia zanim stworzą problem poprzez rozpoznawanie i blokowanie typowych technik rozpowszechniania malware, chroniąc dzięki temu urządzenia końcowe przed nieznanymi zagrożeniami i likwidując ich podatność na zagrożenia dnia zerowego.

Efektywne wykrywanie zagrożeń typu ransomware

Technologia CryptoGuard wykrywa samoczynne szkodliwe szyfrowanie danych zatrzymując zagrożenia ransomware w trakcie ich działania. Nawet w przypadku gdy zaufane pliki lub procesy zostały zmienione lub zhakowane, Sophos Endpoint Protection zatrzyma ich działanie i przywróci je do stanu poprawnego bez potrzeby żadnej interakcji ze strony użytkowników lub personelu IT. CryptoGuard działa w ukryciu na poziomie systemu plików, śledząc działanie procesów usiłujących zmodyfikować dokumenty i inne pliki na zdalnych i lokalnych komputerach.

Analiza źródeł problemu

Identyfikacja malware, jego izolacja i usunięcie jest tylko doraźnym rozwiązaniem problemu. Nie ma pewności jakie szkody wyrządziło ono zanim zostało usunięte, a przede wszystkim nie wiadomo w jaki sposób przedostało sie do środowiska IT. Analiza źródeł problemu pokazuje wszystkie wydarzenia które poprzedziły wykrycie zagrożenia. Umożliwia to uzyskanie informacji które pliki, procesy oraz klucze rejestru zostały naruszone przez szkodliwe oprogramowanie oraz aktywuje zaawansowany system pozwalający na cofnięcie stanu systemu do czasu sprzed infekcji.

Ochrona nowej generacji uzupełniająca tradycyjne zabezpieczenia

Sophos Intercept X uzupełnia istniejące implementacje antywirusowe i anty malware zapewniając ochronę nowej generacji przed zagrożeniami typu exploit i ransomware, której brak w tradycyjnych produktach. Sophos Intercept X, poprzez eliminację sposobów i środków ataku których tradycyjne rozwiązania nie blokują, pomaga zwiększyć bezpieczeństwo i odporność.

Uproszczenie zarządzania i wdrożenia

Zarządzanie bezpieczeństwem za pomocą Sophos Central eliminuje potrzebę instalacji dodatkowych serwerów w celu zabezpieczenia urządzeń końcowych. Sophos Central zawiera domyślne polityki oraz rekomendowane konfiguracje zapewniające już od pierwszego dnia najbardziej efektywną ochronę.

Cztery kroki do ochrony

1. Aby wypróbować odwiedź sophos.com/intercept-x
2. Utwórz konto administratora w Sophos Central.
3. Ściągnij i zainstaluj agenta Intercept X.
4. Zarządzaj ochroną z Sophos Central.

Specyfikacja techniczna

Sophos Intercept X obsługuje Windows 7 i wyższe, 32 oraz 64 bit. Zarządzanie z Sophos Central zapewnia współpracę z Sophos Endpoint Protection Advanced. Może także działać obok systemów innych firm do ochrony antywirusowej i urządzeń końcowych, dodając do nich rozwiązanie zwalczające exploity, ransomware i zapewniające analizę źródeł problemu.

		SKU	Intercept X	Central Endpoint Advanced + Intercept X
		Licencjonowanie	*Na użytkownika*	*Na użytkownika*
ZAPOBIEGANIE	ZANIM DOTRZE DO URZĄDZEŃ	Bezpieczeństwo sieci WWW		✓
		Reputacja w oparciu o liczbę ściągnięć		✓
		Kontrola sieci WWW / Blokowanie URL w oparciu o kategorie		✓
		Kontrola urządzeń (np. USB)		✓
		Kontrola aplikacji		✓
		Ochrona przez exploitami wykorzystującymi luki w przeglądarkach	✓	✓
	ZANIM ZOSTANIE URUCHOMIONE NA URZĄDZENIACH	Skanowanie anty malware plików		✓
		Ochrona w trakcie działania		✓
		Analiza zachowania jeszcze przed uruchomieniem / HIPS		✓
		Blokowanie potencjalnie niechcianych aplikacji		✓
		Ochrona przed zagrożeniami typu exploit, wykorzystującymi luki w aplikacjach	✓	✓
WYKRYCIE	ZATRZYMANIE DZIAŁANIA ZAGROŻENIA	Analiza zachowania podczas działania / HIPS		✓
		Wykrywanie podejrzanego ruchu	✓	✓
		Ochrona CryptoGuard przed ransomware	✓	✓
REAKCJA	BADANIE I USUNIĘCIE	Automatyczne usuwanie malware	✓	✓
		Synchronizacja z Security Heartbeat	✓	✓
		Analiza źródła problemu	✓	✓
		Sophos Clean	✓	✓

Dotychczasowi klienci Sophos Endpoint Protection zarządzający punktami końcowymi za pomocą Enterprise Console lub UTM muszą przełączyć ich zarządzanie na Sophos Central. Aby uzyskać więcej informacji odwiedź sophos.com/migrate.

Wypróbuj teraz

Zarejestruj się na sophos.com/intercept-x aby otrzymać 30-dniową wersję próbną

Dział sprzedaży w Polsce
Email: salesee@sophos.com

2016-12-13 DS-PL (NP)

SOPHOS