Panoramica di Intercept X, XDR ed MTR

Con gestione da Sophos Central

SOPHOS
Cybersecurity evolved.

		FUNZIONALITÀ	INTERCEPT X ESSENTIALS	INTERCEPT X ADVANCED	INTERCEPT X ADVANCED WITH XDR	INTERCEPT X WITH MTR STANDARD	INTERCEPT X WITH MTR ADVANCED
	MANAGEMENT	Criteri multipli		✓	✓	✓	✓
		Aggiornamenti controllati		✓	✓	✓	✓
PREVENZIONE	RIDUZIONE DELLA SUPERFICIE DI ATTACCO	Controllo delle applicazioni		✓	✓	✓	✓
		Controllo periferiche		✓	✓	✓	✓
		Controllo web / Blocco degli URL in base alla categoria di appartenenza		✓	✓	✓	✓
		Reputazione dei download	✓	✓	✓	✓	✓
		Web Security	✓	✓	✓	✓	✓
	PRIMA DELL'ESECUZIONE NEI DISPOSITIVI	Rilevamento antimalware con Deep Learning	✓	✓	✓	✓	✓
		Scansione antimalware dei file	✓	✓	✓	✓	✓
		Live Protection	✓	✓	✓	✓	✓
		Analisi del comportamento in pre-esecuzione (HIPS)	✓	✓	✓	✓	✓
		Blocco delle applicazioni potenzialmente indesiderate (PUA)	✓	✓	✓	✓	✓
		Intrusion Prevention System (IPS)	✓	✓	✓	✓	✓
	BLOCCO DELLE MINACCE IN ESECUZIONE	Data Loss Prevention (prevenzione della perdita di dati)	✓	✓	✓	✓	✓
		Analisi del comportamento in fase di esecuzione (HIPS)	✓	✓	✓	✓	✓
		Antimalware Scan Interface (AMSI)	✓	✓	✓	✓	✓
		Rilevamento del traffico malevolo (Malicious Traffic Detection, MTD)	✓	✓	✓	✓	✓
		Prevenzione degli exploit (dettagli a pag. 5)	✓	✓	✓	✓	✓
		Mitigazione degli antagonisti attivi (dettagli a pag. 5)	✓	✓	✓	✓	✓
		Protezione antiransomware per i file (CryptoGuard)	✓	✓	✓	✓	✓
		Protezione del disco e del record di avvio (WipeGuard)	✓	✓	✓	✓	✓
		Protezione contro gli attacchi man-in-the-browser (Safe Browsing)	✓	✓	✓	✓	✓
		Ottimizzazione del lockdown delle applicazioni	✓	✓	✓	✓	✓

L'elenco delle funzionalità continua nella pagina successiva

Panoramica di Intercept X, XDR ed MTR

SOPHOS
Cybersecurity evolved.

Con gestione da Sophos Central (continua)

		FUNZIONALITÀ	INTERCEPT X ESSENTIALS	INTERCEPT X ADVANCED	INTERCEPT X ADVANCED WITH XDR	INTERCEPT X WITH MTR STANDARD	INTERCEPT X WITH MTR ADVANCED
RILEVAMENTO E INDAGINE	RILEVAMENTO	Live Discover (formulazione di query SQL su ambienti diversi per il threat hunting e la protezione dell'integrità delle IT security operation)			✓	✓	✓
		Libreria di query SQL (query pre-compilate e completamente personalizzabili)			✓	✓	✓
		Accesso rapido, archiviazione dei dati su disco (fino a 90 giorni)			✓	✓	✓
		Origini dati che coinvolgono prodotti multipli, ad es. Firewall, Email			✓	✓	✓
		Query su prodotti multipli			✓	✓	✓
		Sophos Data Lake (archiviazione dati nel cloud)			30 giorni	30 giorni	30 giorni
		Query pianificate			✓	✓	✓
	INDAGINE	Casi di minaccia (Root Cause Analysis)		✓	✓	✓	✓
		Analisi antimalware con Deep Learning			✓	✓	✓
		Dati di intelligence avanzata sulle minacce disponibili su richiesta, forniti direttamente dai SophosLabs			✓	✓	✓
		Esportazione dei dati attraverso analisi approfondite			✓	✓	✓
RISPOSTA	CORREZIONE	Rimozione automatizzata del malware	✓	✓	✓	✓	✓
		Synchronized Security Heartbeat	✓	✓	✓	✓	✓
		Sophos Clean	✓	✓	✓	✓	✓
		Live Response (accesso remoto al terminal a scopo di ulteriore indagine e risposta)			✓	✓	✓
		Isolamento degli endpoint su richiesta			✓	✓	✓
		Disinfezione e blocco con un solo clic			✓	✓	✓
SERVIZIO GESTITO	THREAT HUNTING E RISPOSTA ALLE MINACCE CON SUPERVISIONE UMANA	Threat hunting con indizi 24h su 24				✓	✓
		Controlli dello stato di integrità della sicurezza				✓	✓
		Conservazione dei dati				✓	✓
		Report sulle attività				✓	✓
		Rilevamento degli active adversary				✓	✓
		Neutralizzazione delle minacce e azioni correttive				✓	✓
		Threat hunting senza indizi 24h su 24					✓
		Contatto dedicato nel team Threat Response					✓
		Supporto diretto e dedicato					✓
		Gestione proattiva del profilo di sicurezza					✓

Panoramica di Intercept X, XDR ed MTR

SOPHOS
Cybersecurity evolved.

Confronto tra sistemi operativi

		FUNZIONALITÀ	WINDOWS	macOS
PREVENZIONE	RIDUZIONE DELLA SUPERFICIE DI ATTACCO	Web Security	✓	✓
		Reputazione dei download	✓	
		Controllo web / Blocco degli URL in base alla categoria di appartenenza	✓	✓
		Controllo periferiche	✓	✓
		Controllo delle applicazioni	✓	✓
	PRIMA DELL'ESECUZIONE NEI DISPOSITIVI	Rilevamento antimalware con Deep Learning	✓	
		Scansione antimalware dei file	✓	✓
		Live Protection	✓	✓
		Analisi del comportamento in pre-esecuzione (HIPS)	✓	
		Blocco delle applicazioni potenzialmente indesiderate (PUA)	✓	✓
		Intrusion Prevention System (IPS)	✓	
	BLOCCO DELLE MINACCE IN ESECUZIONE	Data Loss Prevention (prevenzione della perdita di dati)	✓	
		Analisi del comportamento in fase di esecuzione (HIPS)	✓	
		Antimalware Scan Interface (AMSI)	✓	
		Rilevamento del traffico malevolo (Malicious Traffic Detection, MTD)	✓	✓
		Prevenzione degli exploit (dettagli a pag. 5)	✓	
		Mitigazione degli antagonisti attivi (dettagli a pag. 5)	✓	
		Protezione antiransomware per i file (CryptoGuard)	✓	✓
		Protezione del disco e del record di avvio (WipeGuard)	✓	
		Protezione contro gli attacchi man-in-the-browser (Safe Browsing)	✓	
		Ottimizzazione del lockdown delle applicazioni	✓	

L'elenco delle funzionalità continua nella pagina successiva

Panoramica di Intercept X, XDR ed MTR

SOPHOS
Cybersecurity evolved.

Confronto tra sistemi operativi (continua)

		FUNZIONALITÀ	WINDOWS	macOS
RILEVAMENTO E INDAGINE	RILEVAMENTO	Live Discover (formulazione di query SQL su ambienti diversi per il threat hunting e la protezione dell'integrità delle IT security operation)	✓	✓
		Libreria di query SQL (query pre-compilate e completamente personalizzabili)	✓	✓
		Accesso rapido, archiviazione dei dati su disco (fino a 90 giorni)	✓	✓
		Origini dati che coinvolgono prodotti multipli, ad es. Firewall, Email	✓	In arrivo
		Query su prodotti multipli	✓	In arrivo
		Sophos Data Lake (archiviazione dati nel cloud)	✓	In arrivo
		Query pianificate	✓	In arrivo
	INDAGINE	Casi di minaccia (Root Cause Analysis)	✓	✓
		Analisi antimalware con Deep Learning	✓	
		Dati di intelligence avanzata sulle minacce disponibili su richiesta, forniti direttamente dai SophosLabs	✓	
		Esportazione dei dati attraverso analisi approfondite	✓	
RISPOSTA	CORREZIONE	Rimozione automatizzata del malware	✓	✓
		Synchronized Security Heartbeat	✓	✓
		Sophos Clean	✓	
		Live Response (accesso remoto al terminal a scopo di ulteriore indagine e risposta)	✓	✓
		Isolamento degli endpoint su richiesta	✓	
		Disinfezione e blocco con un solo clic	✓	✓
SERVIZIO GESTITO	THREAT HUNTING E RISPOSTA ALLE MINACCE CON SUPERVISIONE UMANA	Threat hunting con indizi 24h su 24	✓	✓
		Controlli dello stato di integrità della sicurezza	✓	✓
		Conservazione dei dati	✓	✓
		Report sulle attività	✓	✓
		Rilevamento degli active adversary	✓	✓
		Neutralizzazione delle minacce e azioni correttive	✓	✓
		Threat hunting senza indizi 24h su 24	✓	✓
		Contatto dedicato nel team Threat Response	✓	✓
		Supporto diretto e dedicato	✓	✓
		Gestione proattiva del profilo di sicurezza	✓	✓

Funzionalità di Sophos Intercept X

SOPHOS
Cybersecurity evolved.

Dettagli delle funzionalità di Intercept X

	Funzionalità	
PREVENZIONE DEGLI EXPLOIT	Implementazione della Data Execution Prevention (DEP)	✓
	Uso obbligatorio di ASLR (Address Space Layout Randomization)	✓
	ASLR bottom-up	✓
	Null Page (protezione contro Null Dereference)	✓
	Heap Spray Allocation	✓
	Dynamic Heap Spray	✓
	Stack Pivot	✓
	Stack Exec (MemProt)	✓
	Misure di mitigazione ROP basate su stack (chiamante)	✓
	Misure di mitigazione ROP branch-based (assistite da hardware)	✓
	Protezione strutturata contro la sovrascrittura del gestore eccezioni (Structured Exception Handler Overwrite Protection, SEHOP)	✓
	Filtraggio importazione della tabella indirizzi (Import Address Table Filtering, IAF)	✓
	Load Library	✓
	Reflective DLL Injection	✓
	Shellcode	✓
	VBScript God Mode	✓
	WoW64	✓
	Syscall	✓
	Hollow Process	✓
	DLL Hijacking	✓
	Squiblydoo Applocker Bypass	✓
	Protezione contro le APC (Double Pulsar / AtomBombing)	✓
	Privilege escalation dei processi	✓
	Protezione dinamica dello shellcode	✓
	EFS Guard	✓
	CTF Guard	✓
	ApiSetGuard	✓

	Funzionalità	
ANTIRAN-SOMWARE	Protezione antiransomware per i file (CryptoGuard)	✓
	Recupero automatico dei file (CryptoGuard)	✓
	Protezione del disco e del record di avvio (WipeGuard)	✓
LOCKDOWN DELLE APPLICAZIONI	Browser web (incluso HTA)	✓
	Plugin dei browser web	✓
	Java	✓
	Applicazioni multimediali	✓
	Applicazioni Office	✓
PROTEZIONE CON DEEP LEARNING	Rilevamento antimalware con Deep Learning	✓
	Blocco delle applicazioni potenzialmente indesiderate (PUA) con deep learning	✓
	Eliminazione dei falsi positivi	✓
RISPOSTA INVESTI-GAZIONE RIMOZIONE	Casi di minaccia (Root Cause Analysis)	✓
	Sophos Clean	✓
	Synchronized Security Heartbeat	✓
BLOCCO DEGLI ATTACCHI DEI CYBERCRIMINALI	Protezione contro il furto di credenziali	✓
	Mitigazione di code cave	✓
	Protezione contro gli attacchi man-in-the-browser (Safe Browsing)	✓
	Malicious Traffic Detection (Rilevamento del traffico malevolo)	✓
	Rilevamento shell Meterpreter	✓

Managed Threat Response (MTR)

SOPHOS
Cybersecurity evolved.

Sophos Managed Threat Response (MTR) offre un servizio completamente gestito con opzioni di ricerca, rilevamento e risposta alle minacce, disponibile 24h su 24 e 7gg su 7 e gestito direttamente dal nostro team di esperti. Per i clienti MTR è inclusa anche Intercept X Advanced with XDR.

Sophos MTR: Standard

Threat hunting con l'utilizzo di indizi, operativo 24h su 24/7gg su 7

Elementi o attività identificate come dannosi (indicatori importanti) vengono automaticamente bloccati o terminati, facendo risparmiare tempo prezioso ai threat hunter, che possono ora dedicarsi all'individuazione delle minacce seguendo gli indizi raccolti. Questo tipo di intercettazione delle minacce prevede l'aggregazione di eventi causali e adiacenti (indicatori minori), per rilevare nuovi indicatori di attacco (IoA) e indicatori di compromissione (IoC), che precedentemente erano impossibili da rilevare.

Controllo dello stato di integrità della sicurezza

Ottimizzazione della performance di Intercept X, a partire da Intercept X Advanced with XDR, grazie alle analisi proattive delle condizioni operative e ai consigli sull'ottimizzazione della configurazione.

Report sulle attività

I riepiloghi delle attività dei casi consentono al personale di comunicare e di attribuire la giusta priorità agli eventi, per cui il vostro team saprà esattamente quali sono le minacce individuate e quali azioni di risposta sono state intraprese in ogni periodo di reporting.

Rilevamento degli active adversary

La maggior parte degli attacchi di successo si basano sull'esecuzione di un processo che, agli strumenti di monitoraggio, può sembrare legittimo. Grazie all'utilizzo di tecniche di indagine sviluppate internamente, il nostro team determina la differenza tra i comportamenti legittimi e le tattiche, tecniche e procedure (TTP) utilizzate dagli autori degli attacchi.

Sophos MTR: Advanced *Include tutte le funzionalità del servizio Standard, con in più:*

Threat hunting senza l'utilizzo di indizi, operativa 24h su 24

Utilizzando data science, dati di intelligence sulle minacce e il fenomenale intuito di espertissimi threat hunter, raccogliamo e confrontiamo tutte le informazioni relative al profilo della vostra azienda, alle risorse principali e agli utenti ad alto rischio, per anticipare i comportamenti degli autori degli attacchi e intercettare nuovi indicatori di attacco (Indicators of Attack, IoA).

Telemetria ottimizzata

Le indagini sulle minacce vengono arricchite dai dati di telemetria provenienti dagli altri prodotti Sophos Central, che vanno oltre la semplice analisi degli endpoint per fornire un quadro completo delle attività degli antagonisti.

Miglioramento proattivo della condizione generale del sistema

Miglioramento proattivo della condizione di sicurezza generale del sistema con potenziamento della protezione, grazie a indicazioni prescrittive volte a risolvere le vulnerabilità nelle configurazioni e nelle architetture, che possono diminuire le capacità complessive di sicurezza.

Contatto dedicato per la risposta alle minacce

All'identificazione di un incidente, viene fornito un contatto dedicato per la risposta alle minacce, che collaborerà direttamente con le vostre risorse on-premise (un team interno o un partner esterno), fino alla neutralizzazione completa della minaccia.

Supporto diretto e dedicato

Il vostro team può usufruire di accesso diretto e dedicato ai nostri Security Operations Center (SOC). Il nostro MTR Operations Team è disponibile 24h su 24 e può contare sull'assistenza di team di supporto situati in 26 località in tutto il mondo.

Individuazione delle risorse

Da informazioni sulle risorse che includono versioni del sistema operativo, applicazioni e vulnerabilità, fino all'identificazione delle risorse gestite e di quelle non gestite, offriamo importanti analisi approfondite, che sono disponibili per valutare l'impatto di un incidente, per svolgere azioni di threat hunting e per fornire consigli su come migliorare proattivamente lo stato generale del sistema.