Domande frequenti su Intercept X Essentials e Intercept X Essentials for Server

Intercept X Essentials e Intercept X Essentials for Server sono nuove licenze che permettono di usufruire della protezione leader di settore di Intercept X, ma con funzionalità di controllo e gestione ridotte.

Quali sono le nuove licenze?

- Intercept X Essentials (CIXE)
- Intercept X Essentials for Server (SVRCIXE)

Entrambe saranno disponibili per la vendita a partire dal 1º luglio 2021.

Qual è il target adatto?

Intercept X Essentials e Intercept X Essentials for Server sono ideali per le organizzazioni di piccole dimensioni che desiderano il massimo della protezione con un'unica policy, ma che non hanno bisogno di tutte le funzionalità di controllo e gestione. Se un cliente richiede policy multiple e configurabili oppure opzioni come il controllo delle periferiche, meglio proporre Intercept X Advanced/ Intercept X Advanced for Server o soluzioni di fascia più alta.

Queste licenze includono funzionalità di Deep Learning e anti-ransomware?

Sì. Intercept X Essentials e Intercept X Essentials for Server includono tecnologie di Intelligenza Artificiale basate sul Deep Learning, con funzionalità anti-ransomware e anti-exploit che non erano presenti in Central Endpoint Protection e Central Server Protection.

Quali sono le funzionalità che non sono incluse in Intercept X Essentials/Intercept X Essentials for Server?

- **Policy multiple**
  I Clienti devono utilizzare le policy di base.
- **Controllo delle periferiche**
  I Clienti non possono imporre limiti sui tipi di dispositivo connessi dagli utenti.
- **Aggiornamenti controllati**
  I Clienti non possono posticipare gli aggiornamenti e scegliere quando implementarli.
- **Controllo web**
  I Clienti non possono impedire agli utenti di accedere a siti web inappropriati.
- **Controllo delle applicazioni**
  I Clienti non sono in grado di controllare i tipi di applicazione che possono essere installati ed eseguiti.
- **Casi di minacce**
  I Clienti non hanno accesso ai casi sulle minacce, che forniscono informazioni dettagliate sugli eventi che si sono verificati durante un incidente.
- **Monitoraggio dell'integrità dei file (File Integrity Monitoring)**
  I Clienti non possono individuare eventuali tentativi di manomissione dei file essenziali sui server.
- **Cloud Security Posture Management (CSPM)**
  I Clienti non hanno visibilità sull'ambiente cloud esteso, come ad esempio funzioni e database senza server.
- **Lockdown del server**
  I Clienti non possono bloccare i server in una configurazione di base.

I Clienti Essentials possono effettuare l'upgrade alle licenze Advanced/EDR?

Sì. I Clienti che utilizzano Intercept X Essentials/ Intercept X Essentials for Server possono eseguire l'upgrade a Intercept X Advanced/Intercept X Advanced for Server oppure a Intercept X Advanced with EDR/ Intercept X Advanced for Server with EDR. Potranno così usufruire di policy multiple, ulteriori opzioni di controllo e potenti funzionalità di Endpoint Detection and Response (EDR).

I Clienti possono utilizzare licenze Essentials e Advanced/EDR nello stesso ambiente?

No, gli ambienti misti non sono consentiti.

SOPHOS

Confronto dettagliato delle funzionalità

Funzionalità	Intercept X Essentials/ Intercept X Essentials for Server	Intercept X Advanced/ Intercept X Advanced for Server
Supporto di policy multiple	Solo criterio di base	X
Aggiornamenti controllati		X
Controllo web/Blocco degli URL in base alla categoria di appartenenza		X
Controllo delle periferiche		X
Controllo delle applicazioni		X
Data Loss Prevention (prevenzione della perdita di dati)		X
Casi di minacce		X
Early Access Program		X
Web Security	X	X
Download Reputation	X	X
Rilevamento antimalware con Deep Learning	X	X
Scansione antimalware dei file	X	X
Live Protection	X	X
Analisi del comportamento in pre-esecuzione (HIPS)	X	X
Blocco delle applicazioni potenzialmente indesiderate (PUA)	X	X
Intrusion Prevention System (IPS)	X	X

Funzionalità	Intercept X Essentials/ Intercept X Essentials for Server	Intercept X Advanced/ Intercept X Advanced for Server
Analisi del comportamento in fase di esecuzione (HIPS)	X	X
Antimalware Scan Interface (AMSI)	X	X
Rilevamento del traffico malevolo (Malicious Traffic Detection, MTD)	X	X
Exploit Prevention	X	X
Mitigazione degli Active Adversary	X	X
Protezione anti-ransomware per i file (CryptoGuard)	X	X
Protezione del disco e del record di avvio (WipeGuard)	X	X
Protezione contro gli attacchi man-in-the-browser (Safe Browsing)	X	X
Ottimizzazione del lockdown delle applicazioni	X	X
Rimozione automatizzata del malware	X	X
Synchronized Security	X	X
Sophos Clean	X	X
Gestione da Sophos Central	X	X

Funzionalità specifiche per i server

Monitoraggio dell'integrità dei file (File Integrity Monitoring)		X
Lockdown del server		X
Cloud Security Posture Management (CSPM)		X

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

17/05/21 IT (NP)

SOPHOS