MINISTERO DELL'INTERNO
Dipartimento della Pubblica Sicurezza

DIREZIONE CENTRALE DEI SERVIZI TECNICO LOGISTICI E DELLA GESTIONE PATRIMONIALE

Capitolato Tecnico

Fornitura di una Piattaforma "End Point Protection" con relativi servizi professionali a supporto per il Dipartimento della Pubblica Sicurezza

INDICE

1. Premessa

Il presente documento disciplina gli aspetti tecnici, relativi la fornitura di un sistema Antimalware per la protezione e la sicurezza delle postazioni client e server per le esigenze del Dipartimento della Pubblica Sicurezza. L'obbiettivo è quello di rafforzare l'architettura di rete interna, per far fronte ad eventuali "Cyber Threats" relative alle postazioni client e server.

La durata del contratto è di **36 mesi.**

Si rappresenta che in caso di **eventuale** discrepanza tra documenti tecnici, farà fede questo documento denominato ***"Capitolato Tecnico parte seconda".***

2. Sigle e acronimi

Nell'ambito del presente Capitolato Tecnico sono stati usati i seguenti acronimi:

Tabella - Sigle e acronimi

ACRONIMO	DESCRIZIONE
Fornitore	l'Impresa aggiudicataria della gara, eventualmente mandataria di un RTI;
Fornitura	quanto indicato come Oggetto di Fornitura e descritto dettagliatamente;
HW	Hardware
SW	Software
ICT	Information Communication Technologies
LdS	Livelli di Servizio
SLA	Service Level Agreement
DEC	Direttore esecuzione del contratto
RUP	Responsabile unico del Procedimento

3. Definizioni

Nel seguito del documento si ricorrerà più volte ad alcuni termini cui è attribuito il seguente significato:

- **Amministrazione**: l'Amministrazione contraente, ovvero il Ministero dell'Interno;
- **Capitolato Tecnico parte seconda**: il presente documento**;**

- **Committente**: l'Amministrazione responsabile del contratto, ovvero il Dipartimento della Pubblica Sicurezza;
- **Fornitore:** l'Impresa aggiudicataria della gara, eventualmente mandataria di un RTI;
- **Fornitura**: quanto indicato come Oggetto di Fornitura e descritto dettagliatamente;
- **Impresa**: l'Impresa aggiudicataria della gara, eventualmente mandataria di un RTI;
- **Listini:** elenchi di prodotti e di servizi, corrispondenti a varie tecnologie, predisposti dal Committente oppure offerti dall'Impresa sulla base dei requisiti del presente Capitolato, da cui è possibile attingere gli oggetti delle varie acquisizioni;
- **Manutenzione**: l'insieme delle operazioni volte a mantenere in efficienza e/o ripristinare la piena funzionalità dei Sistemi richiesti nel Capitolato Tecnico;
- **Responsabile del progetto/servizio**: soggetto individuato dal Committente, che per una determinata attività progettuale o per un servizio, assume la responsabilità della conduzione dello stesso e, in particolare, costituisce l'interlocutore principale del fornitore nell'esecuzione delle attività.
- **Servizio/i:** il servizio o l'insieme dei servizi connessi alla Fornitura in oggetto.
- **Guasto bloccante**: Si intende per guasto bloccante un malfunzionamento per cui è impedito l'uso di tutto il sistema o di una o più funzioni essenziali.
- **Guasto non bloccante**: Si intende per guasto non bloccante un malfunzionamento per cui è impedito l'uso di funzionalità non essenziali o critiche del sistema in alcune condizioni per cui non si ha un effetto penalizzante sull'operatività degli utenti.
- **Incidente**: eventi negativi che compromettono alcuni aspetti dell'asset, della rete o della sicurezza.
- **Malfunzionamento**: è un impedimento all'esecuzione dell'applicazione /funzione o gli effetti che un errore ha causato sulla base dati o il riscontro di differenze fra l'effettivo funzionamento del software applicativo e quello atteso, come previsto dalla relativa documentazione.

4. Oggetto della fornitura

Sono oggetto della fornitura:

- 25.000 licenze software Antimalware per postazioni client Windows versioni >=8 in modalità ONPREMISE;
- 1000 licenze software Antimalware per postazioni Server Windows versione >=2012 in modalità ONPREMISE;
- 40 gg a **consumo** per assistenza ed **eventuale** attività di migrazione e configurazione (design , progettazione e tuning della piattaforma.).
- 5 gg di formazione da svolgere presso la sede di Roma**.**

5. Descrizione della fornitura

Di seguito sono indicate le caratteristiche tecniche **minime** da rispettare a **pena esclusione**. Si precisa che per alcune caratteristiche è indicato un **valore minimo**, per altre è riportato l'esatto valore richiesto.

Criterio di aggiudicazione	Minor Prezzo
Ordinamento delle offerte	Al ribasso
Unità di misura delle offerte	Valuta euro
Valore Appalto specifico	**€ 700.000,00 IVA esclusa**
Durata del contratto	36 mesi
Soglia rilevanza comunitaria	Sopra soglia
Numero di lotti	1
Descrizione tecnica	• Licenze Software • Servizi professionali
Nome commerciale	• Sophos • McAfee • Trend Micro • Symantec • Cisco

I requisiti della piattaforma di End Point Protection sono suddivisi come di seguito:

- **Requisiti Gestionali**
- **Requisiti della componente Antimalware:**
  La soluzione proposta deve disporre delle seguenti funzionalità di sicurezza:
  - Componente antimalware;
  - Protezione contro tipologie di malware/spyware: anti-rootkit, anti-ransomware;
  - Personal Firewall;
  - Host Intrusion Detection System;
  - Application control;
  - Data loss prevention;
- **Requisiti Sistemistici**
- **Requisiti Architetturali della soluzione proposta**

6. Requisiti Gestionali

La soluzione deve poter prevedere una **console di gestione** centralizzata, di facile utilizzo, consultabile via web (Web based) che sia nativamente Multitenant, abbia una reportistica unificata che includa tutti i dati ed eventi provenienti dalle varie piattaforme. La consultazione dei log centralizzati deve essere filtrabile per utente, in modo da ottenere dei report unici raggruppando elementi provenienti da differenti tecnologie (ad es. server, endpoint, dispositivi mobili), deve essere possibile una comunicazione integrata con tutte le altre console, che si potranno poi gestire singolarmente. La piattaforma **deve** inoltre offrire le seguenti funzionalità:

Requisito	**Conformità al requisito**
Autenticazione degli operatori: la console di amministrazione deve disporre di processi di autenticazione con la possibilità di integrazione con gli attuali sistemi di autenticazione basati su Microsoft Active Directory.	
Profilatura degli accessi: la console deve supportare diversi profili autorizzativi per gli amministratori (segregation of duties); come esempio: 1. Profilo Amministratore in grado di amministrare tutta l'infrastruttura senza restrizioni (root admin). 2. Profilo in grado di fare solo monitoraggio e visualizzazione dei LOG/Report.	
Reportistica estesa: dovranno essere garantite funzionalità di reporting esteso. Dai report si dovranno evidenziare, tra le altre informazioni: • Eventi occorsi per ogni singola componente di sicurezza; • Statistiche sull'andamento delle infezioni (suddivisi per tipologie di virus e per macchina protetta); • Statistiche sulle macchine maggiormente esposte ad attacchi; • Stato dell'intera infrastruttura: dovranno essere incluse tutte le informazioni relative alle versioni (motore antivirus e pattern scaricato) installate sia lato server di management che lato macchina protetta; • Grafici in grado di dare una panoramica veloce sullo stato dell'intera infrastruttura; • Stato di eventuali attacchi di rete subiti dalle macchine con chiara indicazione della sorgente e della tipologia di attacco; • I report devono poter essere pianificati o generati su richiesta;	

Device Control: la console dovrà gestire e controllare l'utilizzo dei singoli device presenti sui client gestiti. Il device control dovrà rilevare o bloccare l'utilizzo di: Storage Device (CD/DVD/Floppy/USB Keys/External HD. ecc), Wireless Connection (Bluetooth/IrDA/Wifi.. ecc). Inoltre, in caso di blocco, dovrà permettere la creazione di eccezioni e permettere l'utilizzo di singoli dispositivi riconoscibili tramite vendor e numero seriale. Infine, nel caso di modem o schede wireless, dovrà permettere il blocco della singola funzionalità del bridging tra la suddetta interfaccia di rete e la rete LAN interna.	
Allarmistica: La soluzione deve consentire l'invio agli amministratori tramite email, syslog, trap snmp, msn messenger di eventuali notifiche relative a eventi pericolosi (fault, assenza di comunicazione tra le componenti della piattaforma, epidemie, etc.)	
Notifica tramite dashboard: la soluzione deve essere in grado di visualizzare nella dashboard situazioni potenzialmente pericolose (es. versioni dei client non aggiornate, pattern non aggiornati, client antivirus che non comunicano con la console);	
Rimozione remota dell'agent: possibilità di disinstallazione remota degli agent attraverso console di amministrazione	
Competitive Unistall: La soluzione fornita deve prevedere la rimozione automatica di software anti-malware già presenti in fase di installazione.	
Servizi di Threat Intelligence: La soluzione deve poter accedere al servizio cloud del produttore per recuperare informazioni di intelligence in maniera totalmente anonimizzata. Deve essere possibile disabilitare l'invio di informazioni verso il servizio di intelligence del produttore senza alcuna limitazione funzionale o di sicurezza.	

7. Requisiti della componente Antimalware

La soluzione deve disporre di funzionalità di protezione *antimalware* di ultima generazione, essere efficace contro minacce zero-day ed adottare tecnologie di rilevamento in pre-esecuzione di tipo *deep learning* (sistemi Windows). Il presente paragrafo descrive le funzionalità minime che la componente Antimalware deve disporre:

Requisito	**Conformità al requisito**
Real Time Detection: la componente anti-malware deve disporre di funzionalità di detection real-time	
Signature: la componente anti-malware deve disporre di funzionalità di detection basate su firma (pattern matching)	
Euristica: la componente anti-malware deve disporre di funzionalità di detection basate su tecniche euristiche	
Cleaning: la soluzione deve essere in grado di effettuare il cleaning del malware individuato	
Quarantena: la soluzione deve essere in grado di effettuare la quarantena del malware individuato	
Rollback/Restore: la soluzione deve essere in grado di effettuare il rollback/restore dei file rilevati come infetti e messi in quarantena	
Ignore: la soluzione deve essere in grado di effettuare l'operazione di Ignore (pass) nei casi di CVE exploit durante le scansioni Real-Time, In tutti gli altri casi (scansioni manuali o pianificate) deve essere possibile assegnare tale azione anche alle altre categorie di malware (es. Joke, Trojan, Virus, Packer, ecc)	
Scan Scheduling: la soluzione deve essere in grado di effettuare l'operazione di pianificazione delle scansioni complete (scan scheduling) con possibilità di gestire il livello di carico della CPU dell'endpoint per garantire sempre una elevata esperienza d'uso dell'utente ottimizzando le risorse disponibili sulla macchina. Inoltre il prodotto deve essere in grado di sospendere, con ripresa al giorno seguente, una scansione schedulata non terminata entro una fascia oraria definita dagli amministratori.	
Scansione ottimizzata: per migliorare le proprie prestazioni di scansione la soluzione deve essere in grado di memorizzare i risultati delle scansioni on-demand precedenti in modo tale da poter evitare di scansionare nuovamente gli stessi file.	
Manual full Scan: la soluzione deve essere in grado di avviare manualmente una scansione completa (manual scan)	
Scan File&Folder: la soluzione deve essere in grado di avviare manualmente una scansione di singoli file/cartelle (manual scan file&folder). La soluzione deve consentire all'utente di eseguire la scansione di un singolo	

file/cartella tramite il menù contestuale a right click.	
Scan Removable Media: la soluzione deve disporre di funzionalità di Scan Removable Media in grado di rilevare malware presenti nei supporti rimuovibili (ad esempio chiavetta USB, scheda SD, ecc.) La soluzione deve essere in grado di disabilitare l'esecuzione automatica dell'autorun.inf su dispositivi USB removibili.	
Auto Update e 0-days: la soluzione deve disporre di funzionalità di auto update in grado di aggiornare automaticamente il proprio database dei pattern e/o la componente client, inoltre deve disporre di funzionalità 0days e l'ausilio del cloud per limitare e ridurre potenziali nuove minacce non ancora presenti nelle firme virali	
Size Limit: la soluzione deve permettere di impostare la dimensione massima dei file da analizzare durante le scansioni	
Exclusion: la soluzione deve consentire di impostare una lista di file e cartelle da escludere durante le scansioni	
Pre-Execution Machine Learning: la soluzione deve integrare una tecnologia di Machine Learning che consenta la verifica statica di caratteristiche di file potenzialmente dannosi comparandole con caratteristiche simili di file già noti al servizio di intelligence del produttore del software.	
Runtime Machine Learning: la soluzione deve integrare una tecnologia di Machine Learning che consenta la verifica di azioni effettuate da file potenzialmente dannosi comparandoli con azioni simili effettuate da file già noti al servizio di intelligence del produttore del software.	
Memory inspection: la soluzione deve rilevare e prevenire applicazioni malevole in esecuzione in memoria	

8. Protezione contro tipologie di malware/spyware:

La piattaforma deve includere delle funzionalità di protezione avanzata e preventiva degli endpoint mediante l'integrazione di patch virtuali proattive nella sicurezza antimalware e dalle minacce del desktop. La soluzione proposta deve rilevare ed eventualmente bloccare **almeno** le seguenti tipologie di malware:

Requisito	**Conformità al requisito**
Protezione contro tipologie di spyware & grayware: La soluzione proposta deve rilevare ed eventualmente bloccare le seguenti tipologie di spyware & grayware: • Spyware; • AdWare; • Dialer; • Joke Program; • Hacking Tool; • Password Cracking Application;	
Worm: programmi che non richiedono l'intervento dell'utente per diffondersi; un worm invece che infettare file esistenti, utilizza la rete per inviare copie di sè stesso.	
Trojan: programmi che si installano sul computer; possono causare danni al sistema, raccogliere informazioni confidenziali o permettere un accesso non controllato alle risorse della macchina protetta; si diffondono tipicamente via e-mail e sono "nascosti" all'interno di altri programmi apparentemente innocui.	
Rootkit: malware disegnato per avere pieno controllo del sistema grazie all'esecuzione automatica di processi privilegiati e "nascosti", tipicamente non visibili, tramite le API standard del Sistema Operativo.	
Protezione da malware offuscati: malware che si propagano utilizzando tecniche di elusione.	
Exploit: codice che, sfruttando un bug o una vulnerabilità, porta all'esecuzione di codice non previsto, il cui risultato può portare all'acquisizione dei privilegi di root di una macchina protetta.	
Ransomware: tipo di malware che limita l'accesso ai dati del dispositivo che infetta, richiedendo un riscatto da pagare per rimuovere la limitazione	

9. Componente Personal Firewall, Host IPS e Web Reputation

La soluzione deve includere delle componenti di Personal Firewall , Host IPS e Web Reputation.
Personal Firewall: ovvero la funzionalità di network firewalling in grado di gestire gli accessi alla postazione per singolo indirizzo IP o range di indirizzi, per singola porta TCP/UDP o range di porte o per protocollo.
Host IPS: protezione proattiva contro attacchi di rete (IPS) con Protezione delle vulnerabilità***:***

Web Reputation: La soluzione proposta deve contenere la funzionalità di controllo e filtraggio di eventuali comunicazioni verso siti web al fine di bloccare eventuali comunicazioni malevole (ad esempio Command & Control) tramite la verifica della reputazione del sito stesso;

Requisito	**Conformità al requisito**
Stateful Firewall: la soluzione deve prevedere la funzionalità di Stateful Personal Firewall	
No zero PING : la soluzione deve prevedere che l'installazione del Personal Firewall sul client non interrompa il flusso dei pacchetti TCP/IP	
Host IPS • La soluzione proposta deve contenere la protezione proattiva contro attacchi di rete (IPS) con Protezione delle vulnerabilità***:*** disporre di funzionalità di scoperta delle vulnerabilità in grado di riconoscere eventuali patch mancanti (sia di Sistema Operativo sia applicative) e di rilevare, segnalare e/o bloccare il tentativo di sfruttamento su server gestiti in base a criteri personalizzabili anche su host non in dominio (workgroup); • La protezione da vulnerabilità integrata nella componente IPS dovrà consentire agli amministratori di identificare nella regola il codice CVE (common vulnerability exploit) ed in caso di vulnerabilità Microsoft dovrà essere indicata anche la patch MS di riferimento ove rilasciata; • Le regole IPS devono poter essere filtrate per severity e dovranno poter gestire l'applicazione della regola in modalità prevent o detect su scelta dell'amministratore; • Il modulo IPS, deve poter operare in modalità Tap Mode, in modo tale da poter lavorare in sola detection sul traffico replicato sulla scheda di rete;	
Web Reputation La soluzione proposta deve contenere la funzionalità di controllo e filtraggio di eventuali comunicazioni verso siti web al fine di bloccare eventuali comunicazioni malevole (ad esempio Command & Control) tramite la verifica della reputazione del sito stesso; • La soluzione proposta deve consentire di poter personalizzare le whitelist/blacklist fornite dal produttore con un elenco ad hoc; • La soluzione proposta deve poter utilizzare un cloud database contenente il censimento della reputazione dei file in termini di maturità e diffusione a livello mondiale e locale; • La soluzione deve potersi integrare con strumenti SIEM di terze parti tramite il protocollo Syslog e SNMP;	

10. Componente Application Control

Al fine di potenziare le difese dai malware o dagli attacchi mirati, impedendo l'esecuzione di applicazioni sconosciute o indesiderate, la soluzione deve prevedere la possibilità di inibire l'avvio di specifiche applicazioni (come ad esempio: Voip, File Sharing o Toolbar di Browser, Game e IM. Ecc.) sulla base di numerose categorie software con aggiornamenti dinamici in modo da consentire agli utenti di installare applicazioni valide in base a molte variabili basate sulla reputazione come prevalenza, utilizzo regionale e maturità .

Requisito	**Conformità al requisito**
Gold Image: la soluzione deve consentire la possibilità di definire la lista delle applicazioni autorizzate creando la "base line" con scansione sul client di riferimento in cui è installato il software.	
Lockdown: la soluzione deve permettere di censire le applicazioni installate, al di fuori delle quali ogni altra applicazione non è consentita.	
Application Restriction: la soluzione deve permettere di poter limitare i privilegi di esecuzione delle applicazioni su più livelli, minimo 2 (Trusted – Untrusted).	
Granularità dei filtri statici: la soluzione deve consentire di definire la ricerca di applicazioni in base a: • singola applicazione o inventario • software certificato • file hash • percorso d'installazione Tali query devono potersi eseguire combinando i criteri sopraelencati	
Liste di ricerca: la soluzione deve consentire di definire - con criteri di ricerca tra quelli elencati sopra - liste di applicazioni, da salvare per essere utilizzate per indagini	

periodiche.	
Versioning Applicativo: la soluzione deve consentire di verificare la versione delle applicazioni installate permettendo l'attivazione di policy per consentire l'esecuzione o il blocco di specifiche versioni dello stesso applicativo.	
Sorgenti attendibili: la soluzione deve poter autorizzare specifiche applicazioni per installare nuovi programmi o effettuare modifiche alle macchine protette	

11. Componente Data Loss Prevention

La soluzione deve prevedere un modulo di controllo del flusso di informazioni. Dovrà essere possibile creare delle policy per il controllo delle informazioni che dal pc dei dipendenti vengono trasferite all'esterno (p. es. periferiche di massa USB, allegato email, upload su siti web). In caso di violazione di policy si potrà decidere di bloccare il trasferimento del file, di permettere il trasferimento e di loggare l'evento, o di avvisare l'utente che il trasferimento comporta una possibile violazione della sicurezza. Le policy dovranno essere basate sul contenuto o sulla tipologia dei file. Dovrà essere possibile la creazione di policy ad hoc per identificare eventuali dati sensibili particolari (tramite la creazione di *regular expression* di riconoscimento del *pattern*.

Requisito	**Conformità al requisito**
Data Loss Prevention: • Identificare contenuti specifici all'interno di un documento in termini di corrispondenza a parole chiave, espressioni regolari o modelli forniti dal produttore del software; • Controllare i seguenti canali di trasmissione da parte dell'endpoint: e-mail, webmail, upload via web, FTP, trasferimento su dispositivi USB, upload tramite software di Instant Messaging, condivisione di rete, print screen, masterizzazione su cdrom/dvd; • Sulla base dell'analisi della movimentazione dei file dovrà essere possibile effettuare le seguenti azioni: registrare alert, notifica ad amministratori, utenti o terze parti, blocco del trasferimento o cifratura dei files in caso di copia su dispositivi rimovibili integrandosi con la soluzione di File & Media Encryption fornita dallo stesso produttore della soluzione anti-malware; • L'inserimento di commenti da parte dell'utente in modo da poter allegare gli stessi nel sistema di logging della soluzione;	

12. Requisiti Sistemistici

Le protezioni agent-based dovranno avere un consumo di risorse limitato ed ottimizzato (in termini di RAM e CPU), in modo da minimizzare l'impatto sull'operatività. le soluzioni proposte devono inoltre integrarsi con Microsoft Active Directory.

Requisito	**Conformità al requisito**
Compatibilità con ambienti fisici e virtuali: la componente di protezione anti-malware deve supportare sia gli ambienti fisici, sia gli ambienti virtualizzati. Inoltre, deve essere garantita la piena integrazione con la tecnologia VMWare NSX e vRealize Operation Manager.	
Il vendor deve fornire supporto in lingua locale, attraverso personale qualificato in Italia e non tramite call center.	

13. Requisiti Architetturali

Di seguito è possibile indicare ad alto livello le caratteristiche tecniche del Design relativo all'architettura della soluzione proposta.

Requisito	**Descrizione**
Design e flessibilità della soluzione proposta: descrivere l'architettura della soluzione proposta.	
Modalità di distribuzione degli aggiornamenti: gli aggiornamenti, sia in termini di Update Agent che pattern antivirali, devono poter essere distribuiti tramite un'architettura gerarchica e distribuita geograficamente al fine di ridurre al massimo l'occupazione di banda.	
Approccio alla scalabilità: la soluzione proposta deve consentire la scalabilità dell'ambiente architetturale installato in termini sia di numeri che di funzionalità, mantenendo l'architettura gestionale presente adeguandola nei quantitativi qualora fosse necessario. Riportare le caratteristiche architetturali della soluzione per garantire un sufficiente grado di scalabilità. Le funzionalità di reportistica dovranno necessariamente essere accessibili da un'unica console globale indipendente dall'architettura proposta con una logica Role Based Access Control e conseguente profilazione.	

14. Consegna, installazione e verifica di conformità

La consegna deve avvenire presso le sedi indicate dall'Amministrazione. Entro un massimo di 20 gg lavorativi dalla consegna di tutto il materiale, l'Amministrazione procederà alla verifica di conformità inventariale della fornitura, che si concluderà con la redazione di apposito certificato di conformità.

Il Fornitore dovrà presentare ogni documentazione necessaria ad attestare l'effettiva fornitura.

L'amministrazione si riserva la facoltà di effettuare ulteriori motivate verifiche, che ritenga opportuno.

Il Fornitore deve garantire tutta l'assistenza necessaria e mettere a disposizione dell'Amministrazione tutte le apparecchiature e mezzi essenziali per l'effettuazione delle verifiche.

Al completamento della fase di installazione del pacchetto licenze il fornitore dovrà procedere alle attività di configurazione di tutti i sistemi previsti in fornitura. Nell'ambito delle prove finalizzate alla verifica funzionale, il fornitore dovrà redigere e consegnare, entro il termine delle attività di configurazione, un rapporto contenente l'articolazione delle prove per la verifica dei requisiti. La Verifica di conformità si intende positivamente superata solo quando le prestazioni contrattuali siano state eseguite a regola d'arte sotto il profilo tecnico e funzionale, in conformità e nel rispetto delle condizioni, modalità, termini e prescrizioni espresse nel presente Capitolato Tecnico.

Nel caso di esito negativo della verifica di conformità, il Fornitore dovrà eliminare i vizi accertati entro il termine massimo che sarà concesso dall'Amministrazione.

Il Fornitore dovrà nominare un proprio Responsabile Generale di Progetto (Project Manager) con funzioni di coordinamento e di unica interfaccia tecnica con l'Amministrazione e di tale nomina dovrà essere data comunicazione all'Amministrazione.

15. Giornate professionali a consumo per Attività di analisi, configurazione, Progettazione e Tuning

Per **eventuali** attività di configurazione dovranno essere fornite un congruo numero di giorni uomo di un mix di figure professionali con conoscenza dei sistemi in argomento.

Sono richiesti **nr. 40 gg a consumo, da erogarsi nell'arco di 36 mesi, per attività varie di analisi, configurazione, progettazione e tuning della piattaforma.**

Tale servizio si svolgerà nell'ambito della settimana lavorativa articolata in cinque giorni dal lunedì al venerdì. L'orario di lavoro coinciderà per quanto possibile con l'orario dell'Amministrazione (09.00/18.00).

Si fa presente che eventuali giornate residuali, potranno essere erogate anche post verifica inventariale.

L'Amministrazione richiederà tale servizio con un preavviso di almeno 7 giorni solari.

Le configurazioni definite saranno oggetto di verifica da parte dell'Amministrazione. Il fornitore si impegnerà ad apportare eventuali modifiche e integrazioni su indicazione dell'Amministrazione

Modalità di erogazione del servizio

La regolamentazione contrattuale del servizio è **su richiesta a chiamata.** Per l'erogazione del servizio si dovrà garantire la presenza di personale con competenze certificate a soddisfare con professionalità il servizio richiesto presso le sedi indicate dall'Amministrazione.

Monitoraggio sull'erogazione del servizio

Le singole presenze del personale impiegato nell'erogazione dei servizi oggetto della fornitura saranno registrate e dovrà essere redatto per l'amministrazione un riepilogo delle giornate lavorative prestate.

L'Amministrazione potrà verificare la professionalità del personale impiegato nell'erogazione dei servizi durante il periodo in esame, utilizzando come parametri di qualità l'adeguatezza delle competenze, l'efficacia e l'efficienza degli interventi. Qualora una singola valutazione risultasse insufficiente, il fornitore su richiesta dell''Amministrazione dovrà sostituire il personale coinvolto senza aver riconosciuto l'onere della prestazione eseguita.

Nella presentazione dell'offerta economica il concorrente dovrà indicare **il costo unitario della singola giornata, pena esclusione.**

16. Formazione

Attraverso personale certificato è richiesta la formazione al personale della Polizia di Stato tramite un corso da svolgere nelle sede di Roma presso i locali dell'Amministrazione.

Il corso, da tenersi in lingua italiana, prevedere la partecipazione di massimo 25 discenti e dovrà essere organizzato in un'unica sessione della durata minima di 5 giorni lavorativi (8 ore dalle 8.00 alle 17.00); l'Amministrazione si riserva il diritto di far partecipare numero 3 (tre) osservatori.

Il Fornitore dovrà organizzare il corso:

- fornendo tutto il materiale didattico necessario
- prevedendo l'alternarsi di fasi teoriche e pratiche, allo scopo di illustrare tutte le funzionalità offerte dal sistema.

Le date di inizio e le modalità di svolgimento dei attività di formazione dovranno esser concordate con l'Amministrazione. In particolare il Fornitore dovrà definire un **Piano Formativo** per un adeguato addestramento teorico e pratico per il personale, approvato dall'Amministrazione.

Sono a carico del Fornitore i costi di eventuali trasferte, trasferimenti, vitto ed alloggio.

17. Help Desk

Il fornitore deve garantire il servizio di Help Desk fruibile via mail e con numero telefonico dedicato, dalle ore 9:00 alle 13:30 e dalle 14:30 alle 17:30 dei giorni lavorativi (dal lunedì al venerdì) ed avrà il compito di supportare il personale della Polizia di Stato incaricato, in merito ai seguenti ambiti:

- Supporto all'apertura di ticket (case) verso il Supporto Tecnico del fornitore della soluzione software;
- Aggiornamenti sullo stato dei ticket aperti;
- Nuovi aggiornamenti software della soluzione Antimalware fornita, disponibili per tutto il periodo di validità (36 mesi);

- Maintenance delle release e patches della soluzione software Antimalware.

18. Supporto Tecnico e interventi di assistenza on site.

Il **servizio di supporto sui software forniti** dovrà essere erogato secondo le modalità di seguito specificate. Nello specifico, le richieste di assistenza tecnica verranno gestite secondo le seguenti priorità:

- Severità 1 - (sistema bloccato e attività interrotta);
- Severità 2 - (mancata disponibilità di feature importanti, con una minore funzionalità del servizio);
- Severità 3 - (livello standard richieste relative a caratteristiche e funzionalità del prodotto; mancata disponibilità di caratteristiche significative, risolvibili con workround; oppure non disponibilità di caratteristiche poco significative in assenza di workround);
- Severità 4 - (richiesta di informazioni o chiarimenti sulla documentazione).

Per un malfunzionamento di "Severità 1" e "Severità 2", le attività di risposta alla chiamata dovranno essere eseguite entro i seguenti tempi:

- massimo entro 8 (otto) ore lavorative dalla ricezione della comunicazion, nel 95% dei malfunzionamenti;
- massimo entro 12 (dodici) ore lavorative dalla ricezione della comunicazione via fax o mail, nel restante 5% dei malfunzionamenti segnalati, salva diversa comunicazione dell'Amministrazione per malfunzionamenti che necessitano di tempi di intervento differenti.

Ai fini del rispetto dei precedenti termini è ammessa anche una fix temporanea, una circumvention o un bypass.

19. Base d'asta

L'importo a base d'asta complessivo è fissato in **700.000,00 IVA esclusa;** non saranno, quindi, ammesse offerte economiche che comportano una spesa superiore.

20. Criterio di Aggiudicazione delle Offerte

Considerato che i prodotti con le caratteristiche necessarie all'Amministrazione sono individuati con specifiche tecniche puntualmente identificate, la richiesta di offerta verrà aggiudicata con il criterio del minor prezzo, ai sensi dell'art. 95 comma 4, lett.b), del D.lgs. 50/2016.

21. Presentazione dell'offerta economica

L'offerta economica dovrà essere presentata preferibilmente mediante la compilazione della seguente tabella, ovvero, in qualsiasi altra forma stilistica purché rappresenti medesimi livelli di dettaglio e di informazioni:

PRODOTTO	**Q.TA'**	**COSTO UNITARIO** *(€ iva esclusa)*	**PREZZO COMPLESSIVO** *(€ iva esclusa)*
Piattaforma Antimalware Protezione Client	**25.000 Licenze**		
Piattaforma Antimalware Protezione Server	**1000 Licenze**		
Servizio di Assistenza	**1 x 36 mesi**		
Formazione	**5gg**		
Giornate a consumo di configurazione e/o migrazione	**40gg**		
TOTALE			
oneri relativi ai rischi di sicurezza aziendali ai sensi dell'art. 95, comma 10, del D. Lgs.vo nr.50/2016			