ALLEGATO 2

CAPITOLATO TECNICO

APPALTO SPECIFICO NELL'AMBITO DELLO SDA ICT PER LA MANUTENZIONE E L'EVOLUZIONE DELLA PIATTAFORMA MCAFEE DI INAIL - ID 2080

1 PREMESSA 3
2 IL CONTESTO TECNOLOGICO E GLI OBIETTIVI 4
2.1 Contesto tecnologico 4
2.2 La piattaforma di sicurezza McAfee 5
2.3 Obiettivi perseguiti attraverso l'evoluzione della piattaforma 6
3 DEFINIZIONE DELLA FORNITURA 8
3.1 Oggetto 8
3.2 Durata 8
3.3 Responsabile del Servizio 8
3.4 Luogo di lavoro 8
4 DEFINIZIONE DEI BENI E DEI SERVIZI OGGETTO DELLA FORNITURA 9
4.1 Upgrade tecnologico dei prodotti installati e relativa manutenzione 9
4.2 Rinnovo della manutenzione dei prodotti installati 10
4.3 Servizio di supporto sistemistico on site McAfee Platinum Enterprise 10
4.4 Servizio di sviluppo Custom Parser per ESM 10
4.5 Servizio di addestramento 10
4.6 Servizi professionali di supporto specialistico (a consumo) 11
4.7 Nuovi prodotti software in sottoscrizione o in licenza d'uso perpetua e nuove apparecchiature hardware (appliance), con relativi servizi di manutenzione e supporto connessi (in opzione) 11
5 MODALITÀ DI ESECUZIONE DELLA FORNITURA 13
5.1 Manutenzione dei prodotti software e delle apparecchiature hardware 13
5.2 Servizio di Supporto Sistemistico on site McAfee Platinum Enterprise 15
5.3 Servizio di sviluppo Custom Parser per ESM 15
5.4 Servizio di addestramento 16
5.5 Servizi Professionali di supporto specialistico 17
5.6 Fornitura di nuovi prodotti software in sottoscrizione o in licenza d'uso perpetua e nuove apparecchiature hardware 26

1 PREMESSA

Nell'ambito della Convenzione stipulata tra INAIL e Consip S.p.A. in data 03/12/2018, l'INAIL ha affidato a Consip la presente acquisizione, relativa alla manutenzione ed all'evoluzione della piattaforma di sicurezza McAfee, da diversi anni utilizzata dall'Istituto e già oggetto di precedenti analoghe iniziative.

Questo documento ha lo scopo di definire le caratteristiche e i requisiti relativi alla fornitura, da intendersi quali requisiti minimi della fornitura stessa.

Ai fini del presente documento, i termini di cui appresso devono essere intesi come segue:

- INAIL o Istituto: l'Istituto Nazionale per l'Assicurazione contro gli Infortuni sul Lavoro (INAIL o anche I.N.A.I.L), che usufruisce dei servizi e dei prodotti oggetto dell'iniziativa;
- Società o Impresa: la Società/R.T.I. fornitrice, aggiudicataria dell'Appalto Specifico;
- Contratto: il contratto che verrà stipulato tra INAIL e l'Impresa, recante le clausole che disciplineranno i rapporti giuridici tra le parti nell'esecuzione dei Servizi;
- Servizi: il complesso dei servizi e delle attività oggetto dell'iniziativa;
- Malfunzionamento: qualsiasi anomalia funzionale e ogni difformità di quanto acquisito rispetto alla relativa documentazione tecnica e manualistica d'uso o alle specifiche del presente Capitolato Tecnico;
- Responsabile delle attività contrattuali o Responsabile del Servizio: la persona individuata dalla Società come interlocutore dell'Istituto e responsabile di tutte le attività contrattuali;
- Piattaforma: la Piattaforma software McAfee utilizzata per l'erogazione dei Servizi;
- RUP/DEC: il Responsabile Unico del Procedimento ed il Direttore dell'Esecuzione del Contratto che hanno ruoli e funzioni definiti all'art. 31 del D.lgs. 50/2016.

2 IL CONTESTO TECNOLOGICO E GLI OBIETTIVI

2.1 Contesto tecnologico

Il sistema informativo dell'INAIL è, in estrema sintesi, costituito dai seguenti componenti:

- sistemi di elaborazione centrali grandi (mainframe e open) e intermedi (open) siti presso i Data Center della Direzione Centrale Organizzazione Digitale (DCOD);
- sistemi di elaborazione medi siti presso il CED del Centro Protesi di Vigorso di Budrio;
- sistemi di elaborazione periferici medi siti presso le Sedi territoriali;
- postazioni di lavoro (PC e stampanti) ad uso del personale, postazioni di servizio, personal computer portatili;
- Web Server Farm, sita presso i Data Center della DCOD, per la gestione dei servizi di interoperabilità, dei servizi web e di cooperazione applicativa. E' costituita da sistemi in alta affidabilità ridondati per gli ambienti di sviluppo, test e produzione;
- rete geografica SPC (Sistema Pubblico di Connettività) che interconnette le sedi INAIL tra loro (contesto Intranet), con le altre Pubbliche Amministrazioni (contesto Infranet) e verso la rete pubblica (contesto Internet);
- reti locali (LAN) presso le Sedi Locali, le Direzioni Regionali e le Direzioni Centrali (ivi compresi il Centro Protesi di Vigorso di Budrio e il CRM di Volterra);
- rete fonia VoiP (Voice over IP), apparecchi di telefonia mobile assegnati, prevalentemente, a dirigenti, professionisti e personale direttivo e ispettivo;
- diverse tipologie di software di base.

L'INAIL ha recentemente avviato il progetto "Data Center Transformation", innescando un percorso di trasformazione e rinnovamento complessivo dal punto di vista tecnologico, impiantistico, gestionale e organizzativo. Il progetto ha una durata pluriennale e, alla sua conclusione, doterà l'Istituto di due Data Center di tier 3+ (come definito da TEIA-942 e Uptime Institute).

Uno dei pilastri fondamentali del progetto è la virtualizzazione dei server grazie alla quale sono stati ridotti in tempo reale consumi e costi di gestione, aumentando efficienza, affidabilità e disponibilità della potenza di calcolo, consolidando l'infrastruttura di Storage e Backup e riducendo allo stesso tempo il footprint dei Data Center dell'istituto.

Sono state unificate SAN e LAN, semplificando la connettività, con un utilizzo pressoché totale di fibre in sostituzione delle connessioni più vecchie e meno funzionali in rame.

I server sono stati raggruppati in POD (Pool Of Devices) omogenei composti da più rack, che sono stati soggetti a una lineare standardizzazione e si configurano come la struttura base da replicare in caso di espansione.

I singoli server sono stati tutti attualizzati, portati allo stadio tecnologico di ultima generazione e, in futuro, saranno gestiti e sostituiti, come il resto dell'infrastruttura, secondo i cicli di vita previsti dai produttori, in modo da evitare i pericoli dell'obsolescenza che inducono oneri di gestione e limitano le possibilità evolutive e l'efficienza dell'Organizzazione.

2.2 La piattaforma di sicurezza McAfee

La piattaforma di sicurezza McAfee è utilizzata dall'Istituto da diversi anni ed è stata oggetto di numerose evoluzioni. Attraverso la precedente fornitura, che ha portato alla stipula del contratto attualmente in essere ed in scadenza a gennaio 2019, INAIL ha provveduto a realizzare le attività di adeguamento tecnologico ed ampliamento delle soluzioni McAfee in esercizio, mantenendo alto il livello di sicurezza dell'infrastruttura ICT e delle informazioni attraverso:

- la migrazione di tutti gli endpoint gestiti alla suite CEE (Complete Endpoint Protection Advanced) per assicurare una migliore protezione anti virus e anti intrusione a bordo dei sistemi;
- la distribuzione sugli endpoint gestiti della suite CDP (Complete Data Protection), per avere la possibilità di cifrare e mettere in sicurezza i dati di tutti gli utenti;
- la distribuzione sugli endpoint gestiti del modulo TIE (Threat Intelligence Exchange) al fine di rilevare e reagire immediatamente alle minacce denominate "zero-day", rendendo operative le informazioni relative ad un nuovo file compromesso e non ancora noto come malevolo su tutte le altre soluzioni di sicurezza McAfee, grazie alla combinazione tra le informazioni sui vettori di infezioni a livello mondiale e quelle acquisite a livello locale, riducendo il ritardo fra individuazione e contenimento;
- la copertura dei sistemi gestiti tramite la distribuzione della suite Server Security Advanced (DTS, Data Center Suite) a protezione degli host fisici e virtuali, Windows e Linux, server e client, indipendentemente dalla natura delle piattaforme e dei sistemi operativi in uso nei Data Center;
- la creazione e la messa in esercizio di un canale condiviso di comunicazione basato su protocollo Open DXL (Data Exchange Layer), messo a disposizione gratuitamente da McAfee, per condividere gli eventi di sicurezza tra le piattaforme McAfee e con soluzioni di sicurezza di terze parti che implementino il protocollo Open DXL;
- il completamento della copertura in monitoraggio attivo anti intrusione su entrambi i Data Center di INAIL di tutti i segmenti di Rete istituzionale di esercizio e la protezione delle infrastrutture dedicate a ISI (Click-Day) tramite la soluzione IPS Network Security Platform;

- l'introduzione dell'Advanced Threat Defense (ATD), attualmente in produzione, attivo e ridondato su entrambe i Data Center di INAIL, per l'analisi dinamica e comportamentale in ambiente protetto (SandBox) di file potenzialmente malevoli non ancora categorizzati come pericolosi;

- la sostituzione del Risk Advisor con l'Event Reporter (Enterprise Security Manager, ESM), attualmente in produzione, attivo e ridondato su entrambe i Data Center di INAIL, un concentratore dedicato in primis alle soluzioni di sicurezza McAfee, ma integrabile con soluzioni di sicurezza di terze parti, atto alla correlazione intelligente e azionabile di eventi di sicurezza provenienti da sorgenti e apparati eterogenei;

- il consolidamento del sistema di controllo anti malware, dei contenuti WEB e URL Filtering, mediante adeguamento della soluzione Web Gateway, attualmente in produzione, attiva e ridondata su entrambe i Data Center di INAIL;

- il completamento dell'architettura Vulnerability Manager, attualmente in produzione, attiva e ridondata su entrambe i Data Center di INAIL, per la gestione delle vulnerabilità informatiche e dell'analisi del rischio tecnologico correlato alla rilevanza della vulnerabilità e alla valenza degli Asset istituzionali.

Tutte le attività operative e le politiche inerenti alle soluzioni citate, oltre ad essere governate da un unico punto di raccordo, ovvero la singola console della piattaforma di gestione unificata epo (ePolicy Orchestrator Server), si interfacciano in tempo reale con i feed del Global Threat Intelligence di McAfee, che sfrutta l'attività di milioni di sensori in tutto il mondo e le ricerche di un ampio gruppo di analisti dei McAfee Labs, rendendo disponibili le informazioni sulle minacce. Questo servizio, basato sul cloud e sempre attivo, rende possibile una protezione accurata contro le minacce note e in rapida emersione, grazie a dei parametri che tengono conto della diffusione e della reputazione di una minaccia.

2.3 Obiettivi perseguiti attraverso l'evoluzione della piattaforma

Gli obiettivi perseguiti da INAIL attraverso il consolidamento e l'ottimizzazione della piattaforma possono essere così riassunti:

- Garanzia di un maggiore livello di sicurezza dei propri sistemi informatici e dei dati gestiti a fronte di rischi di danneggiamenti causati da virus o da attacchi esterni;

- Protezione in tempo reale dalle minacce informatiche, su ogni vettore (file, web, e-mail, rete), per tutti i dispositivi, server e macchine virtuali fino a PC e dispositivi mobili;

- Protezione immediata in presenza di nuovi attacchi scoperti a livello globale;

- Prevenzione delle minacce informatiche, attraverso lo scambio e l'utilizzo collettivo delle informazioni ad esse associate fra tutti gli strumenti di sicurezza, al fine di ridurre il più possibile il ritardo fra l'individuazione ed il contenimento delle stesse;

- Garanzia dell'integrità dei dati, protezione del patrimonio applicativo, prevenzione dalla eventuale perdita di dati, protezione della riservatezza dei dati;
- Contrasto e rimedio alle vulnerabilità;
- Gestione del rischio e delle vulnerabilità;
- Gestione unificata e semplificata di tutti gli strumenti di prevenzione e protezione.

Il rinnovo, consolidamento ed ottimizzazione dell'infrastruttura di sicurezza, si basano sui componenti McAfee descritti nelle pagine seguenti.

3 DEFINIZIONE DELLA FORNITURA

3.1 Oggetto

La fornitura prevede le seguenti componenti:

- **Fornitura Base**
    - Rinnovo della manutenzione e upgrade tecnologico dei prodotti software in licenza d'uso perpetua e delle apparecchiature hardware (appliance) già in possesso dell'Istituto;
    - Servizio di supporto sistemistico on site McAfee Platinum Enterprise
    - Servizio di addestramento per il personale INAIL
    - Servizi professionali di supporto specialistico (a consumo)
- **Fornitura Opzionale**
    - Nuovi prodotti software in licenza d'uso perpetua e nuove apparecchiature hardware (appliance), con relativi servizi di manutenzione e supporto connessi.

3.2 Durata

Il contratto avrà durata pari a 36 mesi decorrenti dalla data di accettazione della fornitura. Nell'ambito della durata contrattuale, al Fornitore potranno essere richiesti i servizi professionali a consumo.

3.3 Responsabile del Servizio

Entro cinque giorni dalla stipula del contratto, la Società aggiudicataria dovrà comunicare a INAIL il nominativo del proprio rappresentante designato quale Responsabile del Servizio.

Il Responsabile del Servizio sarà l'interlocutore unico dell'Istituto per gli aspetti amministrativi, l'organizzazione ed il coordinamento delle attività contrattuali.

Sarà cura del responsabile verificare il rispetto di tutti gli adempimenti contrattuali, curando in particolare il rispetto dei tempi e delle modalità di consegna della documentazione e dei prodotti.

Per facilitare e velocizzare l'attività amministrativa di entrambe le parti, ogni comunicazione riguardante aspetti contrattuali dovrà essere scambiata tra il responsabile INAIL e quello della Società aggiudicataria.

3.4 Luogo di lavoro

L'aggiudicatario dovrà eseguire le prestazioni contrattuali presso le sedi INAIL individuate dall'Istituto, localizzate a Roma.

4 DEFINIZIONE DEI BENI E DEI SERVIZI OGGETTO DELLA FORNITURA

Nel presente paragrafo sono elencati i beni ed i servizi oggetto della fornitura.

4.1 Upgrade tecnologico dei prodotti installati e relativa manutenzione

E' richiesto l'upgrade tecnologico e la manutenzione delle seguenti componenti infrastrutturali, come meglio dettagliato nel Capitolato Tecnico parte I, generato dal Sistema.

- Up-grade EDR Endpoint Threat defense and response
  - EDRCDE-AT MFE EP Threat Def and Resp 15.000 Licenza e man. 1 anno
  - EDRYFM-AT MFE EP Threat Def and Resp 15.000 Manutenzione 2 anni
- Up-grade Secure Content Management
  - WBG-5500-D MFE Web Gateway 5500 Appl-D 8 Appliance
  - WBG5500DNBD MFE Web Gateway 5500 Appl-D 8 Manutenzione 3 anni
  - MAP-10G4-FBRD MFE 10GB Fbr PCIe Card - D Model 8 Appliance
  - RB10G4FBRD MFE 10GB Fbr PCIe Card - D Model 8 Manutenzione 3 anni
- Up-grade Intrushield (Network Security Platform)
  - NSM-MAPL-NG MFE Network Security Manager Appl NG 2 Appliance
  - NYVMAPLNGARMA MFE Net Sec Mngr Appl NG 1Yr ARMA 2 Manutenzione 3 anni
  - NMGECE-AA MFE Net Sec Mngr Global SW 1:1 BZ Sub 1 **Sottoscrizione 3 anni**
  - IPS-NS9300 MFE Net Sec IPS-NS9300 Appliance 2 Appliance
  - IPSNS9300NBD MFE Net Sec IPS-NS9300 Appliance 2 Manutenzione 3 anni
  - IAC-1600AC-PS MFE Net Sec 1600W AC PSU 2 Appliance
  - RBIAC1600ACPS MFE Net Sec 1600W AC PSU 2 Manutenzione 3 anni
  - IAC-4P1GMM62-MOD NS 4pt FO Mod 10-1GigE 850nm 62.5um 8 Appliance
  - RBIAC4P1GMM62MOD NS 4pt FO Mod 10-1GigE 850nm 625um 8 Manutenzione 3 anni
  - IAC-AFOCH-KT2 Active FailOpen Chassis 4 Appliance
  - RBAFOCHKT2 Active FailOpen Chassis 4 Manutenzione 3 anni
  - VC3CAE-AB MFE vNSP Cloud Large (1Gbps) Perp Lic 10 Licenza d'uso
  - VC3YCM-AB MFE vNSP Cloud Large (1Gbps) 10 Manutenzione 3 anni
- Up-Grade ESM Enterprise Security Manager
  - ETM-X11 MFE Ent Sec Mgr X11 Appliance 2 Appliance
  - ETMX11NBD MFE Ent Sec Mgr X11 2 Manutenzione 3 anni
  - ELM-6050 MFE Ent Log Mgr 6050 Appliance 2 Appliance
  - ELM6050NBD MFE Ent Log Mgr 6050 2 Manutenzione 3 anni
  - ERC-4700 MFE Event Receiver 4700 Appliance 8 Appliance
  - ERC4700NBD MFE Event Receiver 4700 8 Manutenzione 3 anni
  - ACE-4700 MFE Adv Corr Eng 4700 Appliance 2 Appliance
  - ACE4700NBD MFE Adv Corr Eng 4700 2 Manutenzione 3 anni
  - APM-3500 MFE App Data Mon 3500 Appliance 2 Appliance
  - APM3500NBD MFE App Data Mon 3500 2 Manutenzione 3 anni
  - DAS-100 MFE Dir Attached Storage 100 4 Appliance
  - RBDAS100ARMA MFE Dir Attached Storage 100 4 Manutenzione 3 anni
  - ELSVME-AA MFE ELS VM 8 Cores 2 Licenza
  - ELSVYE-AA MFE ELS VM 8 Cores 2 Manutenzione 3 anni
  - ELS4AE-AA MFE ELS VM 4 Cores Add-On 6 Licenza
  - ELS4YE-AA MFE ELS VM 4 Cores Add-On 6 Manutenzione 3 anni
  - GTEETMX11GIEAD MFE GTI for ETM-X11 2 **Sottoscrizione 3 anni**
- Up-Grade ATD Advance Threat Defense
  - ATD-6100 MFE Adv Threat Def 6100 Standard HW 6 Appliance
  - ATD6100GLNBD MFE Adv Threat Def 6100 Standard HW 6 Manutenzione 3 anni

4.2 Rinnovo della manutenzione dei prodotti installati

E' richiesto il rinnovo della manutenzione delle seguenti componenti infrastrutturali, come meglio dettagliato nel Capitolato Tecnico parte I, generato dal Sistema.

- Rinnovo Client Server Data Protection Suite
  - CTPYFM-AA MFE Complete EP Threat Protection 15.000 Manutenzione 3 anni
  - CDAYFM-AA MFE CompleteDataPrtxn Adv 15.000 Manutenzione 3 anni
  - CWAYFM-AB MFE Cloud Workload Sec Adv 2.000 Manutenzione 3 anni
  - MOVYFM-AA MFE MOVE AV for Virtual Dsktops 500 Manutenzione 3 anni
  - PSMYFM-AA MFE Sec for MS SharePoint 15.000 Manutenzione 3 anni
- Rinnovo Secure Content Management
  - WPSECE-AA MFE Web Protection Suite 12.500 Manutenzione 3 anni
  - RFCH1PM72 MFE MCS-CH1P-M72 M7 2 **Manut. 29 mesi**
  - RFBLDE1XH MFE MCS-BLDE-1XXHW 32 **Manut. 29 mesi**
- Rinnovo Intrushield (Network Security Platform)
  - RB10AFO85 Opt (850nm) 10 Gigabit AFO 38 **Manut. 17 mesi**
  - RB62F1KT7 Opt 62.5 Gigabit AFO 16 **Manut. 17 mesi**
  - IPSNS9300NBD MFE Net Sec IPS-NS9300 Appl 2 Manutenzione 3 anni
  - RBIAC8P10NETMOD MFE Net Sec 8port I/O Mod 10/1GigE 12 Manutenzione 3 anni
  - IPSNS9300NBD MFE Net Sec IPS-NS9300 Appl 2 Manutenzione 3 anni
  - RBIAC1600ACPS MFE Net Sec 1600W AC PSU 2 Manutenzione 3 anni
  - RBIAC4P1GMM62MOD NS 4pt FO Mod 10-1GigE 850nm 625um 8 Manutenzione 3 anni
- Rinnovo ESM Enterprise Security Manager
  - ETM6000ELMARMA MFE EntSecMgr,EL EvtRec 6000 2 Manutenzione 3 anni
- Rinnovo ATD Advance Threat Defense
  - ATD6000ADM MFE Adv Threat Def 6000 Standard HW 2 Manutenzione 3 anni

4.3 Servizio di supporto sistemistico on site McAfee Platinum Enterprise

E' richiesto, per tutta la durata della fornitura, il servizio di supporto sistemistico on site McAfee Platinum Enterprise, composto dai seguenti elementi:

- PRSYDM-AT Resident SAM Enterprise Support 1 Supporto sist. 3 anni
- PSAYDM-AT Assigned Product Specialist 1 Supporto sist. 3 anni

4.4 Servizio di sviluppo Custom Parser per ESM

E' richiesto lo sviluppo e la personalizzazione dei seguenti Custom Parser:

- ESM-CUSTOM-PARSER MFE ESM Custom Parser Developmnt 3 Sviluppo a corpo

4.5 Servizio di addestramento

E' richiesta l'erogazione delle seguenti sessioni di addestramento all'utilizzo delle tecnologie McAfee per il personale INAIL:

- TRN-SITE3-Z1 Solution Svcs Onsite 3 Day 2 Education
- TRN-SITE4-Z1 Solution Svcs Onsite 4 Day 3 Education

4.6 Servizi professionali di supporto specialistico (a consumo)

Sono richiesti i seguenti servizi di supporto specialistico, da erogare a consumo:

•	MD-SA-SECC-Z1 Security Architect - Senior Consulant	347	Consulenza
•	MD-CONSULT-DY-Z1 Security Consultant Product Specialist	617	Consulenza

4.7 Nuovi prodotti software in sottoscrizione o in licenza d'uso perpetua e nuove apparecchiature hardware (appliance), con relativi servizi di manutenzione e supporto connessi (in opzione)

Sono richieste in opzione le seguenti componenti infrastrutturali ed i relativi servizi di manutenzione e supporto connessi, come dettagliato nel Capitolato Tecnico parte I, generato dal Sistema.

•	ESM Enterprise Security Manager			
	o	MBAECE-AA	MFE Behavioral Analytics	1	Sottoscrizione 1 anno
•	CLOUD Protection (Skyhigh)			
	o	C13ECE-AA	MFE Skyhigh SwIT O365 MailShp1Drv	15.000	Sottoscrizione **3 anni**
	o	C28ECE-AA	MFE Skyhigh Custom Apps Other	15.000	Sottoscrizione **3 anni**
	o	C22ECE-AA	MFE Skyhigh Azure	1	Sottoscrizione 1 anno
	o	C02ECE-AA	MFE Skyhigh ShadowIT	1	Sottoscrizione 1 anno
	o	C03ECE-AA	MFE Skyhigh SalesCloud	1	Sottoscrizione 1 anno
	o	C04ECE-AA	MFE Skyhigh SalesCloud Encr	1	Sottoscrizione 1 anno
	o	C05ECE-AA	MFE Skyhigh ServiceCloud	1	Sottoscrizione 1 anno
	o	C06ECE-AA	MFE Skyhigh ServiceCloud Encr	1	Sottoscrizione 1 anno
	o	C07ECE-AA	MFE Skyhigh ServiceNow	1	Sottoscrizione 1 anno
	o	C08ECE-AA	MFE Skyhigh ServiceNow Encr	1	Sottoscrizione 1 anno
	o	C09ECE-AA	MFE Skyhigh O365 Mail	1	Sottoscrizione 1 anno
	o	C10ECE-AA	MFE Skyhigh O365 Shrpoint1Drv	1	Sottoscrizione 1 anno
	o	C11ECE-AA	MFE Skyhigh O365 Shrpt1Drv Malw	1	Sottoscrizione 1 anno
	o	C12ECE-AA	MFE Skyhigh O365 MailShrpt1Drv	1	Sottoscrizione 1 anno
	o	C14ECE-AA	MFE Skyhigh Box	1	Sottoscrizione 1 anno
	o	C15ECE-AA	MFE Skyhigh Box malware	1	Sottoscrizione 1 anno
	o	C16ECE-AA	MFE Skyhigh Dropbox	1	Sottoscrizione 1 anno
	o	C17ECE-AA	MFE Skyhigh SLACK	1	Sottoscrizione 1 anno
	o	C18ECE-AA	MFE Skyhigh Google Drive	1	Sottoscrizione 1 anno
	o	C29ECE-AA	MFE Skyhigh Google Mail	1	Sottoscrizione 1 anno
	o	C19ECE-AA	MFE Skyhigh CustomApps CiscoSpark	1	Sottoscrizione 1 anno
	o	C23ECE-AA	MFE Skyhigh Custom Apps CTERA	1	Sottoscrizione 1 anno
	o	C24ECE-AA	MFE Skyhigh Custom Apps Egynte	1	Sottoscrizione 1 anno
	o	C25ECE-AA	MFE Skyhigh CustomApps Facebook	1	Sottoscrizione 1 anno
	o	C26ECE-AA	MFE Skyhigh Custom Apps GitHub	1	Sottoscrizione 1 anno
	o	C27ECE-AA	MFE Skyhigh Custom Apps Jive	1	Sottoscrizione 1 anno
	o	C20ECE-AA	MFE Skyhigh AWS	1	Sottoscrizione 1 anno
	o	C21ECE-AA	MFE Skyhigh AWS DLP	1	Sottoscrizione 1 anno
	o	T01YCM-AA	MFE Skyhigh TEC ACT MNG	1	**Supporto Business 1**
	o	T02YCM-AA	MFE Skyhigh TEC ACT MNG ENT	1	**Supporto Enterprise 1**
•	Intrushield (Network Security Platform)			
	o	IAC-4P40NET-MOD	MFE Net Sec 40GigE 4 port Net Mod	1	Appliance
	o	RBIAC4P40NETMOD	MFE Net Sec 40GigE 4 port Net Mod	1	Manutenzione 1 anno
	o	IAC-2P40NET-MOD	MFE Net Sec 2port I/O Mod 40GigE	1	Appliance
	o	RBIAC2P40NETMOD	MFE Net Sec 2port I/O Mod 40GigE	1	Manutenzione 1 anno
	o	IAC-QSFP-FOT	MFE Net Sec QSFP+ 40G Fiber Trans	1	Appliance

- RBIACQSFPFOT MFE Net Sec QSFP+ 40G Fiber Trans 1 Manutenzione 1 anno
- IAC-AFOCH40-KT2 Active FailOpen 40G Chassis 1 Appliance
- RBAFOCH40KT2 Active FailOpen 40G Chassis 1 Manutenzione 1 anno
- IAC-2P40FOSR4-KIT MFE Net Sec 40GE 2prt SR4 AFO Kit 1 Appliance
- RBIAC2P40SR4FOKIT MFE Net Sec 40GE 2prt SR4 AFO 1 Manutenzione 1 anno
- IAC-2P40FOBD-KIT MFE Net Sec 40GE 2prt BiDi AFO Kit 1 Appliance
- RB2P40FOBDKIT MFE Net Sec 40GE 2prt BiDi AFO Kit 1 Manutenzione 1 anno
- IAC-2P40FO-KIT MFE Net Sec 40GigE 2port AFO Kit 1 Appliance
- RBIAC2P40FOKIT MFE Net Sec 40GigE 2port AFO Kit 1 Manutenzione 1 anno
- VC3ECE-AB MFE vNSP Cloud Large (1Gbps) 1:1 BZ 1 Sottoscrizione 1 anno
- AT1ECE-AB MFE Adv Threat ATD-VM1008 1:1 BZ 1 Sottoscrizione 1 anno

- DLP Network
  - DLP-6600-A MFE DLP 6600A 1 Appliance
  - DLP6600ANBD MFE DLP 6600A Appl. 1 Manutenzione 1 anno
  - DMOCKE-AA MFE DLP Monitor SW 1 Licenza e man. 1 anno
  - DMOYCM-AA MFE DLP Monitor SW 1 Manutenzione 1 anno
  - DPVCKE-AA MFE DLP Prevent 1 Licenza e man. 1 anno
  - DPVYCM-AA MFE DLP Prevent 1 Manutenzione 1 anno
  - DDSCKE-AA MFE DLP Discover SW 1 Licenza e man. 1 anno
  - DDSYCM-AA MFE DLP Discover 1 Manutenzione 1 anno

5 MODALITÀ DI ESECUZIONE DELLA FORNITURA

Nel seguito sono descritte in dettaglio le modalità di esecuzione dei Servizi oggetto della presente fornitura.

5.1 Manutenzione dei prodotti software e delle apparecchiature hardware

Per tutta la durata della fornitura l'Impresa dovrà garantire:

- servizi di supporto e manutenzione per ciascuna delle licenze perpetue e delle apparecchiature hardware già in possesso dell'Amministrazione;
- servizi di supporto e manutenzione per ciascuna delle licenze perpetue acquisite nel corso della fornitura, a partire dal termine del previsto periodo di garanzia;
- servizi di supporto e manutenzione per ciascuno dei prodotti software in sottoscrizione e delle apparecchiature hardware acquisite nel corso della fornitura, a partire dalla data di accettazione della fornitura stessa.

Il servizio di supporto e manutenzione in garanzia, relativo alle licenze d'uso perpetue di nuova acquisizione, sarà della durata di 12 mesi decorrenti dalla data di accettazione della fornitura e dovrà essere erogato a propria cura e spese e senza alcun onere aggiuntivo per l'Istituto, intendendosi ricompreso nel corrispettivo per l'acquisto delle licenze. Il servizio di supporto e manutenzione deve essere erogato in modalità "on-site", su chiamata, dal lunedì al venerdì, escluso i festivi, dalle ore 8:00 alle ore 18:00.

La manutenzione comprende ogni prestazione necessaria all'eliminazione dei malfunzionamenti. Si precisa che per malfunzionamento si intende qualsiasi anomalia funzionale che, direttamente o indirettamente, provochi l'interruzione o la non completa disponibilità del servizio all'utenza e, in ogni caso, ogni difformità dei prodotti in esecuzione dalla relativa documentazione tecnica e manualistica d'uso.

Relativamente al software, il servizio di manutenzione comprende, a titolo esemplificativo e non esaustivo:

- invio delle migliorie (correzioni, aggiornamenti e miglioramenti) dei Prodotti e relativa documentazione;
- invio delle riparazioni e aggiornamenti che l'Impresa mette a disposizione dei propri clienti;
- consegna di ogni update dei prodotti, dove per update si intende sia nuove release che nuove versioni dei prodotti. L'Istituto avrà facoltà di utilizzare le nuove versioni e/o di continuare ad usare le precedenti.

L'Istituto comunicherà all'Impresa i malfunzionamenti per telefono, per e-mail o via web. In caso di comunicazione per telefono, si precisa che i termini per l'eliminazione dei malfunzionamenti decorrono dalla conferma per e-mail o via web. L'Impresa confermerà la presa in carico del problema via e-mail.

Per i prodotti software, in presenza di errori bloccanti anche dovuti al rilascio di aggiornamenti che provochino disservizio alle apparecchiature dell'Istituto, il blocco deve essere rimosso ed il servizio ripristinato entro 4 ore lavorative dalla presa in carico, formalizzata secondo le modalità sopra descritte. In presenza di errori non bloccanti

sui prodotti software, l'Impresa dovrà ripristinare il servizio entro 24 ore lavorative dalla presa in carico, formalizzata secondo le modalità sopra descritte.

Per le apparecchiature hardware ritenute critiche per il buon funzionamento del sistema informativo dell'Istituto, si richiedono tempi di intervento e di ripristino entro le 6 ore lavorative successive alla presa in carico, formalizzata secondo le modalità sopra descritte.

Ai fini del rispetto dei precedenti termini è ammessa anche una fix temporanea, una circumvention o un bypass, purché seguito dalla correzione definitiva del malfunzionamento.

Le parti di ricambio hardware - che dovranno essere preferibilmente identiche o comunque equipollenti alle parti sostituite, purché con caratteristiche e funzionalità identiche o migliorative rispetto alla parti sostituite verranno fornite dalla Impresa senza alcun onere aggiuntivo per l'Istituto; le parti sostituite verranno ritirate dall'Impresa stessa che ne riacquisirà pertanto la proprietà. Le parti fornite - salvo diverso accordo - dovranno essere nuove, restando l'Impresa impegnata a quanto previsto contrattualmente in termini di garanzia.

L'Impresa potrà apportare le modifiche e i miglioramenti tecnici ritenuti opportuni al fine di elevare il grado di affidabilità delle apparecchiature e/o di semplificare la manutenzione provvedendo a proprie spese alle relative installazioni.

Ove l'eliminazione del malfunzionamento e/o del fermo richieda un tempo superiore a quello stabilito o comporti il trasferimento delle apparecchiature in luogo diverso dai locali dell'Istituto, l'Impresa dovrà provvedere alla sostituzione delle apparecchiature stesse con altre aventi le medesime caratteristiche tecniche e funzionali, sino al momento del ripristino definitivo o della sostituzione delle apparecchiature. L'Impresa dovrà adoperarsi, per quanto possibile, al recupero degli archivi presenti sulle apparecchiature da sostituire. Il ritiro delle apparecchiature da sostituire e di quelle fornite in loro sostituzione, nonché la consegna delle apparecchiature in sostituzione e di quelle ripristinate dovranno essere effettuati a cura e spese dell'Impresa con le modalità e nei termini che verranno concordati con l'Istituto.

Per ogni intervento di manutenzione dovrà essere redatta da un incaricato dell'Istituto e da un incaricato della Impresa una apposita nota di ripristino, in formato cartaceo od elettronico, nella quale dovranno essere registrati l'ora della chiamata e quella dell'avvenuto ripristino, nonché le prestazioni effettuate.

5.2 Servizio di Supporto Sistemistico on site McAfee Platinum Enterprise

Il servizio di supporto McAfee Platinum Enterprise, che l'Istituto ha già adottato in passato e che è richiesto per tutta la durata della fornitura, è disponibile H24 e prevede un Support Account Manager (SAM), presente negli orari di lavoro presso l'Istituto, nonché la disponibilità di diversi Specialisti di Prodotto, ognuno dedicato ad una specifica linea di prodotti McAfee, sempre contattabili telefonicamente e via email. In particolare sono richiesti:

Codice McAfee	Descrizione	Quantità
PRSYDM-AT	Resident SAM Enterprise Support 1 Yr	1
PSAYDM-AT	Assigned Product Specialist 1 Yr	1

Il servizio rappresenta un valore aggiunto in relazione a molteplici aspetti, tra cui un unico e fidelizzato punto di contatto per la gestione delle Richieste di Supporto, un costante monitoraggio della postura di sicurezza dell'Istituto attraverso il controllo e la consulenza sull'efficiente utilizzo dei prodotti e delle soluzioni in esercizio, l'allerta sulle più recenti vulnerabilità e frodi telematiche correlate con lo stato di protezione dei sistemi istituzionali più rilevanti, la linea diretta con i laboratori McAfee in caso di eventi di sicurezza particolarmente importanti e la costante disponibilità di una Squadra di tecnici altamente specializzati che possono fornire assistenza immediata su tematiche di Sicurezza Informatica, siano esse inerenti a nuove tecnologie, a comparazioni di soluzioni diverse che rispondano alle esigenze dell'Istituto o a presentazioni e formazione sui prodotti McAfee in collaudo ed esercizio.

Si precisa che per l'erogazione del Servizio devono essere utilizzate esclusivamente risorse del produttore McAfee.

5.3 Servizio di sviluppo Custom Parser per ESM

Al fine di garantire la connettività e la ricezione dei log di tutti i device presenti presso l'Istituto verso la soluzione ESM, è richiesta la predisposizione di parser personalizzati. In particolare i parser previsti sono i seguenti:

Codice McAfee	Descrizione	Device previsto	Quantità
ESM-CUSTOM-PARSER	MFE ESM Custom Parser Developmnt-Prepaid	DNS Firewall - INETSIM (nuova fonte del SOC)	**1**
ESM-CUSTOM-PARSER	MFE ESM Custom Parser Developmnt-Prepaid	CA API Gateway	**1**
ESM-CUSTOM-PARSER	MFE ESM Custom Parser Developmnt-Prepaid	EWC Controller (Servizio Captive)	**1**

La fornitura dei parser sopra indicati deve essere comprensiva di agent per l'interfacciamento con il Mainframe, in modo che sia possibile inviare i log del Mainframe alla soluzione ESM. **I parser dovranno essere resi disponibili entro sei mesi dalla data di stipula del contratto**.

5.4 Servizio di addestramento

La fornitura prevede l'erogazione di 5 sessioni di addestramento all'utilizzo di specifiche tecnologie McAfee per il personale INAIL, al fine di garantire un aggiornamento delle competenze al personale dell'Istituto. In particolare sono richiesti i seguenti corsi ufficiali McAfee in aula, per un massimo di 6 persone a corso:

Corso Ufficiale McAfee	Giorni	Codice McAfee	Quantità
Corso di aggiornamento Complete Endpoint Threat Protection Suite (CTP)	4	TRN-SITE4-Z1	1
Corso di aggiornamento Advanced Threat Defense (ATD)	3	TRN-SITE3-Z1	1
Corso di aggiornamento Network IPS (NSP)	4	TRN-SITE4-Z1	1
Corso di aggiornamento Web gateway	3	TRN-SITE3-Z1	1
Corso di aggiornamento ESM	4	TRN-SITE4-Z1	1

Dovrà essere rilasciata documentazione ufficiale McAfee del corso per ogni partecipante.

L'Istituto si riserva di richiedere in tutto o in parte l'erogazione delle sessioni di addestramento previste, sulla base delle esigenze che emergeranno in corso di vigenza contrattuale.

L'Istituto richiederà all'Impresa l'erogazione delle suddette sessioni mediante apposita comunicazione scritta contenente l'indicazione delle sessioni richieste e la data o il periodo in cui richiede che tali sessioni vengano erogate.

L'Impresa entro 5 giorni lavorativi dall'invio della richiesta dell'Istituto dovrà fornire un Piano operativo comprendente le date in cui propone l'erogazione delle sessioni richieste. Il Piano operativo sarà sottoposto ad approvazione da parte dell'Istituto. In caso di mancata approvazione, l'Istituto comunicherà all'Impresa i motivi del dissenso che l'Impresa recepirà aggiornando il Piano e consegnandolo all'Istituto entro 5 giorni lavorativi.

Le sessioni di addestramento dovranno essere tenute dall'Impresa dal lunedì al venerdì, escluso i festivi, all'interno dell'orario 9:00-18:00, e potranno svolgersi su richiesta dell'Amministrazione presso la Direzione Centrale per l'Organizzazione Digitale – Via Santuario Regina degli Apostoli, 33 00145 Roma - ovvero presso una sede messa a disposizione dell'Impresa ma comunque ubicata in Roma.

5.5 Servizi Professionali di supporto specialistico

L'obiettivo principale della consulenza specialistica McAfee è quello di ottenere il massimo dei benefici dalle soluzioni già implementate e ancora da implementare presso l'Istituto. I servizi vengono utilizzati sia per consolidare, ottimizzare ed aggiornare le soluzioni in produzione che per integrare al meglio nell'ambiente nuove soluzioni.

La seguente tabella descrive i profili delle due figure professionali richieste.

Security Senior Consultant (SSC) - Codice McAfee MD-SA-SECC-Z1
Ricopre il ruolo di interfaccia di alto livello con il cliente, soprattutto in relazione alla gestione dei diversi team che lavorano in parallelo sul cliente. Ha la responsabilità di coordinare ed integrare le informazioni delle singole pianificazioni dei progetti, stabilire le priorità in accordo col cliente e definire le macro-schedulazioni con i Project Leader, a vantaggio delle sinergie ed evitando sovrapposizioni di uso di risorse non condivisibili. Diventa il gestore delle Escalation e delle Change Request.
Security Consultant Product Specialist (SCPS) - Codice MacAfee MD-CONSULT-DY-Z1
Corrisponde alla figura tecnica del Senior Consultant sulla soluzione specifica. Il ruolo di Senior si acquisisce tramite la partecipazione a numerosi progetti di cui si è parte tecnica e in base alle certificazioni conseguite. Il suo ruolo consiste nel guidare le parti operative di implementazione, nell'interfacciarsi con la parte tecnica del cliente per la normale operatività e l'analisi dei requisiti tecnici e nel riportare al Project Leader il risultato delle fasi operative, oltre ad essere di supporto in tutte le fasi di approfondimento tecnico.

L'ambito di intervento della consulenza McAfee è riconducibile alle attività di Upgrade (aggiornamento e/o refresh tecnologico) delle seguenti componenti McAfee:

Componente	Funzione/Attività
Refresh tecnologico delle suite Complete Endpoint Threat Protection Suite - (CTP)	Sono le suite Endpoint necessarie alla messa in sicurezza delle postazioni di lavoro e dei server. Le attività prevedono l'aggiornamento e la migrazione delle suite alle ultime versioni disponibili.
Refresh tecnologico Secure Content Management	Il sistema Secure Content Management web gateway è la componente di sicurezza che protegge le postazioni di lavoro e i server dalle minacce durante la navigazione web. L'attività prevede l'aggiornamento della componente hardware e software in produzione alle ultime release disponibili.
Aggiornamento architettura Secure Content Management	Questa attività prevede l'aggiornamento della architettura di riferimento utilizzando delle appliance McAfee modello 5500.
Refresh tecnologico Intrushield Network Intrusion Prevention System	In questa fase saranno aggiornate le componenti hardware e software dell'architettura Network intrusion prevention esistente.
Aggiornamento architettura Intrushield Network IPS	L'attività prevede l'aggiornamento dell'architettura di riferimento Network IPS, implementata presso l'Istituto, per innalzare il livello di sicurezza.
Refresh tecnologico di ESM Enterprise Security Manager	L'attività prevede il refresh tecnologico della componente ESM, portando le componenti in produzione al livello software dell'ultima release disponibile.

Aggiornamento architettura ESM Enterprise Security Manager	L'attività prevede l'aggiornamento dell'architettura di riferimento della componente McAfee ESM per migliorare l'elaborazione complessiva degli eventi e per fornire una migliore visione di insieme.
Refresh tecnologico ATD Advanced Threat Defence	Il sistema di analisi delle nuove vulnerabilità non ancora scoperte, si basa su un sistema di sandboxes. Tale componente dialoga con i sistemi di network security ed end point già in produzione presso l'Istituto. L'attività prevede il refresh tecnologico delle componenti già in produzione presso l'Istituto.
Aggiornamento architettura delle componenti ATD Advanced Threat Defence	Sarà aggiornata l'architettura di riferimento per bilanciare meglio il carico di lavoro e innalzare il livello di sicurezza.

I servizi di supporto specialistico dovranno essere svolti presso la Direzione Centrale per l'Organizzazione Digitale- Via Santuario Regina degli Apostoli, 33 – 00145 - Roma dal lunedì al venerdì, esclusi i festivi, durante il normale orario lavorativo compreso dalle 8:00 alle 20:00.

L'Amministrazione si riserva di richiedere in tutto o in parte i giorni/persona previsti, sulla base delle esigenze che emergeranno in corso di vigenza contrattuale. L'Istituto richiederà all'Impresa l'erogazione dei servizi mediante apposita comunicazione scritta contenente le attività richieste ed il periodo in cui prevede che tale attività debbano essere effettuate.

L'Impresa, entro 5 giorni lavorativi dall'invio della richiesta dell'Istituto, dovrà fornire un **Piano operativo** contenente almeno:

- la descrizione dettagliata delle attività che verranno eseguite;
- la documentazione tecnica a supporto delle attività;
- la stima dell'impegno in giorni/persona previsto per l'esecuzione delle attività, suddiviso per le figure professionali previste nel presente Capitolato Tecnico;
- nominativi e curriculum vitae delle risorse che intende utilizzare;
- le date ovvero il periodo in cui le attività verranno eseguite;
- la necessità di supporto da parte dell'Amministrazione.

Il Piano operativo sarà sottoposto ad approvazione da parte dell'Istituto. In caso di mancata approvazione, l'Istituto comunicherà all'Impresa i motivi del dissenso che l'Impresa recepirà aggiornando il Piano e consegnandolo all'Istituto entro 5 giorni lavorativi. Una volta terminata l'attività descritta nel suddetto Piano, l'Istituto procederà alla Verifica di conformità secondo le modalità contrattualmente previste.

Per le attività di supporto specialistico è prevista una rendicontazione su base mensile. La rendicontazione dovrà avvenire tramite invio di un rapporto dettagliato di intervento, realizzato su modulo McAfee "Timesheet", a cura del responsabile del servizio. Per tutte le attività di supporto specialistico l'erogazione e la rendicontazione sono previste in giorni/persona.

Di seguito vengono illustrate brevemente le attività previste e viene fornita una stima di massima dell'impegno ipotizzato, sia per le attività di carattere generale che per ogni componente specifica.

Gestione attività e documentazione

In questa fase sarà realizzata l'analisi iniziale e la documentazione di riferimento architetturale per l'integrazione, l'aggiornamento e il refresh tecnologico di tutte le componenti in evoluzione.

Attività analisi e documentazione	Codice McAfee	GG/Persona
Analisi iniziale propedeutica alla realizzazione di un documento di architettura.	MD-SA-SECC-Z1	15
Redazione di un documento architetturale con il dettaglio dell'integrazione per ogni singolo componente.	MD-SA-SECC-Z1	20
TOTALE giorni		**35**

Refresh tecnologico delle suite Complete Endpoint Threat Protection Suite - (CTP)

Refresh tecnologico delle suite Complete End point	GG/Persona MD-SA-SECC-Z1	GG/Persona MD-CONSULT-DY-Z1
Assessment iniziale per installazione componenti	5	-
Aggiornamento ePO ultime release e hotfix per compatibilità con suite end point	2	5
Installazione e aggiornamento componenti evolutive	5	15
configurazione policy per le componenti evolutive	5	10
Test e verifiche funzionamento TIE	5	5
Redazione Procedure collaudo	1	5
Collaudo	2	2
Totale GG/Persona per figura professionale	***25***	***42***
TOTALE GG/Persona	**67**	

Aggiornamento architettura Secure Content Manager

Aggiornamento architettura Secure Content Manager web gateway	GG/Persona MD-SA-SECC-Z1	GG/Persona MD-CONSULT-DY-Z1
Assessment iniziale per installazione componenti Web gateway	5	5
Installazione componenti evolutive	5	10
Configurazione policy web gateway	10	10
Test e verifiche	-	10
Redazione Procedure collaudo	5	5
Collaudo	1	2
Totale GG/Persona per figura professionale	***26***	***42***
TOTALE GG/Persona	**68**	

Refresh tecnologico Secure Content Manager

Secure Content Manager refresh tecnologico	GG/Persona MD-SA-SECC-Z1	GG/Persona MD-CONSULT-DY-Z1
Preparazione ambiente secure content manager web gateway per upgrade tecnologico	-	5
Installazione iniziale nuove release	5	5
Configurazione policy di sicurezza e tuning delle stesse sul sistema	5	3
Processo di migrazione dalla vecchia infrastruttura alla infrastruttura evolutiva	2	10
Test e verifiche	1	5
Redazione Procedure collaudo	5	2
Collaudo	1	2
Totale GG/Persona per figura professionale	**19**	**32**
TOTALE GG/Persona	**51**	

Refresh tecnologico Intrushield Network Intrusion Prevention system

Intrushield Network IPS – Refresh Tecnologico	GG/Persona MD-SA-SECC-Z1	GG/Persona MD-CONSULT-DY-Z1
Preparazione ambiente iniziale per upgrade tecnologico	-	5
Installazione ultima release	3	10
Configurazione policy	5	-
Configurazione reportistica	5	-
Test e verifiche	2	5
Redazione Procedure collaudo	5	2
Collaudo	1	2
Totale GG/Persona per figura professionale	**21**	**24**
TOTALE GG/Persona	**45**	

Aggiornamento Architettura Intrushield Network IPS

Network IPS - Aggiornamento architettura	GG/Persona MD-SA-SECC-Z1	GG/Persona MD-CONSULT-DY-Z1
Assessment iniziale per individuazione segmenti da proteggere	5	10
Installazione componenti evolutive	5	10
Configurazione e integrazione reportistica e benchmark	15	10
Test e verifiche	2	10
Redazione Procedure collaudo	5	2
Collaudo	1	5
Totale GG/Persona per figura professionale	**33**	**47**
TOTALE GG/Persona	**80**	

Refresh tecnologico di ESM Enterprise Security Manager

Refresh tecnologico di ESM Enterprise Security Manager	GG/Persona MD-SA-SECC-Z1	GG/Persona MD-CONSULT-DY-Z1
Preparazione ambiente iniziale per upgrade tecnologico	2	5
Installazione ultima release software disponibile	5	5
Configurazione e porting template di reportistica	5	5
Test e verifiche	-	4
Redazione Procedure collaudo	3	4
Collaudo	1	2
Totale GG/Persona per figura professionale	**16**	**25**
TOTALE GG/Persona	**41**	

Aggiornamento architettura ESM Enterprise Security Manager

Aggiornamento architettura ESM	GG/Persona MD-SA-SECC-Z1	GG/Persona MD-CONSULT-DY-Z1
Preparazione ambiente iniziale	5	10
Installazione componenti evolutive ESM	8	15
Configurazione policy di reportistica	8	10
Supporto al deploy dei parser personalizzati	15	10
Creazione dashboard e correlazione	8	15
Test e verifiche	5	5
Redazione Procedure collaudo	4	2
Collaudo	2	2
Totale GG/Persona per figura professionale	**55**	**69**
TOTALE GG/Persona	**124**	

Refresh tecnologico ATD Advanced Threat Defence

Refresh tecnologico ATD Advanced Threat Defence	GG/Persona MD-SA-SECC-Z1	GG/Persona MD-CONSULT-DY-Z1
Preparazione ambiente iniziale	2	10
Installazione ultima release SW disponibile	3	5
Configurazione policy	5	3
Test e verifiche	3	5
Redazione Procedure collaudo	3	1
Collaudo	1	2
Totale GG/Persona per figura professionale	**17**	**26**
TOTALE GG/Persona	**43**	

Aggiornamento architettura ATD Advanced Threat Defence

Aggiornamento architettura ATD	GG/Persona MD-SA-SECC-Z1	GG/Persona MD-CONSULT-DY-Z1
Preparazione ambiente iniziale e assessment di rete	5	10
Installazione componenti evolutive ATD	5	10
Configurazione policy	3	3
Test e verifiche	3	4
Redazione Procedure collaudo	3	1
Collaudo	1	2
Totale GG/Persona per figura professionale	**20**	**30**
TOTALE GG/Persona	**50**	

Supporto specialistico (secondo e terzo anno di fornitura)

Durante il secondo ed il terzo anno di fornitura è richiesto supporto specialistico per tutte le attività di verifica, aggiornamenti, tuning e personalizzazioni che si renderanno necessarie sulle componenti di sicurezza implementate in produzione.

Figura professionale	GG/Persona MD-SA-SECC-Z1	GG/Persona MD-CONSULT-DY-Z1
Supporto specialistico per il 2° anno all'intera infrastruttura di sicurezza coinvolta nelle attività	40	140
Supporto specialistico per il 3° anno all'intera infrastruttura di sicurezza coinvolta nelle attività	40	140
Totale GG/Persona per figura professionale	80	280
TOTALE GG/Persona	**360**	

Riepilogo

Nella seguente tabella si fornisce il riepilogo dei servizi professionali di supporto specialistico richiesti per l'intero periodo di validità del contratto (36 mesi).

Figura professionale	Codice McAfee	Giorni/persona
Security Senior Consultant (SSC)	MD-SA-SECC-Z1	347
Security Consultant Product Specialist (SCPS)	MD-CONSULT-DY-Z1	617
TOTALE giorni/persona		**964**

Previsione d'impegno

Nella seguente tabella si fornisce una previsione di utilizzo dei servizi professionali di supporto specialistico richiesti nei tre anni di validità del contratto, in relazione alle attività precedentemente illustrate.

Servizi professionali	1° anno	2° anno	3° anno	Totale
Attività analisi e documentazione	25	5	5	35
Refresh tecnologico suite Complete End point Threat Protection - (CTP)	67	10	10	87
Aggiornamento architettura Secure Content Manager	68	30	30	128
Refresh tecnologico Secure Content Manager	51	12	12	75
Refresh tecnologico Intrushield - Network Intrusion Prevention system	45	12	10	67
Aggiornamento architettura Intrushield - Network IPS	60	28	28	116
Refresh tecnologico di ESM Enterprise Security Manager	41	28	28	97
Aggiornamento architettura ESM Enterprise Security Manager	100	50	50	200
Refresh tecnologico ATD Advanced Threat Defence	43	12	12	67
Aggiornamento architettura ATD Advanced Threat Defence	40	27	25	92
Totale	**540**	**214**	**210**	**964**

5.6 Fornitura di nuovi prodotti software in sottoscrizione o in licenza d'uso perpetua e nuove apparecchiature hardware

La consegna di nuovi prodotti software in sottoscrizione o in licenza d'uso perpetua e nuove apparecchiature hardware dovrà essere eseguita dall'Impresa entro il termine di 30 (trenta) giorni solari decorrenti da una richiesta formale dell'Amministrazione, che avverrà a mezzo comunicazione scritta. Tale comunicazione conterrà l'elenco dei prodotti software e delle corrispondenti quantità, l'elenco delle apparecchiature hardware e delle corrispondenti quantità, che l'Istituto intende acquisire. I prodotti software e le apparecchiature hardware, nonché le relative quantità, saranno compresi tra gli oggetti di fornitura previsti dal presente Capitolato Tecnico.

Le consegne dovranno avvenire presso la Direzione Centrale per l'Organizzazione Digitale - Via Santuario Regina degli Apostoli, 33 00145 Roma - a totale carico del Fornitore. L'impresa dovrà concludere il processo di installazione, configurazione e personalizzazione dei prodotti, nonché renderli operativi, entro il termine indicato nel Piano di lavoro approvato dall'Istituto e, comunque, non oltre 60 giorni solari decorrenti dalla data di consegna.

Ultimate le operazioni di installazione, configurazione e personalizzazione, l'Impresa dovrà consegnare all'Istituto un "Rapporto di Fine Installazione" recante le seguenti indicazioni: tipo, modello e numero seriale delle versione dei prodotti hardware e software installati, nonché la dichiarazione di rispondenza dei prodotti forniti alle specifiche del Capitolato Tecnico e le articolazioni delle prove proposte per la Verifica di conformità.