

## **ALLEGATO 1**

### **CAPITOLATO TECNICO**

**APPALTO SPECIFICO NELL'AMBITO DELLO SDA ICT PER IL  
SERVIZIO DI MANUTENZIONE E L'EVOLUZIONE DELLA  
PIATTAFORMA MCAFEE DI INAIL ED. 4 - ID 2414**



<b>1</b>	<b>PREMESSA.....</b>	<b>3</b>
<b>2</b>	<b>IL CONTESTO TECNOLOGICO E GLI OBIETTIVI .....</b>	<b>4</b>
2.1	Contesto tecnologico.....	4
2.2	La piattaforma di sicurezza McAfee .....	5
<b>3</b>	<b>DEFINIZIONE DELLA FORNITURA .....</b>	<b>8</b>
3.1	Oggetto.....	8
3.2	Durata.....	8
3.3	Responsabile del Servizio .....	8
3.4	Luogo di lavoro .....	9
<b>4</b>	<b>DEFINIZIONE DEI BENI E DEI SERVIZI OGGETTO DELLA FORNITURA .....</b>	<b>10</b>
4.1	Upgrade tecnologico dei prodotti installati e relativo servizio di manutenzione.....	10
4.2	Rinnovo del servizio di manutenzione o della sottoscrizione dei prodotti installati	11
4.3	Servizio di supporto sistemistico on site McAfee Premier Success Plan (PSP).....	13
4.4	Servizio di Starter KIT .....	13
4.5	Servizio di formazione .....	14
4.6	Servizi professionali di assistenza specialistica (a consumo) .....	14
4.7	Componenti opzionali .....	14
<b>5</b>	<b>MODALITÀ DI ESECUZIONE DELLA FORNITURA.....</b>	<b>16</b>
5.1	Manutenzione dei prodotti software e delle apparecchiature hardware.....	16
5.2	Servizio di Supporto Sistemistico on site McAfee Premier Success Plan .....	18
5.3	Assistenza specialistica sui prodotti.....	20
5.4	Servizio di formazione .....	29
5.5	Erogazione dei servizi di starter kit per UCEA.....	30
5.6	Fornitura di nuovi prodotti software in sottoscrizione o in licenza d'uso perpetua e nuove apparecchiature hardware.....	30



# 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 al servizio di 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 di grandi dimensioni (mainframe e open) e intermedi (open) siti presso i Data Center della Direzione Centrale Organizzazione Digitale (DCOD), siti in Roma e ad Acilia, per la gestione dei servizi di interoperabilità, dei servizi web e di cooperazione applicativa in alta affidabilità ridondati per gli ambienti di sviluppo, test e produzione;
- piattaforme Cloud per l'erogazione e l'utilizzo di servizi IAAS, PAAS e SAAS;
- sistemi di elaborazione centrali di medie dimensioni situati presso il CED del Centro Protesi di Vigorso di Budrio;
- sistemi di elaborazione periferici di medie dimensioni situati presso le Sedi territoriali;
- postazioni di lavoro (PC e stampanti) ad uso del personale, postazioni di servizio, personal computer portatili, tablet, dispositivi di fonia mobile;
- rete geografica 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);
- diverse tipologie di software di base.

INAIL sta conducendo il progetto "Data Center Transformation", in linea con le buone prassi suggerite da AGID, 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 2 (due) Data Center di tipologia TIER 3+ (come definito da TEIA942 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 aggiornati, 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.

La recente introduzione di piattaforme Cloud ha inoltre consolidato e ampliato le funzionalità dei Data Center, rendendo disponibili funzionalità ibride in termini di stack architetturali e applicativi.

## **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 le precedenti forniture e alla stipula del contratto attualmente in corso, INAIL ha provveduto a garantire continuità e adeguamento alle soluzioni McAfee in esercizio, profondamente integrate con le infrastrutture ICT dell'Istituto, gestite anche dal personale interno del presidio, e ad avviare un processo di ampliamento ed evoluzione dei servizi, per assicurare l'alto livello di sicurezza richiesto dai progetti strategici di INAIL. Di seguito alcuni degli interventi realizzati e obiettivi assicurati con le soluzioni e i servizi McAfee nell'ultimo triennio:

- il consolidamento di un unico punto di raccordo per il governo delle attività operative e delle politiche inerenti a tutte le soluzioni McAfee, ovvero la singola console della piattaforma di gestione unificata ePO (ePolicy Orchestrator Server);
- la distribuzione a bordo di tutti gli endpoint gestiti della suite CTP (Complete Endpoint Threat Protection) per assicurare una migliore protezione anti virus e anti intrusione a bordo dei sistemi e del modulo Endpoint Advanced Threat Prevention (ENS ATP), al fine di potenziare le capacità di contenimento e rilevamento di minacce sconosciute, sulla base di meccanismi di analisi avanzata basati su machine learning e contenimento dinamico;
- 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 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;
- il consolidamento dell'uso della tecnologia McAfee Open Data Exchange Layer (DXL), grazie alla quale sono state predisposte una serie di integrazioni a valore aggiunto con soluzioni infrastrutturali di terze parti, già acquistate



dall'Istituto, quali Check Point per i nuovi Firewall perimetrali, Cisco ISE per il controllo degli accessi sulle reti multivendor cablate e wireless e le connessioni VPN remote, InfoBlox per la gestione del SecureDNS e DHCP;

- il consolidamento 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;
- il consolidamento 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;
- il consolidamento della tecnologia SIEM (Enterprise Security Manager, ESM), un concentratore dedicato in primis alle soluzioni di sicurezza McAfee, ma integrabile con soluzioni di sicurezza di terze parti, atto alla raccolta dei log di tutti i sistemi istituzionali (nel rispetto delle normative del Garante) e alla correlazione intelligente e azionabile di eventi di sicurezza provenienti da sorgenti e apparati eterogenei;
- il consolidamento ed upgrade del sistema di controllo sulla Navigazione Internet per quanto riguarda potenziali malware e contenuti WEB non desiderati, mediante adeguamento della soluzione Web Gateway, attiva, ridondata e con connettività in fibra a 10Gbps su entrambi i Data Center di INAIL e la conseguente espansione dei suddetti criteri di protezione della navigazione anche ai dispositivi connessi a Internet al di fuori della rete interna e/o in Smart Working, mediante la progressiva attivazione del modulo McAfee Client Proxy;
- la messa in esercizio della piattaforma di protezione cloud McAfee MVISION Cloud (precedentemente nota come SkyHigh Networks), per monitorare e mettere in sicurezza dati e comportamenti degli utenti su servizi Cloud di varia natura, come Office365, ServiceNow, GoogleDrive, Dropbox, piattaforme IaaS, PaaS, SaaS e per visibilità e controllo sull'utilizzo di sistemi cloud non autorizzati (Shadow IT);
- la progressiva attivazione su tutte le soluzioni McAfee sopra elencate dell'integrazione nativa con i feed del Global Threat Intelligence (GTI) di McAfee, che, grazie alle informazioni condivise da milioni di sensori in tutto il mondo attraverso il Cloud, arricchite dalle ricerche degli analisti dei McAfee Labs, rende possibile una protezione accurata contro vettori malevoli ancora sconosciuti, grazie alla valorizzazione per rischio di parametri che tengono conto della diffusione e della reputazione di una minaccia.
- il rinnovo ed estensione del Servizio di Supporto Platinum Enterprise, rivelatosi un valore aggiunto ed un ritorno pratico sugli investimenti svolti in passato;
- l'erogazione di Servizi Professionali per un continuo miglioramento dell'efficienza ed efficacia della gestione degli strumenti di sicurezza McAfee, corredata da una dettagliata pianificazione delle singole iniziative progettuali concordate così come per la formazione al personale dell'Istituto.

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.



## 3 DEFINIZIONE DELLA FORNITURA

### 3.1 Oggetto

La fornitura prevede le seguenti componenti:

- **Fornitura Base**
  - Rinnovo del servizio di manutenzione e della sottoscrizione dei prodotti software in licenza d'uso perpetua e delle apparecchiature hardware (appliance) già in possesso dell'Istituto;
  - 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 Premier Success Plan
  - Servizi di Starter Kit
  - Servizio di addestramento per il personale INAIL
  - Servizi professionali di assistenza specialistica (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. Nel corso del contratto, 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 relativo servizio di manutenzione

È richiesto l'upgrade tecnologico e il servizio di manutenzione delle seguenti componenti infrastrutturali:

Upgrade tecnologico				
Tipologia	McAfee SKU	Nome Prodotto	Quantità	Durata anni
Upgrade Secure Content Management & CDA				
Appliance/Hardware Fee	WBG-5500-E	McAfee Web Gateway WG5500-E Appliance	8	1
Support Fee	WBG5500ENBD	McAfee Web Gateway WG5500-E Appliance	8	3
Appliance/Hardware Fee	MAP-10G4-FBRE	McAfee 10 Gigabit Fiber PCIe Card - E Model Appliances	8	1
Support Fee	RB10G4FBRE	McAfee 10 Gigabit Fiber PCIe Card - E Model Appliances	8	3
Upgrade SIEM				
Appliance/Hardware Fee	DAS-250	McAfee Direct Attached Storage 250	6	1
Support Fee	RBDAS250NBD	McAfee Direct Attached Storage 250	6	3
Appliance/Hardware Fee	ENMELM-6075	McAfee Enterprise Security, Enterprise Log Manager and Event Receiver 6075 Combination	2	1
Support Fee	ENMELM6075NBD	MFE EntSecMgr, ELM, EvtRec 6075 1YrBZ+NBD	2	3
Appliance/Hardware Fee	ELS-6075	McAfee Enterprise Log Search 6075	2	1
Support Fee	ELS6075NBD	1yr Business Software Support & Onsite Next Business Day Hardware Support	2	3
Upgrade ATD Advance Threat Defense				
Appliance/Hardware Fee	ATD-6200	McAfee Advanced Threat Defense 6200	8	1
Support Fee	ATD6200NBD	1yr Business Software Support & Onsite Next Business Day Hardware Support	8	3



<b>Upgrade IPS (Network Security Platform)</b>				
Appliance/Hardware Fee	IAC-4P10FOSR-KIT	MFE Net Sec 4port 10GE SR AFO Kit	19	1
Support Fee	RBIAC4P10FOSRKIT	MFE Net Sec 4port 10GE SR AFO 1yr RMA	19	3
Appliance/Hardware Fee	IAC-AFOCH40-KT2	Active FailOpen 40G Chassis	7	1
Support Fee	RBAFOCH40KT2	Active FailOpen 40G Chassis 1yr RMA	7	3
Appliance/Hardware Fee	IAC-AF85062-KT1	Active FO 850nm Opt 62.5um Gigabit Mod	16	1
Support Fee	RBAF85062KT1	Active FO 850nm Opt 62.5um Gigabit 1yRMA	16	3
<b>Upgrade cloud</b>				
subscription	PL1ECE	McAfee API	1	3
subscription	C43	MVISION DLP and Malware Pooled	10	3
subscription	C59	MVISION Cloud Workload Protection Platform (CWPP)	2000	3
subscription	MV3	Mvision Mobile	2000	3

## 4.2 Rinnovo del servizio di manutenzione o della sottoscrizione dei prodotti installati

È richiesto il rinnovo della manutenzione delle seguenti componenti infrastrutturali:

<b>Rinnovo Servizio di Manutenzione / Sottoscrizioni</b>				
<b>Tipologia</b>	<b>McAfee SKU</b>	<b>Nome Prodotto</b>	<b>Quantità</b>	<b>Durata anni</b>
<b>Rinnovo End Point and Server Security</b>				
Subscription Fee	MV6ECE-AA	MVISION Protect Plus and EDR Premium for Endpoint	15000	3
Support Fee	CWRECE-AA	McAfee Cloud Workload Security Detect and Respond	2000	3
Support Fee	MOVYFM-AA	McAfee MOVE AntiVirus for Virtual Desktops (VDI)	500	3
Support Fee	PSMYFM-AA	McAfee Security for Microsoft SharePoint	15000	3



Support Fee	GSSYFM-AA	MFESec for MS Exch ePO 1yrBZ[P+]	15000	3
<b>Rinnovo Secure Content Management</b>				
Support Fee	WBG5500DNBD	McAfee Web Gateway WG5500-D Appliance	8	3
Support Fee	RB10G4FBRD	McAfee 10 Gigabit Fiber PCIe Card - D Model Appliances	8	3
<b>Rinnovo SIEM (ESM)</b>				
Support Fee	ETMX11NBD	McAfee Enterprise Security Manager X11	2	3
Support Fee	ELM6050NBD	McAfee Enterprise Log Manager 6050	2	3
Support Fee	ERC4700NBD	McAfee Event Receiver 4700	8	3
Support Fee	ACE4700NBD	McAfee Advanced Correlation Engine 4700	2	3
Support Fee	APM3500NBD	McAfee Application Data Monitor 3500	2	3
Support Fee	RBDAS100ARM A	McAfee Direct Attached Storage 100	4	2
Support Fee	ELSVYE-AA	McAfee Enterprise Log Search VM (8 Cores)	2	2
Support Fee	ELS4YE-AA	McAfee Enterprise Log Search VM (4 Core Add-On)	6	2
Subscription Fee	GTEETMX11GIE AD	McAfee Global Threat Intelligence (Module for ESM) - ETM X11-N Appliance	2	3
Support Fee	ETM6000ELMN BD	McAfee Enterprise Security, Enterprise Log Manager and Event Receiver 6000 Combination	2	0,05
<b>Rinnovo ATD Advance Threat Defense</b>				
Support Fee	ATD6100GLNBD	McAfee Advanced Threat Defense 6100	6	3
Support Fee	ATD6000NBD	McAfee Advanced Threat Defense 6000	2	0,15
<b>Rinnovo IPS (Network Security Platform)</b>				
Support Fee	IPSNS9300NBD	McAfee Network Security IPS NS9300 Appliance	6	3
Support Fee	RBIAC1600ACPS	McAfee Network Security 1600W AC Spare Power Supply for NS9x00	4	3
Support Fee	RBIAC8P10NET MOD	McAfee Network Security 8-Port 10/1 GigE SFP+/SFP Network I/O Expansion Module (without Built-In Fail-Open)	12	3



Support Fee	RBIAC4P1GMM 62MOD	McAfee Network Security 4-Port 10/1 GigE 10GBASE-SR/1000BASE-SX 62,5Å, 10µm MM Net I/O Exp Mod(w/ Built-In FailOpen)	16	3
Subscription Fee	NMGECE-AA	McAfee Network Security Manager Software Subscription Global Edition	1	3
Support Fee	RBAFOCHKT2	McAfee Network Security Active 1/10G Fail-Open Chassis	4	3
Support Fee	VC3YCM-AB	MFE vNSP Cloud Large (1Gbps)	10	3
Support Fee	NYVMAPLNGAR MA	McAfee Network Security Manager Next Generation Appliance-Only for Standard, Global, Failover and Central manager	2	3
<b>Rinnovo cloud</b>				
Subscription Fee	UCAECE-AA	MVISION Unified Cloud Edge Advanced	12500	3
Subscription Fee	C42ECE	MVISION Cloud Security Posture Management (CSPM) Account Pooled	7	3

#### 4.3 Servizio di supporto sistemistico on site McAfee Premier Success Plan (PSP)

E' richiesto, per tutta la durata della fornitura, il servizio di supporto sistemistico on site McAfee Premier Success Plan, secondo le quantità di seguito elencate:

<b>Supporto Sistemistico On Site McAfee Premier Success Plan</b>			
<b>McAfee SKU</b>	<b>Product Name</b>	<b>Quantità</b>	<b>Durata anni</b>
PSPLANU	Premier Success Plan	1	3
PSPLAN-RESCSM-ADDON	Premier Success Plan - Resident Customer Success Manager Add-On	1	3
PSA-ADDON	McAfee Customer Success Plan Technical Support Engineer Add-on	3	3

#### 4.4 Servizio di Starter KIT

E' richiesta l'erogazione del servizio dei seguenti Starter KIT per l'avvio in esercizio della soluzione CASB:

<b>McAfee SKU</b>	<b>Nome Prodotto/Device provisto</b>	<b>Quantità</b>
MD-SK-SDIT-EM-10K	Starter Kit UCEA SHADOW IT	2
MD-SK-SCIT-API-EM	Starter Kit UCEA Sanctioned	3
DEPLOY-REMLOC-PP	Starter Kit UCEA DLP	3



#### 4.5 Servizio di formazione

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

McAfee SKU	Nome Prodotto	Quantità
TRN-SITE4-Z1	Training	6

#### 4.6 Servizi professionali di assistenza specialistica (a consumo)

Sono richiesti i seguenti servizi di assistenza specialistica, da erogare a consumo nel corso di durata contrattuale:

McAfee SKU	Product Name	Quantità (gg/p)
CONS-SA-DY-Z1	Security Architect Consulting Daily	399
CONS-DY	Custom Consulting Daily	550

#### 4.7 Componenti opzionali

Sono richieste opionalmente le seguenti componenti infrastrutturali ed i relativi servizi di manutenzione e supporto connessi, si tratta di nuovi prodotti software in sottoscrizione o in licenza d'uso perpetua e nuove apparecchiature hardware (appliances) con relativi servizi di manutenzione e supporto connessi.

Prodotti e Servizi Opzionali				
Tipologia	McAfee SKU	Prodotto	Quantità	Durata anni
<b>Opzione End Point</b>				
Subscription License	MV5ECE-AA	MVISION EDR Premium for Endpoint	5	1
Subscription License	MV7ECE-AA	MVISION Protect Plus and EDR Premium for Endpoint	5	1
<b>Opzione IPS (Network Security Platform)</b>				
Appliance/Hardware Fee	IPS NS9500	Network IPS Appliances: NS9500 Series	1	1
Support Fee	RBIPSN9500NBD	MFE Net Sec IPS-NS9500 Appl 1Yr NBD	1	1
Software Fee	NS9500-30GBPS	McAfee IPS NS9500 - 30Gbps Software license (Throughput based entitlement)	1	1
Support Fee	NS95X30YCM-AT	MFE NS9500 (30Gbps) 1Yr BZ	1	1
Appliance/Hardware Fee	IAC-NSCABLEPK1	NS 3M FO QSFP28 Cable 5 Pack for NS9x00	1	1
Subscription	IPS NS9500 30GB-SSL	McAfee Network Security IPS NS9500 30GB Appliance - Inbound/Outbound SSL	1	1
<b>Opzione SIEM</b>				



Appliance/Hardware Fee	ETM-X11-N	MFE Ent Sec Mgr X11-N Appl	1	1
Support Fee	ETMX11NNBD	MFE Ent Sec Mgr X11-N 1Yr BZ+NBD	1	1
Appliance/Hardware Fee	ELM-6075	MFE Ent Log Mgr 6075 Appl	1	1
Support Fee	ELM6075NBD	MFE Ent Log Mgr 6075 1Yr BZ+NBD	1	1
Appliance/Hardware Fee	ERC-SSD-6	MFE Event Receiver SSD-6 Appl	1	1
Support Fee	ERCSSD6NBD	MFE Event Receiver SSD-6 1Yr BZ+NBD	1	1
Appliance/Hardware Fee	ACE-SSD-6	MFE Adv Corr Eng SSD-6 Appl	1	1
Support Fee	ACESSD6NBD	MFE Adv Corr Eng SSD-6 1Yr BZ+NBD	1	1
Appliance/Hardware Fee	APM-3575	MFE App Data Mon 3575 Appl	1	1
Support Fee	APM3575NBD	MFE App Data Mon 3575 1Yr BZ+NBD	1	1
<b>Opzione CLOUD</b>				
subscription	UCEFI	MVISION Unified Cloud Edge Full Isolation AddOn	12500	1
subscription	C41ECE-AA	MVISION Cloud for SaaS Pooled	1	1



## 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 del contratto 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 manutenzione, che dovrà essere prestato con le modalità indicate nel presente Capitolato Tecnico, comprende tutti gli oneri necessari per la perfetta e puntuale esecuzione del servizio stesso, nonché ogni altro onere per mantenere e/o riportare le apparecchiature hardware e i prodotti software in stato di funzionamento coerente con la documentazione, nonché le modifiche tecniche atte ad elevare il grado d'affidabilità, a migliorarne il funzionamento ed aumentarne la sicurezza.

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.

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.

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.

Ricevuta la comunicazione di cui sopra, l'Impresa si obbliga confermare la presa in carico del problema mediante comunicazione via mail all'Istituto, entro 1 ora lavorativa.

L'Impresa si impegna ad attivarsi al fine di ripristinare la funzionalità delle apparecchiature e dei prodotti software entro i seguenti termini perentori:





- entro 4 ore lavorative dalla presa in carico, nel caso di problemi bloccanti intervenuti su prodotti software, anche dovuti al rilascio di aggiornamenti che provochino disservizio alle apparecchiature dell'Istituto (siano esse Server, Personal Computer o Appliance);
- entro 24 ore lavorative dalla presa in carico, nel caso di problemi non bloccanti intervenuti su prodotti software;
- entro 6 ore lavorative dalla presa in carico, nel caso di problemi bloccanti intervenuti su apparecchiature hardware ritenute critiche per il buon funzionamento del sistema informativo dell'Istituto.

Ove la soluzione del malfunzionamento non intervenga entro il termine di cui al precedente comma, l'Istituto applicherà le penali previste all' articolo intitolato "Penali" del Contratto, salvo in ogni caso il risarcimento al maggior danno.

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 entro nuovi termini temporali da concordarsi tra le parti il cui rispetto sarà soggetto a verifica e ad eventuale applicazione di penali in caso di ritardo.

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 alle parti sostituite - verranno fornite dall'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 garanzie.

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, previa comunicazione all' Istituto, dovrà provvedere alla sostituzione delle apparecchiature stesse con altre aventi le medesime caratteristiche tecniche e funzionali, ferma restando l'applicazione delle penali previste dal Contratto, 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. Qualora il fermo o il malfunzionamento di una apparecchiatura comporti il mancato utilizzo di altre apparecchiature funzionalmente collegate, la Committente procederà all'applicazione delle penali anche per tali altre apparecchiature.



## 5.2 Servizio di Supporto Sistemistico on site McAfee Premier Success Plan

Il livello di Supporto Enterprise richiesto è il McAfee Premier Success Plan, comprensivo di un Customer Success Manager (reperibile h24 e residente negli orari di lavoro presso gli stabili dell'Istituto) e di vari Specialisti di Prodotto dedicati ad ogni linea di prodotto McAfee (sempre contattabili telefonicamente e via email); esso deve comprendere: un unico punto di contatto dedicato 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.

Nel dettaglio, il McAfee Premier Success Plan (PSP) deve prevedere una serie di risorse e di servizi integrati per trarre il massimo valore dagli investimenti nelle soluzioni McAfee scelte da INAIL e ottimizzare le operazioni di sicurezza, tra cui:

1. Un Customer Success Manager assegnato e residente per orchestrare tutte le soluzioni da implementare sia a breve che a lungo termine (configurazioni, distribuzioni, aggiornamenti, report sui casi aperti e sulla postura di sicurezza);
2. Tre contatti tecnici assegnati (ATC) e dedicati a INAIL per collaborare con il CSM e INAIL per garantire una migliore esperienza nel supporto tecnico, affrontando proattivamente i problemi e gestendo le escalation;
3. L'accesso a tecnici senior del supporto tecnico (TSE) in tutto il mondo, assegnati ad INAIL, per guidare la risoluzione dei problemi;
4. Una risorsa di contatto tecnico specifica per Cloud (C-ATC);
5. Il McAfee Health Watch, un servizio che fornisce un rapporto diagnostico approfondito e un riepilogo delle azioni di manutenzione consigliate e attuabili per garantire che le piattaforme McAfee siano completamente ottimizzate;
6. Servizi di consulenza avanzata sulla Cybersecurity e laboratori di prova e di studio sulle soluzioni McAfee.

In particolare, con riferimento al (resident) Customer Success Manager si indica che:

**Resident Customer Success Manager (CSM)** Si tratta di una risorsa specializzata e dedicata all'Istituto per tutta la durata del contratto. Risiede fisicamente presso la DCOD e lavora a stretto contatto con i referenti INAIL e con i consulenti esterni per le tematiche inerenti alla sicurezza informatica e alle tecnologie del fornitore utilizzate dall'Istituto. Tra le sue mansioni fondamentali, si occupa di coordinare, controllare e semplificare le attività delle risorse incluse nel "Premier Success Plan", vale a dire:



- Assigned Technical Contact (ATC), è un consulente McAfee che collabora da remoto con INAIL per garantire una migliore esperienza nel supporto tecnico, affrontando proattivamente i problemi, i ticket e la gestione delle escalation;
- Cloud Assigned Technical Contact (C-ATC), un consulente McAfee che collabora da remoto per ottimizzare le soluzioni sulla sicurezza del Cloud implementate da INAIL;
- 3 Technical Support Engineer assegnati e dedicati a INAIL (gli Assigned Product Specialist già inclusi nella fornitura del 2018), sono 3 tecnici altamente specializzati che lavorano da remoto sugli aspetti di supporto tecnico nelle 3 aree "core" ("Rete-Web-Malware", "Endpoint" e "SIEM") della sicurezza informatica dell'Istituto

Il Resident CSM, inoltre, guida i task dei Servizi Professionali, d'accordo con i referenti INAIL, per agevolare la buona riuscita dei progetti di installazione, upgrade, migrazione e integrazione delle soluzioni McAfee scelte dall'Istituto, secondo le priorità e i tempi stabiliti.

In aggiunta, attingendo a quanto incluso nel "Premier Success Plan", il CSM:

- orchestra il McAfee Health Watch, un servizio che fornisce un rapporto diagnostico approfondito e un riepilogo delle azioni di manutenzione consigliate e attuabili per garantire che le piattaforme McAfee siano utilizzate al meglio, secondo i più alti standard di sicurezza ed efficacia.
- si occupa del delivery di servizi di consulenza avanzata sulla Cybersecurity (ad esempio, con workshop mirati alla revisione dei processi interni di Gestione e Risposta agli Incidenti e di Protezione dei Dati) e laboratori di collaudo e studio sulle soluzioni McAfee, tagliati sulle esigenze dei gruppi tecnici che ne abbiano bisogno.

Si faccia riferimento alla lista dei codici e quantità previste del par. 4.3 per il livello di supporto richiesto nei 36 mesi.

L'obiettivo principale della consulenza specialistica McAfee è quello di ottenere il massimo dei benefici dalle installazioni Software e hardware implementate e da implementare presso la rete dell'Istituto, tali benefici devono rispondere a criteri di:

- Gestione centralizzata delle soluzioni e monitoraggio totale del sistema;
- Mantenimento di un elevato livello di sicurezza dell'infrastruttura nel tempo;
- Capacità di adeguamento nel tempo alle nuove minacce;
- Controllo e rendicontazione periodica sul livello di sicurezza del sistema informativo dell'Istituto attraverso analisi manuali e automatica, fornendo documenti dettagliati sia sull'AS IS e sia fornendo indicazioni sulle eventuali contromisure da implementare.
- Integrazione nativa di tutte le componenti McAfee, sia quelle nuove e sia quelle già presenti presso l'Istituto.

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



### 5.3 Assistenza specialistica sui prodotti

La consulenza specialistica McAfee viene utilizzata per aggiornare e consolidare le soluzioni esistenti già installate e in produzione, che l'Istituto già utilizza.

La tabella che segue descrive il profilo delle figure professionali.

<b>Security Senior Consultant (SSC) - Codice MD-SA-SECC-Z1</b>
Ricopre il ruolo di interfaccia di alto livello con il cliente e soprattutto di gestione dei team di coinvolto nelle attività 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 macroschedulazioni con i Project Leader a vantaggio delle sinergie evitando sovrapposizioni di uso di risorse non condivisibili. Diventa il gestore delle Escalation e delle Change Request.
<b>Security Consultant Product Specialist (SCPS) - Codice MD-CONSULT-DY-Z1</b>
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 nelle attività consiste nel guidare le parti operative di implementazione supportato dallo Junior Specialist, nell'interfacciarsi con la parte tecnica del cliente per la normale operatività ed analisi dei requisiti tecnici in cooperazione col PL e nel riportare al PL 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 e refresh tecnologico delle componenti McAfee elencate in tabella:

<b>Componente</b>	<b>Funzione/Attività</b>
Gestione attività e documentazione	Fase di analisi e stesura documentazione e architettura.
Aggiornamento tecnologico della suite MVISION Protect Plus and EDR Premium for Endpoint (MV7ECE-AA)	È la suite end point antimalware necessaria alla messa in sicurezza delle postazioni di lavoro e dei dispositivi mobili. Le attività prevedono l'aggiornamento e la migrazione alla nuova suite e funzionalità MV7.
Aggiornamento architettura 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 cyber durante la navigazione web. Questa attività prevede l'aggiornamento della architettura di riferimento utilizzando delle appliance McAfee modello 5500-E.
Refresh tecnologico Intrushield Network Intrusion Prevention system	In questa fase saranno aggiornate le componenti hardware e software dell'architettura Network intrusion prevention esistente.
Refresh tecnologico di ESM Enterprise Security Manager	L'attività prevede l'aggiornamento tecnologico della componente ESM, portando le componenti in produzione al livello software dell'ultima release disponibile.



Aggiornamento 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 l'aggiornamento ai nuovi sistemi ATD 6200.
Refresh tecnologico SharePoint for Server	Il Sistema di gestione della sicurezza dei documenti che vengono aggiunti o caricati da sharepoint, sarà effettuata una attività di refresh tecnologico della versione SW.
Refresh tecnologico ESM	Il Sistema ESM Enterprise Security Manager e tutte le component facenti parti il sistema saranno aggiornate alle ultime versioni SW.
Aggiornamento Tecnologico CASB MVISION Unified Cloud Edge Advanced (UCEA)	La nuova Suite UCEA permette di unificare i servizi CASB, DataProtection e Webgateway SAAS in un unico sistema con gestione centralizzata, l'attività prevede l'aggiornamento tecnologico con la nuova suite e l'attivazione delle nuove funzionalità.
Aggiornamento tecnologico McAfee Cloud Workload Security Detect and Respond	È la suite per la sicurezza degli ambienti virtuali e server, sarà effettuato un aggiornamento tecnologico della piattaforma attualmente in produzione.
Refresh tecnologico McAfee MOVE AntiVirus for Virtual Desktops (VDI)	È la suite per la protezione dei desktop virtuali, sarà effettuato un refresh tecnologico, aggiornando l'attuale piattaforma con le ultime versioni SW.

#### **Piano attività**

I servizi di assistenza specialistica 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 assistenza specialistica 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 assistenza specialistica 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 architettuale, l'integrazione, l'aggiornamento e il refresh tecnologico di tutte le componenti evolutive:

Attività analisi e documentazione	SKU McAfee (codice)	Giorni uomo
Analisi iniziale propedeutica alla realizzazione di un documento di architettura.	MD-SA-SECC-Z1	10
Redazione di un documento architettuale con il dettaglio dell'integrazione per ogni singolo componente.	MD-SA-SECC-Z1	15
<b>TOTALE giorni</b>		<b>25</b>

#### **Aggiornamento tecnologico della suite MVISION Protect Plus and EDR Premium for Endpoint (MV7)**

La suite end point MV7 costituisce la componente di sicurezza delle postazioni di lavoro e dei device mobili, sarà effettuato un aggiornamento tecnologico delle componenti già in produzione alla nuova suite MV7 per innalzare il livello di sicurezza. Le attività previste sono:

Aggiornamento tecnologico suite End point MV7	GG/Persona SKU MD-SA-SECC-Z1	GG/Persona SKU 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 suite MV7 sui sistemi client	5	5



Test e verifiche funzionamento suite MV7 sui sistemi Mobili	5	5
Redazione Procedure collaudo	1	5
Collaudo	2	2
Totale giorni per singolo SKU	30	47
<b>TOTALE giorni</b>	<b>77</b>	

#### **Aggiornamento architettura Secure Content Manager**

La componente Secure Content Manager web gateway mette in sicurezza la navigazione Internet delle postazioni di lavoro, l'attività prevede l'introduzione delle componenti evolutive web gateway al fine di bilanciare meglio il carico di lavoro e garantire un elevato livello di sicurezza. Le attività previste sono:

<b>Aggiornamento architettura Secure Content Manager web gateway</b>	<b>GG/Persona SKU MD-SA-SECC-Z1</b>	<b>GG/Persona SKU MD-CONSULT-DY-Z1</b>
Assessment iniziale per installazione componenti Web gateway	5	5
Installazione componenti evolutive appliance 5500-E	5	10
Processo di migrazione dalla vecchia infrastruttura alla infrastruttura evolutiva	5	10
configurazione policy web gateway	5	5
Test e verifiche	2	10
Redazione Procedure collaudo	5	5
Collaudo	1	2
<b>Totale giorni per singolo SKU</b>	<b>28</b>	<b>47</b>
<b>TOTALE giorni</b>	<b>75</b>	

#### **Refresh tecnologico Intrushield Network Intrusion Prevention system**

La componente Network IPS sarà aggiornata alle ultime release HW e SW, per migliorare la sicurezza e la visibilità complessiva. Le attività prevedono:

<b>Intrushield Network IPS – Refresh Tecnologico</b>	<b>GG/Persona SKU MD-SA-SECC-Z1</b>	<b>GG/Persona SKU MD-CONSULT-DY-Z1</b>
Preparazione ambiente iniziale per upgrade tecnologico	5	5



Installazione ultima release	3	10
Aggiornamento componenti HW	5	5
Configurazione policy	5	-
Configurazione reportistica	5	-
Test e verifiche	2	5
Redazione Procedure collaudo	5	2
Collaudo	1	2
<b>Totale giorni per singolo SKU</b>	<b>31</b>	<b>29</b>
<b>TOTALE giorni</b>	<b>60</b>	

#### Refresh tecnologico di ESM Enterprise Security Manager

La componente ESM sarà aggiornata alle nuove release SW, per migliorare la sicurezza e la visibilità complessiva.

Le attività prevedono:

Refresh tecnologico di ESM Enterprise Security Manager	GG/Persona SKU MD-SA- SECC-Z1	GG/Persona SKU MD- CONSULT- DY-Z1
Preparazione ambiente iniziale per upgrade tecnologico	5	5
Installazione ultima release software disponibile	10	5
Configurazione e porting template di reportistica	10	5
Ottimizzazione dashboard di visualizzazione	5	10
Test e verifiche	-	5
Redazione Procedure collaudo	3	5
Collaudo	1	2
<b>Totale giorni per singolo SKU</b>	<b>34</b>	<b>37</b>
<b>TOTALE giorni</b>	<b>71</b>	

#### Aggiornamento architettura ATD Advanced Threat Defence

L'attività prevede l'aggiornamento dell'architettura ATD, inserendo nuove appliance ATD per meglio bilanciare il carico di lavoro:

Aggiornamento architettura ATD	GG/Persona SKU MD-SA- SECC-Z1	GG/Persona SKU MD- CONSULT- DY-Z1
--------------------------------	-------------------------------------	--





Preparazione ambiente iniziale e assessment di rete	5	10
Installazione componenti evolutive ATD	5	15
Configurazione policy	3	5
Test e verifiche	3	5
Redazione Procedure collaudo	5	2
Collaudo	1	2
<b>Totale giorni per singolo SKU</b>	<b>22</b>	<b>39</b>
<b>TOTALE giorni</b>	<b>61</b>	

#### Refresh tecnologico McAfee Security for SharePoint

L'attività prevede il refresh tecnologico della piattaforma Security for Sharepoint al fine di allineare le versioni SW alle ultime disponibilità e massimizzare il livello di sicurezza.

Refresh tecnologico piattaforma Security for Sharepoint	GG/Persona SKU MD-SA- SECC-Z1	GG/Persona SKU MD- CONSULT- DY-Z1
Preparazione ambiente iniziale e assessment della piattaforma	5	10
Aggiornamento software delle componenti Security for Sharepoint	5	15
Configurazione e ottimizzazione policy	3	5
Test e verifiche	3	5
Redazione Procedure collaudo	5	2
Collaudo	1	2
<b>Totale giorni per singolo SKU</b>	<b>22</b>	<b>39</b>
<b>TOTALE giorni</b>	<b>61</b>	

#### Aggiornamento Tecnologico CASB MVISION Unified Cloud Edge Advanced (UCEA)

L'attività prevede l'aggiornamento tecnologico della piattaforma CASB, CDA e C13 alla nuova piattaforma Unified Cloud Edge Advanced (UCEA)

Aggiornamento tecnologico CASB Mivision Cloud UCEA	GG/Persona SKU MD- SA-SECC-Z1	GG/Persona SKU MD-CONSULT-DY-Z1
Preparazione ambiente iniziale e assessment della piattaforma	10	10



Preparazione alla migrazione della piattaforma WPS a UCEA	3	10
Preparazione all'aggiornamento della componente CDA a UCEA	4	10
Preparazione all'aggiornamento della componente C13 a UCEA	5	10
Migrazione alla nuova piattaforma unificata UCEA	5	10
Configurazione e ottimizzazione policy	3	5
Test e verifiche	3	5
Redazione Procedure collaudo	3	2
Collaudo	1	2
<b>Totale giorni per singolo SKU</b>	<b>37</b>	<b>64</b>
<b>TOTALE giorni</b>	<b>101</b>	

#### **Refresh tecnologico McAfee Cloud Workload Security Detect and Respond**

L'attività prevede il refresh tecnologico della piattaforma McAfee Cloud Workload Security Detect and Respond dedicata ai server virtuali e fisici nel cloud.

<b>Refresh tecnologico McAfee Cloud Workload Security Detect and Respond</b>	<b>GG/Persona SKU MD-SA-SECC-Z1</b>	<b>GG/Persona SKU MD-CONSULT-DY-Z1</b>
Preparazione ambiente iniziale e assessment della piattaforma	5	10
Installazione nuove versioni	5	10
Configurazione e ottimizzazione policy	3	5
Test e verifiche	3	5
Redazione Procedure collaudo	4	2
Collaudo	1	2
<b>Totale giorni per singolo SKU</b>	<b>21</b>	<b>34</b>
<b>TOTALE giorni</b>	<b>55</b>	

#### **Refresh tecnologico McAfee MOVE AntiVirus for Virtual Desktops (VDI)**

L'attività prevede il refresh tecnologico della piattaforma McAfee MOVE dedicata ai virtual desktop

<b>Refresh tecnologico McAfee MOVE AntiVirus for Virtual Desktops (VDI)</b>	<b>GG/Persona SKU MD-SA-SECC-Z1</b>	<b>GG/Persona SKU MD-CONSULT-DY-Z1</b>
---	-------------------------------------	--



Preparazione ambiente iniziale e assessment della piattaforma MOVE	5	10
Installazione nuove versioni per sicurizzazione virtual desktop	5	10
Configurazione e ottimizzazione policy	3	5
Test e verifiche	3	5
Redazione Procedure collaudo	3	2
Collaudo	1	2
<b>Totale giorni per singolo SKU</b>	<b>19</b>	<b>34</b>
<b>TOTALE giorni</b>	<b>53</b>	

Durante il 2° e 3° anno di fornitura sarà garantito un'assistenza specialistica per tutte le attività di verifica, aggiornamenti, tuning e personalizzazioni che si rendono necessarie durante il periodo di produzione delle componenti di sicurezza implementate.

Figura professionale	GG/Persona SKU MD-SA- SECC-Z1	GG/Persona SKU MD- CONSULT-DY- Z1
Assistenza specialistica per il 2° anno all'intera infrastruttura di sicurezza coinvolta nelle attività	65	90
Assistenza specialistica per il 3° anno all'intera infrastruttura di sicurezza coinvolta nelle attività	65	90
<b>Totale giorni per singolo SKU</b>	<b>130</b>	<b>180</b>
<b>TOTALE giorni</b>	<b>310</b>	

#### Servizi di consulenza/assistenza sistemistica - Tabelle riepilogative

Nella seguente tabella si fornisce il riepilogo del totale giornate comprensivo di supporto sistemistico alla gestione per l'intero periodo di validità del contratto (36 mesi).

Figura professionale	SKU McAfee (codice)	Giorni uomo
Security Senior Consultant (SSC)	MD-SA-SECC-Z1	399
Security Consultant Product Specialist (SCPS)	MD-CONSULT-DY-Z1	550



<b>TOTALE giorni</b>		<b>949</b>
----------------------	--	------------

**Fornitura Servizi Professionali per anno/attività**

Previsione impegno in giornate uomo (GP) per anno e complessive di fornitura:

Servizi professionali	1° anno	2° anno	3° anno	Totale
Attività analisi e documentazione	25	10	10	45
Aggiornamento tecnologico suite End point MV7	77	15	15	107
Aggiornamento architettura Secure Content Manager	75	25	25	125
Refresh Tecnologico - Intrushield Network IPS	60	10	10	80
Refresh tecnologico di ESM Enterprise Security Manager	71	10	10	91
Aggiornamento architettura ATD	61	20	20	101
Refresh tecnologico piattaforma Security for Sharepoint	61	15	15	91
Aggiornamento tecnologico CASB Mivision Cloud UCEA	101	30	30	161
Refresh tecnologico McAfee Cloud Workload Security Detect and Respond	55	10	10	75
Refresh tecnologico McAfee MOVE AntiVirus for Virtual Desktops (VDI)	53	10	10	73
<b>Totale</b>	<b>639</b>	<b>155</b>	<b>155</b>	<b>949</b>

**Previsione impegno GG/Persona/Anno, per figura professionale**



FP	Attività analisi e documentazione			Aggiornamento tecnologico suite End point MV7			Aggiornamento architettura Secure Content Manager			Refresh tecnologico Intrushield Network IPS			Refresh tecnologico di ESM Enterprise Security Manager			Aggiornamento architettura ATD			Refresh tecnologico piattaforma Security for Sharepoint			Aggiornamento tecnologico CASB Mivision Cloud UCEA			Refresh tecnologico McAfee Cloud Workload Security Detect and Respond			Refresh tecnologico McAfee MOVE AntiVirus for Virtual Desktops (VDI)		
	A1	A2	A3	A1	A2	A3	A1	A2	A3	A1	A2	A3	A1	A2	A3	A1	A2	A3	A1	A2	A3	A1	A2	A3	A1	A2	A3	A1	A2	A3
MD-SA-SECC-Z1	25	10	10	30	5	5	28	10	10	31	5	5	34	5	5	22	5	5	22	5	5	37	10	10	21	5	5	19	5	5
MD-CONSULT-DY-Z1	-	-	-	47	10	10	47	15	15	29	5	5	37	5	5	39	15	15	39	10	10	64	20	20	34	5	5	34	5	5
Totale	25	10	10	77	15	15	75	25	25	60	10	10	71	10	10	61	20	20	61	15	15	101	30	30	55	10	10	53	10	10

Il Fornitore deve supportare gli utenti nell'utilizzo dei prodotti oggetto della presente fornitura, per tutto il periodo contrattuale, tramite la suddetta assistenza professionale specialistica, in modalità "a consumo" di giorni persona.

#### 5.4 Servizio di formazione

La fornitura prevede l'erogazione di n° 6 training ufficiali McAfee in aula per un massimo di 6 persone a corso al fine di garantire un aggiornamento delle competenze al personale dell'Istituto. McAfee rilascerà documentazione ufficiale del training per ogni partecipante al corso.

Corso Ufficiale McAfee	Giorni	SKU McAfee (codice)	Quantità
Corso di aggiornamento della suite MV7 sulla componente EDR	4	TRN-SITE4-Z1	1
Corso di aggiornamento Advanced Threat Defense (ATD)	4	TRN-SITE4-Z1	1
Corso di aggiornamento Network IPS (NSP)	4	TRN-SITE4-Z1	1
Corso di aggiornamento ENS/ATP	4	TRN-SITE4-Z1	1
Corso di aggiornamento ESM	4	TRN-SITE4-Z1	1
Corso CASB UCEA	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 Erogazione dei servizi di starter kit per UCEA**

Al fine di garantire la corretta esecuzione dei controlli e verifiche delle applicazioni nel cloud per la soluzione CASB è necessario prevedere dei servizi di starter kit per l'avvio in esercizio di tali funzionalità, dedicati alla pianificazione, installazione, consulenza e configurazione degli ambienti cloud presenti nell'elenco della fornitura.

### **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 operativo 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 versioni 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.