SISTEMA SANITARIO REGIONALE
ASL RIETI

REGIONE LAZIO

Azienda Sanitaria Locale Rieti

U.O.S.D. SISTEMA INFORMATICO

DETERMINAZIONE DIRIGENZIALE

n° 650 del 10 APR. 2018

Oggetto: Affidamento a seguito di RDO MEPA alla Società Akito S.r.l., della fornitura di Licenze per Servizi **Web Security** e **Content Filtering WEBSENSE -- WEB SECURITY GATEWAY ANYWHERE e MODULO INTEGRATIVO Advanced Malware Detection Cloud - WEB, Modules** (800 utenti), per il periodo di 36 mesi (01/04/2018-01/04/2021).
Importo della spesa € 138.714,00 Iva Compresa.
CIG: 7419469382

Il Dirigente sottoscrivendo il presente provvedimento, attesta che lo stesso, a seguito dell'istruttoria effettuata, nella forma e nella sostanza, è totalmente legittimo, ai sensi dell'art. 1 della L. n. 20/1994 e ss.mm.ii., assumendone di conseguenza la relativa responsabilità, ex art. 4, comma 2, L. n. 165/2001, nonché garantendo l'osservanza dei criteri di economicità, di efficacia, di pubblicità, di imparzialità e trasparenza di cui all'art. 1, comma 1°, L. n. 241/1990, come modificato dalla L. n. 15/2005. Il dirigente attesta, altresì, che il presente provvedimento è coerente con gli obiettivi dell'Azienda ed assolutamente utile per il servizio pubblico ai sensi dell'art. 1, L. n. 20/1994 e ss.mm.ii.;

L'Estensore

Dott.ssa Daisy Di Luca Firma Daisy Di Luca Data 3/4/2018

Il Responsabile del Sistema Informatico

Ing. Roberto Campogiani Firma [signature] Data 3/4/2018

Il Direttore della U.O.C. Economico Finanziaria con la sottoscrizione del presente atto attesta che lo stesso non comporta scostamenti *sfavorevoli* rispetto al budget economico.

Voce del conto economico su cui imputare la spesa 502020106 → AUT. 10/2018
e PATRIMONIO 1010104021 → PROV. 133 - AUT. 58-7/2018

Data 06/04/2018 Firma [signature]
Dott.ssa Barbara Proietti

DETERMINAZIONE DIRIGENZIALE

Visto l'art. 4, comma 2, del D.Lgs. 30 marzo 2001, n. 165 concernente le attribuzioni dei dirigenti nelle amministrazioni pubbliche;

Visto l'Atto Aziendale approvato con DCA n.113 del 18/3/2015 pubblicato sul B.U.R.L. n. 33 S.O. n.1 del 23 aprile 2015 da cui si rileva l'organizzazione aziendale ed il funzionigramma;

Vista la deliberazione n.7/D.G. del 12.12.2017 di attribuzione delle deleghe al Direttore Amministrativo, al Direttore Sanitario ed ai dirigenti delle strutture aziendali in relazione agli incarichi formalmente conferiti ed i conseguenti successivi atti di delega, integrata con Deliberazione n. 222/D.G. dell'12.03.2018;

IL RESPONSABILE DELLA *U.O.S.D. SISTEMA INFORMATICO*

PREMESSO che

- con deliberazione n.198/D.G. del 27/03/2015 l'Azienda USL di Rieti ha acquistato su Mercato Elettronico Consip 1 Licenza Multi-utente (800 utenti) per i Servizi Web secutiry e Content Filtering per il controllo e la regolamentazione degli accessi ai contenuti Web, comprensive di protezione contro le minacce di nuova generazione, per il periodo (01/04/2015 – 01/04/2018);

- tale licenza è giunta a scadenza e si è reso necessaria l'indizione su Mepa di una RDO al fine di aggiudicare la fornitura di Licenze per Servizi **Web Security** e **Content Filtering WEBSENSE – WEB SECURITY GATEWAY ANYWHERE** e **MODULO INTEGRATIVO Advanced Malware Detection Cloud - WEB, Modules** (800 utenti), per il periodo di 36 mesi (01/04/2018-01/04/2021).

PRESO ATTO che:

- su Mercato Elettronico CONSIP mediante RdO n° 1900322 del 20.03.2018, sono stati invitati a presentare offerta tecnico-economica n. 5 fornitori al fine di aggiudicare la fornitura di Licenze per Servizi **Web Security** e **Content Filtering WEBSENSE – WEB SECURITY GATEWAY ANYWHERE** e **MODULO INTEGRATIVO Advanced Malware Detection Cloud - WEB, Modules** (800 utenti), per il periodo di 36 mesi con importo a base di gara € 120.000,00 oltre Iva (*Allegato n. 1- Dati Generali della Procedura*)

- in risposta alla Richiesta d'Offerta RdO n° 19000322 sono state presentate n. 2 offerte tecnico economiche;

- è risultata vincitrice la Società Akito, per aver offerto il prezzo più basso (*Allegato n.2 - Riepilogo delle attività di Esame delle Offerte Ricevute*);

VISTA l'offerta tecnico/economica relativa all' RdO n° 1900322 dalla Società Akito S.r.l che prevede la seguente fornitura (*Allegato n. 3 – Offerta Tecnica e Offerta Economica*);

DESCRIZIONE	DURATA	Totale esclusa IVA
Licenze per Servizi Web Security e Content Filtering WEBSENSE – WEB SECURITY GATEWAY ANYWHERE per il periodo di 36 mesi per 800 utenti	36 mesi	€ 80.100,00
Modulo integrativo per analisi in tempo reale di ransomware, nuovi virus e siti sospetti non ancora censiti.	36 mesi	€ 28.100,00
n. 10 gg/uomo per Upgrade della versione esistente e sistemazione Proxy	36 mesi	€ 550,00

Per un totale di € 113.700,00 Iva Esclusa;

RITENUTO opportuno nominare:

- quale Responsabile Unico del Procedimento Ing. Roberto Campogiani;
- quale Assistente al DEC il Sig. Piero Bolognini;

DATO ATTO che la proposta è coerente con il vigente Piano Triennale Aziendale della Prevenzione della Corruzione e del Programma Triennale per la Trasparenza e l'Integrità;

D E T E R M I N A

- Di aderire alla proposta presentata della Società Akito S.r.l risultata vincitrice della RdO n° 1900322, e di affidare alla stessa la fornitura di Licenze per Servizi **Web Security** e **Content Filtering WEBSENSE – WEB SECURITY GATEWAY ANYWHERE** e **MODULO INTEGRATIVO Advanced Malware Detection Cloud - WEB, Modules** (800 utenti), per il periodo 01/04/2018 – 01/04/2021;

- Di includere l'onere del presente provvedimento di € 138.714,00 Iva Inclusa, cos' come appresso specificato:
  - € 6.710,00 nel conto 502020106 "servizi di assistenza informatica" esercizio anno 2018;
  - € 132.004,00 nel costo 101010401 "Diritti di brevetto e diritti di utilizzazione delle opere d'ingegno – altri" esercizio 2018;

- Di dichiarare il presente provvedimento immediatamente esecutivo non essendo sottoposto al controllo regionale, ai sensi del combinato disposto dell'art. 30 della L.R. n. 18/94 e successive modificazioni ed integrazioni e degli artt. 21 e 22 della L.R. n. 45/96.

- Di disporre che il presente atto venga pubblicato nell'albo pretorio on-line aziendale ai sensi dell'art. 32, comma 1, della legge 18.09.2009, n. 69 e del D.Lgs 14.03.2013 n. 33;

in oggetto ☐ per esteso ☒

Il Direttore della U.O.S.D. Sistema Informatico
Ing. Roberto Campogiani

VERIFICATA DAL DIRETTORE AMMINISTRATIVO O DAL DIRETTORE SANITARIO:

IL DIRETTORE AMMINISTRATIVO
Dott.ssa Anna Petti

☑ Il Direttore Amministrativo: Dott.ssa Anna Petti _____

☐ Il Direttore Sanitario: Dott.ssa Velia Bruno _____

La presente Determinazione è inviata al Collegio Sindacale in data 10 APR. 2018

La presente Determinazione è esecutiva ai sensi di legge 10 APR. 2018

La presente Determinazione viene pubblicata all'albo pretorio on-line aziendale ai sensi dell'art. 32, comma 1, della legge 18.09.2009, n. 69 e del D.Lgs 14.03.2013 n. 33 in data _____

in oggetto ☐ per esteso ☒ 10 APR. 2018

Rieti lì 10 APR. 2018

IL FUNZIONARIO

acquistinretepa.it

Dati generali della procedura

Numero RDO:	1900322
Descrizione RDO:	Licenze per Servizi Web Security e Content Filtering WEBSENSE – WEB SECURITY GATEWAY ANYWHERE con UPGRADE di quello attualmente in uso e MODULO INTEGRATIVO, per il periodo di 36 mesi per 800 utenti
Criterio di aggiudicazione:	Prezzo piu' basso
Numero di Lotti:	1
Unita' di misura dell'offerta economica:	Valori al ribasso
Amministrazione titolare del procedimento	AUSL RIETI 00821180577 VIA DEL TERMINILLO, 42 RIETI RI
Punto Ordinante	ROBERTO CAMPOGIANI
Soggetto stipulante	Nome: ROBERTO CAMPOGIANI Amministrazione: AUSL RIETI
Codice univoco ufficio - IPA	UFX1HE
(RUP) Responsabile Unico del Procedimento	Roberto Campogiani
Inizio presentazione offerte:	20/03/2018 09:55
Termine ultimo presentazione offerte:	30/03/2018 12:00
Temine ultimo richieste di chiarimenti:	29/03/2018 12:00
Data Limite stipula contratto (Limite validità offerta del Fornitore)	30/05/2018 12:00
Giorni dopo la stipula per Consegna Beni / Decorrenza Servizi:	10
Bandi / Categorie oggetto della RdO:	SERVIZI/Servizi per l'Information & Communication Technology
Numero fornitori invitati:	5
Segnalazione delle offerte anomale:	si

Lotto 1 - Dettagli

Denominazione lotto	Licenze per Servizi Web Security e Content Filtering WEBSENSE – WEB SECURITY GATEWAY ANYWHERE con UPGRADE di quello attualmente in uso e MODULO INTEGRATIVO, per il periodo di 36 mesi per 800 utenti
CIG	7419469382
CUP	
Dati di consegna	Via del terminillo n. 42Rieti - 02100 (RI)
Dati di fatturazione	Aliquota IVA di fatturazione: 22%Indirizzo di fatturazione:Via del terminillo n. 42Rieti - 02100 (RI)
Termini di pagamento	60 GG Data Ricevimento Fattura
Importo dell'appalto oggetto di offerta (base d'asta)	120000,00

Lotto 1 - Schede tecniche

Nome Scheda Tecnica	gg/uomo per Upgrade della versione esistente e sistemazione Proxy
Quantita'	10

I campi contrassegnati con * sono obbligatori

Nr.	Caratteristica	Tipologia	Regola di Ammissione	Valori
1	Marca	Tecnico	Nessuna regola	
2	* Codice articolo produttore	Tecnico	Nessuna regola	
3	* Nome del servizio di manutenzione Software	Tecnico	Nessuna regola	
4	* Descrizione tecnica	Tecnico	Valore unico ammesso	UPGRADE VERSIONE ESISTENTE
5	* Tipo contratto	Tecnico	Valore unico ammesso	Acquisto
6	* Oggetto	Tecnico	Valore unico ammesso	UPGRADE
7	* Modalità di erogazione	Tecnico	Valore unico ammesso	GG/UOMO

8	* Durata del contratto [mesi]	Tecnico	Nessuna regola	
9	* Unità di misura	Tecnico	Nessuna regola	
10	Tipo di manutenzione	Tecnico	Valore minimo ammesso	Manutenzione software
11	Denominazione del software	Tecnico	Nessuna regola	
12	* Prezzo	Economico	Nessuna regola	

Lotto 1 - Schede tecniche

Nome Scheda Tecnica	SW Forcepoint Triton Web Security Gateway Anywhere per 800 utenti 36 mesi
Quantita'	1

I campi contrassegnati con * sono obbligatori

Nr.	Caratteristica	Tipologia	Regola di Ammissione	Valori
1	* Marca	Tecnico	Valore unico ammesso	FORCEPOINT
2	* Codice articolo produttore	Tecnico	Nessuna regola	
3	* Nome del servizio di manutenzione Software	Tecnico	Nessuna regola	
4	* Descrizione tecnica	Tecnico	Valore unico ammesso	RINNOVO SW Forcepoint Triton Web Security Gateway Anywhere
5	* Tipo contratto	Tecnico	Valore unico ammesso	Acquisto
6	* Oggetto	Tecnico	Valore unico ammesso	RINNOVO SW Forcepoint Triton Web Security Gateway

				Anywhere
7	Modalità di erogazione	Tecnico	Nessuna regola	
8	* Durata del contratto [mesi]	Tecnico	Nessuna regola	
9	* Unità di misura	Tecnico	Valore minimo ammesso	Licenza
10	Tipo di manutenzione	Tecnico	Valore minimo ammesso	Manutenzione software
11	Denominazione del software	Tecnico	Valore minimo ammesso	SW SECURITY
12	* N. UTENTI	Tecnico	Valore minimo ammesso	800
13	* PERIODO (MESI)	Tecnico	Valore minimo ammesso	36
14	* Prezzo	Economico	Nessuna regola	

Lotto 1 - Schede tecniche

Nome Scheda Tecnica	Modulo integrativo per analisi in tempo reale di ransomware, nuovi virus e siti sospetti non ancora censiti.
Quantita'	1

I campi contrassegnati con * sono obbligatori

Nr.	Caratteristica	Tipologia	Regola di Ammissione	Valori
1	* Marca	Tecnico	Valore unico ammesso	FORCEPOINT
2	* Codice articolo produttore	Tecnico	Nessuna regola	
3	* Nome del servizio di manutenzione Software	Tecnico	Nessuna regola	
4	* Descrizione tecnica	Tecnico	Valore unico ammesso	MODULO INTEGRATIVO Advanced

				Malware Detection Cloud
5	* Tipo contratto	Tecnico	Valore unico ammesso	Acquisto
6	* Oggetto	Tecnico	Valore unico ammesso	Advanced Malware Detection Cloud - WEB, Modules
7	* Modalità di erogazione	Tecnico	Nessuna regola	
8	* Durata del contratto [mesi]	Tecnico	Valore unico ammesso	36
9	* Unità di misura	Tecnico	Nessuna regola	
10	Tipo di manutenzione	Tecnico	Valore minimo ammesso	Manutenzione software
11	Denominazione del software	Tecnico	Nessuna regola	
12	* Prezzo	Economico	Nessuna regola	

Documentazione Allegata alla RdO

Descrizione	Riferimento	Documento	Link Esterno
Capitolato Tecnico	Licenze per Servizi Web Security e Content Filtering WEBSENSE – WEB SECURITY GATEWAY ANYWHERE con UPGRADE di quello attualmente in uso e MODULO INTEGRATIVO, per il periodo di 36 mesi per 800 utenti	Capitolato Tecnico Websense.doc.p7m (94.84KB)	

Richieste ai partecipanti

Descrizione	Lotto	Tipo	Modalita'	Obbligatorio	Documento

		Richiesta	risposta		unico per operatori riuniti
Eventuale documentazione relativa all'avvalimento	Gara	Amministrativa	Invio telematico	Facoltativo, ammessi più documenti	Si
Eventuali atti relativi a R.T.I. o Consorzi	Gara	Amministrativa	Invio telematico	Facoltativo, ammessi più documenti	Si
Capitolato Tecnico	Licenze per Servizi Web Security e Content Filtering WEBSENSE – WEB SECURITY GATEWAY ANYWHERE con UPGRADE di quello attualmente in uso e MODULO INTEGRATIVO, per il periodo di 36 mesi per 800 utenti	Amministrativa	Invio telematico con firma digitale	Obbligatorio	Si
Offerta Tecnica	Licenze per Servizi Web Security e Content Filtering WEBSENSE – WEB SECURITY GATEWAY ANYWHERE con UPGRADE di quello attualmente in uso e MODULO INTEGRATIVO, per il periodo di 36 mesi per 800 utenti	Tecnica	Invio telematico	Obbligatorio, ammessi più documenti	Si
Offerta Economica (fac-simile di sistema)	Licenze per Servizi Web Security e Content Filtering	Economica	Invio telematico con firma digitale	Obbligatorio	Si

	WEBSENSE – WEB SECURITY GATEWAY ANYWHERE con UPGRADE di quello attualmente in uso e MODULO INTEGRATIVO, per il periodo di 36 mesi per 800 utenti				

Elenco fornitori invitati

Nr.	Ragione Sociale	Partita iva	Codice fiscale	Comune(PR)	Regione	Modalità di inclusione
1	AKITO SRL	03526780543	03526780543	PERUGIA(PG)	UMBRIA	SCELTO
2	ELMEC INFORMATICA	01490000120	01490000120	BRUNELLO(VA)	LOMBARDIA	SCELTO
3	REDCO TELEMATICA	01878730124	07960130156	BUSTO ARSIZIO(VA)	LOMBARDIA	SCELTO
4	SINERGY	11185120158	11185120158	SEGRATE(MI)	LOMBARDIA	SCELTO
5	VAR GROUP SPA	03301640482	03301640482	EMPOLI(FI)	TOSCANA	SCELTO

Relativamente ai Fornitori inclusi con esecuzione di filtri o con sorteggio, i parametri impostati per l'inclusione sono i seguenti: *nessun filtro ulteriore*

ALL. 1
PAG. 1 di 3

SISTEMA SANITARIO REGIONALE
ASL RIETI

REGIONE LAZIO

AZIENDA SANITARIA LOCALE RIETI
Via del Terminillo, 42 – 02100 RIETI - Tel. 0746.2781 – PEC: asl.rieti@pec.it
C.F. e P.I. 00821180577

CAPITOLATO TECNICO

ART. 1 - OGGETTO

La presente capitolato tecnico ha per oggetto la descrizione della fornitura di:

"Licenze per Servizi **Web Security** e **Content Filtering WEBSENSE – WEB SECURITY GATEWAY ANYWHERE e MODULO INTEGRATIVO Advanced Malware Detection Cloud - WEB, Modules,** per il periodo di 36 mesi per 800 utenti

CIG: 7419469382

Il presente documento descrive le caratteristiche tecniche minime e i requisiti di conformità che devono necessariamente rispondere quanto descritto nell'art. 2 del presente capitolato, pena l'esclusione dalla gara.

ART.2 - DESCRIZIONE DELLA FORNITURA

Si richiede la fornitura di licenze per servizi **Web Security** e **Content Filtering** per il periodo di 36 mesi per 800 utenti consistente nei seguenti requisiti minimi:

A) Rinnovo delle licenze per servizi **Web Security** e **Content Filtering**

1) categorizzazione del web, in termini di siti e protocolli, in un database unico
2) Aggiornamento notturno di tutte le categorie siti web e protocolli
3) Gestione intuitiva delle disposizioni del filtro (permetti, blocca, warning, quota di tempo) sulle diverse categorie.
4) Reattività nei 5 minuti ad aggiornamenti relativi alle categorie Security (RTSU – Real Time Security Update) per la gestione proattiva di tutte le nuove minacce in rete.
5) Classificazione Dinamica in ottica web 2.0, e valutazione real time in base per esempio ai puntatori o agli oggetti contenuti nelle pagine
6) Content Analysis di traffico cifrato SSL (https)
7) opzioni di configurazione della policy

Lo strumento permetterà di creare policy avanzate, con numerose opzioni che consentono la massima granularità delle regole. Attraverso l'integrazione con il sistema di autenticazione sarà infatti possibile creare regole sulla base dell'account utilizzato per accedere

all'infrastruttura di rete o dell'appartenenza ad un particolare gruppo definito sulla directory LDAP.

Per ogni categoria sarà quindi possibile definire diverse disposizioni:

Permetti: Categoria di siti permessa
Blocco: Categoria di siti bloccata
Continua: L'utente viene bloccato, una pagina web lo informa del motivo per cui il sito è stato filtrato ed offre all'utente la possibilità di sbloccare la navigazione ed accedere al sito.
Quota Tempo: L'utente visualizza una pagina web che gli consentirà di spendere una serie di gettoni di tempo che consentiranno la navigazione sulle categorie bloccate per un certo numero di minuti. Una volta consumate tutte le sessioni a disposizione l'utente dovrà attendere il giorno successivo per avere nuovi gettoni a disposizione
Blocco per fascia oraria: Il software consentirà di bloccare o permettere l'accesso a determinate categorie anche rispetto a determinate fasce orarie. In questo caso, nella pagina di blocco che l'utente visualizza sarà possibile anche conoscere l'ora in cui un dato sito diverrà disponibile.
Blocco per soglia di Banda: vedi capitolo successivo
Blocco per tipi di file: La policy consentirà di bloccare il download di determinati tipi di file a seconda della categoria di appartenenza del sito che lo ospita.

8) Profilazione Utenze di navigazione

Attraverso l'integrazione con un servizio di directory aziendale consentire di assegnare le policy di navigazione sulla base di:

- Indirizzo IP sorgente
- Subnet
- Nome utente
- Gruppo di Appartenenza

I servizi di directory supportati sono:

- Microsoft Active Directory

Il riconoscimento dell'utente può avvenire in modalità trasparente sia per i sistemi Microsoft attraverso agent di identificazione trasparente in grado di colloquiare con i server di autenticazione.

9) Modulo sicurezza Attiva

bloccare l'accesso a siti classificati come ad alto rischio sicurezza, ovvero siti compromessi o creati ad hoc allo scopo di diffondere in modo silente software malevolo, software Spyware o keylogger volto alla raccolta di dati confidenziali, siti di phishing e bot network.
Contenuti dinamici e siti in continua evoluzione sono analizzati per identificare e bloccare all'occorrenza codice malizioso e pericoloso per la rete.

10) Web Anti-Virus

All.1
Pag. 10 di 13

Il motore di antivirus web deve controllare il flusso dei contenuti per minacce binarie note. L'antivirus web deve proattivo nello scanning delle minacce web, identificare nuovi file maliziosi che si trovano sparsi sulla rete prima che abbiano la possibilità di arrivare da un utente.

11) Controllo Social Web 2.0

Il controllo Social Web consentono all'amministratore di controllare in modo molto granulare alcuni tra i portali Web 2.0 più importanti (**Facebook, Twitter, YouTube, LinkedIn, ecc...**)

12) Funzionalità in-the cloud (SaaS)

Offrire la possibilità di integrare il prodotto installato in casa con i servizi in-the-cloud e gestito attraverso la console unica ed integrata. Questa funzionalità, attivabile in qualsiasi momento deve consentire le seguenti funzionalità:

- Funzione di gestione utenti remoti su rete UMTS
- Funzione di disaster recovery per indisponibilità dei servizi in casa

13) Data loss prevention su canale WEB

14) Gestione di utenti remoti/laptop

15) Assistenza 24 x 7 (servizio di assistenza 24 ore su 24 , 7 giorni su 7)

B) Upgrade di versione e modifiche per l'attivazione del proxy:
   - n° 10 giornate per assistenza specialistica, installazione, training on the job, formazione che verranno fatturate a consuntivo.

C) Modulo integrativo per analisi in tempo reale di ransomware, nuovi virus e siti sospetti non ancora censiti (**Advanced Malware Detection Cloud - WEB, Modules**).

Nell'offerta economica dovranno essere esplicitate le voci per i punti A, B e C.

Art. 3 - FATTURAZIONE

Si precisa che la fattura dovrà essere emessa obbligatoriamente in modalità elettronica, utilizzando il Codice Univoco Ufficio **UFX1HE**.

Art. 4 - LIQUIDAZIONI E PAGAMENTI

Il pagamento delle fatture sarà effettuato a mezzo mandato a 60 (sessanta) giorni dalla data ricevimento della fattura.

Art. 5 - DEPOSITO CAUZIONALE DEFINITIVO

A garanzia dell'esatto adempimento del servizio, ai sensi dell'art. 103 del D.Lgs. m. 50/2016 e s.m.i., l'aggiudicataria dovrà provvedere alla costituzione di un deposito cauzionale definitivo pari al 10% dell'importo contrattuale di fornitura.

La fidejussione bancaria o la polizza assicurativa, che dovrà avere validità per tutta la durata del contratto deve prevedere espressamente la rinuncia al beneficio della preventiva escussione del debitore principale, la rinuncia all'eccezione di cui all'art. 1957, comma 2, del Codice Civile, nonché l'operatività delle garanzie medesime entro 15 (quindici) giorni, a semplice richiesta scritta dell'Azienda USL. La garanzia copre gli oneri per il mancato o inesatto adempimento e cessa di avere effetto solo a seguito del riscontro di regolare esecuzione.

Art. 6 - CESSIONE DEL CREDITO

Il contratto che consegue all'aggiudicazione di gara esclude in modo esplicito e formale la cessione dei crediti della Ditta aggiudicataria, a qualsiasi titolo e per qualsivoglia motivo, se non preventivamente e formalmente autorizzati dall'Azienda Sanitaria (art. 1260 del C.C.).

Art. 7 - IPOTESI DI RISOLUZIONE DEL CONTRATTO

L'Azienda USL si riserva la facoltà di risolvere, ai sensi e per gli effetti dell'art. 1456 c.c., qualora una determinata obbligazione e/o prestazione e/o servizio, oggetto dell'appalto non sia adempiuta o esattamente adempiuta, secondo le modalità previste dalla presente lettera invito.

La risoluzione del contratto potrà avvenire per i seguenti motivi, enunciati a titolo esemplificativo e non esaustivo:

- Applicazione dell'art. 108 del D.Lgs. m. 50/2016 e s.m.i
- Ragioni di pubblico interesse e di cui alla insindacabile valutazione da parte dell'Azienda USL di Rieti;
- Inadempimento (es. mancata attivazione del servizio, personale non in regola con le disposizioni vigenti in materia);
- Sospensione o abbandono del servizio;
- Sopravvenuta incapacità giuridica dell'appaltatore;
- Utilizzo di materiale o attrezzature non in conformità alle vigenti normative;
- Incapacità o negligenza nell'espletamento del servizio (con ripercussioni sull'esatto adempimento dello stesso);
- Comportamento scorretto degli addetti al servizio nei confronti degli utenti o di dipendenti

dell'Azienda USL di Rieti;

ART. 8 - OBBLIGHI DERIVANTI DAL D.P.R. N. 62 DEL 16 APRILE 2013 "REGOLAMENTO RECANTE CODICE DI COMPORTAMENTO DIPENDENTI PUBBLICI, A NORMA DELL'ART. 54 DEL DECRETO LEGISLATIVO 30 MARZO 2001, N. 165"

La Società Fornitrice, ai sensi dell'art. 2, comma 3, del D.P.R. n. 62 del 16 aprile 2013, con riferimento alle prestazioni oggetto del presente contratto, prende atto del Codice di comportamento dei dipendenti pubblici, adottato dall'Azienda USL di Rieti con atto deliberativo n. 89/DG ff. del 31/01/2014, reso disponibile sul sito internet aziendale e si impegna ad osservare ed a fare osservare ai propri collaboratori, a qualsiasi titolo, gli obblighi di condotta in esso previsti.

A tal fine la Società Fornitrice si impegna a trasmettere e mettere a disposizione il richiamato codice aziendale ai propri dipendenti e collaboratori a qualsiasi titolo impiegati nell'appalto. La violazione degli obblighi di cui al D.P.R. n.62/2013 costituisce causa di risoluzione del contratto.
L'Azienda USL, verificata l'eventuale violazione, contesta per iscritto il fatto alla Società Fornitrice assegnando un termine non superiore a dieci giorni per la presentazione di eventuali controdeduzioni. Ove queste non fossero presentate o non risultassero accolte l'Azienda USL, fatto salvo il risarcimento dei danni subiti, procederà alla risoluzione del contratto.

ART. 9- CLAUSOLA ANTI PANTOUFLAGE

Con riferimento all'articolo 53, comma 16-ter, del D. Lgs. 165/2001, la Società aggiudicataria, sottoscrivendo il presente contratto, attesta di non aver concluso contratti di lavoro subordinato o autonomo e comunque di non aver conferito incarichi ad ex dipendenti che hanno esercitato poteri autoritativi o negoziali per conto della Committente e/o della Stazione Appaltante nei propri confronti per il triennio successivo alla cessazione del rapporto.

Art. 10 OBBLIGHI DELL'APPALTATORE RELATIVI ALLA TRACCIABILITÀ DEI FLUSSI FINANZIARI

Ai sensi dell'art. 3 della Legge n. 136 del 07/09/2010 e s.m.i., così come modificato dalla Legge n. 217 del 17/12/2010, a pena di nullità assoluta del contratto stipulato, l'operatore economico aggiudicatario è tenuto al rispetto degli obblighi di tracciabilità dei flussi finanziari.
L'aggiudicatario deve rendere gli estremi identificativi dei conto correnti "dedicato" alla presente commessa pubblica e le generalità e il codice fiscale delle persone delegate ad operare su di essi.

All. 1
PAC. 13/13

Qualora, nel corso del rapporto contrattuale, si dovessero registrare modifiche agli estremi identificativi anzi detti, queste devono essere comunicate entro 7 giorni.

L'aggiudicatario deve riportare il codice CIG assegnato a ciascun lotto, in tutte le comunicazioni e operazioni relative alla gestione contrattuale, e in particolare nel testo dei documenti di trasporto e delle fatture.

L'aggiudicatario deve verificare che nei contratti sottoscritti con i subappaltatori e i subcontraenti della filiera delle imprese a qualsiasi titolo interessate al servizio in oggetto, sia inserita, a pena di nullità assoluta, un'apposita clausola con la quale ciascuno di essi assume gli obblighi di tracciabilità dei flussi finanziari di cui alla legge sopra richiamata.

Art. 11 REQUISITI GENERALI DI PARTECIPAZIONE

Al fine della partecipazione alla gara in oggetto, ai sensi degli artt. 46 e 47, 75 e 76 del D.P.R. 28.12.2000, n. 445 e ss.mm.ii., consapevole delle responsabilità penali cui può andare incontro nel caso di dichiarazioni mendaci, nonché' delle conseguenze amministrative di esclusione dalle gare di cui al d.lgs. 50/2016 e alla normativa vigente in materia, il partecipante sottoscrivendo questo capitolato dichiara di non trovarsi in nessuna delle cause di esclusione di cui all'art. 80 del D.Lgs n. 50/2016.

Art. 12 RINVIO A NORME VIGENTI

Per quanto non espressamente previsto si rinvia al decreto legislativo 50/2016 e alla normativa statale e regionale vigente in materia.

Art. 13 FORO COMPETENTE

Il Foro competente per tutte le controversie giudiziali che dovessero insorgere in dipendenza della presente lettera invito, sarà esclusivamente quello di Rieti.

Art. 14 ACCETTAZIONE

La società aggiudicataria accetta tutte le clausole sopra riportate, nessuna esclusa od eccettuata.

Letto, approvato, si sottoscrive digitalmente per accettazione.

Il presente capitolato dovrà essere firmato digitalmente e allegato alla Documentazione Amministrativa.

acquistinretepa.it
Il Portale degli acquisti della Pubblica Amministrazione

Riepilogo delle attivita' di Esame delle Offerte ricevute

Numero RDO:	1900322
Descrizione RDO:	Licenze per Servizi Web Security e Content Filtering WEBSENSE – WEB SECURITY GATEWAY ANYWHERE con UPGRADE di quello attualmente in uso e MODULO INTEGRATIVO, per il periodo di 36 mesi per 800 utenti
Criterio di aggiudicazione:	Prezzo piu' basso
Unita' di misura dell'offerta economica:	Valori al ribasso
Amministrazione titolare del procedimento	AUSL RIETI 00821180577 VIA DEL TERMINILLO, 42 RIETI RI
Punto Ordinante	ROBERTO CAMPOGIANI
Soggetto stipulante	Nome: ROBERTO CAMPOGIANI Amministrazione: AUSL RIETI
Codice univoco ufficio - IPA	UFX1HE
(RUP) Responsabile Unico del Procedimento	
Inizio presentazione offerte:	20/03/2018 09:55
Termine ultimo presentazione offerte:	30/03/2018 12:00
Temine ultimo richieste di chiarimenti:	29/03/2018 12:00
Data Limite stipula contratto (Limite validità offerta del Fornitore)	30/05/2018 12:00
Giorni dopo la stipula per Consegna Beni / Decorrenza Servizi:	10
Bandi / Categorie oggetto della RdO:	SERVIZI/Servizi per l'Information & Communication Technology

Lotto esaminato: 1 Licenze per Servizi Web Security e Content

Filtering WEBSENSE – WEB SECURITY GATEWAY ANYWHERE con UPGRADE di quello attualmente in uso e MODULO INTEGRATIVO, per il periodo di 36 mesi per 800 utenti

CIG	7419469382
CUP	
Oggetto di Fornitura 1	gg/uomo per Upgrade della versione esistente e sistemazione Proxy/10/
Oggetto di Fornitura 2	SW Forcepoint Triton Web Security Gateway Anywhere per 800 utenti 36 mesi/1/
Oggetto di Fornitura 3	Modulo integrativo per analisi in tempo reale di ransomware, nuovi virus e siti sospetti non ancora censiti./1/
Importo dell'appalto oggetto di offerta (base d'asta)	120000,00

Concorrenti

#	Denominazione	Forma di Partecipazione	Partita IVA	Data Invio Offerta
1	AKITO SRL	Singola	03526780543	27/03/2018 15:03
2	REDCO TELEMATICA	Singola	01878730124	28/03/2018 15:15

ESAME DELLA BUSTA AMMINISTRATIVA	Inizio	Fine
	30/03/2018 15:23:43	30/03/2018 15:28:45

Richieste Amministrative di Gara

Concorrente	Eventuale documentazione relativa all'avvalimento		Eventuali atti relativi a R.T.I. o Consorzi	
	Valutazione	Note	Valutazione	Note
AKITO SRL		nessuna		nessuna

REDCO TELEMATICA		nessuna		nessuna

Richieste Amministrative di Lotto

Concorrente	Capitolato Tecnico	
	Valutazione	Note
AKITO SRL	Approvato	nessuna
REDCO TELEMATICA	Approvato	nessuna

ESAME DELLA BUSTA TECNICA	Inizio	Fine
	30/03/2018 15:28:56	30/03/2018 15:31:02

Concorrente	Offerta Tecnica	
	Valutazione	Note
AKITO SRL	Approvato	nessuna
REDCO TELEMATICA	Approvato	nessuna

ESAME DELLA BUSTA ECONOMICA	Inizio	Fine
	30/03/2018 15:31:12	30/03/2018 15:37:57

Concorrente	Offerta Economica (fac-simile di sistema)	
	Valutazione	Note
AKITO SRL	Approvato	nessuna
REDCO TELEMATICA	Approvato	nessuna

Classifica della gara (Prezzo più basso)

Concorrente	Valore complessivo dell'Offerta
AKITO SRL	113700,00
REDCO TELEMATICA	118900,00

Note di gara	nessuna
Note specifiche lotto 1	nessuna

AKITO
IT FOR CHOICE

QUINEL
Azienda certificata ISO/IEC 27001:2013, certificato n° C - 0002

Spett.le
Azienda USL Rieti
Via del Terminillo,42
02100 Rieti

Roma, 27 marzo 2018

Ns. Rif. :18_GF_ASL Rieti_Forcepoint

Oggetto: Documentazione Tecnica gara Forcepoint – R.d.O. Mepa n° 1900322

Con riferimento alla gara in oggetto e alla relativa richiesta di documentazione tecnica, siamo a confermare che il contenuto della nostra proposta risponde a quanto da voi dichiarato nel capitolato tecnico della gara stessa.

Ad ulteriore completamento delle informazioni sulla soluzione Forcepoint alleghiamo anche un documento ufficiale del produttore.

Le attività richieste saranno svolte, in accordo tra le parti, per:
-aggiornare la versione della soluzione esistente, già in uso presso la ASL, all'ultima versione possibile
-attivare le funzionalità di proxing, attraverso nuova configurazione del sistema
-installare e attivare il nuovo modulo di sanboxing cloud web

Ringraziando per la cortese attenzione, colgo l'occasione per porgere distinti saluti.

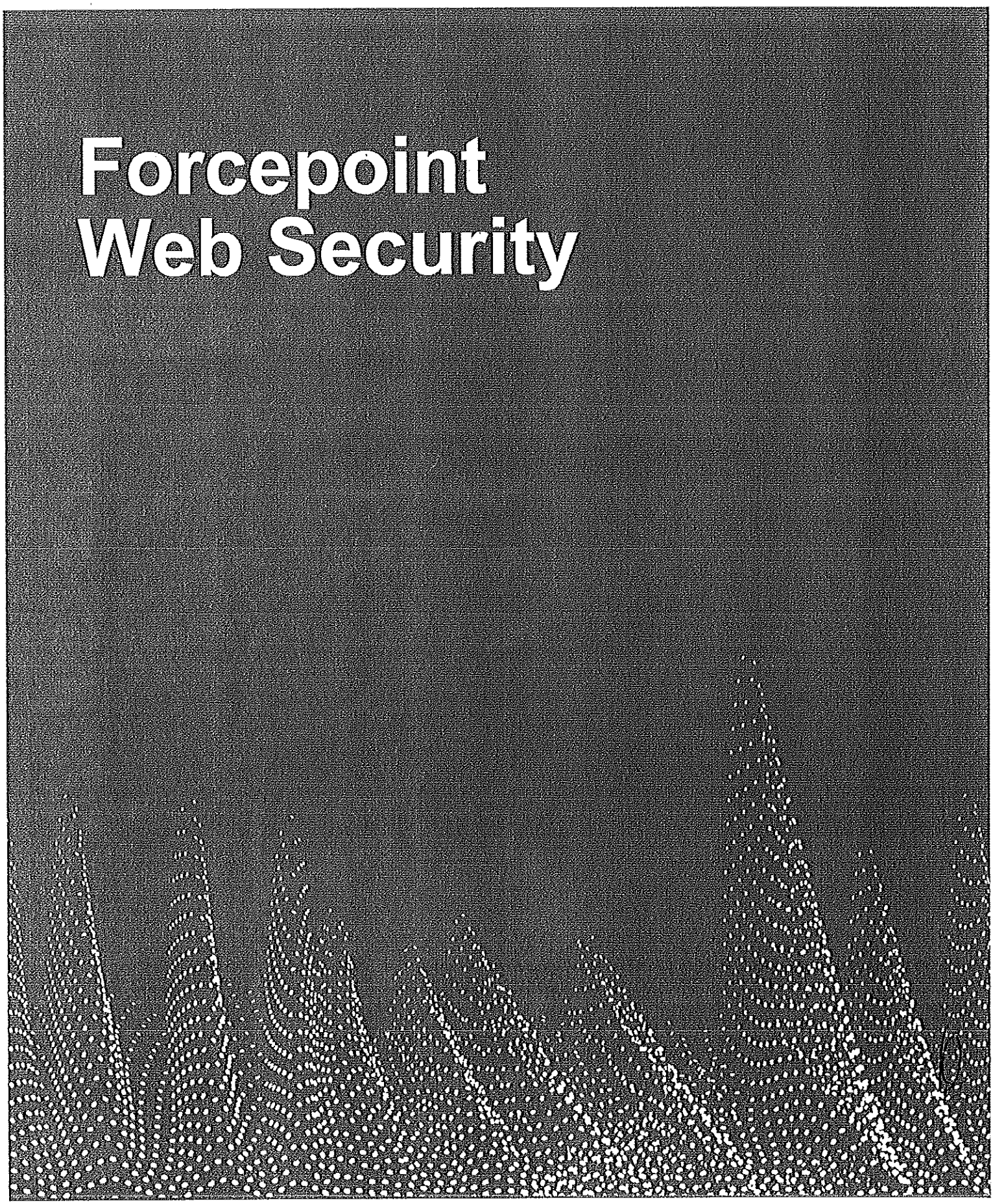
AKITO SRL
Giulio Faita

Akito s.r.l.
Sede legale Perugia: Strada Lacugnano Giardino 14 Cap 06132 - Fax: 0759975563 - P.I. 03526780543 - C.F. 03526780543
Capitale Sociale 80.000,00 Euro I. V. REA 295560
Filiale Roma: Via Riccardo Gigante 18 Cap 00143 - Fax: 06.88921039 - Tel. 06.88921039

AL-3
RAC-2(a)

FORCEPOINT
POWERED BY Raytheon

Forcepoint Web Security



ALL 3
PAG. 3 di 20

Introduzione

Il 2015 è stato un anno particolarmente attivo dal punto di vista della sicurezza, molto significativo il seguente passaggio tratto dal rapporto di sicurezza Clusit 2015:

"La vera questione per i difensori (con riferimento ai dati, alle infrastrutture informatiche ed a tutti quei servizi, molti dei quali critici, oggi realizzati tramite l'ICT) non è più "se", ma "quando" si subirà un attacco informatico (dalle conseguenze più o meno dannose), e quali saranno gli impatti conseguenti".

Nel rapporto Clusit 2016 tale affermazione è stata ripresa e confermata:

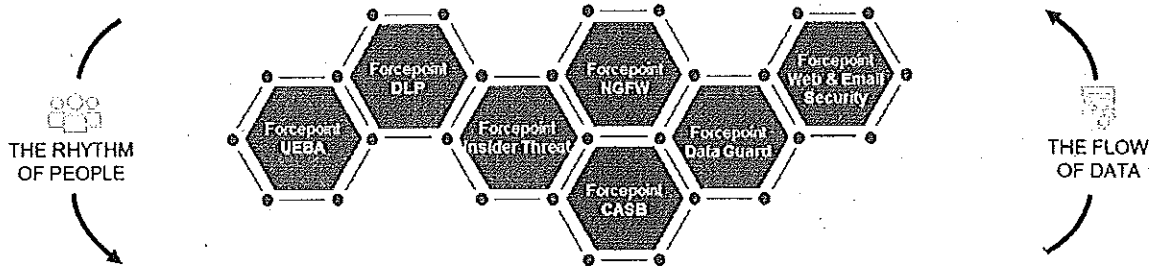
"Questa tendenza si è ulteriormente consolidata nell'anno passato e nel 2016 il principale problema non sarà tanto che si verrà attaccati (tutti lo sono ormai costantemente, per lo più tramite sistemi automatizzati, nella sfera personale e professionale, per i motivi più disparati), ma quali saranno gli impatti degli attacchi andati a buon fine sulla sicurezza di organizzazioni, utenti, clienti e partner, e come impedire al maggior numero possibile di incidenti di verificarsi."

La riduzione di budget dedicato alla Cyber Security contrasta con la diffusione sempre più ampia di malware avanzati di cui i Ransomware (Cryptolocker, CryptoWall e CBTLocker i più comuni) sono solo la punta di un Iceberg enorme fatto di migliaia di possibili malware che vengono riversati sul marcato underground ed aggiornati con cadenza giornaliera.
Con la diffusione di tecnologie quali social media, internet of things e dispositivi portatili sempre più complessi e connessi con la realtà aziendale diventa sempre più difficile monitorare e proteggere il proprio core business. In un momento storico in cui tutte le aziende spingono verso la digitalizzazione dei contenuti e sulla mobilità degli utenti diventa sempre più complesso trovare il giusto equilibrio tra disponibilità e fruizione dei contenuti e sicurezza. Spesso dati critici come elenchi clienti, informazioni di pagamento o finanziarie, documenti riservati o progetti d'ingegneria possono transitare attraverso supporti esterni, caselle di posta personali o dispositivi mobili.
In uno scenario di minacce in continua evoluzione che si pongono come unico obiettivo la catturare di dati riservati o sensibili è necessaria una soluzione avanzata in grado di proteggere le informazioni senza essere invasiva, ma sopratutto fornire visibilità su rischi e minacce che riescono a superare il perimetro di sicurezza per ridurre quanto più possibile la finestra di infezione.
Forcepoint, azienda leader su scala mondiale nelle soluzioni di sicurezza integrata per Web, email e dati, fornisce la propria tecnologia a più di 44 milioni di dipendenti in organizzazioni in tutto il mondo. Forcepoint è una azienda unica nel settore della sicurezza dei contenuti: la protezione delle informazioni sensibili è al centro della nostra attività.
Le soluzioni di Forcepoint sono utilizzate in comparti quali sanitario, finanziario, bancario, assicurativo, nella pubblica amministrazione, nel manifatturiero, nel settore legale, tecnologico, nella distribuzione, nei servizi e nell'istruzione.

All. 3
Pag. 1 di 20

1. UNIFIED SECURITY

Forcepoint offre un'ampia gamma di soluzioni in grado di rispondere alle esigenze di sicurezza e di protezione di infrastrutture, utenti e dati di aziende ed enti governativi.
Le soluzioni Forcepoint sono nativamente integrate e collaborano tra loro per innalzare il livello di visibilità rispetto alle minacce attuali legate a quello che ormai viene definito lo "Zero Perimeter World".
Qualunque sia il punto di partenza, le soluzioni Forcepoint consentono di espandere il livello di sicurezza seguendo il ritmo dei vostri utenti ed il flusso dei vostri dati



ANALYTICS MANAGEMENT ORCHESTRATION

FORCEPOINT WEB

La soluzione gateway per la protezione della navigazione di Forcepoint protegge i principali canali di infezione web.
Disponibili in configurazione totalmente on premise, ibrida o full cloud, questi prodotti consentono di rispondere alle esigenze architetturali di ogni azienda.

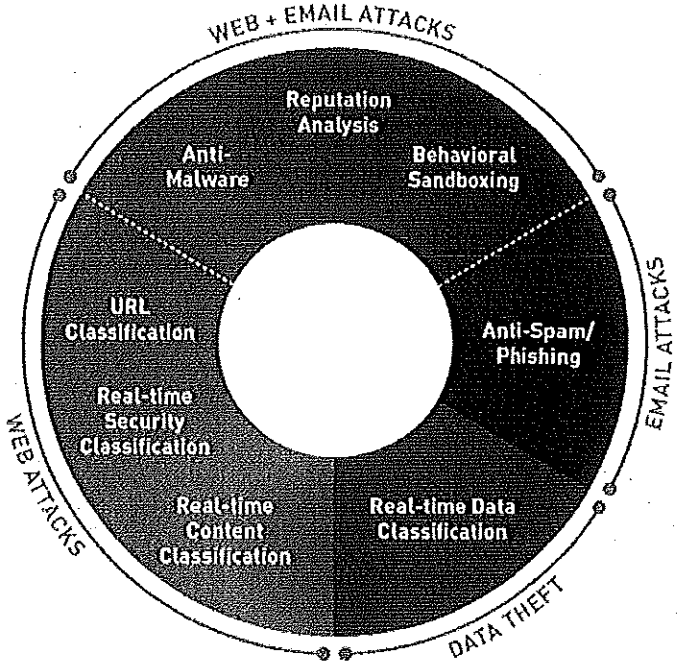
Forcepoint Web security offre i più alti livelli di sicurezza presenti sul mercato per indirizzare le minacce tradizionali come quelle più moderne ed i cosiddetti Zero Day, garantendo la massima protezione.

FORCEPOINT ADVANCED MALWARE DETECTION

Forcepoint Advanced Malware Detection (AMD) è un sistema di protezione avanzata dal malware, soprattutto dagli attacchi cosiddetti "zero day".
Come prodotto nativamente integrato con Forcepoint Web, sarà sufficiente fare click sul tab dadicato per attivare il servizio attraverso il cloud per alta affidabilità, scalabilità e zero gestione.

Come in una Sandbox, Forcepoint AMD fornisce un ambiente simulato per l'esecuzione del malware ma a differenza dei sistemi tradizionali di sandboxing che hanno visibilità solo a livello di sistema operativo, Forcepoint offre un ambiente unico di isolamento ed ispezione che simula l'intero host, incluse le CPU, la RAM e tutti i device.
Una inspezione approfondita integragisce con il malware per osservarne tutte le azioni possibili all'interno di questo environment completo ed è in grado di identificare anche codice dormiente per analisi particolari.
Tutto questo ha permesso a questo sistema di ottenere un rate del 100% di identificazione del malware con 0 falsi positivi nei test di NSS Labs.

FP ADVANCED CLASSIFICATION ENGINE



La tecnologia alla base di tutte le soluzioni Forcepoint si chiama Advanced Classification Engine o ACE.
ACE utilizza difese contestuali online e in tempo reale per il web, le email, i dati e la sicurezza mobile grazie ad un sistema di classificazione composita del rischio e analisi predittive per garantire la sicurezza più efficace disponibile sul mercato. ACE minimizza l'esposizione a rischi mediante un'analisi del traffico in ingresso e in uscita e difese orientate ai dati per la protezione contro il furto.
Oltre 10.000 analisi in otto aree di difesa includono classificatori in tempo reale, sandboxing comportamentale e altre funzionalità avanzate, permettendo ad ACE di rilevare e bloccare più minacce.
ACE è il principale dispositivo di difesa alla base delle soluzioni Forcepoint SECURITY MANAGER ed è supportato da Forcepoint ThreatSeeker® Intelligence Cloud, che raccoglie dati da oltre 900 milioni di endpoint e analizza da 3 a 5 miliardi di richieste web al giorno.
Di seguito entreremo nel merito di tutti i moduli che fanno parte del motore ACE.

URL CLASSIFICATION

Tutta la conoscenza e la categorizzazione del web, in termini di siti e protocolli, è racchiusa in un database unico per la sua completezza e il suo livello di aggiornamento. Forcepoint si appoggia su un database che categorizza URL e protocolli e ad oggi contiene oltre 60 milioni di siti Web. Il Forcepoint Master Database rappresenta il database più completo al mondo per la categorizzazione del web:

- Aggiornamento notturno di tutte le categorie per 60 milioni di siti web e 120 protocolli, in oltre 50 lingue.
- Gestione intuitiva delle disposizioni del filtro (permetti, blocca, warning, quota di tempo) sulle diverse categorie.
- Reattività nei 5 minuti ad aggiornamenti relativi alle categorie Security (RTSU – Real Time Security Update) per la gestione proattiva di tutte le nuove minacce in rete.

L'aggiornamento del database è automatico e giornaliero. Il database potrà inoltre essere customizzato in base alle esigenze specifiche, con creazione di nuove categorie e ricategorizzazione di siti specifici.
Il database viene utilizzato non solo dalla soluzione WEB per la gestione della navigazione ma anche dalla soluzione MAIL che lo utilizza per analizzare gli indirizzi URL incastonati all'interno dei messaggi di posta elettronica.

REAL-TIME CONTENT CLASSIFICATION

CATEGORIZZAZIONE DI SITI E APPLICAZIONI WEB 2.0

Siti in ottica Web 2.0 come per esempio facebook, twitter, linked-in e Blog offrono la possibilità di personalizzare le pagine e creare veri e propri siti personali, è quindi riduttiva una categorizzazione statica del dominio come "Social Networking", considerando che lo stesso può ospitare pagine per esempio di natura diversa. Da un'analisi quindi degli elementi nelle pagine realmente richieste (linguaggio, immagini, colori, fonts, titoli, background, ecc...) è possibile categorizzare porzioni di sito (quelle relative a particolari utenti) in real time con algoritmi proprietari Forcepoint.
Sempre in ottica Web 2.0, usando algoritmi proprietari implementati on board del proxy, tutti i siti non

categorizzati possono essere analizzati per valutare una categorizzazione real time in base per esempio ai puntatori o agli oggetti contenuti nelle pagine con una riduzione significativa del costo totale di esercizio della soluzione.

ANTI-MALWARE ENGINE

Il motore di anti-malware onboard controlla il flusso dei contenuti per minacce binarie note. Differisce da uno standard per il fatto che le signatures sono create e distribuite al motore AV onboard direttamente dalla rete ThreatSeeker la quale, proattivo nello scanning delle minacce web, identifica nuovi file maliziosi che si trovano sparsi sulla rete prima che abbiano la possibilità di arrivare da un cliente. Al contrario, con i motori AV standard si possono solo generare firme in risposta ad un report di minaccia conosciuta generata da un cliente.
Il motore Antimalware di Forcepoint utilizza inoltre le seguenti tecniche per migliorare la sua efficacia:

- Class based signatures: identifica nuove varianti di malware sulla base di elementi in comune e condivisi tra molti virus polimorfici e worm
- Heuristics: identifica varianti di malware basate su packer e fingerprint di function call

Tutti i file maliziosi riscontrati sono immediatamente registrati e cancellati. La soluzione ha la possibilità di ispezionare i file archiviati e compressi e i parametri di controllo sono configurabili dalla console del sistema.

REAL TIME SECURITY SCANNING

Il sistema Real Time Security Scanning (RTSS) è un esclusivo meccanismo di rilevamento del malware, che deriva dalle analitiche di detection di malware ThreatSeeker. I RTSS combinano una serie di tecniche che sono progettate per rilevare gli attacchi conosciuti e sconosciuti e vengono propagati in diversi modi. Il cuore del sistema è l'uso di un profilo delle minacce. RTSS utilizza le versioni onboard delle analytics ThreatSeeker per normalizzare tutti gli elementi di un sito web e li paragona con gli elementi contenuti all'interno dei profili che rappresentano gli elementi comuni contenuti nei siti dannosi. Questa analisi è combinata con altri meccanismi di seguito elencati:

- Analisi generica di tipo Web Kit: questo sistema identifica i tool kit usati per generare nuovi exploit attraverso l'analisi delle impronte digitali derivati dalla tecnologia Forcepoint DLP
- Analisi di Exploit: è un sottoinsieme delle analitiche di exploit e analizza elementi contenuti negli script che sono progettati per compromettere i flussi di applicazioni
- Analisi di obfuscation: questo sistema analizza gli elementi di script utilizzati per occultare codice maligno incorporato in routine comuni
- Analisi di shell code: analizza il contenuto per shell code noti e le tecniche di heap spray compromise.

REPUTATION ANALYSIS

Il sistema di reputazione Forcepoint è alla base delle soluzioni WEB SECURITY ed EMAIL SECURITY e consente non solo di bloccare connessioni verso siti o server di posta noti come fonte di malware o SPAM ma anche di caratterizzare la reputazione di un sito contribuendo a denire il livello di analitiche da attivare.

BEHAVIORAL SANDBOX

La soluzione di sandboxing di Forcepoint analizza i comportamenti dei file web ed email per scoprire minacce nuove, avanzate e persistenti, fornendo all'administrator una reportistica di tipo forense in maniera rapida ed efficace.
Forcepoint integra le funzionalità Sandbox all'interno della console Security Manager per garantire una sinergia tecnologica unica fra le soluzioni Web, Email e Data security, basate sul motore di Advanced Classification Engine, ACE.

All-3
Pag. 712

Il modulo di Sandboxing consente una gestione in solo monitoraggio per il canale WEB, ovvero nel caso si proceda al download di un contenuto "sospetto" non si blocca l'utente ma parallelamente al download il contenuto viene inviato anche al modulo sandbox che procede a detonare il file ed analizzarne il comportamento. Per quanto riguarda il canale Email è invece disponibile anche la modalità di enforcing.

1. LA SOLUZIONE WEB SECURITY

FORCEPOINT WEB SECURITY rappresenta la soluzione più accurata ed efficace per il controllo dei contenuti Web 2.0 e la protezione contro le minacce di nuova generazione, permettendo alle aziende di valorizzare i processi di business senza preoccuparsi di tematiche quali sicurezza, produttività e rischi per l'affidabilità come contenuti pericolosi e inappropriati e perdita dei dati.
WEB SECURITY è in grado di offrire un deployment flessibile e dinamico: ovvero può essere implementata come soluzione software, come appliance o, aggiungendo il modulo Hybrid, in modo Ibrido integrando una parte software as a service.
Qualsiasi sia il tipo di implementazione scelta sarà possibile utilizzare la soluzione attraverso l'interfaccia unificata Security Manager.

CARATTERISTICHE TECNICHE

Alla base della soluzione WEB SECURITY ci sono le funzionalità di Web Proxy e Cache, integrabili con sistemi di autenticazione basati su LDAP, da implementare in linea rispetto alla navigazione dell'utenza.
Il proxy può essere implementato in due modalità, explicit e transparent o entrambe contemporaneamente.
La soluzione WEB SECURITY integra i motori di:

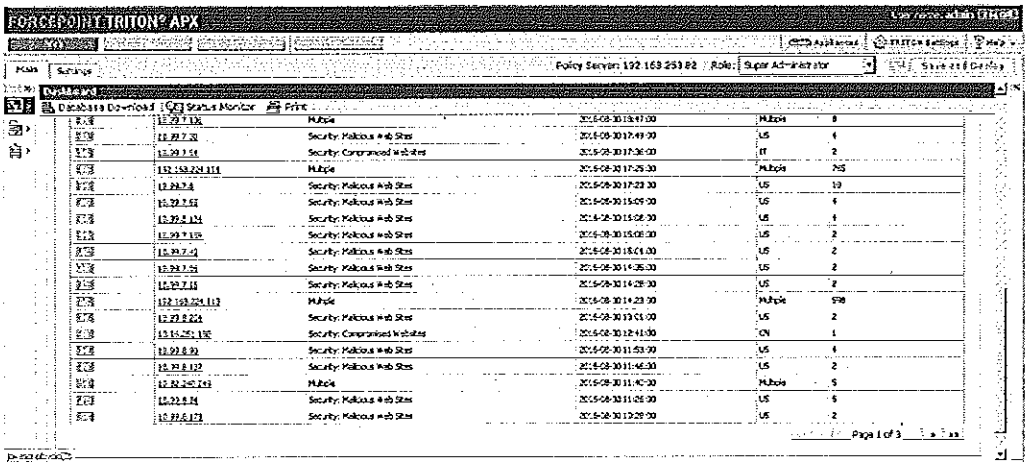
- URL Filtering
- Anti-Malware Engine
- Reputation Analysis
- Real-Time Categorization
- Real-Time Security Scanning.
- Monitoraggio Application Cloud

Alla soluzione di base possono essere successivamente aggiunti i moduli aggiuntivi per sfruttare le funzionalità avanzate di sicurezza.
Di seguito presentiamo la lista delle caratteristiche fondamentali della soluzione WEB SECURITY.

SECURITY THREAT DASHBOARD

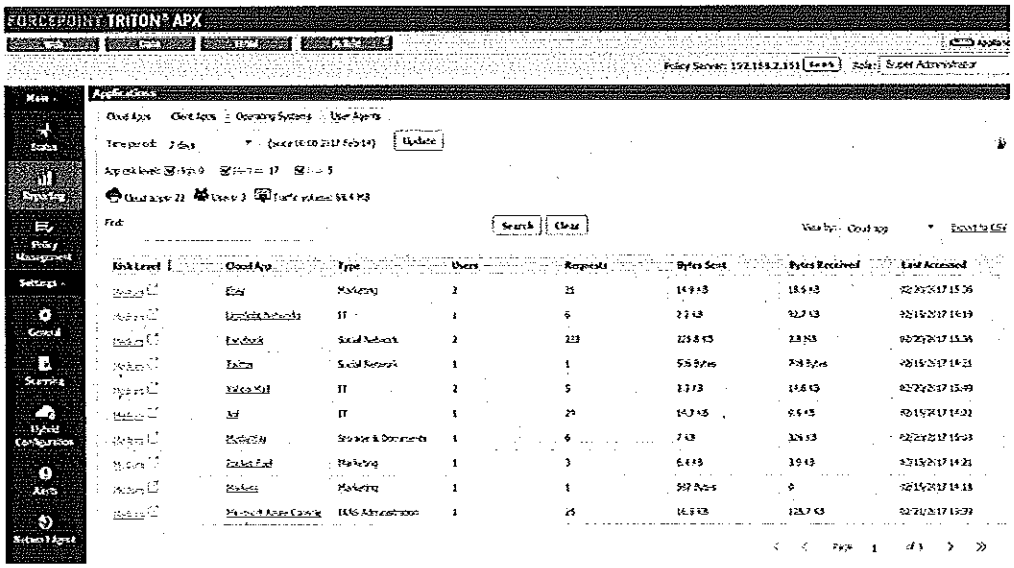
Una delle funzionalità più importanti introdotte riguarda la visibilità e la correlazione di incidenti di sicurezza attraverso una dashboard dedicata.
Ogni incidente viene classificato rispetto ad una scala di valori basata su quattro diversi livelli di guardia a partire dallo stato LOW fino a CRITICAL; ogni incidente viene geolocalizzata all'interno di una mappa interattiva con la quale l'amministratore può interagire.

Incidenti multipli da parte dello stesso utente sono aggregati in una lista unica completa di tutti i dettagli, di seguito un esempio molto esplicativo che mostra non solo i dettagli relativi all'utente ed alla minaccia ma, in integrazione con il modulo AP-DATA, anche i dettagli del dato inviato in upload.



MONITORAGGIO CLOUD APPLICATION

A partire dalla release 8.3 WEB SECURITY implementa un nuovo engine di analisi basato su tecnologia CASB in grado di monitorare tutte le Cloud Apps che transitano attraverso il sistema. Un database Cloud Apps è incluso nel software di protezione web. Una dashboard dedicata permette di analizzare non solo i dati di traffico e gli utenti che le utilizzano, ma anche il livello di rischio associato ad ognuna ed i dettagli di ogni singola App.



Con l'ultima versione è inoltre possibile attivare blocchi di cloud app non adeguate alle policy aziendali.

Queste funzionalità che permettono visibilità e blocco costituiscono un opportunità di miglioramento nel garantire la sicurezza dei dati aziendali.

Le cloud app sono state aggiunte come ulteriore categoria disponibile nelle policy in modo da facilitare anche il processo di attivazione.

LE OPZIONI DI CONFIGURAZIONE DELLA POLICY

Lo strumento permetterà di creare policy avanzate, con numerose opzioni che consentono la massima granularità delle regole. Attraverso l'integrazione con il sistema di autenticazione sarà infatti possibile creare regole sulla base dell'account utilizzato per accedere all'infrastruttura di rete o dell'appartenenza ad un particolare gruppo definito sulla directory LDAP.
Per ogni categoria sarà quindi possibile definire diverse disposizioni:

- Permetti: Categoria di siti permessa

- Blocco: Categoria di siti bloccata
- Continua: L'utente viene bloccato, una pagina web lo informa del motivo per cui il sito è stato filtrato ed offre all'utente la possibilità di sbloccare la navigazione ed accedere al sito.
- Quota Tempo: L'utente visualizza una pagina web che gli consentirà di spendere una serie di gettoni di tempo che consentiranno la navigazione sulle categorie bloccate per un certo numero di minuti. Una volta consumate tutte le sessioni a disposizione l'utente dovrà attendere il giorno successivo per avere nuovi gettoni a disposizione
- Blocco per fascia oraria: Il software consentirà di bloccare o permettere l'accesso a determinate categorie anche rispetto a determinate fasce orarie. In questo caso, nella pagina di blocco che l'utente visualizza sarà possibile anche conoscere l'ora in cui un dato sito diverrà disponibile.
- Blocco per soglia di Banda: vedi capitolo successivo

Blocco per tipi di file: La policy consentirà di bloccare il download di determinati tipi di file a seconda della categoria di appartenenza del sito che lo ospita.

- Policy dedicate per la navigazione quando l'utenza e' all'esterno dall'ufficio, garantendo cosi massima flessibilità e protezione.

PROFILAZIONE UTENZE DI NAVIGAZIONE

Attraverso l'integrazione con un servizio di directory aziendale la soluzione consente di assegnare le policy di navigazione sulla base di:

- Indirizzo IP sorgente
- Subnet
- Nome utente
- Gruppo di Appartenenza o Organizzational unit

I servizi di directory supportati sono:

- Microsoft Active Directory
- Novell E-Directory
- Sun Directory

Il riconoscimento dell'utente avviene in modalità trasparente per i sistemi Microsoft grazie al protocollo NTLM o Kerberos.
Nel caso di integrazione a server LDAP la gestione dei gruppi di navigazione può avvenire grazie all'utilizzo di opzioni LDAP inserite all'interno del Full Distingued Name.

PORT AGNOSTIC MONITORING - FORCEPOINT APPLICATION CONTROL

WEB SECURITY include un controllo delle applicazioni e dei protocolli di sistema che monitora e controlla più di 150 applicazioni come File Transfer, E-Mail, IM, P2P, video streaming e accesso remoto. Inoltre il sistema monitorizza e blocca comunicazioni in uscita da parte dei clienti "botnet" e identifica i tentativi di comunicazione da altri agenti dannosi come worm di rete.
Il rilevamento e controllo di applicazioni che utilizzano protocolli e porte diverse da HTTP, HTTPS e FTP avviene tramite la tecnologia di Forcepoint Network Agent. Il Network Agent si connette al segmento di rete protetto attraverso una porta span o un dispositivo tap e controlla tutto il traffico visibile sul segmento. I protocolli di applicazione sono identificati attraverso delle fingerprint che vengono create e distribuite dai Forcepoint Security Labs attraverso il sistema di Real Time Security Update. Le fingerprint di rete consentono l'identificazione ed il controllo delle applicazioni che utilizzano la tecnica di "port hopping" per aggirare i meccanismi di controllo normale.
Le sessioni di traffico delle applicazioni possono essere registrate per ulteriori analisi, rendendo disponibili i seguenti meccanismi di controllo attraverso il sistema di gestione unificata delle policy:

- Block: sessioni di applicazioni possono essere bloccate utilizzando la tecnologia TCP Reset. Il blocco basato su policy è granulare ed a gruppi di utenti diversi può essere consentito o negato l'uso di applicazioni specifiche
- Allow: alcuni gruppi di utenti possono essere autorizzati ad utilizzare applicazioni particolari
- Log: offre la possibilità di registrare i dati di utilizzo di un protocollo da parte di utenti o gruppi

Protocolli personalizzati possono essere definiti dall'amministratore tramite porte TCP o UDP, intervallo di porte o di indirizzi IP. Le capacità di controllo sopra elencate possono quindi essere applicate ai protocolli personalizzati e utilizzate per costruire policy, in modo da rendere la soluzione port agnostic.

SOCIAL WEB 2.0 CONTROLS

I Social Web controls consentono all'amministratore di controllare in modo molto granulare alcuni tra i portali Web 2.0 più importanti, di seguito alcuni esempi:

- Facebook
- Twitter
- YouTube
- LinkedIn

Nel caso di facebook sarà quindi possibile bloccare in modo selettivo lo scambio di messaggio, la richiesta di amicizia, l'upload di foto o video fino ad arrivare a fornire all'utenza il solo accesso senza possibilità di effettuare azioni attive ma solo la consultazione del social network.

SSL INSPECTION

Il traffico https può rappresentare una back door per ogni policy di sicurezza, dato che ogni contenuto così veicolato non può normalmente essere sottoposto ai consueti controlli; nel 2017 circa la metà del traffico internet è criptato. Con questo modulo Forcepoint è possibile decifrare il traffico SSL, così da avere una reale ed efficate analisi dei contenuti, per poi cifrare il traffico in uscita e consentire che la comunicazione sia completa. Il modulo è quindi "in the middle" della trasmissione SSL.
Molto spesso l'introduzione di una tecnologia invasiva come l'ispezione HTTPS risulta di difficile applicazione, per questo il motore ACE offre la possibilità di Bypass delle funzionalità di ispezione per intere categorie di siti Web, sarà quindi possibile effettuare il controllo solo sulle categorie di siti di interesse mentre non effettuare alcun controllo su siti considerati a rischio di privacy.

BANDWIDTH OPTIMIZER

È lo strumento che permette di stabilire le priorità sul tipo di accesso alla risorsa banda, per prediligere le attività business-critical a discapito di quelle non legate all'attività professionale.
La discriminazione può avvenire secondo due modalità:

- Soglia in uscita: le nuove richieste di banda vengono rifiutate quando il traffico totale in uscita supera il livello stabilito.
- Soglia per applicazione: le nuove richieste per un'applicazione specifica vengono rifiutate quando la banda totale utilizzata per tale applicazione supera la soglia stabilita.

INTEGRAZIONE SIEM E PROTOCOLLO SYSLOG

Forcepoint supporta l'invio di log a strumenti di correlazione esterni attraverso il protocollo SYSLOG. Nativamente la soluzione supporta i formati CEF, LEEF e in alternativa è possibile selezionare un formato customizzato con il quale definire tutti i parametri in modo personalizzato. Grazie a questo, la soluzione può inoltrare gli eventi a qualsiasi strumento SIEM o di log manager in uso.

All. 3
PAC 12820

DELEGATED ADMINISTRATION

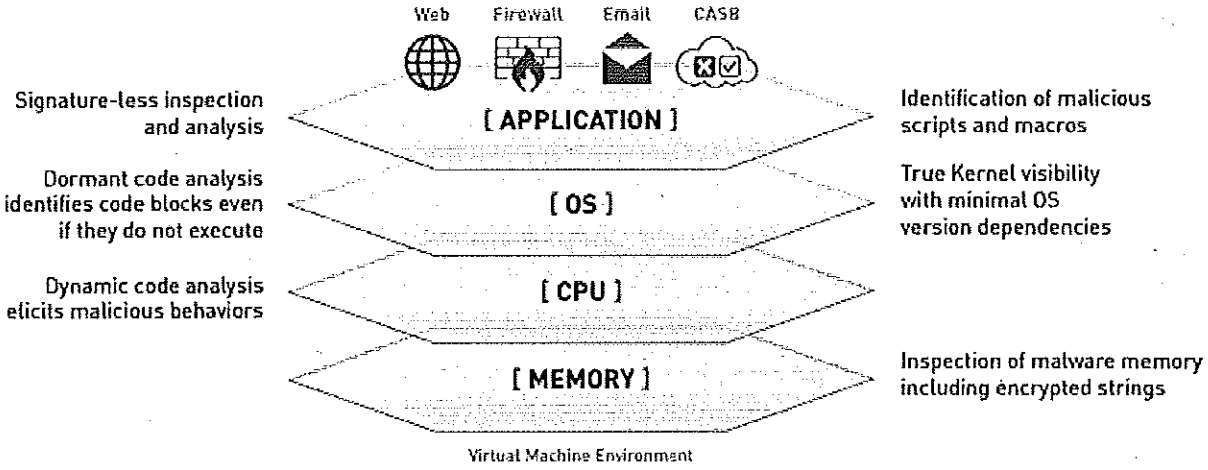
La soluzione consente di gestire le policy tra dipartimenti, organizzazioni e server remoti con distribuzione centralizzata della configurazione. Semplifica il controllo distribuito delle policy di sicurezza per una maggiore flessibilità e massimo controllo, in dettaglio questa funzionalità consente di:

- Definire una serie di ruoli ai quali associare determinati utenti (tramite OU o Gruppi di Active Directory) o Subnet
- Definire una lista di categorie bloccate che gli utenti delegati non possono sbloccare
- Denire degli accessi di audit in grado di verificare la configurazione di tutti i ruoli ma senza l'autorità per effettuare una modifica.
- Per ogni ruolo l'amministratore delegato potrà gestire a proprio piacimento tutte le categorie non bloccate dalla corporate, ricategorizzare determinati URL (configurazione valida solo per il proprio ruolo) ed accedere alla reportistica in modo anonimo o completo.
- Definire chi può gestire la sezione di cloud app.

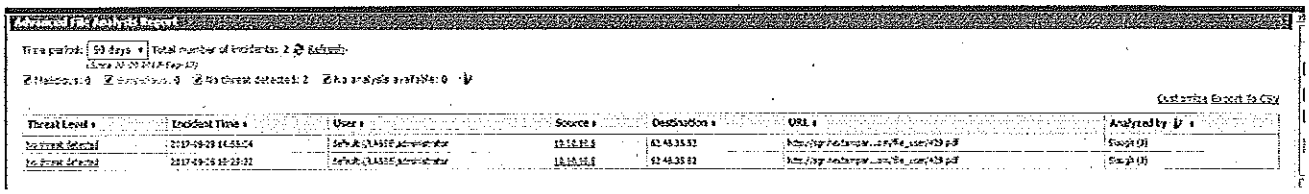
Nella figura successiva viene presentato un esempio di gestione delegata, ogni ruolo è legato ad una particolare OU dove vengono definiti uno o più utenti in grado di accedere la configurazione e fare delle modifiche. L'utente 3 è inoltre gestore della propria OU ma può accedere i log della OU marketing per verificare la gestione degli utenti.

REPORTISTICA AVANZATA

La reportistica avanzata di Forcepoint consente di archiviare su un database SQL tutte le informazioni relative alla navigazione, comprensive di utente e gruppo che ha richiesto la pagina. I dati possono essere archiviati fino ad esaurimento risorse dell'applicativo o può essere configurato un orizzonte massimo temporale oltre il quale il software cancella i log più vecchi per far posto ai nuovi.
L'archiviazione su database consentirà quindi di creare una vasta gamma di report predefiniti e personalizzabili, anche schedulabili per invio a particolari caselle di posta. Sarà altresì possibile effettuare particolari query alla ricerca di particolari URL o attività di determinati utenti o gruppi.
L'accesso alla reportistica è profilabile ed integrato con il sistema di autenticazione.
Report Predefiniti riconoscimento attività sospette: La soluzione prevede una serie di report già pronti (outliers) che evidenziano comportamenti anomali di particolari utenti, oppure è possibile creare report relativi agli utenti che hanno acceduto il maggior numero di accessi a siti compromessi per effettuare una analisi puntuale delle macchine a rischio.
Compatibilità con la legge sulla Privacy (Anonymous Logging): possibilità opzionale di mantenere l'anonimato per il logging delle attività. Protezione della privacy dell'utente e, contemporaneamente, disponibilità di informazioni dettagliate su eventuali rischi potenziali derivati da un particolare uso di Internet.
Selective Logging: possibilità opzionale di registrare le attività Internet solo per determinate categorie di siti. Riduzione dei costi hardware grazie alla diminuzione dell'utilizzo dello spazio disco, migliori prestazioni di reporting e viste semplificate sui rischi
Delegated Reporting offre la possibilità di consentire a specifici utenti di accedere ai tool di reporting web su specifici utenti, gruppi o segmenti di rete. Accesso a informazioni sui rischi per la sicurezza e la produttività pertinenti alle specifiche responsabilità di ruolo, (es.: il IT Manager può vedere solo i report relativi al dipartimento IT).
Cloud App reports: possibilità di visualizzare tutto il traffico verso le cloud app, la quantità di dati in modo da permettere un continuo monitoraggio del fenomeno.



Deep Content Inspection Delivers Unmatched Visibility

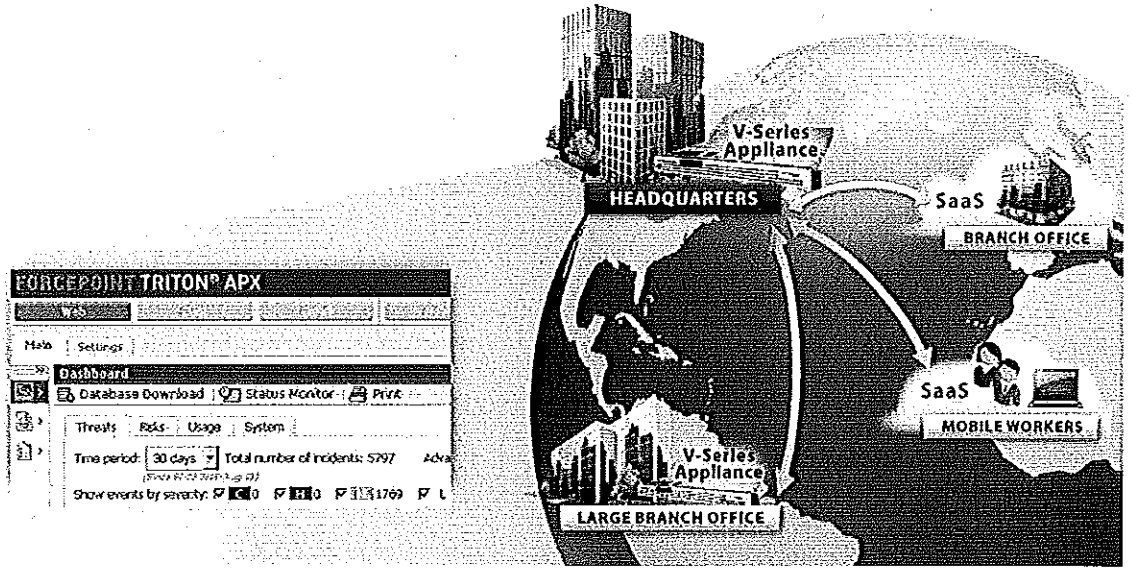


Nel caso della soluzione WEB l'esperienza dell'utente rimane invariata, quando il sistema rileva una possibile minaccia viene generato un report per l'amministratore di sistema, il file viene successivamente classificato come compromesso e bloccato dalla rete ThreatSeeker.

WEB HYBRID MODULE

I dispositivi mobili sono sempre più diffusi ed utilizzati all'esterno dell'azienda. La sfida più importante per gli amministratori di sistema è garantire un accesso veloce alle risorse internet ed intranet senza rinunciare alla sicurezza ed al ridotto costo operativo. Per rispondere a questa esigenza Forcepoint ha sviluppato una modalità di implementazione Ibrida che unisce i vantaggi dei prodotti on-premise alla flessibilità del mondo cloud per offrire una soluzione integrata che possa seguire l'utente anche all'esterno della rete.
Questo modulo estende le funzionalità di protezione della soluzione WEB SECURITY anche all'esterno della rete aziendale grazie alle funzionalità di protezione SAAS dei Datacenter Forcepoint. Questo ci consente di portare sul mercato una modalità di deployment ibrida con parte degli utenti gestiti da soluzioni on-premise quali appliance o software e parte degli utenti gestiti tramite la soluzione CLOUD per estendere la sicurezza del Web sia per gli utenti mobili che per le sedi remote che non hanno infrastruttura locale.

Il vero valore aggiunto della soluzione Security Manager è la possibilità di gestire entrambe le soluzioni in modo integrato andando a sincronizzare la configurazione interna con i cluster esterni ed allo stesso tempo scaricando i log collezionati in modo da avere tutto gestito tramite una singola console.



Questa funzionalità si può quindi utilizzare per due scopi:

- Protezione in mobilità: Installando un end-point sulle macchine degli utenti è possibile forzare la navigazione del computer sugli apparati interni quando collegati alla rete della regione mentre dall'esterno viene utilizzato il proxy in-the-cloud. Il tutto avviene in modo trasparente per l'utente che non deve cambiare alcuna impostazione o inserire password se ha effettuato l'accesso alla macchina con l'account del dominio Regione.
- Backup: I proxy cloud possono essere utilizzati anche quando gli appliance sono indisponibili, ovvero gli utenti possono essere rediretti verso i datacenter Forcepoint per continuare a navigare protetti

acquistinretepa.it
Il Portale degli acquisti della Pubblica Amministrazione

MERCATO ELETTRONICO DELLA PUBBLICA AMMINISTRAZIONE

OFFERTA ECONOMICA RELATIVA A:	
Numero RDO	1900322
Descrizione RDO	Licenze per Servizi Web Security e Content Filtering WEBSENSE – WEB SECURITY GATEWAY ANYWHERE con UPGRADE di quello attualmente in usò e MODULO INTEGRATIVO, per il periodo di 36 mesi per 800 utenti
Criterio di Aggiudicazione	Gara al prezzo piu' basso
Lotto	1 (Licenze per Servizi Web Security e Content Filtering WEBSENSE – WEB SECURITY GATEWAY ANYWHERE con UPGRADE di quello attualmente in uso e MODULO INTEGRATIVO, per il periodo di 36 mesi per 800 utenti)
CIG	7419469382
CUP	Non inserito

AMMINISTRAZIONE	
Nome Ente	AUSL RIETI
Codice Fiscale Ente	00821180577
Nome ufficio	DIREZIONE SISTEMA INFORMATICO
Indirizzo ufficio	VIA DEL TERMINILLO, 42 - RIETI (RI)
Telefono / FAX ufficio	0746279758 / 0746279754
Codice univoco ufficio per Fatturazione Elettronica	UFX1HE
Punto ordinante	CAMPOGIANI ROBERTO / CF:CMPRRT58C07H282C
Firmatari del contratto	GIULIO FAITA / CF:FTAGLI65E01H501W

FORNITORE	
Ragione Sociale	AKITO SRL
Forma di partecipazione	Singolo operatore economico

	(D.Lgs. 50/2016, art. 45, comma 2, lett. a)
Partita IVA impresa	03526780543
Codice Fiscale Impresa	03526780543
Indirizzo Sede Legale	STRADA LACUGNANO GIARDINO 14 - PERUGIA (PG)
Telefono / Fax	3917714321 / 0759975563
PEC Registro Imprese	AKITO@PEC-LEGAL.IT
Tipologia impresa	Società a Responsabilità Limitata
Numero di iscrizione al Registro Imprese/Nome e Nr iscrizione Albo Professionale	03526780543
Data di iscrizione Registro Imprese/Albo Professionale	08/09/2016
Provincia sede Registro Imprese/Albo Professionale	PG
INAIL: Codice Ditta/Sede di Competenza	19901928/57
INPS: Matricola aziendale	5810146638
Posizioni Assicurative Territoriali - P.A.T. numero	22795919/64
PEC Ufficio Agenzia Entrate competente al rilascio attestazione regolarità pagamenti imposte e tasse:	
CCNL applicato / Settore	METALMECCANICO / PICCOLA MEDIA INDUSTRIA
Legge 136/2010: dati rilasciati dal Fornitore ai fini della tracciabilità dei flussi finanziari	
Nessun dato rilasciato	

DATI DELL'OFFERTA	
Identificativo univoco dell'offerta	4486233
Offerta sottoscritta da	FAITA GIULIO
Email di contatto	AKITO@PEC-LEGAL.IT
L'Offerta sarà irrevocabile ed impegnativa fino al	30/05/2018 12:00
Contenuto dell'Offerta - Oggetto di Fornitura (1 di 3)	
Bando	Licenze per Servizi Web Security e Content Filtering WEBSENSE – WEB SECURITY GATEWAY ANYWHERE con UPGRADE di

	quello attualmente in uso e MODULO INTEGRATIVO, per il periodo di 36 mesi per 800 utenti
Categoria	Servizi di manutenzione software
Descrizione Oggetto di Fornitura	gg/uomo per Upgrade della versione esistente e sistemazione Proxy
Quantità	10
PARAMETRO RICHIESTO	**VALORE OFFERTO**
Marca	non inserito
Codice articolo produttore*	gg/uomo per Upgrade
Nome del servizio di manutenzione Software*	gg/uomo per Upgrade della versione esistente e sistemazione Proxy
Descrizione tecnica*	UPGRADE VERSIONE ESISTENTE
Tipo contratto*	Acquisto
Oggetto*	UPGRADE
Modalità di erogazione*	GG/UOMO
Durata del contratto [mesi]*	36
Unità di misura*	giornata
Tipo di manutenzione	non inserito
Denominazione del software	non inserito
Prezzo*	550
Contenuto dell'Offerta - Oggetto di Fornitura (2 di 3)	
Bando	Licenze per Servizi Web Security e Content Filtering WEBSENSE – WEB SECURITY GATEWAY ANYWHERE con UPGRADE di quello attualmente in uso e MODULO INTEGRATIVO, per il periodo di 36 mesi per 800 utenti
Categoria	Servizi di manutenzione software
Descrizione Oggetto di Fornitura	Modulo integrativo per analisi in tempo reale di ransomware, nuovi virus e siti sospetti non ancora censiti.
Quantità	1
PARAMETRO RICHIESTO	**VALORE OFFERTO**
Marca*	FORCEPOINT
Codice articolo produttore*	Modulo integrativo
Nome del servizio di manutenzione Software*	Modulo integrativo per analisi Forcepoint
Descrizione tecnica*	MODULO INTEGRATIVO Advanced Malware Detection Cloud
Tipo contratto*	Acquisto
Oggetto*	Advanced Malware Detection Cloud

	- WEB, Modules
Modalità di erogazione*	licenza
Durata del contratto [mesi]*	36
Unità di misura*	licenza
Tipo di manutenzione	non inserito
Denominazione del software	non inserito
Prezzo*	28100
Contenuto dell'Offerta - Oggetto di Fornitura (3 di 3)	
Bando	Licenze per Servizi Web Security e Content Filtering WEBSENSE – WEB SECURITY GATEWAY ANYWHERE con UPGRADE di quello attualmente in uso e MODULO INTEGRATIVO, per il periodo di 36 mesi per 800 utenti
Categoria	Servizi di manutenzione software
Descrizione Oggetto di Fornitura	SW Forcepoint Triton Web Security Gateway Anywhere per 800 utenti 36 mesi
Quantità	1
PARAMETRO RICHIESTO	**VALORE OFFERTO**
Marca*	FORCEPOINT
Codice articolo produttore*	SW Forcepoint
Nome del servizio di manutenzione Software*	SW Forcepoint Triton Web Security Gateway Anywhere
Descrizione tecnica*	RINNOVO SW Forcepoint Triton Web Security Gateway Anywhere
Tipo contratto*	Acquisto
Oggetto*	RINNOVO SW Forcepoint Triton Web Security Gateway Anywhere
Modalità di erogazione	non inserito
Durata del contratto [mesi]*	36
Unità di misura*	licenza
Tipo di manutenzione	non inserito
Denominazione del software	non inserito
PERIODO (MESI)*	36
N. UTENTI*	800
Prezzo*	80100
Offerta economica per il lotto 1	
Unità di misura dell'offerta economica	Valori al ribasso
Valore dell'offerta per il Lotto 1	**113700,00 Euro (centotredicimilasettecento Euro)**
Oneri di Sicurezza non oggetto di ribasso e non compresi nell'Offerta: *(non specificati)*	
Costi di Sicurezza aziendali concernenti l'adempimento delle	

disposizioni in materia di salute e sicurezza sui luoghi di lavoro di cui all'art. 95, comma 10, del D. Lgs. n. 50/2016, compresi nell'Offerta: **1,00 (Euro)**

INFORMAZIONI DI CONSEGNA E FATTURAZIONE	
Data Limite per Consegna Beni / Decorrenza Servizi	10 giorni dalla stipula
Dati di Consegna	Via del terminillo n. 42Rieti - 02100 (RI)
Dati e Aliquote di Fatturazione	Aliquota IVA di fatturazione: 22%Indirizzo di fatturazione:Via del terminillo n. 42Rieti - 02100 (RI)
Termini di Pagamento	60 GG Data Ricevimento Fattura

SITUAZIONE DI CONTROLLO DI CUI ALL'ART. 2359 C.C.
L'operatore economico non si trova rispetto ad un altro partecipante alla presente procedura di affidamento, in una situazione di controllo di cui all'articolo 2359 del codice civile o in una qualsiasi relazione, anche di fatto, che comporti che le offerte sono imputabili ad un unico centro decisionale

SUBAPPALTO
Il Fornitore dichiara che, in caso di aggiudicazione, per il lotto "1" non intende affidare alcuna attività oggetto della presente gara in subappalto

Dichiarazione necessaria per la partecipazione alla Richiesta di Offerta resa ai sensi e per gli effetti degli artt. 46,47 e 76 del d.P.R. n.445/2000

- Il Fornitore è pienamente a conoscenza di quanto previsto dalle Regole del Sistema di e-Procurement della Pubblica Amministrazione relativamente alla procedura di acquisto mediante Richiesta di Offerta (artt. 46 e 50).
- Il presente documento costituisce una proposta contrattuale rivolta al Punto Ordinante dell'Amministrazione richiedente ai sensi dell'art. 1329 del codice civile, che rimane pertanto valida, efficace ed irrevocabile sino fino alla data sopra indicata ("L'Offerta è irrevocabile ed impegnativa fino al").
- Il Fornitore dichiara di aver preso piena conoscenza della documentazione predisposta ed inviata dal Punto Ordinante in allegato alla Richiesta di Offerta, prendendo atto e sottoscrivendo per accettazione unitamente al presente documento, ai sensi di quanto previsto dall'art. 53 delle Regole del Sistema di e-Procurement della Pubblica Amministrazione, che il relativo Contratto sarà regolato dalle Condizioni Generali di Contratto applicabili al/ai Bene/i Servizio/i offerto/i, nonché dalle eventuali Condizioni particolari di Contratto predisposte e inviate dal Punto Ordinante, obbligandosi, in caso di aggiudicazione, ad osservarle in ogni loro parte.
- Il Fornitore è consapevole che, qualora fosse accertata la non veridicità del contenuto della presente dichiarazione, l'Impresa verrà esclusa dalla procedura per la quale è rilasciata, o, se risultata aggiudicataria, decadrà dalla aggiudicazione medesima la quale verrà annullata e/o revocata, e l'Amministrazione titolare della presente Richiesta di Offerta escute l'eventuale cauzione provvisoria; inoltre, qualora la non veridicità del contenuto della presente dichiarazione fosse accertata dopo la stipula, questa potrà essere risolta di diritto dalla Amministrazione titolare della presente Richiesta di Offerta ai sensi dell'art. 1456 cod. civ.
- Per quanto non espressamente indicato si rinvia a quanto disposto dalle Regole del Sistema di e-Procurement della Pubblica Amministrazione; al Contratto sarà in ogni caso applicabile la disciplina generale e speciale che regolamenta gli acquisti della Pubblica Amministrazione.
- Il Fornitore dichiara che non sussiste la causa interdittiva di cui all'art. 53, comma 16-ter, del D.lgs. n. 165/2001 nei confronti della stazione appaltante e/o della Committente;
- Il Fornitore ha preso piena conoscenza del "Patto di Integrità", eventualmente predisposto dalla Stazione appaltante e/o dalla Committente, allegato alla richiesta di offerta, accettando le clausole ivi contenute e si impegna a rispettarne le prescrizioni;
- Il presente Documento di Offerta è esente da registrazione ai sensi del Testo Unico del 22/12/1986 n. 917, art. 6 e s.m.i., salvo che in caso d'uso ovvero ove diversamente e preventivamente esplicitato dall'Amministrazione nelle Condizioni Particolari di Fornitura della Richiesta di Offerta.

ATTENZIONE: QUESTO DOCUMENTO NON HA VALORE SE PRIVO DELLA SOTTOSCRIZIONE A MEZZO FIRMA DIGITALE