Identificativo: ER4A56001Q07

Data: 12/01/2017

PROCEDURA RISTRETTA PER L'AFFIDAMENTO DEI SERVIZI DI CLOUD COMPUTING, DI SICUREZZA, DI REALIZZAZIONE DI PORTALI E SERVIZI ON-LINE E DI COOPERAZIONE APPLICATIVA PER LE PUBBLICHE AMMINISTRAZIONI (ID SIGEF 1403)

LOTTO 2

CONSIP

SPC L2 - Proposta Adeguamento Servizi

Raggruppamento Temporaneo di Imprese

composto da:

Leonardo SpA

IBM SpA

Sistemi Informativi SpA

Fastweb SpA

Le informazioni contenute nel presente documento sono di proprietà di Leonardo Società per Azioni, IBM Società per Azioni, Sistemi Informativi Società per Azioni, Fastweb Società per Azioni e non possono, al pari di tale documento, essere riprodotte, utilizzate o divulgate in tutto o in parte a terzi senza preventiva autorizzazione scritta delle citate aziende.

[redacted] [redacted]

[redacted]

[redacted]	
[redacted]	
[redacted]	

[redacted]

[redacted]	

[redacted]

[redacted]

[redacted]

[redacted]	

[redacted]

[redacted] [redacted] [redacted] [redacted]

1 SOMMARIO

1 INTRODUZIONE

Il presente documento è volto a presentare le soluzioni tecniche per l'adeguamento ed integrazione dei servizi rispetto all'offerta presentata in sede di gara, al fine di rispondere alle esigenze espresse dalle PP.AA. completando il listino con una serie di servizi complementari e necessari alle Amministrazioni per svolgere le proprie attività in un'ottica di sempre maggior digitalizzazione dei processi.

Quanto riportato nel presente documento si applica a tutte le attività e servizi previsti dal Contratto: «Procedura ristretta per l'affidamento dei servizi di Cloud Computing, di sicurezza, di realizzazione di portali e servizi online e di cooperazione applicativa per le Pubbliche Amministrazioni (ID SIGEF 1403) – Lotto 2 "

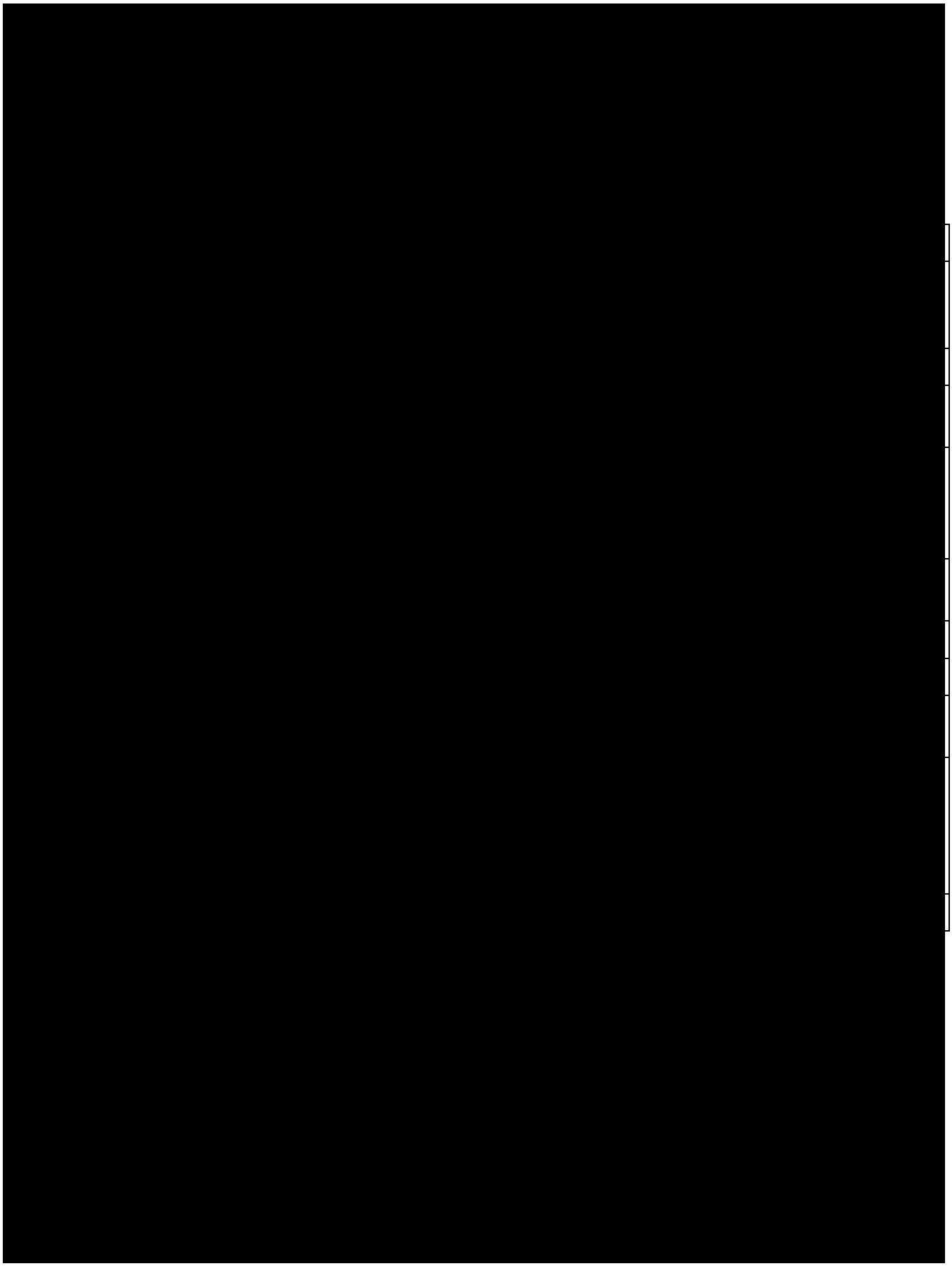
[redacted]

[redacted]

[redacted]

[redacted]

[redacted]



3 SERVIZIO L2.S3.5 – DATA LOSS PREVENTION - TECNOLOGIE CYBER INTUITION

Il seguente capitolo ha lo scopo di illustrare la rispondenza a delle specifiche richieste delle amministrazioni verso un servizio DLP che sia in grado di rilevare e prevenire la perdita di dati dovuta soprattutto a minacce di tipo Ransomware. Tale tipo di malware è ad oggi la minaccia più pericolosa che potenzialmente porta ad una perdita di dati. I bersagli tipici di questo tipo di minaccia sono gli utenti di tipo consumer, e quelli di tipo enterprise; i primi possono essere privati dell'accesso ai loro dati personali, i secondi possono mettere in pericolo dati che riguardano l'intera azienda/amministrazione.

Tipicamente il ransomware utilizza tecniche di injection su processi in esecuzione da parte dell'utente, che permettono al malware di guadagnare il controllo di tali processi (es. Explorer, Adobe Reader, ecc.) e di iniziare la cifratura dei file tipicamente presenti nelle cartelle degli utenti con tecniche di crittografia simmetrica con chiavi di elevata complessità. Una volta cifrati i file, il loro contenuto originario non è più accessibile dai proprietari e da nessuno che non sia in possesso delle chiavi di cifratura. Tali chiavi in genere sono in possesso degli attaccanti nei cosiddetti centri di Comando e Controllo, da dove possono essere rilasciate, spesso con processi automatici, a seguito del pagamento di un riscatto (da qui il nome ransomware). Il comportamento di questo tipo di malware, nelle sue varianti più note, come CryptoWall, Cryakl, Scatter, Mor, CTB-Locker, TorrentLocker , Fury, Lortok, TeslaCrypt , Aura e Shade, è spesso simile e un processo di tipo ransomware, se riconosciuto in tempo può essere bloccato prima che inizi le sue attività di cifratura, o subito dopo, eliminando o riducendo al minimo il rischio di perdita dei dati.

Il ransomware ai giorni nostri è appunto una delle cause principali di perdita dei dati e questa minaccia è sempre più rivolta, oltreché tradizionalmente agli utenti privati, anche ad utenti aziendali; da qui l'esigenza di molte amministrazioni di combattere tale minaccia con tecniche di riconoscimento avanzate che permettano la rilevazione e il blocco delle attività malevole. Tale funzionalità è tipicamente riconducibile ad una tecnica di DLP, servizio giù presente a listino SPC Lotto2 sicurezza (Servizio L2.S3.5 Data Loss/Leak Prevention).

Di seguito sono riassunti i requisiti richiesti a capitolato e la corrispondente mappatura dei requisiti tecnici implementativi.

3.1 REQUISITI FUNZIONALI

Si riportano di seguito i principali requisiti funzionali:

- rilevazione dei dati che transitano nell'organizzazione, ovunque siano archiviati, e valutazione del rischio di perdita di dati (DLP Risk Assessment);
- analisi e classificazione dei dati (DLP Information classification);
- possibilità di creare regole predefinite per la protezione dei dati, identificando i sistemi in cui sono memorizzati (ad esempio porte USB, CD, DVD, porte COM & LPT, dischi rimovibili, dispositivi di acquisizione immagini, modem) per assicurarsi che siano usati in conformità con le politiche di privacy e sicurezza (DLP data at rest);
- generazione automatica di alert nel caso in cui vengano violate le policy di sicurezza definite, visibilità e controllo sui dati in movimento, sia che si trovino in messaggi e-mail, nella mail sul Web, nell'instant messaging, e nei protocolli di rete (DLP data in motion);
- possibilità di generare report di sintesi (executive summary) e di dettaglio (technical report) sulle analisi svolte;
- generazione audit trail e gestione profili di audit;

3.2 REQUISITI TECNICI

Si riportano di seguito i principali requisiti tecnici:

- compatibilità con i maggiori protocolli di rete di livello application quali FTP/SFTP/FTPS, HTTP/HTTPS, SMTP e di livello network e transport;
- compatibilità con i sistemi operativi Windows e Linux;

Di seguito viene esposta la corrispondenza ai suddetti requisiti.

Soluzione tecnologica	**Descrizione della soluzione**: La soluzione software RaPToR (Ransomware Prevention Toolkit and Rescue), di Cyber Intuition di seguito per brevità “Raptor o software”, è una piattaforma software di sviluppo interamente italiano, che si pone come obiettivo la tutela dei dati, presenti all’interno delle memorie di massa della macchina sulla quale il software è installato, da infezioni locali. RaPToR intercetta l'esecuzione dei Ransomware analizzando il comportamento dei processi in esecuzione della macchina e impedendo, ove possibile, la crittografia dei dati utente e di sistema e permettendo il recupero di eventuali dati crittografati mediante il ripristino da copie di sicurezza generate costantemente. Funzionalità RaPToR previene la perdita dei dati dovuti alla crittografia da parte dei Ransomware e ne permette l’eventuale recupero da backup con tecnologia Shadow Copy create automaticamente a cadenza giornaliera o personalizzata qualora una nuova tipologia di Ransomware riesca a bypassare i sistemi di riconoscimento del motore comportamentale. Tale funzionalità, vero e proprio core del software, permette di ridurre al minimo la presenza di falsi positivi. Le funzionalità di base del software si compongono di due moduli distinti con compiti ben definiti: - Motore di analisi comportamentale, con funzionalità di Memory Dump e Honeypot. - Funzionalità di tutela e ripristino dei dati tramite Shadow Copy. Tali funzionalità sono presenti all’interno di una componente agent, snella e leggera, da installarsi sulle macchine (client e server), che permette il monitoraggio dei processi e delle loro attività, e la rilevazione e il blocco degli attacchi. **Le funzionalità offerte** a copertura dei requisiti sono le seguenti: - rilevazione dei dati che transitano nell'organizzazione, ovunque siano archiviati, e **valutazione del rischio di perdita di dati** (DLP Risk Assessment); La piattaforma è in grado di monitorare e analizzare gli accessi che vengono effettuati sui dati da parte dei processi della macchina e degli utenti relativi a questi, classificando i processi

stessi come malevoli e valutando real-time il rischio di perdita di informazioni; Questo viene fatto assegnando dei punteggi di rischio ai processi monitorati. Al superamento delle soglie predefinite, vengono attivate le procedure di protezione.

- **analisi e classificazione dei dati** (DLP Information classification); La piattaforma è in grado di analizzare e classificare i dati di interesse dei processi di tipo ransomware e suggerire una lista di aree/cartelle considerate ad alto rischio, che potrebbero contenere dati sensibili per l'utente.
- **possibilità di creare regole predefinite per la protezione dei dati**, identificando i sistemi in cui sono memorizzati (ad esempio porte USB, CD, DVD, porte COM & LPT, dischi rimovibili, dispositivi di acquisizione immagini, modem) per assicurarsi che siano usati in conformità con le politiche di privacy e sicurezza (DLP data at rest); La piattaforma è in grado di identificare l'accesso ai dati sensibili ovunque essi risiedano (porte USB, CD, DVD, porte COM & LPT, dischi rimovibili, …) e configurare delle policy. Esempi di configurazioni che possono essere eseguite tramite la piattaforma sono:
    - Indicazione di azioni automatiche in conseguenza di un attacco rilevato (es, shutdown temporizzato e forzato della macchina, riavvio esclusivo in modalità provvisoria, semplice notifica di avvenuta infezione).
    - Configurazione della cartella di destinazione utilizzata per il salvataggio dei file di dump.
    - Indicazione di cartelle specifiche classificate dall'utente come ad alto rischio.
- **generazione automatica di alert** nel caso in cui vengano violate le policy di sicurezza definite; - La piattaforma è in grado di generare alert in real-time in conseguenza di una rilevazione di possibile infezione ransomware. Gli alert possono essere visualizzati accedendo alla console.
- **possibilità di generare report di sintesi** (executive summary) **e di dettaglio** (technical report) sulle analisi svolte; E' possibile generare report di sintesi e di dettaglio tramite le funzionalità della console. In particolare è possibile ottenere (sotto forma di report tabellari e/o grafici):
    - Anagrafica e Report del parco macchine, rilevate all'interno della rete, organizzate secondo gruppi definiti dagli operatori che utilizzeranno la console.
    - Anagrafica e Report degli Stati, per ciascuna macchina sulla quale è installato il software; gli stati di funzionamento tra attivo, allarme, errore, inattivo.
    - Anagrafica e Report delle Versioni del SW e stato dell'Aggiornamento.

- **generazione audit trail e gestione profili di audit**: - La piattaforma è in grado di gestire la generazione di log in modalità nativa sulle piattaforma windows. Tali log delle attività rilevate, sono memorizzate in un registro dedicato all'interno del sistema operativo Microsoft, e sono visualizzabili anche tramite la console di gestione. All'interno della console sono configurabili dei profili di audit per l'accesso a questi log, che possono a loro volta essere memorizzati in un archivio interno.
- **compatibilità con i maggiori protocolli di rete** di livello application quali FTP/SFTP/FTPS, HTTP/HTTPS, SMTP e di livello network e transport; La piattaforma, lavorando a livello di endpoint, è in grado di intercettare qualsiasi tipo di accesso ai dati o trasmissione degli stessi.
- **compatibilità con i sistemi operativi Windows e Linux**: la piattaforma è compatibile con i sistemi operativi Microsoft Windows. Alcune componenti della console sono anche fruibili su sistema operativo Linux, tra cui, a titolo esemplificativo, la WebGUI per l'accesso tramite web browser alle funzionalità di visualizzazione dei log.

Interventi presso l'Amministrazione	Supporto all'installazione degli Agent sulle pdl delle Amministrazioni. Installazione della console di gestione presso i Data Center o Uffici delle Amministrazioni. Creazione di una baseline di policy per la rilevazione delle minacce di tipo ransomware.
Compatibilità	La soluzione è installabile sulle seguenti piattaforme: Versione desktop: - Microsoft Windows Vista - Microsoft Windows 7 - Microsoft Windows 8 - Microsoft Windows 8.1 - Microsoft Windows 10 Versione server: - Microsoft Windows Server 2008 - Microsoft Windows Server 2008 R2 - Microsoft Windows Server 2012 - Microsoft Windows Server 2012 R2 - Linux (Web GUI)
Supporto richiesto all'amministrazione	Sistemista per l'installazione dell'Agent, sistemista per la creazione dell'utenza necessaria ai test di assessment

Reportistica	E' possibile generare report di sintesi e di dettaglio tramite le funzionalità della console. In particolare è possibile ottenere (sotto forma di report tabellari e/o grafici): - Anagrafica e Report del parco macchine, rilevate all'interno della rete, organizzate secondo gruppi definiti dagli operatori che utilizzeranno la console. - Anagrafica e Report degli Stati, per ciascuna macchina sulla quale è installato il software; gli stati di funzionamento tra attivo, allarme, errore, inattivo. - Anagrafica e Report delle Versioni del SW e stato dell'Aggiornamento.

Da un punto di vista economico, il servizio, viene offerto allo stesso prezzo di listino proposto.

A complemento delle funzionalità della piattaforma è possibile fornire, sotto forma di servizi professionali attività di:

- Servizi di Intelligence e ricerca di minacce di tipo ransomware basati sulla ricerca di informazioni di tipo OSInt (Open Source Intelligence), con ricerca su Web, Blog, Pad, Siti di settore e Dark/Deep Internet.
- Aggiornamenti dell'agent, comprensivi del motore di analisi comportamentale, per la rilevazione e la protezione verso nuove tipologie di ransomware che si manifestano mediante nuove tipologie di comportamento o di azioni. Tali aggiornamenti sono basati anche sulle ricerche di tipo OSInt, di cui al punto precedente.
- Integrazione dello strumento all'interno delle tecnologie delle Amministrazioni tramite utilizzo di SDK/API esposte e richiamabili tramite Web Services.
- Realizzazione di dashboard personalizzate per le esigenze delle Amministrazioni.
- Supporto alle investigazioni in caso di incidente.
- Deploy degli agent sugli endpoint direttamente tramite strumenti proprietari (console).
- Sviluppo e Gestione di kit di recupero, basato su distribuzioni live presenti su dispositivi USB/CD, finalizzati al recupero e analisi dei dati dei sistemi compromessi.
- Customizzazione ad hoc delle componenti della piattaforma (console e/o agent).
- Servizi di supporto avanzato (patch, bugfix, workaround) ad hoc per le Amministrazioni.
- Personalizzazione delle console e personalizzazione del reporting.
- Eventuale supporto alla produzione dei rescue kit.
- Manutenzione evolutiva e correttiva personalizzata.
- Supporto tecnico alla risoluzione degli incidenti.

4 SERVIZIO L2.S3.6 – DATABASE SECURITY

Il presente capitolo illustra l'equivalenza tecnico/economica delle soluzioni individuate in alternativa a quella proposta in offerta tecnica, basata su prodotti di mercato **McAfee.** Le due soluzioni sono basate su tecnologia IBM Guardium e su tecnologia IMPERVA.

In considerazione della natura della piattaforma IMPERVA rispetto a quella proposta McAfee (appliance vs. SW endpoint), l'RTI si impegna a fornire il servizio con detta tecnologia solo per forniture uguali o superiori ad un numero minimo di 200 istanze.

Di seguito si illustrano in dettaglio le due soluzioni proposte.

4.1 TECNOLOGIA IMPERVA

La prima tecnologia proposta, basata su tecnologia Imperva, è da considerarsi migliorativa, in quanto offre funzionalità aggiuntive a quelle previste dal capitolato tecnico Lotto 2 e dall'offerta tecnica del RTI.

Di seguito sono riassunti i requisiti richiesti a capitolato e la corrispondente mappatura dei requisiti tecnici implementativi.

4.1.1 REQUISITI FUNZIONALI

- monitoraggio dei database presenti all'interno dell'Amministrazione e delle applicazioni web che ne fanno uso;
- definizione di regole di sicurezza personalizzate e blocco di comportamenti non autorizzati;
- identificazione delle potenziali vulnerabilità e indicazione delle relative azioni correttive.
- analisi dei database e valutazione dei rischi mediante controlli di vulnerabilità;
- individuazione delle alterazioni dei dati, degli utenti e dei profili di accesso;
- creazione personalizzata di policy di sicurezza per soddisfare le normative del settore o gli standard internazionali;
- arresto in tempo reale delle sessioni che violano le policy, evitando che i dati vengano compromessi;
- controllo degli accessi ai dati, identificazione e arresto di comportamenti non autorizzati o dannosi;
- classificazione delle minacce per tipologia e/o livelli di severità;
- reporting di sintesi (executive summary) e di dettaglio (technical report) sulle vulnerabilità individuate e indicazione di script correttivi.

4.1.2 REQUISITI TECNICI

- compatibilità con almeno tre dei seguenti sistemi di database: Oracle, Microsoft SQL Server, IBM DB2, SAP Sybase e MySQL.

Di seguito viene esposta la corrispondenza ai suddetti requisiti.

Soluzione tecnologica	L'infrastruttura tecnologica è a tre livelli e si avvale delle seguenti componenti. **SecureSphere Gateway**: Il Gateway è l'appliance responsabile dell'analisi del traffico SQL in tempo reale e dell'enforcement (in collaborazione con l'Agent) delle policy.

Il gateway può essere configurato per il blocco o per la sola segnalazione a seconda della funzionalità e del livello della minaccia.

Le appliance Imperva SecureSphere possono monitorare e proteggere un numero illimitato di database, limitato solo dal throughput espresso in TPS (Transactions Per Second).

SecureSphere Agent: L'Agent è la componente software che, installata sui DB server, cattura tutta l'attività del database e la inoltra al Gateway per l'elaborazione. L'Agent è in ascolto sulle interfacce di rete, loopback, SHM, BEQ, IPC e tutti i connettori che il sistema di database mette a disposizione per l'interrogazione dei dati. L'Agent ha una capacità di elaborazione limitata, per ridurre al minimo l'occupazione di risorse sul DB server; la maggior parte dell'elaborazione e del parsing dei comandi SQL avviene sul Gateway.

SecureSphere MX Management Server: L'unità MX Server è il punto focale di un'architettura di gestione a tre livelli che permette di gestire simultaneamente gateway multipli, rispondendo alle esigenze di scalabilità delle grandi organizzazioni.

Le policy di sicurezza sono gestite centralmente e distribuite ai diversi gateway con un singolo click. L'unità MX funge anche da collettore di dati provenienti dai gateway (gli alert, ad esempio).

L'MX Server riceve gli aggiornamenti automatici di signatures, report, normative, policy predefinite da parte dell'ADC (Application Defense Center, il team Imperva che si occupa di reazione ai problemi di security).

L'unità MX Server include anche le funzionalità DAS. DAS (Discovery and Assessment Server) scansiona la rete alla ricerca di database server, classifica i dati in essi contenuti in base al livello di sensibilità, esegue i vulnerability assessment al database.

Descrizione della soluzione:
La soluzione offre piena visibilità sull'utilizzo dei dati e sulle vulnerabilità che affliggono

i DB, . Essa consente alle Amministrazioni di attivare se necessario, una protezione attiva dei dati contenuti nei database e si pone come strumento di ausilio al raggiungimento delle compliance rispetto alle normative ed agli standard Internazionali.
Il servizio del RTI ed il framework tecnologico offerto permette il controllo tutti gli accessi ai dati da parte di tutti gli utenti compresi quelli privilegiati (come ad esempio il database administrator).
La soluzione è in grado di rilevare in real-time gli attacchi al database, sia in termini di attacchi tecnici (sfruttamento di vulnerabilità del motore DBMS), sia in termini di attacchi logici (lettura non autorizzata di dati, inserimento/modifica/cancellazione non autorizzata di dati, inserimento/modifica/cancellazione di utenti ed oggetti). La protezione dagli attacchi tecnici è comunemente definita con il termine "virtual patching". Tale strumento di protezione (virtual patching) è continuamente aggiornato dai centri di ricerca specializzati del vendor tecnologico rendendo disponibile in breve tempo la contromisura di sicurezza più idonea. Questa funzionalità oltre a ridurre la finestra di esposizione, permette alle Amministrazioni di gestire le attività di patching e/o upgrade in maniera coerente con i propri processi di manutenzione evolutiva dei software.
A fronte della violazione di una policy di qualunque tipo, è previsto il blocco della connessione verso il DB e l'eventuale quarantena di utente/ip. Il blocco della connessione avviene, nella pratica comune, in real-time su criteri della connessione (ip, processo) o in near-real-time su criteri SQL. E' possibile, ma meno comune, abilitare il blocco in real-time per tutti i criteri, aggiungendo una latenza al processo di ispezione.

Le funzionalità offerte dalla soluzione proposta sono le seguenti:

- Intrusion Detection & Prevention
  - protegge in modo evidente i dati dalle minacce, monitorando localmente l'attività su ciascun server database e allertando sulla presenza di utilizzi pericolosi o bloccandoli in tempo reale, anche quando viene eseguito in ambienti virtualizzati o di cloud computing.
- Vulnerability Assessment
  - consente la scansione delle sottoreti dell'Amministrazione individuando tutti i DB presenti. Su tali DB e' possibile poi effettuare le scansioni di Vulnerability Assessment (VA) per individuare le vulnerabilita'. Nell'output del risultato delle scansioni viene fornita anche la procedura correttiva.
- Data Classification
  - Permette di analizzare i dati contenuti nel database e classificarli per tipologia (carte di crediti, dati anagrafici, password, ecc.)
- Virtual Patching
  - Patching semplificato che non richiede downtime. Applicando le patch mancanti e correggendo le configurazioni errate individuate dalla scansione delle vulnerabilità di Database Security Monitoring e' possibile migliorare immediatamente lo stato di sicurezza dei database, senza interrompere la attività in produzione grazie alla tecnologia di patching virtuale. La soluzione. protegge anche i database senza patch contro gli attacchi di tipo zero-day bloccando gli attacchi che possono sfruttare le vulnerabilità note e terminando le sessioni che violano le policy di sicurezza.

- Auditing and Compliance
  - Tracciatura delle operazioni effettuate sul database con altissimi livelli di scalabilità e indipendentemente dalle funzioni di native audit del database stesso.
  - Compliance con i più diffusi standard normativi (CobiT/SOX, PCI DSS, HIPAA, G.d.P Dlgs 196/2003 e DBA 2009, ISO 27001, EU Data Privacy Directive) e con le best practice organizzative
  - Reportistica con un centinaio di template customizzabili
  - Interfaccia di forensics per investigazioni mirate

Interventi presso l'Amministrazione	Installazione dell'Agent sul DB server (tramite utente con privilegi amministrativi) Apertura porte firewall 443 e XXXX dal DB server al SOC Creazione utenza DB con specifici permessi (solo per vulnerability assessment) Apertura porte firewall dal SOC al DB server (solo per vulnerability assessment e data classification)
Compatibilità	La soluzione è compatibile con Oracle, DB2, Microsoft SQL Server, Informix, MySQL, Sybase, Postgres, Netezza, Teradata su sistemi operativi Linux RHEL, Suse, Oracle, Solaris, HP-UX, AIX, Windows Server. A richiesta DB2 su IBM AS400, DB2 e IMS su IBM z/Os, Big Data (sistemi non inclusi nella presente offerta).
Funzionalità richieste	**Analisi dei DB e valutazione dei rischi** – Il processo di Vulnerability Assessment individua le vulnerabilità e gli errori di configurazione dei DB server. Viene fornito un indice di rischio per ogni test effettuato. Conseguentemente a un processo di Data Classification sopra descritto, è possibile avere un indice di rischio per tipologia di dato, anzichè semplicemente per server, permettendo così lo svincolo dalla dislocazione di server e storage. **Individuazione alterazioni** – Tramite le policy di security è possibile individuare tutte le operazioni DML, DDL, DCL e l'utilizzo delle Stored Procedures. **Creazione personalizzata di policy di sicurezza** – Imperva SecureSphere include decine di policy predefinite. E' comunque possibile creare policy personalizzate basate su un set di oltre 30 criteri. **Arresto in tempo reale delle sessioni che violano le policy** – L'arresto delle sessioni avviene in real-time o near-real-time nelle modalità sopra esposte. **Controllo degli accessi, identificazione e arresto dei comportamenti non autorizzati** – Tramite le policy di sicurezza sopra descritte è possibile controllare gli accessi (connettore utilizzato, ip, porta, username, applicazione, utenza e nome macchina a sistema operativo) e bloccare quanto non autorizzato. **Classificazione delle minacce** – Il modulo di Risk Management permette non solo di ottenere un indice di rischio relativo alle singole vulnerabilità, ma di calcolarne il rischio complessivo basandosi sulla classificazione del dato. **Generazione reportistica** – I report sono ampiamente customizzabili. Il prodotto viene fornito con circa 100 template modificabili, che includono best practice e report di compliance alle normative più comuni. Sono disponibili i formati PDF e CSV. I report sono schedulabili e consentono la creazione di grafici e raggruppamenti.

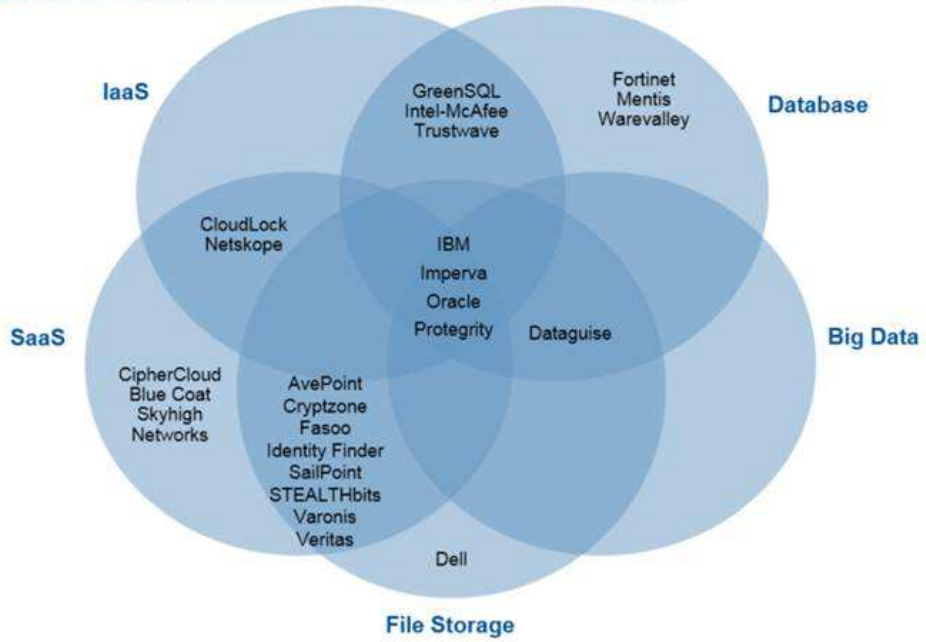
Funzionalità migliorative principali	Policy di alert/blocco su select e su qualunque comando SQL: Riteniamo molto importante anche la protezione da accessi non autorizzati in lettura dei dati sensibili.La protezione dalle sole alterazioni richiesta dal Committente garantisce l'integrità del dato, ma non la sua riservatezza, garantita invece da policy che includano il comando "select". Classificazione dei dati: Tramite la classificazione automatizzata dei dati è possibile taggare le tabelle dei database con la tipologia di dati in esse contenuta. Questo consentirà di creare policy a partire da criteri quali "Tabelle contenenti dati anagrafici" invece che utilizzare nomi statici di tabelle. User chaining: Consente di individuare quando gli utenti privilegiati tentano di anonimizzarsi eseguendo "su root" o "su oracle" dopo il login a sistema con utenza nominale. Negli alert viene visualizzata tutta la catena di utenze. Policy di audit: consentono la tracciatura delle operazioni fatte su DB
Aspetti di efficienza e disponibilità operativa	L'alta affidabilità lato virtual appliance è gestita direttamente dai sistemi Vmware (ad esempio V-Motion). L'alta affidabilità dell'intera catena di connettività è gestita dall'Agent, il quale punta ad un Gateway principale e ad un Gateway secondario opzionale. In caso di irraggiungibilità dei Gateway, viene utilizzato un buffer circolare sul disco del DB server per conservare i dati di traffico
Supporto richiesto all'amministrazione	Sistemista per l'installazione dell'Agent, sistemista o DBA per la creazione dell'utenza necessaria ai test di assessment
Reportistica	I report sono ampiamente customizzabili. Il prodotto viene fornito con circa 100 template modificabili, che includono best practice e report di compliance alle normative più comuni. Sono disponibili i formati PDF e CSV. I report sono schedulabili e consentono la creazione di grafici e raggruppamenti.

Requisiti Funzionali	Imperva	McAfee
monitoraggio dei database presenti all'interno dell'Amministrazione e delle applicazioni web che ne fanno uso	La soluzione Imperva consente il monitoraggio dei database acceduti direttamente o tramite applicazioni web	Sì, come da offerta tecnica
definizione di regole di sicurezza personalizzate e blocco di comportamenti non autorizzati	È possibile creare policy di security e/o audit utilizzando oltre 30 criteri	Sì, come da offerta tecnica
identificazione delle potenziali vulnerabilità e indicazione delle relative azioni correttive	Le funzionalità di security assessment prevedono l'individuazione di vulnerabilità tecniche (mancanza di patch ad esempio) e vulnerabilità configurative	Sì, come da offerta tecnica
analisi dei database e valutazione dei rischi mediante controlli di vulnerabilità	È possibile effettuare l'analisi del rischio per database o per	Sì, come da offerta tecnica

Requisiti Funzionali	Imperva	McAfee
	tipologia di dato classificato	
individuazione delle alterazioni dei dati, degli utenti e dei profili di accesso	Vengono tracciate tutte le operazioni su database incluse le alterazioni di dati e strutture	Sì, come da offerta tecnica
creazione personalizzata di policy di sicurezza per soddisfare le normative del settore o gli standard internazionali	È possibile creare policy di security e/o audit utilizzando oltre 30 criteri	Sì, come da offerta tecnica
arresto in tempo reale delle sessioni che violano le policy, evitando che i dati vengano compromessi	Le policy di security possono scatenare un'azione di blocco della sessione	Sì, come da offerta tecnica
controllo degli accessi ai dati, identificazione e arresto di comportamenti non autorizzati o dannosi	Tramite policy di security	Sì, come da offerta tecnica
classificazione delle minacce per tipologia e/o livelli di severità	Ad ogni minaccia rilevata è associato un indice di severità	Sì, come da offerta tecnica
reporting di sintesi (executive summary) e di dettaglio (technical report) sulle vulnerabilità individuate e indicazione di script correttivi	I report predefiniti sono customizzabili e consentono di creare template riassuntivi così come template di dettaglio destinati ai sistemisti con indicazione delle correzioni	Sì, come da offerta tecnica
Database Supportati		
Oracle	Si	Si
Microsoft SQL Server	Si	Si
IBM DB2	Si	Si
SAP Sybase	Si	Si
MySQL	Si	Si
Altri…..	Teradata, Postgres, Informix, Netezza	
Altre Funzionalità		
Blocking non intrusivo	La funzionalità di blocking avviene tramite reset della sessione, senza interferire con il database	La funzionalità di blocking avviene tramite l'inserimento di Trigger nel database
Performance	Performance scalabili a migliaia di query al secondo	Performance limitate a centinaia di query al secondo
Formato della soluzione	Software, Hardened appliance – hardened virtual appliance	Software

Di seguito riportiamo la tabella di confronto del DCAP (Data-Centric Audit and Protection) Market Analysis Gartner, in cui è evidente la copertura delle 5 macro funzionalità definite Data Silos e DCAP, a vantaggio della tecnologia Imperva verso i competitor in generale, e di Intel-McAfee in particolare.

Figure 2. Schematic Diagram for the DCAP Market Showing a Sample of Vendors



Source: Gartner (December 2015)

	Data Silos					DCAP Capabilities				
	Database	Files	Big Data	SaaS	IaaS	Integrates Policies Across Multiple Silos	Data Classification Is Integrated	Integrated Data Discovery Across Silos	Application Layer PAM	Data Protection Policy Integration
AvePoint		Y		Y		Y	Y	Y		
Blue Coat				Y			Y			Y
CipherCloud				Y			Y			Y
CloudLock				Y	Y	Y	Y	Y		Y
Cryptzone		Y		Y		Y	Y	Y		Y
Dataguise	Y	Y	Y			Y	Y	Y	Y	Y
Dell		Y					Y	Y	Y	
GreenSQL	Y				Y	Y	Y	Y		Y
Fasoo		Y		Y			Y	Y		Y
Fortinet	Y									
IBM	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Identity Finder		Y		Y		Y	Y	Y	Y	Y
Imperva	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Intel-McAfee	Y				Y					
Mentis	Y						Y			Y
Netskope				Y	Y	Y	Y	Y		Y
Oracle	Y	Y	Y	Y	Y	Y			Y	Y
Protegrity	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SailPoint		Y		Y		Y				
Skyhigh Networks				Y			Y			Y
STEALTHbits Technologies		Y		Y		Y	Y	Y	Y	Y
Veritas		Y		Y		Y			Y	
Trustwave	Y				Y		Y			
Varonis		Y		Y		Y	Y	Y	Y	
WareValley	Y						Y			

Da un punto di vista economico, il servizio, pur con funzionalità superiori, viene offerto allo stesso prezzo di listino proposto.

4.2 TECNOLOGIA IBM GUARDIUM

La seconda soluzione, basata su tecnologia IBM Guardium, è da considerarsi anch'essa migliorativa, in quanto offre funzionalità aggiuntive a quelle previste dal capitolato tecnico Lotto 2 e dall'offerta tecnica del RTI.

Di seguito riassunti i requisiti richiesti a capitolato:

4.2.1 REQUISITI FUNZIONALI

- monitoraggio dei database presenti all'interno dell'Amministrazione e delle applicazioni web che ne fanno uso;
- definizione di regole di sicurezza personalizzate e blocco di comportamenti non autorizzati;
- identificazione delle potenziali vulnerabilità e indicazione delle relative azioni correttive.
- analisi dei database e valutazione dei rischi mediante controlli di vulnerabilità;
- individuazione delle alterazioni dei dati, degli utenti e dei profili di accesso;
- creazione personalizzata di policy di sicurezza per soddisfare le normative del settore o gli standard internazionali;
- arresto in tempo reale delle sessioni che violano le policy, evitando che i dati vengano compromessi;
- controllo degli accessi ai dati, identificazione e arresto di comportamenti non autorizzati o dannosi;
- classificazione delle minacce per tipologia e/o livelli di severità;
- reporting di sintesi (executive summary) e di dettaglio (technical report) sulle vulnerabilità individuate e indicazione di script correttivi.

4.2.2 REQUISITI TECNICI

- compatibilità con almeno tre dei seguenti sistemi di database: Oracle, Microsoft SQL Server, IBM DB2, SAP Sybase e MySQL.

Di seguito viene esposta la corrispondenza ai suddetti requisiti.

Soluzione tecnologica

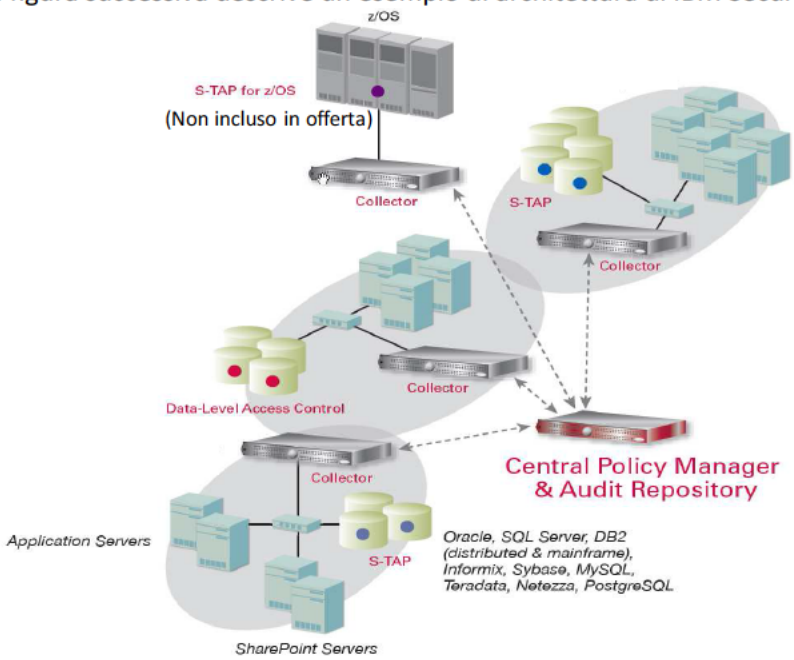
IBM Security Guardium si basa su un'architettura scalabile, multi-tier disegnata per crescere senza problemi dalla protezione di un singolo database alla protezione di migliaia di database geograficamente distribuiti.
L'architettura della soluzione supporta sia la configurazione single-tier che multi-tier e si basa su due tipologie di componenti:

- **Agent,** componente che viene installato sul sistema che ospita il database server e cattura real-time le attività svolte nel database;
- **Appliance**, di due tipi:
  - **Collector** che raccoglie i dati acquisiti dagli Agent
  - **Aggregator** che consolida i dati raccolti dai Collector e, nel caso in cui sia "promosso" a svolgere funzionalità amministrative, diventa Central Manager.

Gli appliance possono essere fisici, quindi dotati di hardware e software di base, oppure virtuali. In quest'ultimo caso essi possono essere ospitati su un'infrastruttura

Intel x86-VMware-Linux.
L'Agent è la componente software che, installata sui DB server, cattura tutta l'attività del database e la inoltra al Collector per l'elaborazione In questo modo la soluzione IBM Security Guardium permette di intercettare non solo le tradizionali comunicazioni client ed application web-based ma anche ogni accesso al DB che abbia origine direttamente sul database server.
L'Agent non richiede nessun cambiamento ai database o alle applicazioni (qualora queste applicazioni non dispongano di tracciamento specifico a parte) e non presenta impatti significativi dal punto di vista prestazionale sui sistemi dove questo viene installato.

IBM Security Guardium consente di avere uno o più Aggregator/Central Manager al fine di ottenere una vista complessiva di tutti i dati monitorati e fornire un unico punto di gestione dei Collector. Questo permette di gestire regole, policy e alert sia a livello di ogni singolo appliance sia a livello enterprise che multi enterprise.
La figura successiva descrive un esempio di architettura di IBM Security Guardium.



Descrizione della soluzione:
IBMSecurity Guardium fornisce il monitoraggio dell'attività dei dati, fornisce la cognitive analytics per rilevare attività insolite attorno ai dati sensibili, impedisce gli accessi degli utenti non autorizzati, fornisce avvisi su attività sospette, automatizza i flussi di lavoro di conformità e fornisce una protezione dalle minacce interne ed esterne. L'applicazione delle policy di sicurezza in tempo reale ed un monitoraggio costante proteggono i dati aziendali, senza modifiche o impatti negativi sulle prestazioni delle fonti dei dati o delle applicazioni. IBM Security Guardium si basa su un'architettura scalabile che fornisce visibilità completa sull'attività dei dati per tutti i principali database e data warehouse.
Fornisce granularità e visibilità al 100% di tutte le transazioni del database, incluse le operazioni SQL, le eccezioni di sicurezza (come login falliti) e le attività degli utenti privilegiati.
IBM Guardium permette di definire le policy più appropriate per monitorare e proteggere i propri dati sensibili presenti su qualsiasi Database (Oracle, SQL Server,

DB2, Sybase, MySQL, Informix, Netezza, PostgreSQL e altri), anche su ambienti IBM z/OS e IBM System i (AS/400) – (non in offerta), senza richiedere modifiche al Database stesso o alle applicazioni, e senza gravare sulle performance del sistema.
IBM Security Guardium è inoltre una soluzione consolidata per fornire valore significativo non solo a qualsiasi database relazionale ma anche alle tecnologie emergenti, ad esempio le architetture Big-Data (Hadoop, Cloudera, BigInsights, ...).
L'architettura di IBM Guardium inoltre:

- offre la capacità, da parte degli agent, di bufferizzare localmente le informazioni di Auditing in mancanza di collegamento di rete.
- può prevedere una configurazione distribuita, in High Availability (HA) e con bilanciamento del carico al fine di garantire l'efficacia e l'efficienza delle attività.
- consente di effettuare attività di crittografia per le comunicazioni tra Agent e Appliance per incrementare la riservatezza delle comunicazioni.

Interventi presso l'Amministrazione	Installazione dell'Agent sul DB server (tramite utente con privilegi amministrativi) Apertura porte firewall 443 e XXXX dal DB server al SOC Creazione utenza DB con specifici permessi Apertura porte firewall dal SOC al DB server
Compatibilità	La soluzione è compatibile con Oracle,Microsoft SQL e SQL Cluster, IBM DB2 LUW,IBM DB2 Purescale, Sybase ASE,Teradata,MySQL,MariaDB,SAP HANA,PostgreSQL,IBM Informix ,Sun MySQL and MySQL Cluster ,IBM Netezza, Cloudera, Aster, Cassandra, CouchDB,Greenplum DB, Horton Works,MongoDB su sistemi operativi Linux RHEL, Suse, Ubuntu, Oracle, Solaris, HP-UX, AIX, Windows Server. A richiesta DB2 su IBM AS400, DB2 e IMS su IBM z/Os (sistemi non inclusi nella presente offerta). L'elenco completo delle piattaforme supportate da IBM Guardium è consultabile a questo link: http://www-01.ibm.com/support/docview.wss?uid=swg27047801
Funzionalità richieste	**Analisi dei DB e valutazione dei rischi** – Il processo di Vulnerability Assessment è parte integrante della soluzione IBM Guardium e consente di fare lo scan della infrastruttura dati al fine rilevare (detect) vulnerabilità e suggerire azioni (remedial). Identifica esposizioni quali patch mancanti, weak passwords, modifiche non autorizzate, misconfigured privileges ed altre aggiuntive continuamente aggiornate in automatico. IBM Guardium segnala inoltre anche esposizioni dovute a comportamenti errati quali condivisione di accounting, eccessivo utilizzo di profili amministrativi e attività non coerenti alle finestre lavorative. **Individuazione alterazioni** – Tramite le policy di security è possibile non solo individuare tutte le operazioni e l'utilizzo delle Stored Procedures ma discriminare operazioni di amministrazione dei DB rispetto a quelle di gestione dei dati o aggregare logicamente i client in base all'indirizzo IP/subnet, all' hostname ed al source program.

Creazione personalizzata di policy di sicurezza – IBM Guardium prevede la possibilità di configurare delle policy di monitoraggio personalizzate per definire le regole di tracciamento . Nelle policy è possibile utilizzare gruppi di utenti per diversificare le regole di tracciamento. I gruppi possono essere alimentati tramite connessione a LDAP esterno (quale ad esempio Active Directory), tramite inserimento manuale, oppure utilizzando specifiche API che consentono il caricamento da file.

Arresto in tempo reale delle sessioni che violano le policy – In tempo reale sono terminare le richieste di accesso ai DB prima ancora di poter accedere ai dati stessi. L'Agent S-TAP intercetta le richieste lanciate dagli utenti (anche priviledge user), verifica le policy ed in caso di violazione effettua la *drop* terminando così la sessione, impedendo ogni possibile modifica ai dati.

Controllo degli accessi, identificazione e arresto dei comportamenti non autorizzati – Tramite le policy di sicurezza sopra descritte è possibile controllare gli accessi (connettore utilizzato, ip, porta, username, applicazione, utenza e nome macchina a sistema operativo) e bloccare quanto non autorizzato.

Classificazione delle minacce – IBM Guardium automaticamente fa la discovery e la classificazione di oggetti e informazioni sensibili. Quando questo vengono rilevati, vengono identificati e classificati in meta-dati (tagged). La classificazione può generare alert immediati, sulla base di politiche predefinite, per aiutare ad identificare e risolvere esposizioni all'interno di processi di business.

Inoltre la funzione di Vulnerability Assessment permette di testare l'infrastruttura e la configurazione del DB rilevando vulnerabilità note sulla rete e definite dall'organismo della MITRE Corporation costantemente aggiornate al dizionario degli identificativi CVE.

Generazione reportistica –E' possibile avere un unico repository centralizzato su cui andare a svolgere attività di reportistica e compliance, ottimizzazione delle performance, investigazioni e analisi forensi. La soluzione fornisce la possibilità di creare report completamente personalizzati, o utilizzare quelli messi già a disposizione per analizzare i dati raccolti. Tutti i report IBM Guardium possono essere esportati in formato sia CSV che PDF.

Funzionalità migliorative principali

Policy di alert/blocco su select e su qualunque comando SQL: Riteniamo molto importante anche la protezione da accessi non autorizzati in lettura dei dati sensibili.La protezione dalle sole alterazioni richiesta dal Committente garantisce l'integrità del dato, ma non la sua riservatezza, garantita invece da policy che includano il comando "select".

Classificazione dei dati: Tramite la classificazione automatizzata dei dati è possibile taggare le tabelle dei database con la tipologia di dati in esse contenuta. Questo consentirà di creare policy a partire da criteri quali "Tabelle contenenti dati anagrafici" invece che utilizzare nomi statici di tabelle.

User chaining: Consente di individuare quando gli utenti privilegiati tentano di anonimizzarsi eseguendo "su root" o "su oracle" dopo il login a sistema con utenza nominale. Negli alert viene visualizzata tutta la catena di utenze.

Policy di audit: consentono la tracciatura delle operazioni di configurazione fatte su DB.

Anomaly Detection: un meccanismo di Self Learning, crea una base di conoscenza

(baseline) del comportamento delle attività sui DB per circa 30 giorni. Dopo tale fase il sistema è in grado di intercettare le operazioni anomale rispetto alla propria base di conoscenza, ed inviare alert sul comportamento anomalo intercettato.

Individuazione di frodi a livello applicativo: gli Application Server usano utenze generiche per effettuare query sui DB, IBM Guardium è in grado di integrarsi con i principali framework (Oracle EBS, PeopleSoft, SAP, Siebel, Business Objects, Cognos…) e applicazioni (WebSphere….) per individuare lo user applicativo che ha generato il particolare comando SQL di accesso sul DB.

Aspetti di efficienza e disponibilità operativa

L'alta affidabilità lato virtual appliance è gestita direttamente dai sistemi Vmware (ad esempio V-Motion).

L'alta affidabilità dell'intera catena di connettività è gestita dall'Agent, il quale punta ad un Collector principale e/o ad un Collector secondario opzionale. In caso di irraggiungibilità dei Collector, viene utilizzato un buffer circolare sul disco del DB server per conservare i dati di traffico

Supporto richiesto all'amministrazione

Sistemista per l'installazione dell'Agent, sistemista o DBA per la creazione dell'utenza necessaria ai test di assessment

Reportistica

I report sono ampiamente customizzabili. Il prodotto viene fornito con circa 100 template modificabili, che includono best practice e report di compliance alle normative più comuni. Sono disponibili i formati PDF e CSV. I report sono schedulabili e consentono la creazione di grafici e raggruppamenti.

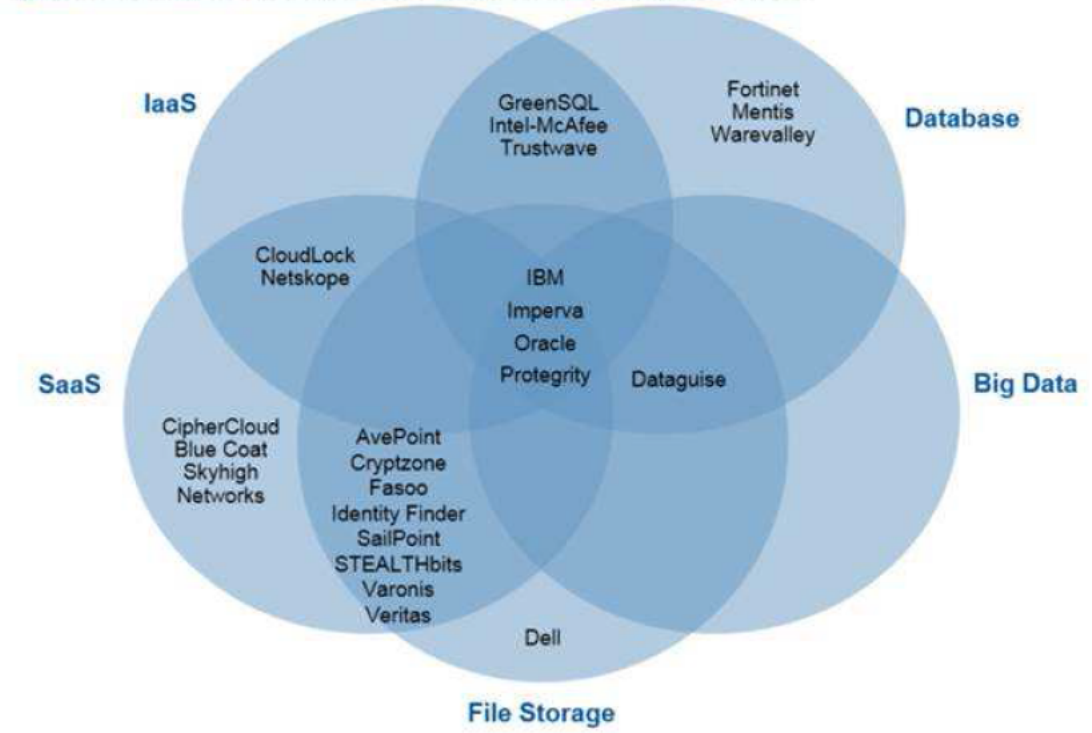
Requisiti Funzionali	IBM Guardium	McAfee
monitoraggio dei database presenti all'interno dell'Amministrazione e delle applicazioni web che ne fanno uso	La soluzione consente il monitoraggio dei database acceduti direttamente o tramite applicazioni web estendendo il numero di DB supportati	Sì, come da offerta tecnica
definizione di regole di sicurezza personalizzate e blocco di comportamenti non autorizzati	È possibile creare policy di security e/o audit completamente personalizzate	Sì, come da offerta tecnica
identificazione delle potenziali vulnerabilità e indicazione delle relative azioni correttive	Il processo di Vulnerability Assessment è parte integrante della soluzione IBM Guardium e consente di fare lo scan della infrastruttura dati al fine rilevare (detect) vulnerabilità e suggerire azioni (remedial). Identifica esposizioni quali patch mancanti, weak passwords, modifiche non autorizzate, misconfigured privileges ed altre aggiuntive continuamente aggiornate in automatico. IBM Guardium segnala inoltre anche esposizioni dovute a comportamenti errati quali	Sì, come da offerta tecnica

Requisiti Funzionali	IBM Guardium	McAfee
	condivisione di accounting, eccessivo utilizzo di profili amministrativi e attività non coerenti alle finestre lavorative.	
analisi dei database e valutazione dei rischi mediante controlli di vulnerabilità	È possibile effettuare l'analisi del rischio per database o per tipologia di dato classificato	Sì, come da offerta tecnica
individuazione delle alterazioni dei dati, degli utenti e dei profili di accesso	Vengono tracciate tutte le operazioni su database incluse le alterazioni di dati e strutture	Sì, come da offerta tecnica
creazione personalizzata di policy di sicurezza per soddisfare le normative del settore o gli standard internazionali	È possibile creare policy di security e/o audit completamente personalizzate	Sì, come da offerta tecnica
arresto in tempo reale delle sessioni che violano le policy, evitando che i dati vengano compromessi	Le policy di security possono scatenare un'azione di blocco della richiesta di accesso al dato attraverso la terminazione della sessione di accesso al DB.	Sì, come da offerta tecnica
controllo degli accessi ai dati, identificazione e arresto di comportamenti non autorizzati o dannosi	Tramite policy di security	Sì, come da offerta tecnica
classificazione delle minacce per tipologia e/o livelli di severità	Ad ogni minaccia rilevata è associato un indice di severità conforme agli standard del MITRE Corporation, CVE	Sì, come da offerta tecnica
reporting di sintesi (executive summary) e di dettaglio (technical report) sulle vulnerabilità individuate e indicazione di script correttivi	I report predefiniti sono customizzabili e consentono di creare template riassuntivi così come template di dettaglio destinati ai sistemisti con indicazione delle correzioni	Sì, come da offerta tecnica
Database Supportati		
Oracle	Si	Si
Microsoft SQL Server	Si	Si
IBM DB2	Si	Si
SAP Sybase	Si	Si
MySQL	Si	Si
Altri…..	Teradata,MariaDB,SAP HANA,PostgreSQL,IBM Informix ,IBM Netezza, Cloudera, Aster, Cassandra, CouchDB,Greenplum DB, Horton Works,MongoDB	
Altre Funzionalità		

Requisiti Funzionali	IBM Guardium	McAfee
Blocking non intrusivo	La funzionalità di blocking avviene tramite reset della sessione, senza interferire con il database che non riceve le richieste di accesso non autorizzate in quanto precedentemente filtrate	La funzionalità di blocking avviene tramite l'inserimento di Trigger nel database
Performance	Performance scalabili a migliaia di query al secondo	Performance limitate a centinaia di query al secondo
Formato della soluzione	La soluzione può essere implementata in modalità: Software:- prevedendo fornitura separate di hw Hardened appliance: appliance hardware preinstallato e configurato in modalità protetta hardened virtual appliance: macchina virtuale software caricabile su macchine virtuali VMWARE Inoltre la soluzione prevede modalità di architettura: Basic Stand Alone: per ambienti i cui DB sono concentrati in un unico Data Center Mid-size: per ambienti suddivisi in due Data Center, il collector ed aggregator saranno installati in una unica macchina. Enterprise size: ambienti distribuiti su diversi Data Center , una architettura a 3 livelli prevede diversi collector, diversi aggregator ed un central manager. Per dettagli architetturali si rimanda al sito https://www.ibm.com/support/knowledgecenter/it/SSMPHH/SSMPHH_welcome.html	Software

Di seguito riportiamo la tabella di confronto del DCAP (Data-Centric Audit and Protection) Market Analysis Gartner, in cui è evidente la copertura delle 5 macro funzionalità definite Data Silos e DCAP, a vantaggio della tecnologia Imperva verso i competitor in generale, e di Intel-McAfee in particolare.

Figure 2. Schematic Diagram for the DCAP Market Showing a Sample of Vendors



Source: Gartner (December 2015)

	Data Silos					DCAP Capabilities				
	Database	Files	Big Data	SaaS	IaaS	Integrates Policies Across Multiple Silos	Data Classification Is Integrated	Integrated Data Discovery Across Silos	Application Layer PAM	Data Protection Policy Integration
AvePoint		Y		Y		Y	Y	Y		
Blue Coat				Y			Y			Y
CipherCloud				Y			Y			Y
CloudLock				Y	Y	Y	Y	Y		Y
Cryptzone		Y		Y		Y	Y	Y		Y
Dataguise	Y	Y	Y			Y	Y	Y	Y	Y
Dell		Y					Y	Y	Y	
GreenSQL	Y				Y	Y	Y	Y		Y
Fasoo		Y		Y			Y	Y		Y
Fortinet	Y									
IBM	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Identity Finder		Y		Y		Y	Y	Y	Y	Y
Imperva	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Intel-McAfee	Y				Y					
Mentis	Y						Y			Y
Netskope				Y	Y	Y	Y	Y		Y
Oracle	Y	Y	Y	Y	Y	Y			Y	Y
Protegrity	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SailPoint		Y		Y		Y				
Skyhigh Networks				Y			Y			Y
STEALTHbits Technologies		Y		Y		Y	Y	Y	Y	Y
Veritas		Y		Y		Y			Y	
Trustwave	Y				Y		Y			
Varonis		Y		Y		Y	Y	Y	Y	
WareValley	Y						Y			

Da un punto di vista economico, il servizio, pur con funzionalità superiori, viene offerto allo stesso prezzo di listino proposto.