

Sommario

Una protezione che si sposta insieme al dato.....	1
Soluzioni per proteggere i dati nel Cloud	2
<i>Crittografia e Cloud</i>	<i>2</i>
<i>HP Atalla Cloud Encryption</i>	<i>3</i>
<i>Come funziona HP Atalla Cloud Encryption.....</i>	<i>4</i>
<i>HP Atalla Cloud Encryption Virtual Key Management Service.....</i>	<i>5</i>
<i>La cifratura a chiave divisa</i>	<i>5</i>
<i>Tecnologia omomorfica per proteggere le chiavi durante l'uso</i>	<i>7</i>
<i>HP Atalla Cloud Encryption Agent</i>	<i>8</i>
<i>L'offerta HP Atalla Cloud Encryption</i>	<i>8</i>
HP Atalla Information Protection and Control.....	9
HP Atalla IPC Suite.....	9
HP Atalla IPC Bridge per i servizi di analisi dei contenuti	10
HP Atalla IPC Scanner	10
Servizio di compliance HP Atalla IPC per Exchange.....	10
HP Atalla IPC AD RMS extensions for Outlook	10
HP Atalla IPC Mobile Support for Microsoft AD RMS	10
Le soluzioni Atalla per la sicurezza dei pagamenti	10
<i>HP Atalla Network Security Processor (NSP).....</i>	<i>11</i>
<i>HP Enterprise Secure Key Manager (ESKM).....</i>	<i>11</i>
HP Enterprise Security	12



HP Atalla: soluzioni enterprise per la protezione dei dati sensibili

*Dott. Riccardo Florio,
Vice President Reportec*

La crescente difficoltà a gestire la tematica del rischio deriva, da una parte dalla complessità tecnologica e di gestione e, dall'altra, dalla complessità legislativa, che rende difficile per chi non abbia alle spalle un team dedicato alla sicurezza districarsi tra leggi, norme e responsabilità.

A livello enterprise, l'esigenza di protezione, in ultima analisi, si concentra sui dati critici per il business. In un contesto dove il perimetro dell'azienda scompare e cresce l'importanza di mobilità e cloud, l'adozione di tecniche di cifratura mette a disposizione delle organizzazioni un livello di sicurezza legato al dato stesso e in grado di spostarsi in modo solidale all'informazione.

Con la gamma d'offerta Atalla, HP propone una serie di soluzioni pensate per cifrare i dati nel cloud, garantire la sicurezza dei pagamenti e proteggere e controllare le informazioni avvalendosi di tecnologie di crittografia con caratteristiche innovative.

Questo white paper analizza la tecnologia di crittografia alla base delle soluzioni HP Atalla e la corrispondente gamma d'offerta.

Una protezione che si sposta insieme al dato

L'esigenza di una crescente sicurezza nell'accesso alle informazioni è fortemente aumentata con la diffusione di Internet e con lo sviluppo di modelli di interazione tra aziende che hanno portato a un concetto di azienda estesa, dove la relazione tra le entità coinvolte si basa sulla certezza dell'interlocutore (sia esso una persona fisica o un programma) e sulla inalterabilità dei dati e delle informazioni (per esempio ordini, fatture, bolle di spedizione, documenti amministrativi e legali, bollette) che sono scambiate nel corso delle usuali attività di business.

I nuovi modelli Cloud e l'affermazione della mobilità hanno ulteriormente contribuito a complicare lo scenario della gestione del rischio. Per esempio, la componente di Cloud pubblica rende difficoltoso sia conoscere la collocazione fisica dei dati di business affidati al proprio Cloud provider sia riuscire a seguirli nei loro spostamenti.

Indipendentemente dall'approccio di sicurezza seguito, il dato rappresenta, in ultima analisi, l'elemento da proteggere.

Proteggere i dati significa molte cose: garantirne la disponibilità, l'accessibilità, la conservazione ma, dal punto di vista del business, una delle esigenze

primarie è quella di impedirne la diffusione non autorizzata e la riservatezza.

In molti casi mantenere i dati privati e sicuri costituisce anche un requisito di conformità, per esempio alle norme Sarbanes-Oxley (SOX), al Payment Card Industry Data Security Standard (PCI DSS) o alle direttive sulla protezione dei dati dell'Unione Europea che richiedono che le organizzazioni proteggano i loro dati a riposo e garantiscano efficaci difese contro le minacce.

L'adozione di tecnologie di crittografia consente di predisporre un livello di sicurezza intrinseco al dato stesso, che viene esercitato al momento stesso della sua creazione e che è in grado di spostarsi insieme all'informazione.

Questo livello di protezione è alla base dell'offerta di soluzioni HP Atalla, sviluppate per proteggere i dati inattivi, attivi e in uso nel corso del loro intero ciclo di vita, all'interno di ambienti cloud, on-premises e mobili.

 <p>Payments security</p> <p>Secure payments and transacting systems</p>	 <p>Cloud and Data Security</p> <p>Encrypt and protect keys and data in public, hybrid, and private clouds</p>	 <p>Information Protection & Control</p> <p>Embed security at the point of creation for sensitive enterprise data</p>
---	---	--

L'offerta HP Atalla

La gamma d'offerta è strutturata attorno a tre macro esigenze di business: soluzioni per la protezione dei dati nel cloud, soluzioni per la protezione e il controllo dei dati e soluzioni per la sicurezza dei pagamenti.

Soluzioni per proteggere i dati nel Cloud

Crittografia e Cloud

Diverse sono i benefici che le aziende possono ottenere spostando applicazioni e dati nel Cloud: dalla scalabilità, all'agilità, alla riduzione dei costi. Tuttavia, ai potenziali vantaggi sono associati anche nuovi rischi. Una dimostrazione di ciò giunge anche da un survey condotto da HP nel novembre 2013 (HP Cloud-public cloud security research) che ha messo in luce come il 16 per cento delle aziende intervistate presenti sul Cloud abbia riportato almeno una violazione del cloud pubblico negli ultimi 12 mesi.

Peraltro, va ricordato che i Cloud provider che offrono servizi di Infrastructure as a Service (IaaS) e Platform as a Service (PaaS) propongono solitamente un modello di "responsabilità condivisa" per le applicazioni e i dati dei loro clienti e, di conseguenza, la responsabilità della sicurezza dei dati nel cloud è un

problema la cui soluzione spetta alle aziende proprietarie dei dati.

La crittografia dei dati è uno dei metodi più efficaci per proteggere i dati a riposo nel cloud, ma non tutte le tecnologie sono identiche. Al fine di selezionare la soluzione più efficace per le proprie specifiche esigenze aziendali, è importante analizzare alcuni aspetti fondamentali legati alla gestione del processo di crittografia e al modo in cui viene esercitata la protezione dei dati in uso o a riposo attraverso ogni fase del loro ciclo di vita e a come viene affrontata la gestione e la sicurezza delle chiavi di crittografia.

Una delle preoccupazioni primarie per chi sceglie modelli Cloud di tipo ibrido o pubblico è proprio quella di garantire la massima segretezza delle chiavi di cifratura riuscendo, nel contempo, a mantenerne la proprietà e il controllo: due obiettivi spesso tra loro antagonisti.

Infatti, tutti i sistemi di crittografia dei dati, sia nel cloud o in un data center fisico, condividono una vulnerabilità comune: hanno bisogno di utilizzare le chiavi di crittografia e, quando queste sono in uso, è possibile, ipoteticamente, rubarle.

Nell'analizzare una soluzione di crittografia è anche opportuno valutarne il livello di versatilità e la sua capacità di supportare i diversi possibili casi d'uso:

crittografia del disco, del database, del file system e dello storage distribuito.

Attraverso la divisione Enterprise Security Products, in risposta a tutte queste esigenze, HP propone HP Atalla Cloud Encryption, una soluzione che adotta numerose precauzioni conosciute e le combina con altre di nuovo tipo.

HP Atalla Cloud Encryption

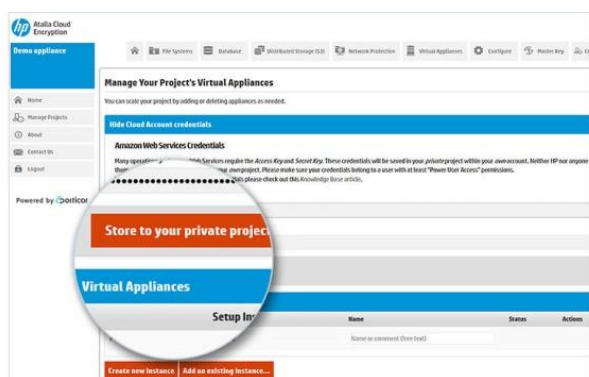
HP Atalla Cloud Encryption, avvalendosi del motore Porticor, combina cifratura allo stato dell'arte implementata su appliance (fisica o virtuale) con una tecnologia brevettata di gestione delle chiavi progettata per proteggere i dati critici in ambienti Cloud di tipo pubblico, ibrido e privato. Questa soluzione permette di crittografare l'intero layer dei dati, inclusi i principali database (Oracle, MySQL, Microsoft SQL Server e IBM DB2), i file e lo storage distribuito all'interno di un Cloud pubblico, ibrido e privato con chiavi che non risultano mai esposte in modo vulnerabile.

Per fornire protezione nel cloud HP Atalla Cloud Encryption utilizza tre tecnologie di base:

- 1 crittografia dei dati basata su standard gestibile attraverso un'interfaccia utente molto semplice;
- 2 un servizio cloud-ready per la gestione delle chiavi che utilizza la

tecnologia brevettata di cifratura con chiave divisa;

3 tecniche di crittografia a chiave omomorfica che proteggono le chiavi anche quando sono in uso.



L'interfaccia grafica per la gestione di Atalla Cloud Encryption

Come funziona HP Atalla Cloud Encryption

HP Atalla Cloud Encryption fornisce la possibilità di inserire la soluzione di crittografia tra l'archiviazione dei dati e l'applicazione o il database server nel cloud. Una volta che è stata concessa l'autorizzazione, la soluzione di crittografia risulta trasparente per l'applicazione e può essere integrata velocemente e con facilità senza modificare alcuna applicazione.

Ogni volta che un'applicazione (per esempio un database server) scrive un blocco dati su un disco, questo passa attraverso un'appliance virtuale sicura in cui i dati vengono crittografati e poi inviati al volume del disco. Tutte le

richieste per leggere i dati dal disco vengono inviati alla appliance virtuale sicura, che legge i blocchi di dati cifrati, li decodifica, e quindi invia i dati di testo in chiaro all'applicazione richiedente.

HP Atalla Cloud Encryption utilizza l'algoritmo di crittografia Advanced Encryption Standard (AES) con chiave a 256 bit. Blocchi multipli sono incatenati con Cipher-Block Chaining (CBC) e lo schema Encrypted Salt-Sector Initialization Vector (ESSIV) viene utilizzato per contrastare i cosiddetti attacchi "watermarking" indirizzati ai metodi di cifratura del disco e in cui la presenza di un blocco di dati appositamente predisposto (per esempio, un file di richiamo) può essere rilevato da un attaccante senza conoscere la chiave di crittografia.

La soluzione proposta da HP può cifrare in modo dinamico:

- *i volumi di un disco*, sia che si presentino alle applicazioni come dischi NFS o come volumi CIFS;
- *i volumi di dischi in una SAN*, tramite il supporto del protocollo iSCSI;
- *lo storage distribuito*, nei casi in cui le applicazioni scrivono l'intero file all'interno di un Web service. Il motore Porticor supporta sia Amazon S3 (Simple Storage

Service) che è attualmente l'implementazione più diffusa sia consente l'integrazione con altre implementazioni.

Oltre alla crittografia, HP Atalla Cloud Encryption mette a disposizione anche altre tecnologie per rafforzare la sicurezza dei dati quali:

- firma digitale per garantire che il dato non venga alterato,
- una tecnologia brevettata di dispersione dei dati e di decostruzione per rendere più difficoltoso trovare i dati nel cloud,
- sistemi di registrazione e di allerta su eventi legati ai dati a supporto delle azioni di auditing e di compliance.

HP Atalla Cloud Encryption Virtual Key Management Service

Le best practice di sicurezza prevedono di non memorizzare la chiave di cifratura accanto ai dati crittografati, in quanto entrambi le componenti potrebbero risultare vulnerabili al medesimo attacco. Nel cloud questo rappresenta un obiettivo irrealizzabile: non è possibile evitare di memorizzare le chiavi nel cloud assieme ai dati poiché si ha bisogno delle chiavi per accedere ai dati memorizzati sui server applicativi e sui database server.

L'approccio seguito da HP per ovviare a questa condizione all'interno della soluzione HP Atalla Cloud Encryption prevede di mettere a disposizione un servizio di gestione delle chiavi ospitato all'interno del cloud che eviti di penalizzare la sicurezza grazie all'utilizzo di una tecnologia di crittografia a chiave divisa e omomorfica.

Questo servizio denominato HP Atalla Cloud Encryption Virtual Key Management (VKM) Service è fornito attraverso il cloud ed è supportato dal partner di HP, Porticor. Il servizio VKM fornisce la capacità di generare chiavi di crittografia che possono essere utilizzate dal software HP Atalla Cloud Encryption implementato nell'infrastruttura cloud.

L'accesso al servizio avviene dal sito Web di HP Atalla Cloud Encryption su connessione <https> attraverso l'integrazione con un'appliance virtuale.

Il servizio è disponibile in modalità 24x7 ed è progettato per fornire un livello di disponibilità (SLO) del 99,99 per cento. Nel caso in cui un disastro di varia natura abbia un impatto sul servizio, HP garantisce il ripristino dell'accesso entro 15 giorni lavorativi.

La cifratura a chiave divisa

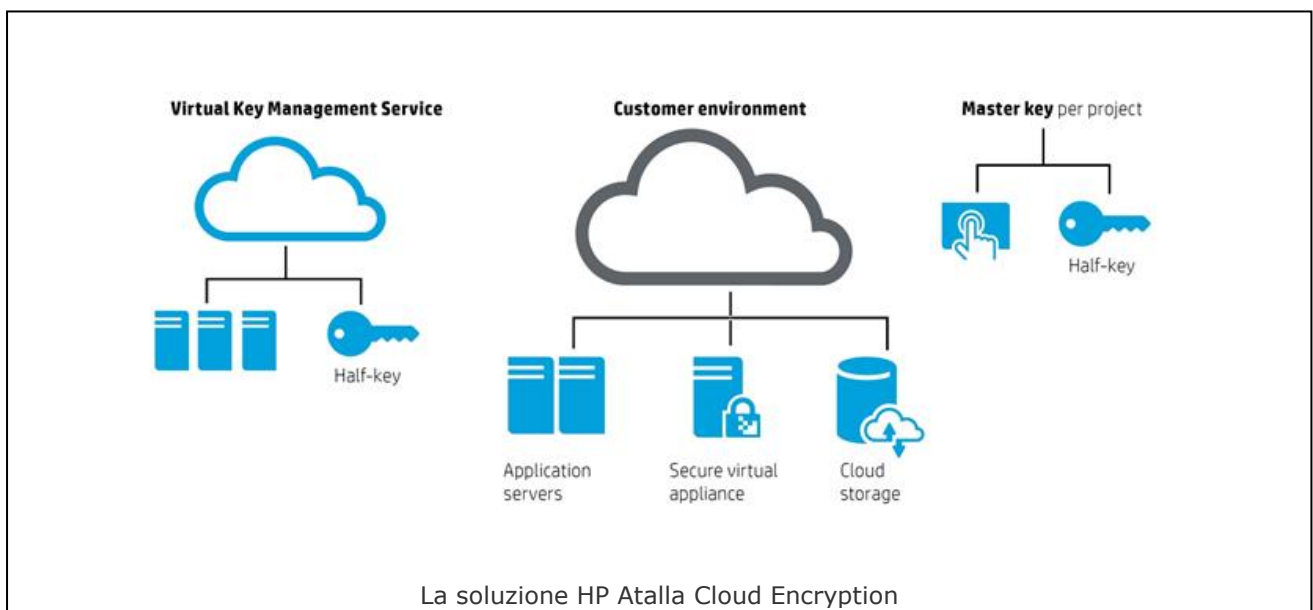
La cifratura a chiave divisa utilizzata nella soluzione HP Atalla Cloud Encryption prevede che ogni "data

object" (per esempio un disco o un file) venga cifrato con un'unica chiave che viene separata in due. La prima parte, la cosiddetta Master Key, è uguale per tutti i "data object" nell'applicazione e rimane in possesso solo del proprietario dell'applicazione mentre è sconosciuta ad HP. La seconda parte della chiave è differente per ogni "data object" e viene generata dall'appliance virtuale sicura all'interno del servizio di gestione delle chiavi e di HP e memorizzata nel Key Management Service dopo averla ulteriormente cifrata con una chiave privata RSA.

Entrambi le chiavi devono essere utilizzate contemporaneamente per svolgere le operazioni crittografiche. Quando un'applicazione accede all'archivio dati, l'appliance combina la chiave master con la seconda chiave per ottenere una chiave che può

effettivamente decifrare un oggetto.

In altre parole, ogni volta che un utente crea un nuovo progetto (applicazione), si genera una sola chiave Master che viene memorizzata in modo sicuro su sistemi on-premises. La chiave Master viene utilizzata dall'appliance virtuale sicura che risiede nel Cloud dell'utente, ma non viene mai trasferita al Key Management Service di HP Atalla Cloud Encryption. Quando un volume di disco o un oggetto Amazon S3 viene crittografato, questo riceve una nuova chiave che è una combinazione matematica della Master Key e di una chiave casuale univoca creata dall'appliance virtuale sicura e conservata in forma crittografata nel Key Management Service. In tal modo, per ogni applicazione o progetto, l'utente deve tenere traccia solo di una Master Key.



Quando non è più necessario l'accesso continuato a un "data object", è possibile utilizzare l'interfaccia di gestione (API) per "bloccare" l'oggetto. La chiave viene poi cancellata, e solo la seconda parte viene conservata (criptata) nel virtual Key Management Service.

L'oggetto in tal modo risulta ancora protetto sia dalla Master Key sia dall'altra chiave e quando la chiave dovesse servire di nuovo per la riattivazione del volume, può essere prelevato dal virtual Key Management Service.

Tecnologia omomorfica per proteggere le chiavi durante l'uso

L'operazione con cui l'appliance virtuale combina le due parti delle chiavi di cifratura solitamente richiederebbe che entrambi le parti della chiave vengano esposte in modo non cifrato.

HP Atalla Cloud Encryption, invece, mantiene sicuri i dati e le chiavi di cifratura anche quando sono in uso nel cloud, grazie all'uso di tecnologia crittografica omomorfica: una tecnica che abilita l'esecuzione di operazioni matematiche su dati cifrati. Di fatto, con HP Atalla Cloud Encryption entrambi le parti della chiave sono cifrate prima e durante il loro utilizzo nell'appliance. Di conseguenza, l'appliance virtuale

fornisce all'applicazione l'accesso all'archivio dei dati senza mai esporre le chiavi Master in modo non cifrato.

La soluzione Atalla cifra la Master Key in modo differente per ogni istanza della virtual appliance sicura. Nel caso improbabile che l'appliance virtuale fosse violata e la chiave di crittografia venisse rubata, solo l'oggetto dati stocasticamente dipendente che è in memoria in quel momento sarebbe esposto. Per accedere al resto dei dati archiviati, il ladro avrebbe bisogno della Master Key del progetto enterprise.

Va osservato che l'esecuzione di un processo di cifratura omomorfica completo consentirebbe di effettuare tutte le operazioni matematiche sui dati cifrati ma richiederebbe un'enorme potenza elaborativa, difficilmente disponibile.

Per ovviare a questo inconveniente HP ha predisposto una tecnologia di cifratura (in attesa di brevetto) parzialmente omomorfica per combinare e separare le chiavi di cifratura, che interessa solo il link più critico del processo di cifratura dei dati all'interno del cloud (di fatto la Master Key) riducendo, in tal modo, il carico elaborativo complessivo.

HP Atalla Cloud Encryption Agent

L'agent HP Atalla Cloud Encryption, consente agli utenti delle soluzioni HP Atalla di crittografare i dati su disco direttamente sul loro server applicativo e anche di generare dischi cifrati virtuali all'interno di file regolari in un file system esistente. Tutti i processi di cifratura e decifratura avvengono localmente sull'host server per massimizzare le prestazioni.

HP Atalla Cloud Encryption Agent si aggiunge alle funzionalità di creazione dei dischi crittografati in modalità inline fornite dall'appliance virtuale di HP Atalla Cloud Encryption.

Come misura di sicurezza aggiuntiva, l'agente HP Atalla Cloud Encryption viene rilasciato utilizzando una chiave API sicura, che permette di accedere alle sue chiavi crittografiche gestite ma non alla Master Key.

Le procedure di cifratura del disco avvengono localmente sull' host server che fa girare HP Atalla Cloud Encryption Agent, e le chiavi di cifratura sono divise tra la virtual appliance HP Atalla Cloud Encryption e il HP Atalla Cloud Encryption Virtual Key Management (VKM) Service.

L'offerta HP Atalla Cloud Encryption

HP Atalla Cloud Encryption viene offerto da HP in molteplici opzioni di deployment, supportando VMware e Amazon Web Services con possibilità di supporto 9x5 e 24x7.

In particolare l'offerta prevede

- HP Atalla Cloud Encryption for Amazon Web Services per virtual appliance ovvero rilasciato nell'ambiente cloud del cliente con un prezzo per appliance virtuale
- HP Atalla Cloud Encryption for VMware per virtual appliance ovvero rilasciato nell'ambiente cloud del cliente con un prezzo per appliance virtuale
- HP Atalla Cloud Encryption agent per istanza su VMware ovvero rilasciato per l'installazione sull' application server nell'ambiente cloud del cliente su sistema operativo Linux e un prezzo per istanza dell'agente su VMware.
- HP Atalla Cloud Encryption agent per istanza su AWS ovvero rilasciato per l'installazione sull' application server nell'ambiente cloud del cliente su sistema operativo Linux e un prezzo per istanza dell'agente su AWS.

HP Atalla Information Protection and Control

HP Atalla Information Protection and Control (IPC) mette a disposizione una serie di soluzioni per la classificazione e la protezione delle informazioni all'interno dell'organizzazione aziendale

L'offerta HP Atalla IPC include software di gestione, reporting e analytics, moduli per la protezione di file e cartelle, protezione dei dati delle applicazioni, protezione della posta e dei dati non strutturati multi-formato.

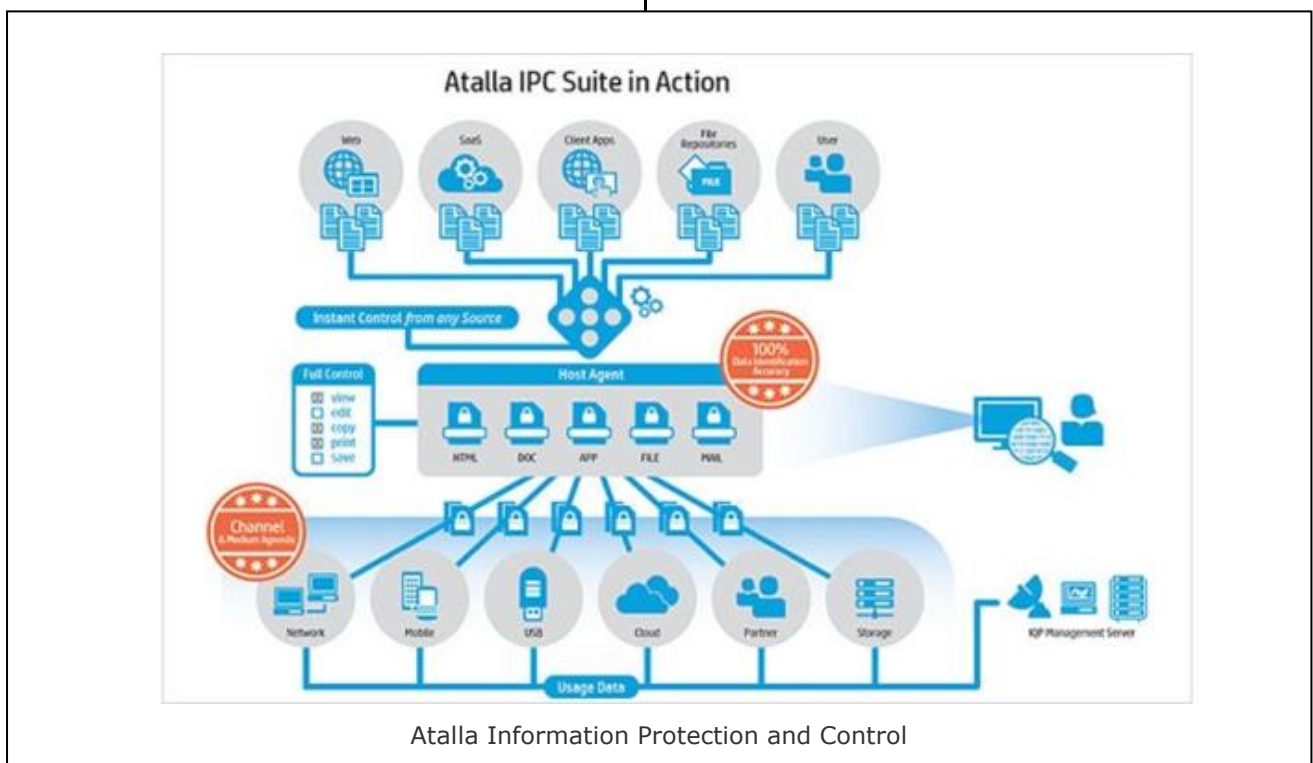
HP Atalla IPC si avvale del motore della piattaforma IQProtector, grazie alla partnership con Secure Islands

Technologies, per fornire una protezione incorporata ai dati al momento della loro creazione. Gli Agenti IQProtector presenti sull'host enterprise, identificano immediatamente e in modo preciso i dati sensibili nuovi, modificati o acceduti da qualsiasi origine, applicandogli un livello avanzato di classificazione, contrassegnandoli e consentendo il controllo completo sul loro accesso e utilizzo.

La famiglia di software HP Atalla IPC è strutturata nelle seguenti componenti.

HP Atalla IPC Suite

È la suite centrale per la protezione delle informazioni che include il software di gestione e i seguenti moduli funzionali:



- Persistent Multi-format File Protection;
- Persistent Email Protection;
- Persistent Web, Application, and Cloud Protection;
- Persistent Information Protection Data Analytics;
- Persistent Protection for Remote Desktop Services (per esempio Citrix/Terminal Services);
- SharePoint Classification and Protection.

HP Atalla IPC Bridge per i servizi di analisi dei contenuti

Viene rilasciato su servizi enterprise quali antivirus, DLP, ricerca, archiviazione, indicizzazione per accedere e scandire contenuti cifrati senza soluzione di continuità.

HP Atalla IPC Scanner

Una soluzione per la classificazione e la protezione. Si tratta essenzialmente di un "document crawler" che passa in scansione classifica e protegge i dati preesistenti sui repository.

Servizio di compliance HP Atalla IPC per Exchange

Un'offerta che mette a disposizione la possibilità di decifrare le email e gli allegati protetti per l'archiviazione e per esigenze di conformità. Questo servizio

viene distribuito sui server Microsoft Exchange e gestito centralmente.

HP Atalla IPC AD RMS extensions for Outlook

Fornisce un modo semplice per applicare la protezione Microsoft Active Directory Rights Management Services (AD RMS) all'interno di Microsoft Outlook per incrementare l'effettivo utilizzo dei servizi RMS all'interno dell'organizzazione. Consente un livello di flessibilità all'utente finale per applicare permessi che si estendono oltre gli standard di Microsoft Outlook.

HP Atalla IPC Mobile Support for Microsoft AD RMS

Mette a disposizione delle organizzazioni la possibilità di collaborare con email ed allegati protetti da servizi di gestione dei diritti (Rights Management Services, RMS) in modo sicuro sui principali sistemi operativi e device mobili come iOS, Android, Windows, BlackBerry.

Le soluzioni Atalla per la sicurezza dei pagamenti

HP Atalla fornisce anche una gamma di soluzioni di sicurezza per pagamenti e transazioni elettroniche che mette a disposizione chiavi di crittografia business-critical. Le soluzioni HP Atalla soddisfano i requisiti degli standard

critici per la sicurezza e la conformità dei servizi finanziari, inclusi NIST, PCI-DSS e HIPAA/HITECH per la protezione dei dati sensibili e la prevenzione delle frodi.

La soluzione per la sicurezza dei pagamenti prevede due componenti che operano congiuntamente per garantire una protezione della rete end-to-end, trasparente per l'utente e a elevate prestazioni.

HP Atalla Network Security Processor (NSP)

Il primo è il modulo di crittografia hardware HP Atalla Network Security Processor (NSP) che soddisfa i più stringenti standard incluso FIPS 140-2 livello 3 a supporto delle attività di gestione delle autorizzazione di pagamento a mezzo carta e delle verifiche di PIN ATM/POS.

Si tratta di un modulo di sicurezza hardware a prova di manomissione, pensato per le soluzioni di cifratura sulle reti di trasferimento elettronico dei fondi, di bancomat e di POS, che fornisce crittografia ad alte prestazioni e capacità di gestione delle chiavi per l'autorizzazione dei pagamenti con carta di credito.



HP Atalla Network Security Processor (NSP)

HP Enterprise Secure Key Manager (ESKM)

Il secondo componente è il sistema sicuro di gestione delle chiavi HP Enterprise Secure Key Manager (ESKM) che consente di ridurre il rischio di danni ai dati crittografati e alla reputazione e che facilita la conformità con le normative del settore. HP ESKM è una soluzione per la creazione, l'archiviazione, la fornitura, il controllo e l'accesso per esigenze di auditing alle chiavi di cifratura dei dati; permette di proteggere e preservare l'accesso alle chiavi di crittografia sia in locale sia da remoto.



HP Enterprise Secure Key Manager

HP Enterprise Security

Attraverso la divisione HP Enterprise Security Products, HP punta ad affrontare le nuove esigenze di protezione attraverso una strategia complessiva di intervento sia sul versante della protezione richiesta dalle aziende, sia per garantire agli utenti un accesso immediato e senza rischi alle corrette risorse aziendali, ponendo le basi per un approccio unificato alla sicurezza enterprise, in un contesto di integrazione che coinvolge servizi, applicazioni e prodotti. L'offerta di HP ESP è articolata nelle famiglie di soluzioni HP ArcSight, HP Fortify, HP Atalla e HP TippingPoint.

Reportec

REPORTEC opera dal 2002 nel settore dell'editoria specializzata sull'ICT professionale, realizzando e pubblicando riviste, report, survey, e-magazine, libri. Pubblica le riviste cartacee Direction, Solutions, Partners (edito dalla consociata Reportrade) e gli e-magazine Update Reportec, Security & Business, Cloud & Business, PartnersFlip. Ha siglato un accordo con **Tom's Hardware Italia** per la gestione dei tre canali B2B IT Pro, Manager e Resellers accessibili all'interno del dominio tomshw.it. Reportec è Media e Content Conference **Partner di IDC Italia**.



Dott. Riccardo Florio Da vent'anni opera nel settore dell'editoria specializzata professionale.

È coautore di rapporti, studi, Survey e libri nel settore dell'ICT. È laureato in Fisica ed è iscritto all'ordine dei giornalisti della Lombardia. È cofondatore

e Vice President di Reportec, dove ricopre la carica di Direttore Responsabile della testata Direction e dell'e-magazine Update Reportec.



HP Atalla: soluzioni enterprise per la protezione dei dati sensibili

© Reportec S.r.l. - Ottobre 2014 - Tutti i diritti riservati

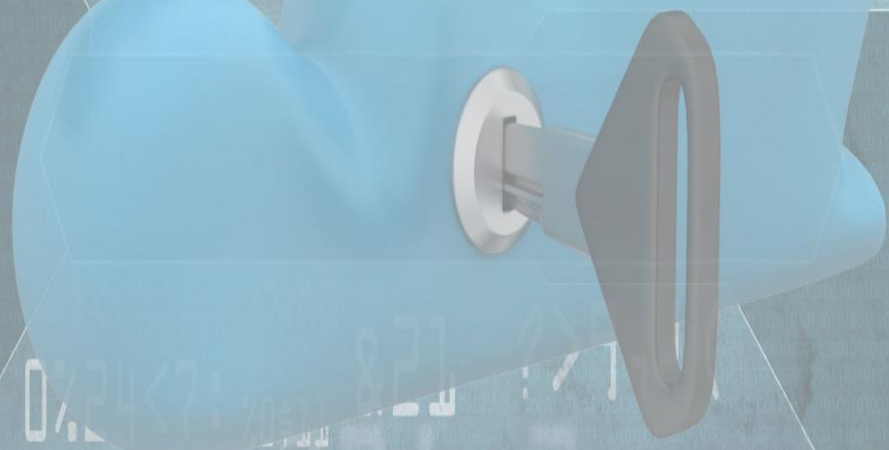
Reportec S.r.l. via Marco Aurelio, 8 - 20127 Milano

Tel: (+39) 02 36580441 Fax: (+39) 02 36580444

www.reportec.it - www.tomshw.it/index/itpro.html - www.tomshw.it/index/manager.html - www.tomshw.it/index/reseller.html

Tutti i marchi citati in questo documento sono registrati e di proprietà delle relative società.

database signature encoding verification trust
hash certificate private public context
communication sensitive solution data authentication
confidential storage business information protection
password data network security exchange biometrics cloud
safe key computer internet cryptography database
ciphertext communication confidential encoding



0%24<7: 821 ?>1
: 9167B)4>@01*01 1/#0359BH5*
%1'*(74 TM-V1 4&' + &225)#! A03'*\$#!9=52A+
571\$*+4 ?(640961)>:F9167B)4>@7(640961)>:F
3&567<10011%#: JA56*
1/#0359BH5* 0%24<79167B)4>@0 3&567<10011%#: JA56*/ &21