



Soluzioni integrate
per la protezione d'impresa:
l'offerta software di
HP Enterprise Security Products

Reportec

Sommario

Il business si trasforma	1
<i>Nuove esigenze di protezione.....</i>	<i>2</i>
La sicurezza enterprise di HP	2
<i>HP ArcSight: la piattaforma di Security Intelligence</i>	<i>3</i>
HP ArcSight ESM.....	4
HP ArcSight Logger	5
HP ArcSight IdentityView	5
HP ArcSight ThreatDetector.....	6
HP ArcSight Express.....	6
ArcSight Application View.....	6
ArcSight Risk Insight.....	8
HP ArcSight Management Center	8
<i>HP Fortify: la sicurezza nello sviluppo applicativo</i>	<i>8</i>
HP Fortify Software Security Center	9
HP Fortify Static Code Analyzer.....	9
HP WebInspect	10
Fortify on Demand	11
<i>HP Atalla: la sicurezza delle transazioni:.....</i>	<i>12</i>
Le risorse HP per aumentare la protezione	13
<i>HP Reputation Security Monitor (RepSM).....</i>	<i>13</i>
<i>HP Threat Central.....</i>	<i>13</i>
<i>HP Security Research.....</i>	<i>14</i>
<i>HP DV Labs.....</i>	<i>14</i>
<i>Zero-Day Initiative</i>	<i>15</i>
<i>HP TippingPoint Web AppDV</i>	<i>15</i>
<i>Digital Vaccine Toolkit (DVToolkit)</i>	<i>16</i>
<i>HP Reputation Digital Vaccine (RepDV)</i>	<i>16</i>
Conclusioni	17



Soluzioni integrate per la protezione d'impresa: l'offerta software di HP Enterprise Security Products

*Dott. Riccardo Florio
Vice President Reportec*

La crescente diffusione di mobilità, cloud computing e social media sta ampliando i rischi a cui si trova esposto il patrimonio informativo aziendale e per far fronte in modo efficace a queste sfide, le aziende puntano sempre più verso una gestione della sicurezza e del rischio integrate.

Per poter affrontare le nuove esigenze di protezione, HP punta a predisporre una strategia complessiva che intervenga 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.

Il business si trasforma

È in atto un processo di "business transformation" che sta ridefinendo completamente i processi aziendali, aumentando la produttività, cambiando le relazioni di lavoro e sviluppando attività completamente nuove.

Gli strumenti di social business o social collaboration ne sono un esempio. Un altro riguarda tutto il mondo delle App mobile che, oltre ad aprire le porte a servizi prima impensabili, sta portando alla nascita di aziende nuove dedicate a nuovi business, mentre il video ad alta definizione sta cambiando il modo di relazionarsi, riducendo gli spostamenti o permettendo servizi di nuovo tipo.

In questo scenario gli attacchi ai sistemi informatici diventano ogni giorno più frequenti e hanno mutato natura, ricadendo oramai completamente nella regia della criminalità organizzata orientata al profitto, arrivando a generare un mercato illegale stimato in oltre 100 miliardi di dollari. Nel contempo, le aziende globali spendono 5 miliardi di dollari all'anno per la compliance, mentre oltre la metà dei dipendenti utilizza i propri dispositivi mobile per accedere ad applicazioni aziendali business critical.

Nuove esigenze di protezione

In questo scenario di profonda trasformazione dell'IT il tema della sicurezza è sempre più pervasivo.

A livello di rete cresce l'impatto degli attacchi DDoS (Distributed Denial of Service) e si affacciano le APT (Advanced Persistent Threat) mentre i sistemi di difesa di tipo più tradizionale mostrano i propri limiti nel rilevare le nuove tipologie di intrusioni o nel contrastare la sofisticazione dei malware più recenti.

La mobilità rimuove gli ultimi limiti in termini di spazio e tempo aprendo enormi opportunità, ma porta con sé nuovi rischi legati alle caratteristiche dei dispositivi, alle componenti applicative e alle modalità d'utilizzo in cui scompare il confine tra personale e aziendale all'insegna del fenomeno noto come BYOD.

I rischi si espandono anche verso l'orizzonte applicativo influenzando i metodi di test dei processi di sviluppo e richiedendo modelli di protezione basati sull'analisi comportamentale anziché sulla mera classificazione del malware.

Un ulteriore aspetto distintivo del nuovo scenario della sicurezza è legato alla crescente diffusione dell'uso di risorse IT sotto forma di servizio o nel cloud, che estende, tra l'altro, le problematiche legate alla conformità normativa poiché

sposta i dati aziendali in un Web privo di confini nazionali.

Da tutto ciò emerge l'esigenza di predisporre una sicurezza dinamica e integrata basata su meccanismi automatizzati e strumenti costantemente aggiornati, in grado di analizzare la posta elettronica, le applicazioni, il traffico Web, i dati e i comportamenti di utenti e dispositivi.

La sicurezza enterprise di HP

Per rispondere alle nuove esigenze di protezione HP ha messo a punto una strategia per la gestione del rischio che prevede interventi sia sul versante della protezione richiesta dalle aziende, sia per garantire agli utenti un accesso sicuro alle corrette risorse aziendali, ponendo le basi per un approccio unificato alla sicurezza enterprise. L'approccio integrato alla sicurezza enterprise di HP risponde anche alle crescenti richieste di sicurezza dei nuovi ambienti virtualizzati e cloud.

Le soluzioni che compongono la piattaforma di sicurezza di HP sono proposte attraverso una divisione specifica denominata Enterprise Security Products (ESP) e comprendono i sistemi di nuova generazione HP TippingPoint per la prevenzione delle intrusioni

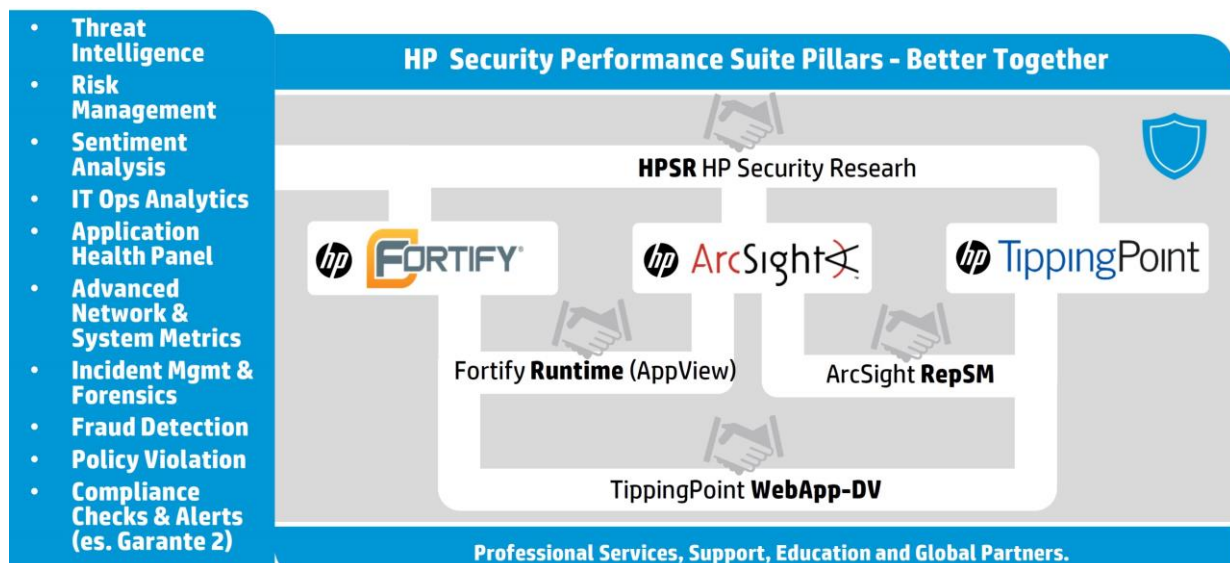
(NGIPS) e firewall (NGFW), le soluzioni di protezione dei dati ArcSight, la famiglia Fortify per la sicurezza dello sviluppo applicativo e Atalla per garantire transazioni sicure, in un contesto di integrazione che coinvolge servizi, applicazioni e prodotti.

Questa gamma di soluzioni segue un processo evolutivo che prevede sia la trasformazione e il miglioramento continuo di ciascuna tecnologia verticale, sia un'integrazione sempre più spinta delle diverse funzionalità al fine di sfruttare al massimo la sinergia di strumenti che affrontano su piani diversi il tema della protezione, migliorando la gestione e incrementando il livello di intelligenza necessario a fronteggiare le nuove minacce che operano in modo sempre più stratificato.

HP ArcSight: la piattaforma di Security Intelligence

HP ha raggruppato all'interno della famiglia ArcSight le soluzioni software indirizzate a proteggere i dati attraverso il monitoraggio, l'analisi e la correlazione di eventi di sicurezza provenienti da differenti tipologie di sorgenti.

Nel suo complesso ArcSight rappresenta una piattaforma integrata di Security Intelligence e Risk Management in grado di abbinare le funzionalità di un Sistema di gestione delle informazioni e degli eventi di sicurezza (SIEM) con un approccio preventivo basato su un modello di analisi intelligente delle minacce, effettuato su scala globale attraverso una serie di servizi predisposti da HP.



Il SIEM rappresenta il centro di controllo dell'Intelligent Security di HP

La piattaforma HP ArcSight Security Intelligence fornisce visibilità sulle attività che interessano l'intera infrastruttura enterprise correlando log, ruoli dell'utente e flussi di rete per individuare eventi legati alla sicurezza in base ai quali definire priorità e predisporre risposte efficaci e preventive a minacce di vario tipo.

L'elemento centrale e abilitante di questa famiglia di soluzioni è il motore di analisi per la gestione di minacce e rischi HP ArcSight ESM.

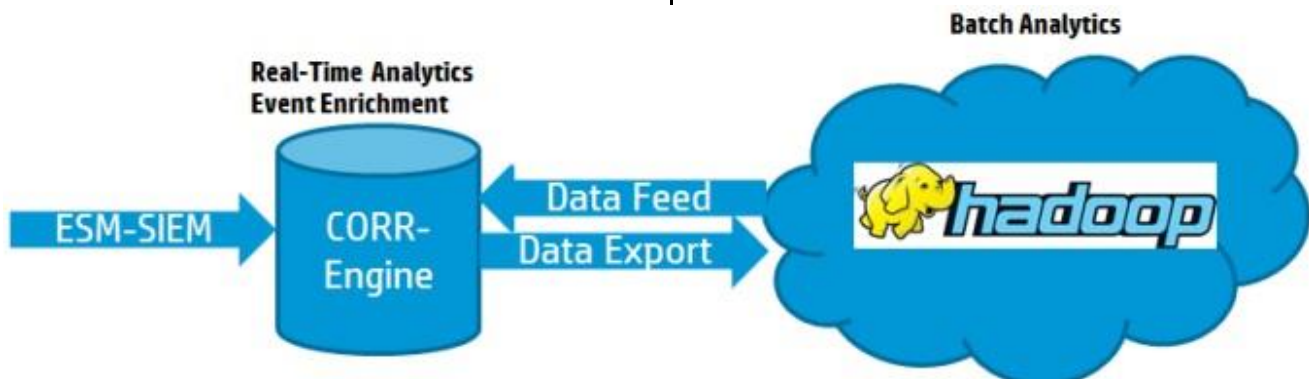
HP ArcSight ESM

HP ArcSight ESM è una soluzione SIEM per la raccolta, l'analisi e la correlazione delle informazioni di sicurezza e degli eventi di rischio, la protezione delle applicazioni e la difesa della rete e per il Governance, Risk management and Compliance (GRC).

HP ArcSight ESM è in grado di effettuare analisi capaci di correlare: minacce esterne come malware e attacchi di hacker, minacce interne come le

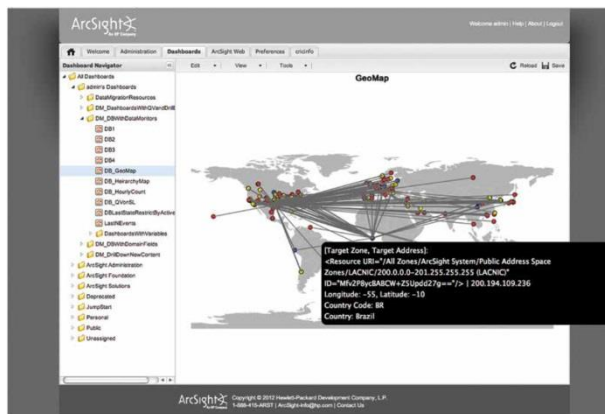
violazioni di dati e le frodi, rischi derivanti da flussi applicativi, modifiche della configurazione e problemi di conformità che scaturiscono dal mancato superamento dei controlli.

ArcSight ESM automatizza le operazioni di ricerca su Terabyte di dati, la produzione di report per la compliance e raccoglie dati di business intelligence. Il fulcro tecnologico di questa soluzione è costituito dalla quinta generazione (con prestazioni molto migliorate rispetto alla versione precedente) del motore di correlazione Correlation Optimized Retention and Retrieval Engine (CORR-Engine) che permette di scalare nel livello di risposta, in funzione della minaccia che si trova a dover affrontare. L'integrazione con Hadoop HDFS consente di sfruttare il CORR-Engine per effettuare funzioni avanzate di analytics in tempo reale oppure di inviare ad Hadoop, a un elevato "rate", i log normalizzati dal CORR-Engine per una lettura da HDFS (per esempio per operazioni di batch analytics).



Integrazione tra ArcSight ESM e Hadoop Distributed File System (HDFS)

ArcSight utilizza anche il motore HP Reputation Security Monitor che permette di analizzare in tempo reale gli indirizzi IP e i DNS potenzialmente dannosi, al fine di contrastare gli attacchi che sfruttano le vulnerabilità delle applicazioni Web.



HP ArcSight ESM

HP ArcSight Logger

All'interno della famiglia ArcSight questa soluzione abilita la raccolta di log provenienti da diversi dispositivi e in qualsiasi formato attraverso oltre 300 connettori. I dati raccolti vengono poi unificati attraverso la normalizzazione e la categorizzazione in un formato eventi comune (registrazione CEF) per poter effettuare ricerche, indicizzazione, generare report, analisi e favorirne la conservazione.

È possibile, in tal modo, migliorare le operazioni IT, dalla conformità alla gestione dei rischi, fino all'intelligence di protezione contro le minacce interne e quelle avanzate e persistenti (APT).

HP ArcSight IdentityView

HP ArcSight IdentityView è una soluzione software pensata per la protezione delle aziende enterprise da possibili minacce interne. Combina capacità di raccolta e analisi SIEM con le informazioni relative a utenti e ruoli relative ai diversi sistemi di accesso utilizzati.

Se l'attività di un utente sulla rete non corrisponde ai controlli di accesso consentiti o ai comportamenti tipici di un utente (valutati sulla base di dati storici correlati), la soluzione contrassegna il suo profilo perché venga sottoposto a indagini approfondite. Questo meccanismo aiuta il team di sicurezza a distinguere tra attività nocive intenzionali e involontarie. Il risultato è un meccanismo efficace per la mitigazione del rischio da minacce interne in tempo reale, che contribuisce a migliorare la governance degli accessi e che offre la possibilità di eseguire analisi forensi più rapidamente.

Questa soluzione, inoltre, arricchisce i log di sicurezza con informazioni sull'utente e il suo ruolo, fornendo un quadro completo delle attività anche per account ad alto rischio, privilegiati e condivisi.

Con il rilascio della versione 2.5 di ArcSight IdentityView, HP ha ampliato i meccanismi di correlazione dell'identità, dei ruoli e delle attività di sicurezza, incrementando di 10 volte il numero di utenti che una singola istanza è in grado di monitorare.

HP ArcSight ThreatDetector

È uno strumento pensato per gli analisti della protezione a cui fornisce gli strumenti necessari per distinguere un evento sospetto dai normali eventi che si verificano in rete.

ThreatDetector identifica il traffico normale e gli schemi di eventi sospetti attraverso un'analisi euristica effettuata sulla base dei dati storici e una serie di strumenti di visualizzazione e analisi del flusso dei dati.

Questo tool semplifica l'individuazione di worm "zero-day" e di attacchi complessi oltre a favorire il rilevamento degli errori di configurazione dei dispositivi di rete, dei sistemi e delle applicazioni. Fornisce, inoltre, supporto alla creazione di regole basate su modelli comportamentali.

HP ArcSight Express

HP ArcSight Express è una soluzione preconfigurata che viene integrata su un'appliance (disponibile in diverse configurazioni e modelli). Riunisce la piattaforma SIEM con la gestione dei log e il monitoraggio dell'attività degli utenti, integrando le funzionalità di IdentityView, Threat Detector e l'analisi del flusso di rete e utilizzo della banda.

In pratica, questa soluzione raccoglie i log da qualsiasi origine dati, consolida le informazioni per migliorare l'efficienza dello storage e mette in correlazione gli

eventi su più dimensioni, tra cui identità, vulnerabilità, analisi statistica e rilevamento di schemi per identificare le minacce avanzate prima che possano danneggiare i sistemi.

ArcSight Application View

Secondo gli analisti di mercato, oltre l'80% delle vulnerabilità totali sono riconducibili alle applicazioni. Un rischio cresciuto ulteriormente con la diffusione delle App: si pensi che il numero di App che individuate dai vendor di soluzioni per la sicurezza IT come potenzialmente nocive per Android ha già superato l'impressionante numero di un milione.

Con il rilascio di ArcSight Application View HP mette a disposizione una soluzione per la visibilità sugli eventi di sicurezza delle applicazioni, combinando le funzionalità di Fortify e di ArcSight ESM.

HP ArcSight Application View è stato progettato in base al presupposto che, il posto migliore per individuare, comprendere e mitigare le minacce legate alle applicazioni, risieda nel software stesso. Questa soluzione controlla automaticamente le applicazioni per fornire un'analisi intelligente sulle minacce combinando i log degli eventi di sicurezza generati dalle diverse applicazioni, incluse quelle legacy o personalizzate che, in molti

casi, non sono state progettate per fornire capacità di registrazione dei log.

HP ArcSight Application View fornisce funzionalità di registrazione dei log senza la necessità di alcuna personalizzazione e mette i dati raccolti a disposizione di HP ArcSight ESM, integrandoli nei suoi dashboard e report.

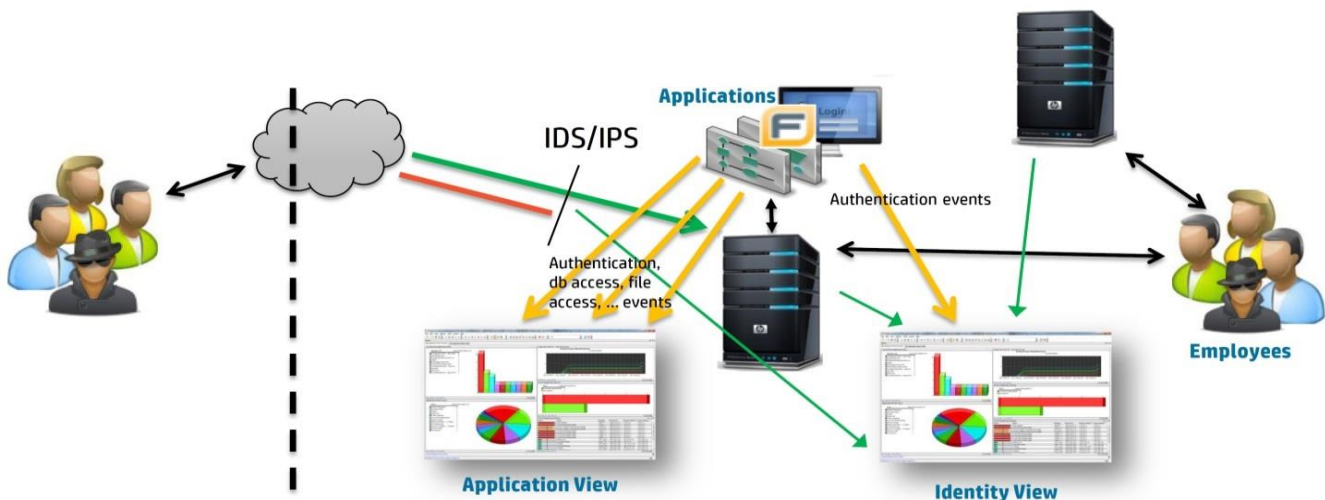
Application View è basato su Fortify Real-Time Analyzer e rappresenta un agent a livello di Application Server, la cui implementazione non richiede di effettuare modifiche alle applicazioni.

Questa soluzione fornisce una capacità di monitoraggio delle applicazioni (Java, .NET e Cold Fusion) sensibile al contesto e può essere utilizzata per contribuire a colmare le lacune di sicurezza legate alle modalità di accesso degli utenti o a un utilizzo improprio delle applicazioni: per esempio, distingue tra l'accesso di un utente autorizzato a un'applicazione

durante il normale orario di lavoro e il suo accesso ripetuto di Sabato a mezzanotte.

Rappresenta anche una soluzione complementare al software HP Identity View focalizzato sul monitoraggio dell'identità degli utenti a cui, di fatto, può mettere a disposizione ulteriori dati legati alla sicurezza; inoltre, consente di correlare le informazioni sugli eventi legati alle applicazioni con quelle associate ai sistemi IDS/IPS: per esempio gli attacchi intercettati dai sistemi IDS/IPS possono essere correlati a uno specifico login alla applicazione, per conseguire una migliore visibilità su ciò che l'attaccante sta cercando di ottenere.

Application View individua e rende disponibili ad ArcSight una serie molto estesa di fenomeni di sicurezza tra cui citiamo, per esempio, errori nel controllo dell'autorizzazione, link interrotti,



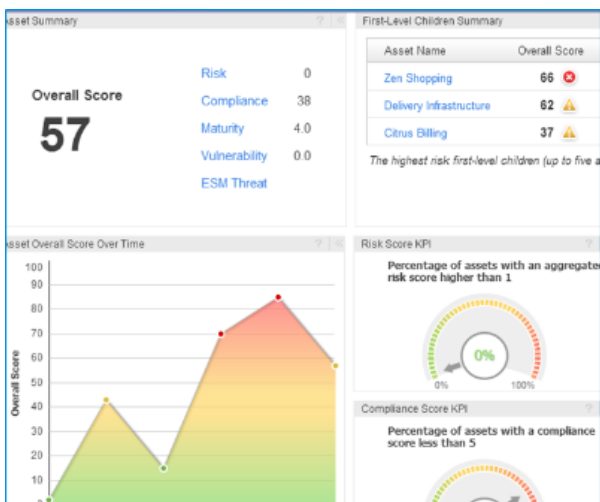
L'azione complementare di ArcSight IdentityView e Application View

tentativi di forzare l'accesso in modalità "forza bruta", Denial of Service, modifiche ai privilegi dell'utente, navigazione nelle directory, buffer overflow, sicurezza dei cookie, violazioni della privacy, sottrazioni dei dati della carta di credito, attacchi spam.

ArcSight Risk Insight

HP ArcSight Risk Insight è una delle soluzioni software aggiunte più recentemente da HP al suo portafoglio d'offerta.

Abilita, tramite ArcSight ESM, funzioni di analisi del rischio e di impatto sul business, fornendo una mappa del rischio dei servizi di business, una mappatura degli asset che estende il modello di ArcSight ESM, indicatori di rischio capaci di aggregare molteplici fonti, analisi di conformità dei processi di business.



Indicatori di rischio in ArcSight Risk Insight

HP ArcSight Management Center

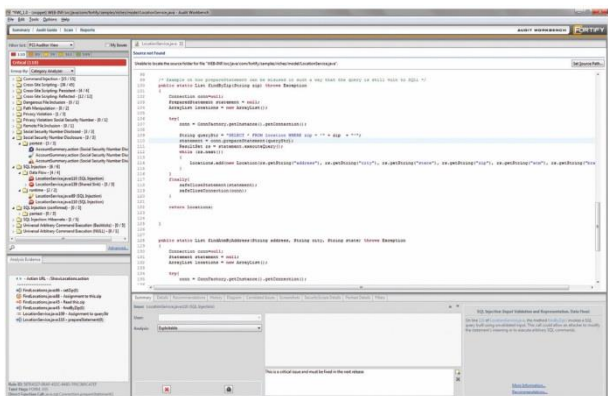
HP ArcSight Management Center è la console di sicurezza unificata e centralizzata di HP che permette di configurare, distribuire e gestire l'analisi dei Log su deployment a larga scala e di fornire funzioni unificate di gestione delle modifiche.

HP Fortify: la sicurezza nello sviluppo applicativo

La diffusione di nuove tecnologie cloud e mobili ha notevolmente incrementato la richiesta di sviluppo di nuovi software contribuendo ad accelerare ulteriormente l'esigenza di fornire in tempi rapidissimi una risposta alle richieste espresse dai clienti. Tutto ciò sta mettendo alla prova la capacità di molte organizzazioni di effettuare test di sicurezza approfondita prima della distribuzione dell'applicazione e l'elevatissimo numero di vulnerabilità associato alle applicazioni, già ricordato in precedenza, ne è un'evidenza.

All'interno della propria visione complessiva per la protezione enterprise, HP fornisce una gamma di strumenti pensati per favorire uno sviluppo sicuro ed eliminare alla fonte le possibili vulnerabilità e per predisporre ambienti di test adatti a verificare le caratteristiche di sicurezza del software.

Questa tecnica analizza ogni percorso che l'esecuzione e i dati possono seguire per identificare ed eliminare le vulnerabilità di sicurezza nel codice sorgente.



HP Fortify audit workbench

Static Code Analyzer ha la capacità di rilevare più di 500 tipi di vulnerabilità in 21 linguaggi di sviluppo e più di 700mila componenti a livello di API.

Per verificare che i problemi più gravi siano affrontati per primi, correla e assegna una priorità ai risultati per fornire una classifica dei rischi e una guida dettagliata su come risolvere le vulnerabilità a livello di linea di codice.

A partire dalla versione 4.0 HP Fortify SCA adotta un nuovo approccio basato sull'analisi di più thread di applicazioni software in parallelo per migliorare le prestazioni di scansione e per velocizzare il rilevamento e la risoluzione delle vulnerabilità.

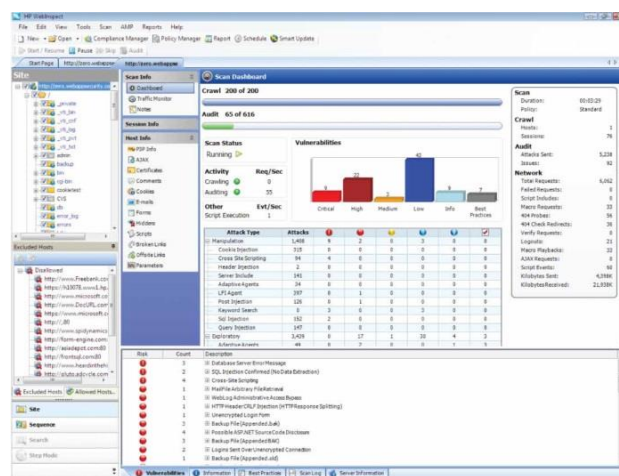
In tal modo è possibile effettuare test di sicurezza più frequenti, consentendo la scansione completa delle applicazioni senza impattare il processo di sviluppo.

Questo approccio consente di ottenere, secondo HP, anche una riduzione dei falsi positivi del 20% rispetto alle versioni precedenti del prodotto e mette a disposizione report di analisi della sicurezza software più dettagliati con classifiche di rischio per applicazioni mobili, Web, client e server.

HP Fortify SCA 4.0 offre opzioni di implementazione flessibili con possibilità di accesso on-premises oppure on-demand.

HP WebInspect

HP WebInspect è uno strumento automatizzato e configurabile che effettua test dinamici sulla sicurezza delle applicazioni Web e test di penetrazione.



HP WebInspect

Imita le tecniche di hacking e gli attacchi, consentendo di analizzare a fondo le applicazioni e i servizi Web per individuare possibili vulnerabilità di sicurezza.

Consente di testare le applicazioni Web dallo sviluppo alla produzione, di gestire in modo efficiente i risultati dei test e favorisce la distribuzione di conoscenza sulla sicurezza all'interno dell'azienda.

Fortify on Demand

HP Fortify on Demand (FoD) è il servizio di tipo Software-as-a-Service di analisi del codice che consente alle aziende di testare la sicurezza del software in modo rapido e accurato, senza la necessità di installare software.

FoD è disponibile per assessment sia statici sia dinamici e con diverse opzioni all'interno di ciascuna di queste categorie.

È possibile acquistare singole valutazioni o un abbonamento di un anno per valutazioni illimitate di una particolare applicazione.

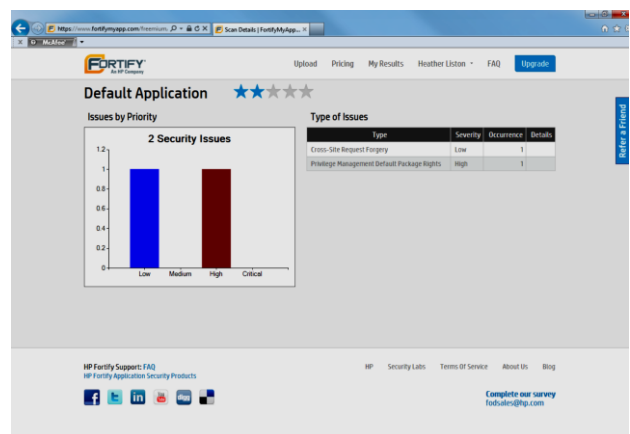
È possibile caricare i file e avviare una valutazione statica del codice oppure, se è stata acquistata una valutazione dinamica, è possibile verificare la URL.

Il team di esperti HP ha creato un processo di scansione automatica che effettua una verifica dell'applicazione in

merito alle vulnerabilità di sicurezza: l'utente fornisce a FortifyMyApp i file di analisi e il codice sorgente e Fortify esegue test automatici. L'utente riceve i risultati in 1-3 giorni lavorativi.

HP Fortify definisce quattro livelli di priorità per classificare la gravità delle vulnerabilità: critico, alto, medio e basso.

I risultati delle valutazioni sono consegnati in un insieme di semplici grafici basati su un sistema coerente di valutazione a cinque stelle, che fornisce informazioni sulla probabilità che la vulnerabilità venga identificata da un outsider e sfruttata e sull'impatto in termini di danno potenziale che un malintenzionato potrebbe fare al patrimonio aziendale sotto forma di perdita finanziaria, violazione della conformità, perdita di reputazione del marchio, pubblicità negativa o altro.



Fortify on Demand

HP Atalla: la sicurezza delle transazioni:

HP Atalla è la 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 più elevati requisiti di conformità agli standard istituzionali e del settore finanziario, inclusi NIST, PCI-DSS e HIPAA/HITECH per la protezione dei dati sensibili e la prevenzione delle frodi.

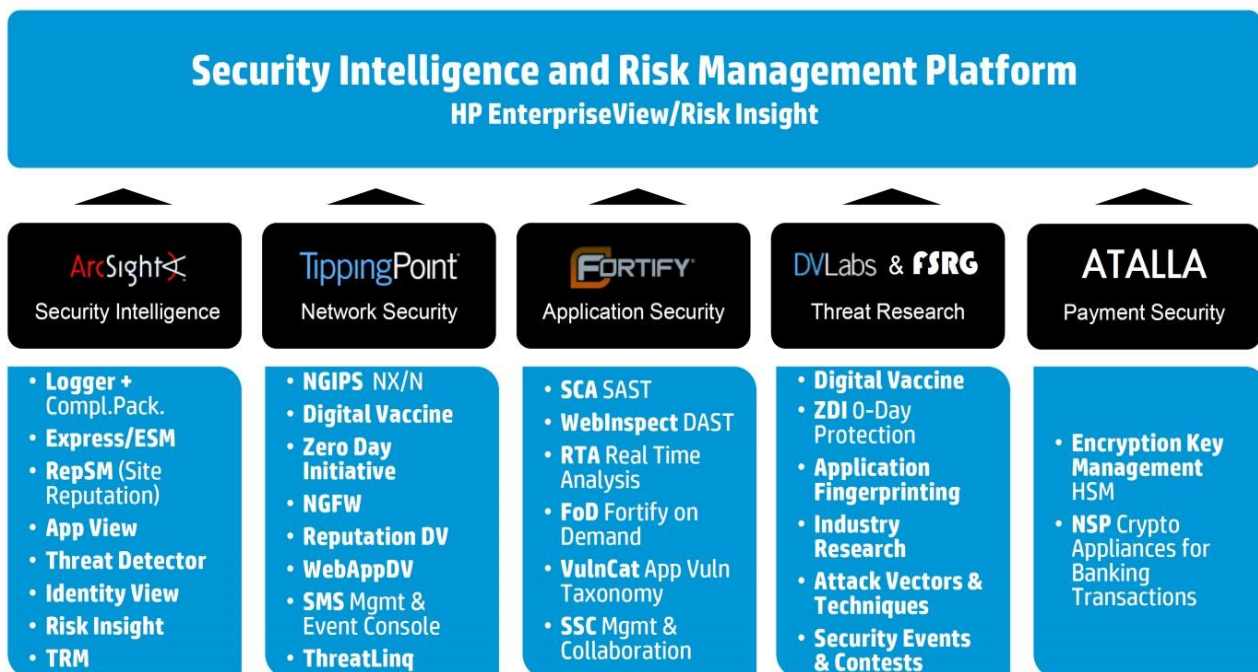
La soluzione prevede due componenti che operano congiuntamente per garantire una protezione della rete end-to-end, trasparente per l'utente e a elevate prestazioni.

Il primo è il modulo di crittografia

hardware HP Atalla Network Security Processor (NSP) che soddisfa i più stringenti requisiti incluso lo standard 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

A questo si affianca 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.

La soluzione Atalla prevede la compatibilità con applicazioni ATM, POS e EFT personalizzate o fornite dai principali produttori.



Le soluzioni che compongono la piattaforma di Security Intelligence e Risk Management di HP

Le risorse HP per aumentare la protezione

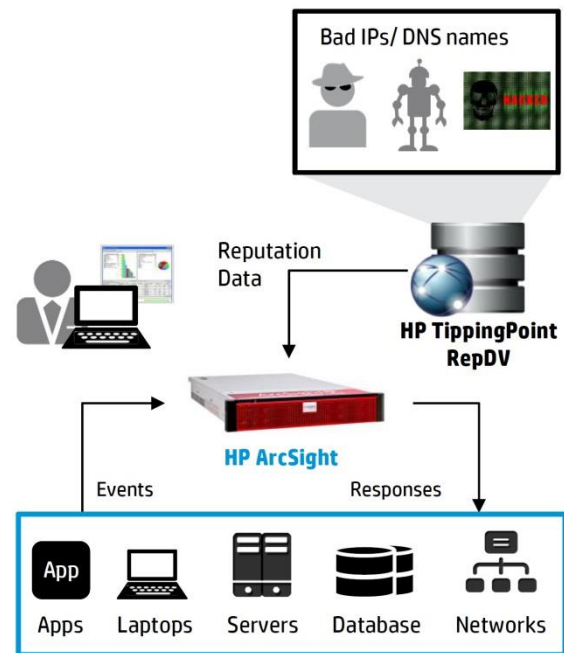
HP Reputation Security Monitor (RepSM)

Si tratta di uno strumento di Threat Intelligence basato su un livello di reputazione che viene definito sulla base di dati provenienti dalla comunità di sicurezza globale e di rilevazioni effettuate da HP.

RepSM fornisce un ulteriore livello di intelligenza al SIEM per operazioni di correlazione in tempo reale, abilitando una risposta attiva in risposta alle attività dannose e stabilendo il livello di priorità con cui fronteggiare attività sospette.

In tal modo fornisce un utile sistema per identificare le APT, che risultano spesso non individuate dai controlli di sicurezza basati su signature e, più in generale, abilita operazioni di sicurezza in risposta ad attacchi sconosciuti con azioni manuali o automatiche.

L'utilizzo di RepSM abbinato ad ArcSight Application View permette di avere visibilità sul comportamento di un malintenzionato all'interno di un'applicazione e di controllare, per esempio, se effettua connessioni esterne e se queste sono verso un sito o un IP da considerare pericolosi.



HP Reputation Security Monitor (RepSM)

HP Threat Central

HP Threat Central è una piattaforma collaborativa di security intelligence, pensata per combattere gli attacchi informatici più avanzati, a uso dei membri di una community di utenti HP.

Favorisce la condivisione di informazioni su minacce, analisi e azioni correttive, e offre funzionalità di Intelligence in tempo reale su vettori di attacco, metodi, motivazioni e autori specifici che si celano dietro gli attacchi. Attraverso HP Threat Central i membri autorizzati di una community, per esempio di operatori del settore bancario (dove frequentemente la stessa tipologia di attacchi viene replicata su più

organizzazioni dello stesso tipo), vengono allertati in tempo reale non appena viene identificata una minaccia, consentendogli di ricercare all'interno delle proprie organizzazioni la presenza di indicatori simili a quelli notificati. Facendo leva sulla piattaforma, i membri della community possono inviare informazioni sulle minacce, analisi e metodi per contrastarle. Lo scambio dei dati all'interno della community avviene in modo sicuro e riservato, sotto la garanzia del Research Group di HP che, peraltro, contribuisce direttamente all'attività della community aggiungendo best practice, risultati delle proprie indagini e suggerimenti operativi.

HP Security Research

HP Security Research è la struttura che conduce ricerche e fornisce servizi di intelligence per l'intero portafoglio di soluzioni HP ESP. HP analizza le informazioni provenienti da diverse fonti, tra cui indagini proprietarie, intelligence open source e feed dei dati attivi generati dai propri prodotti e servizi.

L'ampiezza e la profondità degli asset di sicurezza, della sua base installata e della sua community di sicurezza, collocano HP Security Research nella posizione ideale per agevolare la condivisione dell'intelligence indispensabile per contrastare le minacce.

Pubblicazioni sulle ricerche sul tema della sicurezza e briefing periodici sulle minacce completano i servizi di intelligence HP e offrono un'analisi approfondita del futuro della sicurezza e dei più importanti rischi di violazione che le aziende si troveranno ad affrontare.

HP Security Research, che si occupa di dettare l'agenda della ricerca in materia di sicurezza per conto di HP, si avvale del contributo dei gruppi di ricerca già esistenti che includono HP DVLabs e HP Fortify Software Security Research; inoltre, gestisce il programma Zero Day Initiative (ZDI) che premia i ricercatori di tutto il mondo che individuano nuove vulnerabilità.

HP DVLabs

HP DVLabs è il team di ricerca di sicurezza di HP per la scoperta delle vulnerabilità nel settore della sicurezza. Il team è composto da ricercatori riconosciuti nel settore che applicano tecniche di analisi all'avanguardia nelle loro operazioni quotidiane.

DVLabs trasferisce tutte le scoperte delle vulnerabilità ai produttori di software interessati per favorirli nella creazione di patch e crea filtri di protezione per i suoi sistemi NGFW per proteggere i clienti da potenziali attacchi zero-day prima che le vulnerabilità siano rese note al pubblico.



Esempio di Report fornito dai DV Labs

L'attività svolta dagli HP DV Labs si concentra sulla creazione di filtri per la protezione contro ogni tipo di vulnerabilità e non solo gli exploit noti. I filtri di vulnerabilità prodotti puntano a bloccare tutti gli exploit della vulnerabilità del software, fornendo un elevato livello di accuratezza in modo che i NGFW non blocchino il traffico legittimo mentre proteggono la rete.

Zero-Day Initiative

A supporto di un approccio proattivo alla sicurezza enterprise HP ha sviluppato una serie di tecnologie e iniziative. Tra queste va certamente ricordata la HP Zero-Day Initiative (ZDI), un programma pubblico di ricerca sulle vulnerabilità Zero-Day che da molti anni supporta le soluzioni TippingPoint favorendo una copertura efficace dalle tecniche di attacco sfruttabili "in the wild" e non ancora risolte da patch rilasciate dai produttori.

ZDI arricchisce l'attività svolta dai Laboratori HP DV Labs con metodologie,

competenze e iniziative di ricercatori indipendenti, incoraggia la generazione di report sulle vulnerabilità zero-day attraverso programmi di incentivi per i contributori e permette di incrementare il livello di protezione offerto attraverso i sistemi HP TippingPoint Next Generation Firewall.

HP ZDI mette a disposizione un portale Web per l'invio di vulnerabilità e per monitorare lo stato, filtri NGIPS per combattere le vulnerabilità mentre sono in corso i lavori per predisporre patch efficaci e definire i dati sulle ultime minacce di classe enterprise.

HP TippingPoint Web AppDV

HP TippingPoint mette a disposizione di propri utenti anche Web AppDV, una soluzione pensata per proteggere le applicazioni Web critiche che permette di identificare, monitorare, proteggere e controllare le applicazioni e il loro utilizzo. Attraverso una scansione personalizzata delle applicazioni Web, questo servizio consente lo sviluppo di Vaccini Digitali specifici per l'utente.

WebAppDV, grazie alla tecnologia Adaptive Web Application Firewall (WAF), permette di estendere la protezione alle applicazioni online, attraverso l'identificazione in tempo reale delle vulnerabilità nelle applicazioni Web e la distribuzione di

Conclusioni

Attraverso un'offerta di soluzioni software ampia e diversificata, HP ESP mette a disposizione della aziende enterprise un insieme di componenti e strumenti adatto a rispondere alle esigenze di rilevamento delle minacce esterne e interne e a predisporre azioni di risposta che intervengono per proteggere dati, rete e applicazioni. I centri di ricerca e l'offerta di servizi distribuiti a livello globale mettono a disposizione delle aziende una "intelligence" di sicurezza globale e aggiornata in tempo quasi reale che contribuisce ad accelerare la risposta a minacce e predisporre azioni proattive nei confronti di nuove minacce come le APT. L'offerta software di HP ESP è in ampliamento e l'attività costante rivolta a incrementare il livello di integrazione tra le differenti famiglie di soluzioni software non potrà che contribuire a incrementare ulteriormente l'efficacia complessiva dell'approccio alla sicurezza proposto dal vendor. Le soluzioni hardware Next Generation Firewall e IPS, che non sono state analizzate in questo white paper (*), rappresentano un ulteriore tassello che completa e incrementa il livello di protezione enterprise.

(*) A queste soluzioni Reportec ha dedicato due white paper specifici, disponibili gratuitamente effettuando una richiesta a servizi@reportec.it

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.



Soluzioni integrate per la protezione d'impresa: l'offerta software di HP ESP

© Reportec S.r.l. - Febbraio 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.