

Reportec



**La sicurezza enterprise
di HP ESP**

La sicurezza enterprise di HP ESP

*Dott. Riccardo Florio
Vice President Reportec*

In uno scenario profondamente mutato e in evoluzione rispetto al passato, caratterizzato da cloud computing, virtualizzazione, mobilità e consumerizzazione dell'IT, predisporre una protezione aziendale efficace diventa un compito quanto mai complesso, da affrontare su più livelli.

Le aziende enterprise si devono preoccupare di proteggere la rete che non è più delimitata da un perimetro definito, devono garantire la sicurezza delle informazioni e la non compromissione dei propri asset e, nel contempo, preoccuparsi di verificare che il software risulti affidabile, privo di vulnerabilità e conforme alle policy aziendali di sicurezza.

Per rispondere a queste sfide HP ha predisposto una strategia coerente e un portafoglio d'offerta integrato, combinando tecnologie avanzate con l'attività di alcuni dei principali Laboratori di ricerca al mondo per fornire un approccio proattivo per una corretta gestione del rischio.

Tutto questo confluisce nelle competenze della divisione Enterprise Security Products, delle cui soluzioni trovate di seguito una descrizione.

Sommario

La sicurezza enterprise di HP	2
HP Fortify per lo sviluppo di codice sicuro	4
HP Fortify Software Security Center	5
HP Fortify Static Code Analyzer per l'analisi statica	5
HP WebInspect per l'analisi dinamica	5
HP Fortify on Demand: la sicurezza applicativa come servizio cloud on-demand .	6
<i>Analisi di sicurezza statica</i>	6
<i>Analisi di sicurezza dinamica</i>	7
<i>Analisi delle applicazioni mobile</i>	7
<i>Test delle applicazioni in produzione</i>	7
HP ArcSight: la piattaforma di protezione dei dati.....	8
HP ArcSight Enterprise Security Manager (ESM)	8
HP ArcSight Application View	10
HP ArcSight Threat Response Manager.....	10
HP Reputation Security Monitor (RepSM).....	11
HP ArcSight Risk Insight	12
HP TippingPoint Next Generation Firewall e IPS	13
<i>HP TippingPoint NGFW S1050F</i>	14
<i>HP TippingPoint NGFW S3010F/S3020F</i>	15
<i>HP TippingPoint NGFW S8005F/S8010F</i>	16
HP Atalla: la sicurezza delle transazioni.....	16
Conclusioni.....	17

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

Attraverso la divisione Enterprise Security Products, HP fornisce soluzioni di sicurezza e di compliance per le imprese, promuovendo l'adozione di una metodologia end-to-end come modo migliore per una difesa efficace. La piattaforma HP di Security Intelligence e Risk Management mette a disposizione i sistemi di nuova generazione HP TippingPoint firewall (NGFW) e per la prevenzione delle intrusioni (NGIPS), le soluzioni software per la 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.

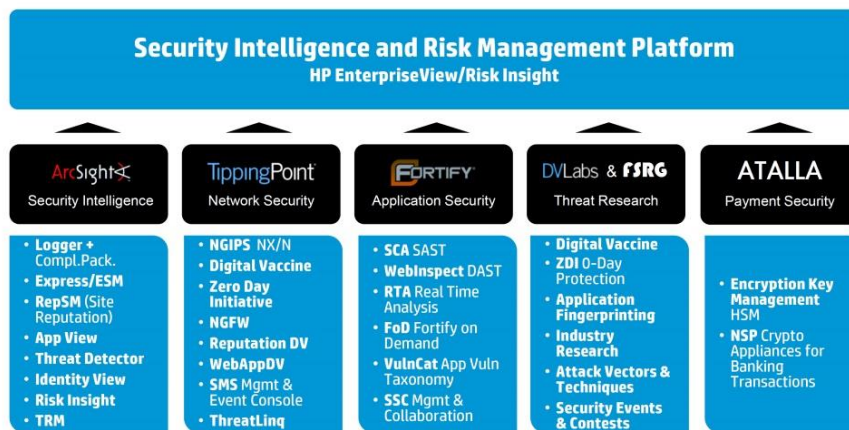
Questa gamma di soluzioni segue un processo evolutivo che prevede sia la trasformazione e il miglioramento continuo di ciascuna tecnologia verticale, sia un'integrazione sempre più spinta delle diverse funzionalità al fine di sfruttare al massimo la sinergia di strumenti che affrontano, su piani diversi, 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.

Le soluzioni di sicurezza di HP sono rese disponibili in diverse modalità, per favorire le differenti esigenze aziendali, per esempio prevedendo suite integrate e servizi erogati via cloud in modalità on-demand.

Alle soluzioni tecnologiche HP affianca una rete di servizi tra le più estese al mondo e il valore aggiunto offerto dalla possibilità di avvalersi di prestigiosi Laboratori di ricerca specializzati. Questi includono **HP Security Research**, la struttura che conduce ricerche e fornisce servizi di intelligence per l'intero portafoglio di soluzioni HP ESP, e **HP DV Labs**, il team di ricerca per la scoperta delle vulnerabilità nel settore della sicurezza, che trasferisce tutte le sue scoperte ai produttori di software interessati (per favorirli nella creazione di patch) e che provvede a creare i filtri di protezione utilizzati sui sistemi HP TippingPoint Next Generation Firewall/IPS.

I DV Labs forniscono anche il servizio HP Reputation Digital Vaccine (RepDV) basato sull'analisi incrociata di milioni di "data stream" raccolti giornalmente dalla rete mondiale di sensori TippingPoint Lighthouse Network, che permette di effettuare operazioni di blocco dell'accesso o di monitoraggio in base al valore di un indicatore di reputazione o di rischio e alla localizzazione geografica. DV Labs gestisce anche il programma pubblico di ricerca **Zero-Day Initiative (ZDI)**, che premia i ricercatori di tutto il mondo in modo che individuano nuove vulnerabilità.

HP Enterprise Security Products, in collaborazione con gli HP Labs, ha anche sviluppato nel 2013 **HP Threat Central**, una piattaforma collaborativa d'informazioni sulla sicurezza che permette di condividere, all'interno di una comunità, dati e analisi sulle minacce fornendo intelligence in tempo reale su hacker, vettori degli attacchi e metodi e motivazioni all'origine delle attuali minacce.



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

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. 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 Fortify Software Security Center

HP Fortify Software Security Center è una suite di soluzioni altamente integrate pensata per automatizzare e gestire la sicurezza applicativa e prevenire le vulnerabilità di sicurezza all'interno delle applicazioni. HP Fortify Software Security Center consente di testare la sicurezza delle applicazioni e di identificare le vulnerabilità sia in modalità on-premises sia on-demand.

Questa suite svolge due attività fondamentali a supporto della gestione di sicurezza del software.

La prima è di mettere a disposizione funzioni di test di sicurezza per identificare le vulnerabilità lungo il ciclo di vita di un'applicazione, sia sviluppata internamente sia esternamente, attraverso tecnologie di test statico, dinamico e di analisi ibrida (statico-dinamica) in tempo reale. La seconda attività riguarda l'analisi del ciclo di vita del processo di sviluppo attraverso funzioni di automazione di gestione, tracciamento, correzione e governance del rischio associato al software enterprise.

HP Fortify Static Code Analyzer per l'analisi statica

HP Fortify Static Code Analyzer (SCA) è la tecnologia sviluppata da HP per valutare il livello di sicurezza del software e rendere sicuro il codice legacy mentre questo viene sviluppato. Questa tecnica analizza ogni percorso che l'esecuzione e i dati possono seguire per identificare ed eliminare le vulnerabilità di sicurezza nel codice sorgente.

La soluzione proposta da HP utilizza diversi algoritmi e una base di conoscenza estesa di regole di codifica sicure per analizzare il codice sorgente di un'applicazione alla ricerca di vulnerabilità che potrebbero essere sfruttate in applicazioni distribuite. Fortify SCA 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.

HP WebInspect per l'analisi dinamica

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

HP Fortify on Demand: la sicurezza applicativa come servizio cloud 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 richiedere l'acquisto di hardware o l'installazione di software.

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

Fortify on Demand non richiede l'acquisto di alcun hardware né l'installazione di alcun software: è sufficiente caricare il codice e scegliere il tipo di test che si desidera effettuare per ottenere un report dettagliato.

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. Questo servizio supporta Web, mobile e applicazioni thick-client, sia sviluppati internamente sia da terze parti.

Analisi di sicurezza statica

L'analisi statica di Fortify on Demand permette di valutare il livello di sicurezza del software e di rendere sicuro il codice legacy mentre questo viene sviluppato. L'utente carica il codice sorgente (byte o binario) di un'applicazione e riceve risultati recensiti manualmente solitamente in meno di 24 ore.

La soluzione proposta da HP utilizza diversi algoritmi e una base di conoscenza estesa di regole di codifica sicure per analizzare il codice sorgente di un'applicazione alla ricerca di vulnerabilità che potrebbero essere sfruttate in applicazioni distribuite.

Questa tecnica analizza ogni percorso che l'esecuzione e i dati possono seguire per identificare ed eliminare più di 500 categorie di vulnerabilità nel codice sorgente.

Analisi di sicurezza dinamica

L'analisi di sicurezza di Fortify on Demand di tipo dinamico combina l'attività di test automatico con una metodologia di test manuale svolta da un gruppo di "application penetration tester" sull'applicazione Web. Questo tipo di test imita le tecniche di attacco dei cyber criminali, consentendo di analizzare a fondo le applicazioni e i servizi Web per individuare possibili vulnerabilità di sicurezza.

Analisi delle applicazioni mobile

L'approccio HP Fortify on Demand ai test delle applicazioni mobile prende in considerazione i tre livelli che costituiscono lo stack tecnologico: client, rete e server. Questo approccio fa in modo che le vulnerabilità presenti in un componente (il client, per esempio) possano essere utilizzate durante il test server per delineare un quadro più veritiero possibile del rischio legato all'applicazione mobile, in modo simile alla metodologia che potrebbe adottare un hacker. Il servizio prevede l'installazione iniziale di un'applicazione per poi eseguire un'analisi preliminare sfruttando tutte le funzioni disponibili e permette di comprendere dove vengono richiesti i dati sensibili, come si spostano attraverso l'applicazione, come sono utilizzati e così via. Viene quindi costruito un diagramma di come questi componenti operano congiuntamente, che viene sfruttato per determinare la progressione della valutazione.

Il test viene eseguito sia su dispositivi mobili di prova sia utilizzando dispositivi simulati, a seconda del tipo di applicazione e delle sue funzionalità.

Test delle applicazioni in produzione

Troppo frequentemente le applicazioni vengono rilasciate in produzione in modo frettoloso, con vulnerabilità non risolte. HP FoD risponde a questo problema fornendo un servizio per effettuare il test delle applicazioni Web in produzione senza causare interruzioni dell'attività. L'approccio seguito da HP parte dal presupposto che le applicazioni di produzione non dovrebbero essere testate con lo stesso approccio aggressivo utilizzato nelle fasi di sviluppo (perché quando si è in produzione sono i dati reali che si espongono a un rischio). Per questo motivo Fortify on Demand offre quattro differenti opzioni metodologiche per la verifica delle applicazioni in produzione.

HP ArcSight: la piattaforma di protezione dei dati

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.

HP ArcSight è 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.

Questa piattaforma 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.

HP ArcSight Enterprise Security Manager (ESM)

HP ArcSight ESM rappresenta l'elemento centrale e abilitante di questa famiglia di soluzioni. Si tratta di 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,
- ❑ problemi di conformità che scaturiscono dal mancato superamento dei controlli.

HP ArcSight ESM automatizza le operazioni di ricerca e analisi su Big Data di informazioni, 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 fino a 30 volte superiori rispetto alla versione precedente) del motore di

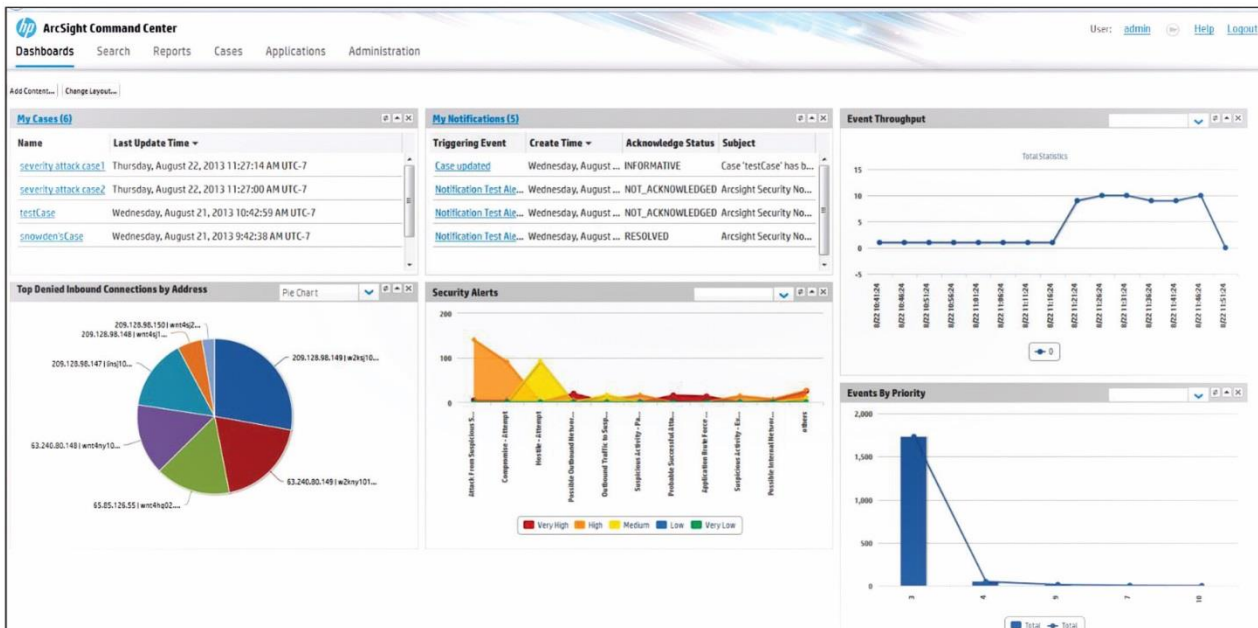
correlazione **Correlation Optimized Retention and Retrieval Engine (CORR-Engine)** che permette di scalare nel livello di risposta, in funzione della minaccia che ci si trova a dover affrontare.

L'integrazione con il file system di Hadoop (HDFS - Hadoop Distributed File System) consente di sfruttare il CORR-Engine per effettuare funzioni avanzate di analytics in tempo reale oppure di inviare ad alta velocità ad Hadoop i log normalizzati dal CORR-Engine per una lettura da HDFS (per esempio per operazioni di batch analytics).

HP 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.

L'interfaccia **HP ArcSight Command Center** riunisce funzionalità amministrative e di reportistica Web-based con funzioni di configurazione, distribuzione, analisi dei log e gestione delle modifiche, attraverso un'impostazione basata su cruscotti altamente personalizzabili.

Anche le applicazioni di terze parti possono essere integrate direttamente all'interno del front end Web di HP ArcSight ESM.



HP ArcSight Command Center

HP ArcSight Application View

HP ArcSight Application View consente di controllare 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.

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 ArcSight Identity View** focalizzato sul monitoraggio dell'identità degli utenti e pensato per proteggere le aziende enterprise da possibili minacce interne 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.

HP ArcSight Threat Response Manager

HP ArcSight Threat Response Manager (TRM) mette a disposizione funzionalità cloud-ready per accelerare il rilevamento delle minacce e le azioni di risposta alle APT.

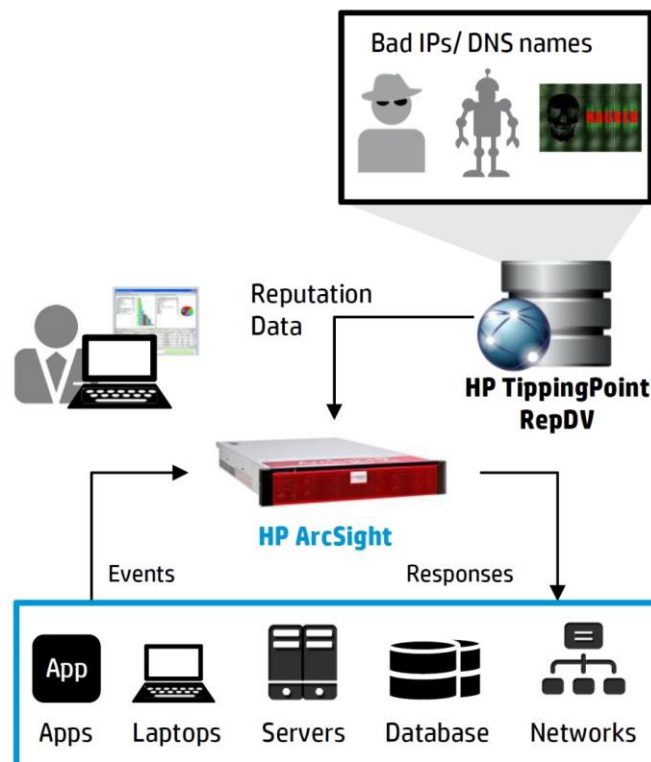
Rilasciato come un add-on cloud-ready per la piattaforma HP ArcSight di Security Information and Event Management (SIEM), ArcSight TRM è una soluzione end-to-end di sicurezza di rete e monitoraggio che accelera il rilevamento delle minacce e automatizza l'intero processo di risposta.

Questa soluzione consente di gestire e elaborare ad alta velocità le informazioni di sicurezza, analizzare i dati (strutturati e non strutturati), monitorare gli eventi e predisporre azioni automatiche una volta che una minaccia è stata rilevata. In caso di rilevamento, prima che il personale di sicurezza provveda a disattivare manualmente l'account, ArcSight TRM interviene per interrompere immediatamente l'accesso.

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 reazione attiva in risposta alle attività dannose e stabilendo il livello di priorità con cui fronteggiare attività sospette.



HP Reputation Security Monitor (RepSM)

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.

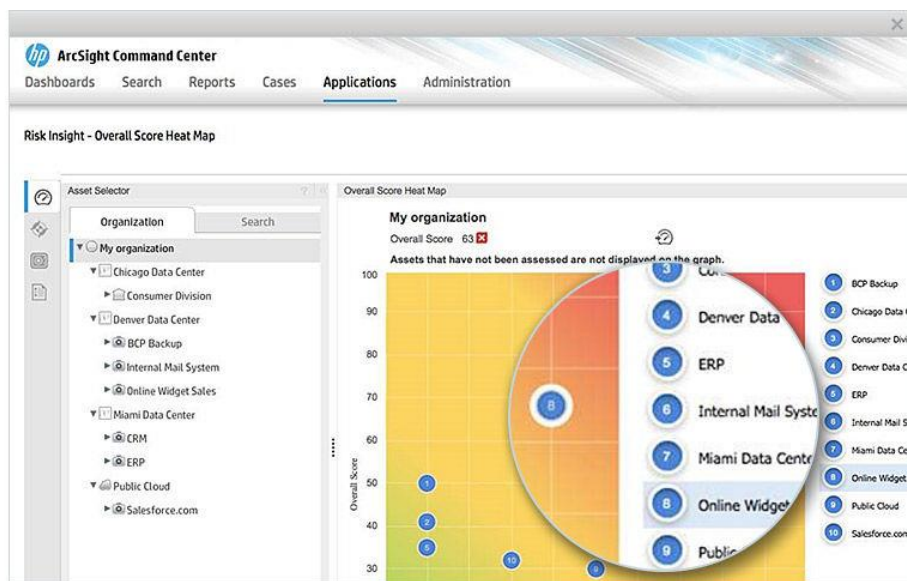
L'utilizzo di RepSM abbinato ad ArcSight Application View permette di avere visibilità sul comportamento di un malintenzionato all'interno di un'applicazione e di controllare, per esempio, se effettua connessioni esterne e se queste sono verso un sito o un IP da considerare pericolosi.

HP 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,
- ❑ una serie di indicatori di rischio capaci di aggregare molteplici fonti,
- ❑ funzioni per l'analisi di conformità dei processi di business.



Mappa degli asset in HP ArcSight Risk Insight

HP TippingPoint Next Generation Firewall e IPS

In un contesto di reti senza perimetro, minacce persistenti e utenti remoti, gli NGFW/NGIPS rappresentano soluzioni versatili per esercitare una protezione che non impatta su processi e infrastruttura

I dispositivi della gamma HP TippingPoint di nuova generazione forniscono il livello di visibilità necessario a riconoscere quali applicazioni stanno girando sulla rete aziendale e chi sta accedendo a tali applicazioni per poi consentire di predisporre le policy richieste per bloccare e controllare le applicazioni non richieste. Questo livello di visibilità e controllo consente alle organizzazioni di restringere l'accesso generale di certi dipendenti alle applicazioni di trasferimento dei file nel cloud, qualora sussista il rischio che la proprietà intellettuale possa essere memorizzata in contrasto alle policy aziendali.

Per fronteggiare i rischi legati alla mobilità i Next Generation Firewall/IPS di HP abilitano il blocco automatico del codice nascosto o dannoso che può introdursi in rete, ricorrendo a capacità di blocco delle vie d'uscita in modo da evitare la fuoriuscita di dati sensibili verso destinazioni "command-and-control".

Per rispondere ai rischi introdotti dal BYOD gli utenti delle soluzioni HP TippingPoint hanno a disposizione controlli sulle policy delle applicazioni a livello granulare, che consentono anche di gestire l'interazione con le più diffuse piattaforme social e consumer come Facebook, Google e Twitter.

Tra i punti distintivi di queste soluzioni vi è anche la semplicità d'uso che le rende adatte anche alle organizzazioni prive di personale specializzato. L'installazione e il rilascio in produzione può avvenire, secondo HP, in meno di un'ora e mettendo a disposizione una singola interfaccia di gestione in grado di condividere la configurazione delle policy per la sicurezza di rete.

L'affidabilità è un altro aspetto su cui HP intende rimarcare il valore dei propri dispositivi mentre, per quanto riguarda l'efficacia della propria tecnologia di protezione nel bloccare possibili minacce, HP mette sul piatto l'attività del team di ricerca DVLabs che ha pubblicato a oggi oltre 7400 filtri e che è costantemente impegnato in operazioni per arrestare gli exploit e bloccare gli attacchi.

Tutti i modelli NGFW dispongono di una porta di rete RJ-45 10/100/1000 per la gestione out-of-band oppure possono essere gestiti in modalità in-band tramite porte di rete. Inoltre è presente una porta seriale RJ-45 per la console.

L'appliance **HP TippingPoint SMS** mette a disposizione un sistema di management centralizzato per la condivisione di configurazioni e policy di sicurezza della rete attraverso i firewall e i sistemi IPS di nuova generazione.

Le soluzioni **HP TippingPoint NGIPS** individuano le nuove vulnerabilità presenti sulla rete e intervengono applicando delle "patch" virtuali che fermano sul nascere la diffusione di traffico dannoso. Di fatto, i sistemi IPS di HP ottimizzano le prestazioni del traffico legittimo effettuando una continua pulizia della rete e assegnando la massima priorità alle applicazioni mission critical.

Queste soluzioni dispongono anche di funzioni di elevata disponibilità e ridondanza e sono caratterizzate da una latenza tipica di pochi microsecondi, per proteggere dispositivi di rete, software di virtualizzazione, sistemi operativi e applicazioni da attacchi senza impattare sulle prestazioni.

HP TippingPoint NGFW S1050F

È la soluzione entry level adatta per le implementazioni di rete delle filiali.

Si tratta di un dispositivo da rack di dimensioni 1U che supporta un throughput fino a 500 Mbps in modalità solo firewall, che lo rende adatto a supportare fino a 250mila connessioni simultanee e fino a 10mila nuove connessioni per secondo; se utilizzato in modalità Firewall+IPS+ApplicationControl il throughput massimo suggerito è di 250 Mbps.

I valori di latenza tipici di questo dispositivo nella modalità d'utilizzo Firewall+IPS sono inferiori a 600 microsecondi. Il throughput a disposizione per la realizzazione di VPN IPsec è di 250 Mbps con la possibilità di creare fino a 1250 tunnel VPN.



HP TippingPoint Next-Generation Firewall S1050F

Il firewall S1050F dispone di 8 GB di storage integrato su memoria Flash CFast rimovibile. La connettività di rete prevede otto porte RJ-45 10/100/1000 più 1 porta 10/100/1000 per l'alta disponibilità.

HP TippingPoint NGFW S3010F/S3020F

I Next Generation Firewall S3010F/S3020F sono apparati di dimensioni 2U indicati per le implementazioni di rete di campus e filiali, essendo adatti per un numero di connessioni simultanee rispettivamente di 500mila e 1 milione.

La capacità storage in dotazione è di 8 GB, mediante memoria Flash CFast rimovibile.



HP TippingPoint Next-Generation Firewall S3010F/3020F

La connettività di rete prevede 8 porte 10/100/1000 e 8 porte 1 Gbps SFP rame/fibra a cui si aggiunge 1 porta 10/100/1000 per l'alta disponibilità.

Il tempo di latenza tipico in modalità Firewall+IPS è inferiore a 120 microsecondi e possono essere stabilite fino a 500mila (S3010F) o un milione (S3020F) di sessioni contemporanee.

Il modello 3010F mette a disposizione un throughput di 500 Mbps in modalità Firewall+IPS+ApplicationControl che sale a 1 Gbps quando utilizzato in modalità di solo Firewall. Una banda di 500 Mbps a disposizione per le VPN IPsec. Il modello S3020F raddoppia il throughput arrivando a 2 Gbps in modalità solo Firewall e 1 Gbps quando opera come Firewall+IPS+ApplicationControl.

HP TippingPoint NGFW S8005F/S8010F

Al top della gamma si collocano i due modelli S8005F e S8010F di dimensioni 2U adatti per 10 e 20 milioni di connessioni simultanee.

Si tratta di apparati indicati per le implementazioni di rete dei data center che dispongono di 32 GB di storage integrato su memoria Flash CFast rimovibile.



HP TippingPoint Next-Generation Firewall S8005F/S8010F

La connettività di rete prevede 8 porte 10/100/1000, 8 porte 1 Gbps SFP rame/fibra, 4 porte 10 Gbps SFP rame/fibra e 2 porte 10/100/1000 per l'alta disponibilità.

Il tempo di latenza tipico in modalità Firewall+IPS è inferiore a 120 microsecondi e possono essere stabilite fino a 50mila nuove connessioni al secondo.

A livello di prestazioni il modello S8005F mette a disposizione un throughput di 5 Gbps in modalità solo Firewall o di 2,5 Gbps in modalità Firewall+IPS+ApplicationControl e 1,5 Gbps per le VPN IPsec; questi numeri raddoppiano sul modello S8010F.

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 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 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 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.

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.

Conclusioni

Le soluzioni di sicurezza HP ESP rappresentano un'offerta coerente e integrata che consente di proteggere in modo efficace la rete aziendale e di predisporre condizioni per ridurre i rischi legati alle vulnerabilità del software.

HP mette, infatti, 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. 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 rappresentano un ulteriore tassello che completa e incrementa il livello di protezione enterprise con capacità di analisi quasi in tempo reale estesa fino al livello applicativo. I centri di ricerca e l'offerta di servizi distribuiti a livello globale rappresentano un ulteriore valore aggiunto che mette a disposizione delle aziende una "intelligence" di sicurezza globale e aggiornata in tempo reale che contribuisce ad accelerare la risposta a minacce e predisporre azioni proattive nei confronti di nuove minacce come le APT.



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.

La sicurezza enterprise di HP ESP

© Reportec S.r.l. – Maggio 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.