

Next Generation IPS:  
le soluzioni  
HP TippingPoint

Reportec





## Next Generation IPS: le soluzioni HP TippingPoint

*Dott. Riccardo Florio  
Vice President Reportec*

*In uno scenario profondamente mutato e in evoluzione rispetto al passato, predisporre misure efficaci di sicurezza diventa un compito sempre più arduo. I sistemi per la prevenzione delle intrusioni di nuova generazione mettono a disposizione dei security manager contromisure che intervengono in modo differenziato e granulare per proteggere la rete aziendale, ormai senza confini, da minacce e intrusioni che sfruttano tutti i vettori disponibili, dai dispositivi mobili alle applicazioni.*

*Tra i principali vendor del settore, HP affronta il tema della sicurezza in modo ampio e integrato attraverso la divisione dedicata Enterprise Security Product in cui confluisce la gamma di soluzioni IPS di nuova generazione HP TippingPoint.*

*Di seguito un'analisi delle caratteristiche e dei punti di forza di queste soluzioni.*

## Uno scenario in mutazione

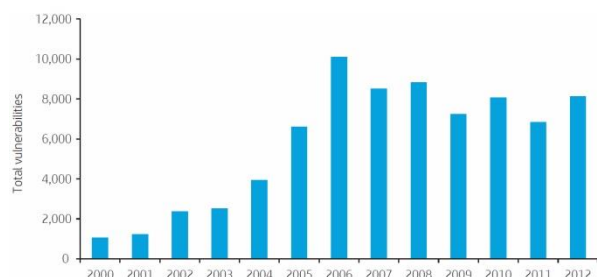
**I**l panorama tecnologico è in continua evoluzione. Il cloud computing, la virtualizzazione e la mobilità hanno drasticamente cambiato il modo di condurre gli affari delle organizzazioni e delle modalità di lavoro delle persone.

Questo cambiamento ha anche costretto le aziende a far fronte a una serie di nuove vulnerabilità. Per esempio, è diventato comune per i dipendenti accedere ai dati aziendali dai propri dispositivi mobili mentre lavorano da casa, introducendo nuovi e seri elementi di rischio per la sicurezza aziendale.

A ciò si affianca un'evoluzione della figura dell'hacker, che ormai opera prevalentemente all'interno di strutture di criminalità organizzata, e delle modalità di attacco utilizzate che sfruttano contemporaneamente diversi vettori e diventano sempre efficaci nel modo di nascondere malware all'interno di pacchetti o applicazioni.

Come conseguenza di ciò le vulnerabilità crescono in numero e in pericolosità. In base alle stime del rapporto annuale *HP 2012 Cyber Security Risk Report*, il volume complessivo delle vulnerabilità ha

raggiunto nel 2012 quota 8.137 con un aumento del 19% rispetto al 2011 mentre una su cinque è risultata in grado di attribuire all'hacker il controllo totale sull'obiettivo del suo attacco.



Numero di vulnerabilità tra il 2000 e il 2012  
(Fonte: HP Cyber Security Risk Report 2012)

Crescono le vulnerabilità in ambito mobile che nel 2012 sono arrivate a essere 266, mentre quasi la metà delle applicazioni mobili tollera accessi non autorizzati.

Le vulnerabilità prevalenti rimangono però quelle Web più note tanto che nel 2012 il 40% del numero complessivo di vulnerabilità è riconducibile a solo quattro categorie di vulnerabilità del Web. Ciononostante, meno dell'1% degli URL testati nell'analisi di HP utilizzavano comuni sistemi di prevenzione.

In questo scenario, dove l'accesso avviene in mobilità, le risorse sono nel cloud e i dipendenti utilizzano una vasta gamma di configurazioni di login da remoto, per la maggior parte delle

imprese la rete si è trasformata in un vero e proprio colabrodo.

L'adozione di difese di tipo tradizionale, sebbene essenziali, in assenza di un'adeguata contestualizzazione globale e della presenza di un'intelligence automatizzata dedicata alla sicurezza, non sono più in grado di fornire una protezione efficace contro le nuove tipologie di attacco.

## L'evoluzione della network security

Predisporre misure efficaci di sicurezza significa affrontare anche una revisione della rete che però non è, come molti pensano, necessariamente di natura tecnologica, ma prevalentemente di carattere strategico.

Ovviamente il problema di come impostare una strategia per l'infrastruttura di rete aziendale si abbina anche al modo di predisporre l'inserimento di nuovi dispositivi partendo dalla situazione preesistente e determinando il minor impatto possibile.

Da questa esigenza specifica, ma basilare nel contesto di un'operatività aziendale che non può subire interruzioni, non possono quindi prescindere i fornitori di piattaforme, che si trovano a dover predisporre modelli architetturali in grado di

adattarsi da subito alle nuove esigenze e ai requisiti di business, integrando l'esistente, elevando le prestazioni e mantenendosi aperti per un'evoluzione scalabile.

Un altro tema da sottolineare nell'evoluzione della network security riguarda il legame tra i requisiti applicativi e le caratteristiche dell'infrastruttura di rete nonché il progressivo orientamento verso un modello orientato ai servizi e al cloud.

Il passaggio da una visione centrata sulla parte "tecnica" di una rete a quella "applicativa" ha profonde implicazioni a livello di sicurezza, anche perché coinvolge nel processo decisionale e di cambiamento un insieme di figure manageriali e aree di responsabilità aziendale più orientate al business e che, per molto tempo, sono state sostanzialmente non interessate a quanto era ritenuto di esclusiva competenza del reparto IT.

La sicurezza del futuro non potrà, quindi, essere un elemento aggiuntivo del sistema informativo o dell'infrastruttura aziendale ma, invece, un componente pervasivo e integrato di entrambi, come pure di tutti gli elementi tecnologici, anche non IT, presenti in azienda.

Un primo elemento che emerge è che sicurezza e rete sono due cose che è

sempre più opportuno siano pensate e sviluppate in modo parallelo. Una tale sinergia appare poi tanto più necessaria quanto più la rete agisce come integratore e come base per applicazioni convergenti e per l'erogazione di servizi.

Si tratta del punto di arrivo di un processo di convergenza tra security e networking che parte da lontano: quando gli switch hanno cominciato a fare i router e questi ultimi hanno iniziato a controllare gli accessi tramite le ACL (Access Control List).

I firewall e gli Intrusion Detection System da un lato e gli Analyzer e i multilayer switch dall'altro, hanno continuato il percorso di avvicinamento che è poi culminato negli Intrusion Prevention System di prima generazione che combinano funzioni di analisi e filtering del traffico con la capacità di controllo della rete.

Un ulteriore elemento in grado di caratterizzare il modello architetturale e condizionare l'efficacia di protezione della rete è la capacità di implementare un livello di intelligenza e di distribuirlo in base agli specifici requisiti di business.

Si tratta di un requisito ormai irrinunciabile, in uno scenario caratterizzato dalla dispersione delle informazioni nel cloud e da modelli di

business innovativi che richiedono di operare in tempo reale su scala globale.

Questo ha favorito l'affermazione di appliance dedicate, pronte a integrare una serie di funzionalità di sicurezza in costante ampliamento ed evoluzione.

### **Le carenze di firewall, IDS e IPS di prima generazione**

Uno dei primi problemi che le aziende si sono poste con l'apertura verso il Web è stato il controllo degli accessi alla rete aziendale, per il quale sono stati sviluppati opportuni protocolli di autenticazione. È stato però subito evidente che dalla Rete potevano arrivare sul sistema e sul Web aziendale dei malintenzionati. Inizialmente, si temeva più che creassero danni per gioco, mentre oggi si sa che vogliono colpire in maniera mirata.

Sono nati i firewall, che si preoccupavano di "chiudere" alcune porte della rete, permettendo il passaggio solo di "traffico giusto". Ben presto, il traffico "cattivo" ha imparato a mascherarsi e i firewall a farsi più furbi e a intensificare i controlli.

L'escalation tra tecniche d'intrusione e sistemi per rilevarle e bloccarle è storia. La rincorsa prosegue, ma il modo di fronteggiarsi tra aspiranti intrusori e aziende ha cambiato ritmo e, da

entrambe le parti, si adottano sistemi più automatizzati e sofisticati.

Il primo passo per contrastare queste minacce è la consapevolezza che qualsiasi connessione che "chieda" alla rete aziendale di entrare, potrebbe trasportare traffico nocivo. Di conseguenza qualunque utente, applicazione e sistema dovesse chiedere accesso alla rete, è necessario controllare chi sia e cosa vuole fare.

Peraltro, va ormai definitivamente abbandonato il concetto di perimetro. Se in precedenza, anche se la connessione poteva avvenire praticamente in qualsiasi punto, una transazione o un'operazione da compiere era sempre riconducibile a una macchina. Con il cloud anche questo punto fermo è saltato.

Una protezione efficace richiede l'adozione di una serie di funzionalità integrate e interoperabili, ognuna ottimizzata per fronteggiare specifiche minacce, capaci di fornire informazioni puntuali e organizzabili secondo viste idonee a comprendere la situazione e a prendere le decisioni che meglio sposino le policy di sicurezza con i rischi e le esigenze di business dell'impresa.

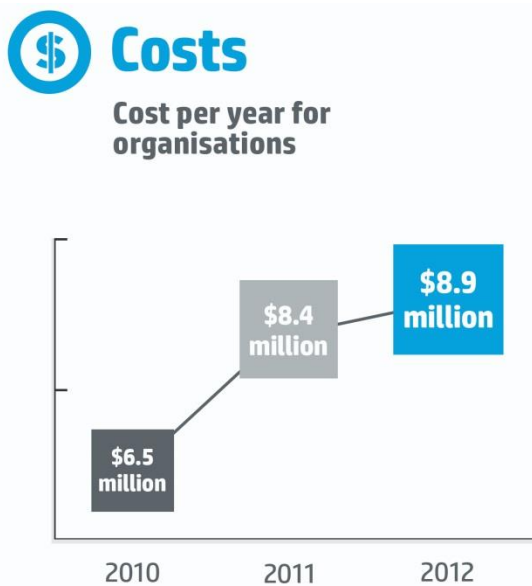
La parola chiave in merito ai rischi di intrusione è dunque una sola: prevenzione.

## La Next Generation della sicurezza

Quanto costa a un'azienda rimediare ai danni creati da un'intrusione ? E qual è il costo causato da un'interruzione o anche solo da un rallentamento nella trasmissione delle informazioni sulla rete aziendale ?

Nel corso degli anni gli analisti e i venditori di soluzioni di sicurezza si sono sforzati di rispondere fornendo una stima economica ottenuta in vari modi.

La risposta più semplice è che costa comunque tanto !



Il costo medio legato al cyber crime valutato da uno studio condotto da Ponemon Research Institute sulla base di un campione di 56 organizzazioni US in vari settori industriali, di cui molte multinazionali con oltre 1000 postazioni (Fonte: Ponemon Research)

I Next Generation Intrusion Prevention System (NGIPS) sono l'ultima soluzione dal punto di vista temporale, nata per rispondere a queste problematiche.

Dopo i firewall di tipo tradizionale inadatti a filtrare in modo efficace il traffico di rete per bloccare le minacce, i sistemi di Intrusion Detection che si limitavano all'individuazione dei rischi ma che nel frattempo lasciavano aperte delle porte alle possibili intrusioni e gli IPS di prima generazione che hanno spostato in linea le operazioni di analisi e rilevamento, gli IPS di prossima generazione si distinguono per una serie di caratteristiche innovative

### Una nuova generazione di IPS

Le appliance IPS di rete hanno rappresentato un metodo tradizionale per rilevare comportamenti anomali, malware e intrusioni. Anche se questi sistemi sono ancora in grado di fornire protezione contro la maggior parte degli attacchi di rete, le imprese ora si trovano ad affrontare minacce avanzate in grado di eludere con piccole modifiche al codice il sistema di rilevazione degli IPS tradizionali, basato sulla corrispondenza tra firma ed exploit, che si limita a rilevare il malware noto e può essere sconfitto da lievi modifiche al codice malware esistente.

Un NGIPS fornisce consapevolezza contestuale olistica, che include la visibilità di endpoint, sistemi operativi, servizi di rete, protocolli, tipi di applicazioni, contenuti e identità dell'utente.

Questa ricchezza di dati migliora la capacità dell'NGIPS di analizzare il traffico di rete e gli eventi. Pertanto, una maggiore consapevolezza contestuale permette a questo tipo di dispositivi di identificare comportamenti sospetti e di portare all'attenzione del security manager anche eventuali attacchi "lenti" che intervengono in modo nascosto su lunghe scale temporali.

Un sistema di prevenzione delle intrusioni di prossima generazione rappresenta quindi una difesa efficace per fermare il malware avanzato e le minacce APT (Advanced Persistent Threat).

In sintesi un Next Generation IPS combina le funzionalità della prima generazione di network firewall e di network Intrusion Prevention Systems, aggiungendo una gamma di funzionalità quali controllo a livello applicativo (layer 7) e di utente, ispezione SSL e SSH, funzioni di filtro per il malware basate sulla reputazione, supporto integrato per Active Directory e meccanismi di sandbox.

Tutto ciò intervenendo in linea: compito non semplice data la grande mole di traffico da analizzare.

### **Le ragioni per adottare un NGIPS**

Gli NGIPS rispondono all'esigenza delle imprese di incrementare il livello di sicurezza e, nel contempo, conseguire una minore complessità grazie all'elevato livello di integrazione.

Le ragioni per indirizzarsi verso un NGIPS sono molteplici ma possiamo evidenziare le principali.

La prima riguarda la possibilità di controllo a livello di applicazione. Il report 2012 HP Security Research già citato in precedenza, evidenzia come fino all'84% delle violazioni sfruttino le vulnerabilità collocate all'interno di applicazioni.

Si tratta di una conseguenza dell'evoluzione e dell'innovazione di approccio degli attacchi che si stanno spostando dalla reti, per sfruttare le falle anche dei sistemi operativi e delle applicazioni. Di conseguenza, dato che gli hacker sono sempre più ingegnosi nello scoprire nuovi percorsi dati, è fondamentale rendere sicuro l'intero flusso.

Un controllo a livello di applicazione è quindi di fondamentale importanza

perché permette alle organizzazioni di impostare policy specifiche per un utente, per ogni applicazione che utilizza.

Un'altra motivazione riguarda la diffusione della mobilità e la crescita fenomenale di App. Il Cyber Risk Report HP 2012 riporta che ben il 77% delle applicazioni per cellulari testata ha dimostrato vulnerabilità in relazione alla possibile perdita o fuoriuscita di dati. Entro la fine del 2013 si prevede che i campioni unici di minacce indirizzati al sistema Android raggiungeranno l'impressionante numero di un milione.

Un'ulteriore motivazione riguarda la constatazione che le nuove minacce come le APT (Advanced Persistent Threat) stanno aumentando di numero, mentre gli obiettivi si estendono progressivamente dalle aziende più grandi per includere, potenzialmente, qualsiasi tipo di organizzazione.

L'importanza delle tecnologie IPS diventa evidente se si considera che la prima fase di un attacco APT è di penetrare le difese di rete in modo inosservato. Dopo la realizzazione di questo obiettivo, l'hacker può eseguire una serie di azioni, come il furto di dati sensibili, il sabotaggio dei sistemi o l'utilizzo illecito delle risorse di calcolo. Questi attacchi sono molto efficaci nel

passare inosservati e possono protrarsi per diversi mesi o addirittura anni.

In un contesto di reti senza perimetro, minacce persistenti e utenti remoti, gli NGIPS rappresentano soluzioni sufficientemente versatili per poter evolvere nel modo di proteggere senza impattare su processi e infrastruttura.

## I requisiti di un NGISP

Per superare i limiti di un IPS tradizionale e fregiarsi del titolo di "next generation", un NGIPS dovrebbe offrire funzionalità avanzate di rilevamento delle minacce, compresa la rilevazione delle anomalie di comportamento, la reputazione IP e analisi di tipo euristico. Questi metodi di rilevamento sono necessari se si vuole sperare di sconfiggere exploit su misura, attacchi zero-day e polimorfici.

Inoltre deve essere in grado di identificare ed effettuare controlli sia a livello di applicazioni sia di utente finale.

Un NGIPS deve essere in grado di raccogliere e analizzare un volume ingente di dati per essere efficace, ma deve svolgere questo compito introducendo una latenza minima e con un impatto trascurabile sulla disponibilità dei sistemi. Per supportare i requisiti di elevato throughput di rete,

prodotti leader NGIPS sono costruiti appositamente con hardware personalizzato per accelerare i processi di controllo e di analisi.

Per supportare i requisiti di larghezza di banda richiesti è importante anche la presenza di un'elevata densità di porte ed è auspicabile il supporto per il 40 GbE (sempre più adottato nelle reti aziendali) e di standard come IEEE 802.1AX Link Aggregation Control Protocol (LACP).

Un NGIPS dovrebbe poter essere implementato come appliance di bridging trasparente poiché, come tale, può essere inserito sulla rete senza richiedere un indirizzo IP o modifiche, semplificando notevolmente il processo di acquisizione, approvazione e distribuzione.

Un altro fattore che influenza il valore di business nella scelta di un NGIPS è la sua predisposizione a supportare le nuove tecnologie come la virtualizzazione e il cloud computing.

Per esempio, le appliance di sicurezza di rete fisiche non sono in grado di controllare le comunicazioni tra macchine virtuali. Di conseguenza, sarebbe auspicabile che un portafoglio di prodotti NGIPS includesse anche appliance virtuali NGIPS per monitorare le comunicazioni tra macchine virtuali e

proteggere completamente ambienti cloud privati, pubblici e ibridi.

Un primo passo compiuto in questa direzione è stato di predisporre virtual appliance IPS come semplici porte del software offerte su appliance hardware NGIPS. In prospettiva, il sistema operativo presente sui dispositivi NGIPS dovrebbe essere progettato avendo in mente gli ambienti virtuali dato che le appliance virtuali non beneficiano dei vantaggi prestazionali offerti da un'accelerazione hardware dedicata.

Infine, un NGIPS dovrebbero offrire anche la possibilità di aggiungere facilmente nuove funzionalità di sicurezza, al fine di adattarsi ai cambiamenti ambientali e al mutamento degli scenari di minaccia nonché alla crescita organizzativa di un'azienda.

## La sicurezza secondo HP Enterprise Security Product

### Le strategie e le architetture

HP, attraverso la divisione Enterprise Security Product, 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.

Per poter affrontare le nuove esigenze di protezione, HP punta a predisporre una strategia complessiva per la gestione del rischio intervenendo 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.

Attraverso la divisione Enterprise Security Product (ESP), la piattaforma HP di Security Intelligence e Risk Management mette a disposizione i sistemi per prevenire possibili intrusioni NGIPS HP TippingPoint, 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.

Questo approccio integrato alla sicurezza enterprise di HP risponde anche alle crescenti richieste di sicurezza dei nuovi ambienti virtualizzati e cloud.

### DVLabs

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 NGIPS per proteggere i clienti da potenziali attacchi zero-day prima che le vulnerabilità siano rese note al pubblico.



Esempio di Report fornito dai DVLabs

L'attività svolta dagli HP DVLabs 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 NGIPS non blocchino il traffico legittimo mentre proteggono la rete.

DVLabs gestisce anche il programma ZDI, che premia i ricercatori di tutto il mondo in modo che individuano nuove vulnerabilità.

## 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 IPS.

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.

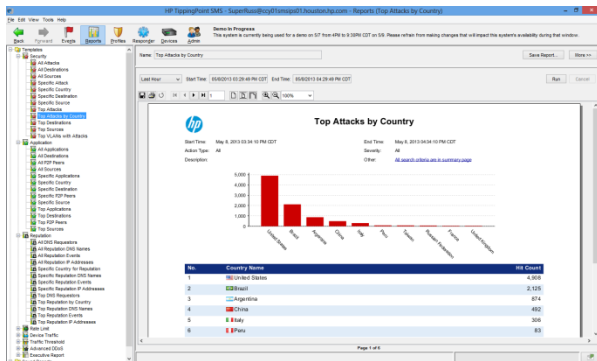
## Le soluzioni NGIPS HP TippingPoint

La piattaforma di Next Generation Intrusion Prevention System (NGIPS) HP TippingPoint è un elemento centrale dell'offerta HP per la sicurezza dell'infrastruttura di rete (dal perimetro alla parte core, al campus fino alle filiali), delle applicazioni e del data center che permette di filtrare il traffico in ingresso e in uscita sulla rete aziendale, di bloccare i contenuti nocivi e di identificare comportamenti pericolosi o tentate violazioni di policy.

Questa soluzione è composta da tre macro componenti:

- ❑ le piattaforme hardware specializzate per la prevenzione delle intrusioni (IPS);
- ❑ le soluzioni appliance e virtual machine HP TippingPoint Security Management System (SMS) che forniscono funzioni di gestione della sicurezza di livello enterprise a tutti i prodotti di sicurezza HP TippingPoint;
- ❑ l'organizzazione di ricerca per la sicurezza DV Labs che effettua una ricerca avanzata delle minacce correlando eventi di sicurezza e di vulnerabilità, per fornire le informazioni intelligenti di sicurezza che alimentano le piattaforme IPS

come il fondamentale Digital Vaccine e il servizio integrativo di reputazione dinamica della rete pubblica RepDV.



HP TippingPoint Security Management System (SMS)

Le soluzioni IPS HP TippingPoint individuano le nuove vulnerabilità presenti sulla rete e intervengono applicando delle "patch" virtuali che ne impediscono lo sfruttamento.

Di fatto, il sistema IPS di HP ottimizza le prestazioni del traffico legittimo effettuando una continua pulizia della rete e assegnando la massima priorità alle applicazioni mission critical.

Il cuore delle soluzioni IPS di HP TippingPoint è rappresentato da una gamma di pacchetti di filtri per la protezione, denominati Digital Vaccine, che vengono sviluppati nei DV Labs e forniti automaticamente all'utente finale.

Questi filtri permettono di proteggere le reti dai diversi tipi di minacce quali vulnerabilità, virus, worm, Trojan, P2P,

spyware, minacce miste, phishing, minacce VoIP, attacchi DoS e DDoS, backdoor, walk-in worm e altri.

Il team di sicurezza dei DV Labs HP TippingPoint sviluppa e distribuisce una vasta gamma di filtri di sicurezza, inclusi filtri basati sul rilevamento di anomalie del traffico e filtri basati sulle vulnerabilità, e li incorpora all'interno dei Vaccini Digitali.

Questi vaccini sono creati non solo per rispondere a specifici exploit, ma anche a potenziali permutazioni di attacco, estendendo così la protezione alle minacce Zero-Day.

## I punti di forza delle soluzioni HP NGIPS TippingPoint

La gamma di soluzioni NGIPS HP TippingPoint IPS fornisce una protezione di rete in linea ad alte prestazioni che non riduce in modo apprezzabile le prestazioni della rete. In particolare, con la più recente soluzione HP TippingPoint S7500NX il throughput per ispezione in linea è stato portato fino a 20 Gbps all'interno di un apparato che occupa 2 unità rack (2U).

All'interno di questi apparati convergono nuovi servizi di sicurezza che consentono di fregiarsi del titolo di sistemi di "next generation" e che includono:

- ❑ blocco intelligente basato sul contesto;
- ❑ HP TippingPoint Reputation Digital Vaccine (RepDV), con livello di reputazione IP DNS definito dagli utenti e policy di sicurezza basate sulla localizzazione (perimetro, core, filiale e così via);
- ❑ riconoscimento, visibilità e controllo dell'applicazione con Deep Packet Inspection (DPI);
- ❑ HP TippingPoint Application Digital Vaccine (AppDV), Web Application Digital Vaccine (WebAppDV) e filtri di protezione personalizzati sviluppati dagli utenti;
- ❑ riconoscimento del tipo di contenuto e controllo per ispezionare specifiche tipologie di file e proteggere le informazioni critiche;
- ❑ integrazione con le altre soluzioni HP Enterprise Security (quali Fortify e ArcSight) per fornire intelligenza di sicurezza aggiuntiva, visibilità e controllo attraverso l'intero data center.

A livello di densità di porte per il data center core HP può vantare nella piattaforma Serie NX, il supporto di fino a 24 segmenti da 1 GbE, 16 segmenti di 10 GbE, o 4 segmenti di 40GbE.

Queste soluzioni dispongono di funzioni di elevata disponibilità e ridondanza e sono caratterizzate da una latenza

tipica inferiore a 40 microsecondi, per proteggere dispositivi di rete, software di virtualizzazione, sistemi operativi e applicazioni da attacchi senza impattare sulle prestazioni.

L'approccio basato su "virtual patch" migliora il livello di protezione da eventi di tipo zero-day, fermando sul nascere la diffusione di traffico dannoso.

La presenza di una serie di funzionalità di gestione della larghezza di banda presenti sulla piattaforma NGIPS HP TippingPoint NX impediscono alle applicazioni potenzialmente dannose come peer-to-peer e streaming media di diffondersi liberamente in tutta la rete.

Attraverso un processo continuo di pulizia del traffico di rete dannoso o indesiderato, le prestazioni di rete sono accelerate a vantaggio delle applicazioni mission-critical ottenendo un incremento della banda disponibile che HP ha stimato tra il 40% e il 70%.

Un altro elemento di forza è dato dal fatto che le soluzioni NGIPS e il sistema di gestione della sicurezza (SMS) possono essere facilmente installati in rete, tipicamente in un tempo che varia da 30 minuti a due ore. Le soluzioni NGIPS sono progettate per la trasparenza della rete e vengono distribuite in rete senza richiedere di associare alcun indirizzo IP o MAC, in

modo che possano iniziare immediatamente a filtrare il traffico dannoso e indesiderato.

Gli NGIPS di HP consentono di gestire le policy di sicurezza con granularità fine. Gli amministratori possono impostare criteri di sicurezza di rete specifici per segmento di rete, VLAN, o Classless Inter-Domain Routing (CIDR). Inoltre, attraverso le funzionalità di reputazione della piattaforma NGIPS e il Reputation Digital Vaccine, gli utenti possono incorporare l'uso di indirizzi IP e dei nomi DNS all'interno della loro gestione delle policy di sicurezza.

Le funzioni avanzate di reporting di sicurezza permettono agli amministratori di mostrare ai revisori interni ed esterni come la rete è protetta dalle minacce più recenti per soddisfare i requisiti di compliance normativi e interni.

La disponibilità degli HP TippingPoint DV Labs e la Zero Day Initiative (ZDI) costituiscono altri punti di forza distintivi rivendicati da HP.

## La gamma d'offerta

### HP TippingPoint IPS Serie NX

La serie HP TippingPoint NX di sistemi di prevenzione delle intrusioni di prossima generazione (Next Generation

IPS ovvero NGIPS) è in grado di fornire in tempo reale protezione in linea dalle intrusioni e una sicurezza proattiva della rete adatte a sostenere l'evoluzione e la crescita dei data center. Utilizza la nuova tecnologia X-Armour di TippingPoint per garantire un sistema di prevenzione delle intrusioni adattivo che protegge dalle minacce informatiche che aggrediscono le applicazioni, le reti e i dati critici.

La serie NX comprende i modelli S2600NX, S5200NX, S6200NX con un throughput di rete di 40 Gbps e una capacità di ispezione rispettivamente di 3, 5 e 10 Gbps.

I modelli S7100NX S7500NX hanno un throughput di rete di 100 Gbps e una capacità di ispezione rispettivamente di 15 e 20 Gbps, supportando fino a 60 milioni di sessioni contemporanee.

Tutti i dispositivi Serie NX hanno tempi di latenza inferiori a 40 microsecondi.



HP TippingPoint NGIPS Serie NX

### HP TippingPoint IPS Serie N

La serie N di appliance NGIPS HP TippingPoint per la prevenzione delle intrusioni mette a disposizione delle

aziende un elevato livello di protezione in-line e in tempo reale attraverso differenti sistemi che si differenziano per prestazioni e capacità di filtro.

I modelli HP 660N e HP 1400N sono i sistemi "entry level" dotati di 10 segmenti con interfaccia a 1 Gbps e supportano una capacità di ispezione IPS rispettivamente di 750 Mbps e 1,5 Gbps.

Alle esigenze di fascia superiore si indirizzano i modelli HP S2500N, S5100N e S6100N dotati di interfacce a 1 e 10 Gbps e adatti a un throughput consigliato rispettivamente di 3, 5 e 10 Gbps.

In particolare la piattaforma TippingPoint 6100N ha una capacità di filtro fino a 10 Gbps e un tempo di latenza di soli 40 microsecondi adatto alle richieste di protezione di traffico in ambienti altamente virtualizzati senza penalizzare la qualità operativa.

Tutti i modelli prevedono il sistema di alimentazione ridondante e altre funzionalità per l'alta disponibilità quali Layer 2 Fallback e Stateful Redundancy.

### HP Core Controller

Sotto la continua spinta del consolidamento a livello di data center, dell'high performance computing (HPC) e delle applicazioni a elevata richiesta di

ampiezza di banda come il video on-demand e il file sharing, le reti "core" utilizzano sempre più spesso tecnologia di rete a 10 Gbps.

Pertanto, l'esigenza di ispezionare il traffico e bloccare le minacce dannose presso i punti caratterizzati da elevato traffico di throughput senza compromettere il livello prestazionale diventa sempre più pressante. Per questo motivo i responsabili della rete e della sicurezza si preoccupano di predisporre sistemi IPS non solo presso il tradizionale perimetro WAN, ma anche tra i principali segmenti di rete all'interno delle reti "core" e dei data center.

HP Core Controller è un sistema dotato di 48 porte 1000Base-T e 6 porte 10GbE che estende la protezione IPS basata su tecnologia TippingPoint ai collegamenti a 10 Gbps.



HP Core Controller

Questa soluzione consente un'ispezione automatizzata del traffico in linea, fino a 20 Gbps, per proteggere dagli attacchi i dispositivi di rete, i software di virtualizzazione, i sistemi operativi e

le applicazioni Web e aziendali. Questa soluzione viene implementata inserendola come elemento di rete, adatto a supportare fino a 3 connessioni di rete a 10 Gbps. Il traffico che entra nel Core Controller viene bilanciato in modo intelligente verso una serie di IPS, mentre quello affidabile viene inviato nuovamente al Core Controller per la distribuzione verso gli appropriati collegamenti a 10 Gbps.

## HP TippingPoint Security Management System

HP TippingPoint SMS è un'appliance che fornisce una vista globale e la possibilità di amministrazione, configurazione, monitoraggio e reporting nelle situazioni di implementazioni su larga scala di molteplici IPS.



Un esempio di visualizzazione fornito da HP TippingPoint Security Management System

Una tipica distribuzione di IPS HP su tutta la rete è costituita da un client

SMS (basato su Java), da un sistema centralizzato SMS e da molteplici IPS. L'SMS prevede livelli di controllo di accesso basati su privilegi di operatore (sola lettura), amministratore e supervisore. Fornisce una vista generale, con analisi sui trend, correlazione e grafici in tempo reale, compresi report con statistiche sul traffico, attacchi filtrati, host di rete e servizi di inventario e stato di salute degli IPS.

Le caratteristiche principali includono:

- ❑ reporting e analisi dei trend a livello enterprise
- ❑ cruscotto che fornisce una vista globale
- ❑ configurazione e monitoraggio del dispositivo
- ❑ reporting automatico
- ❑ meccanismi di Automated Security Response
- ❑ gestione basata su policy
- ❑ gestione del Digital Vaccine
- ❑ gestione e revisione degli eventi
- ❑ risposta automatica a eventi e operazioni di rimedio
- ❑ gestione degli user account e degli accessi.

## HP TippingPoint CloudArmour

HP TippingPoint CloudArmour è una combinazione di prodotti progettati per garantire la sicurezza delle

infrastrutture data center virtualizzate, che controlla e protegge il traffico di macchine virtuali all'interno di server host fisici, offrendo piena capacità IPS.

Si compone di diversi prodotti: la piattaforma fisica NGIPS e le soluzioni software virtual Controller (vController) e virtual Management Center (vMC) e virtual Firewall (vFW).

vController è il software che viene installato nella Service Virtual Machine di ogni host virtualizzato e che si colloca all'interno dell'hypervisor VMware tramite l'API VMsafe.

Una volta installato, vController può analizzare tutto il traffico proveniente da qualsiasi delle macchine virtuali applicative presenti sull'host virtualizzato e permette di applicare all'hypervisor un firewall virtuale che esegue tre compiti:

- ❑ verifica se il traffico è consentito o meno e decide se lasciarlo passare;
- ❑ se il traffico non è consentito, lo blocca completamente a livello di hypervisor;
- ❑ se il traffico è consentito offre la possibilità di ispezionarlo.

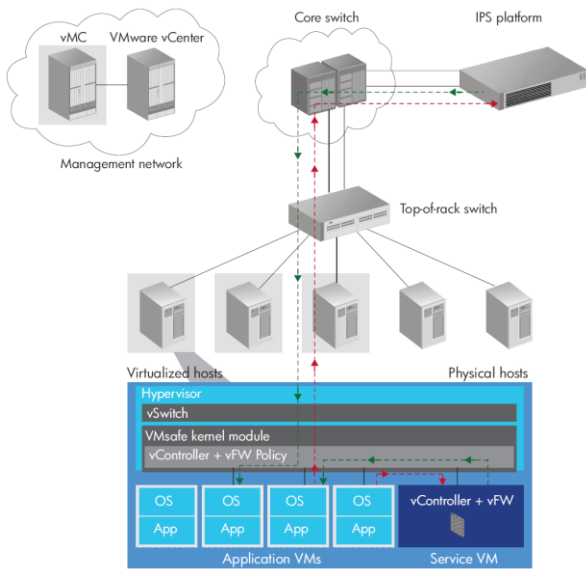
Il vController indirizza il traffico attraverso una VLAN dedicata verso il dispositivo fisico IPS per l'analisi. L'IPS ispeziona il traffico, blocca qualsiasi

contenuto dannoso e quindi passa il traffico ispezionato di nuovo al vController (sempre attraverso una VLAN) che inoltra il traffico verso la sua destinazione originaria.

Questo meccanismo permette di controllare il traffico in entrata e in uscita dal data center al perimetro, quello tra host fisici presenti nel data center, tra host fisici e VM e anche il traffico tra due macchine virtuali sullo stesso host virtualizzato, facendo rispettare le policy di sicurezza.

Dato che ogni vController presente nel data center dispone di tutte le policy di reindirizzamento, viene garantita la medesima condizione di sicurezza per ogni macchina virtuale o applicazione, indipendentemente da dove venga collocata all'interno del data center, su un sistema fisico o virtuale.

La soluzione vController è completamente gestita da virtual Management Center che è pienamente integrato con il Security System Management di HP TippingPoint abilitando, in tal modo, una gestione integrata e che mette sotto il controllo esclusivo del personale addetto alla sicurezza IT tutte le funzioni di gestione della protezione. vMC fornisce la piena visibilità del data center virtualizzato favorendo il controllo e la sicurezza delle macchine virtuali.



HP TippingPoint CloudArmour

### HP TippingPoint SSL

HP TippingPoint S1500 SSL è l'appliance che offre funzionalità di "offloading" e "bridging" sicuro per le attività di ispezione del traffico crittografato SSL (Secure Sockets Layer).

Questa capacità aumenta la sicurezza all'interno dei data center di nuova generazione e consente di prevenire che attacchi crittografati possano compromettere Web server e applicazioni Web, favorendo anche il rispetto della compliance.

### HP Reputation Digital Vaccine (RepDV)

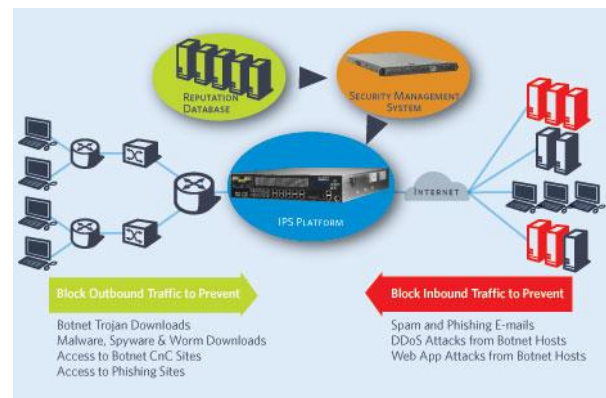
È un servizio offerto tramite i DVLabs, pensato per migliorare la protezione da

botnet e minacce avanzate e persistenti.

Permette di effettuare operazioni di blocco dell'accesso o di monitoraggio in base al valore di un indicatore di reputazione o di rischio fornito dai DVLabs e alla localizzazione geografica, attraverso un feed ricevuto quasi in tempo reale sui server e sui dispositivi infettati o ad alto rischio che sono presenti in Internet.

Il servizio di RepDV abilita le funzionalità di analisi di contesto e geolocalizzazione sulle sonde IPS in aggiunta a quelle di analisi di contenuto di dati e protocolli già presenti nel DV.

Il RepDV si basa sull'analisi incrociata di milioni di data stream raccolti giornalmente dalla rete mondiale di sensori TippingPoint Lighthouse Network e da diversi fornitori specializzati per classificare indirizzi IP e siti pubblici per indice di pericolosità, nazione, tipologia.



HP Reputation Digital Vaccine (RepDV)

Con il RepDV è possibile identificare e bloccare con precisione e senza impatto prestazionale connessioni con siti non affidabili quali depositi di malware e centri di controllo di botnet in uscita e in entrata dalla rete aziendale.

### 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 patch virtuali che consentono di proteggere l'azienda in attesa della disponibilità di un rimedio definitivo.

### Digital Vaccine Toolkit (DVToolkit)

DVToolkit è lo strumento che consente di creare protezioni personalizzate da zero oppure di importare nativamente

firme create in open source, trasformarle in filtri TippingPoint per poi inserirle in un package Digital Vaccine specifico, consentendo alle aziende di integrare la protezione DV con quella dei filtri già realizzati per specifiche applicazioni legacy.



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.

