Next Generation Firewall per elevare la sicurezza di rete: le soluzioni HP TippingPoint

Reportec

Next Generation Firewall per elevare la sicurezza di rete: le soluzioni HP TippingPoint

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 sicurezza di rete efficace diventa un compito quanto mai complesso.

I firewall, che da sempre rappresentano la prima linea di difesa per il network aziendale, hanno dovuto evolvere per riuscire a fronteggiare le nuove minacce. Questo ha determinato l'arrivo di dispositivi di nuova generazione, i Next Generation Firewall (NGFW), più granulari nell'analisi e più efficaci nella difesa.

HP ha introdotto nelle suo portafoglio d'offerta Enterprise Security Product la nuova gamma di Next Generation Firewall HP TippingPoint.

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

Verso la protezione di rete di nuova generazione

Il settore tecnologico è in rapido mutamento sotto la spinta contemporanea di più trend tra loro correlati e ognuno dei quali racchiude in sé le potenzialità per rivoluzionare il modo di concepire l'IT stesso. Parliamo di fenomeni quali cloud computing, virtualizzazione, mobilità e BYOD che cambiano non solo il paradigma tecnologico, ma anche e soprattutto il modo con cui le aziende conducono il proprio business. Questi fenomeni creano non solo opportunità ma anche nuovi rischi di sicurezza.

Il cloud computing introduce nuove modalità per accedere alle applicazioni all'esterno dei confini aziendali, imponendo alle aziende di predisporre le condizioni per proteggere le interazioni con le applicazioni enterprise su cloud, come nel caso del Software-as-a-Service e del cloud storage.

La mobility richiede un controllo e una visibilità delle applicazioni più ampi, indipendentemente dal punto di accesso. Le aziende devono tutelarsi dall'introduzione di malware o da potenziali brecce che potrebbero essere determinate dalla natura di accesso da dispositivo mobile alla rete aziendale.

Il BYOD ha introdotto un utilizzo promiscuo dei dispostivi mobili per attività private e aziendali al fine di favorire la produttività e il coinvolgimento dei dipendenti. Tuttavia, tali dispositivi si collocano ai confini della rete e sono perciò fuori dalla portata dei tradizionali sistemi IPS. Per proteggere le reti dalle potenziali minacce introdotte da questi dispositivi, le aziende devono mettere in atto controlli capaci di operare ai margini esterni della rete.

Le conseguenze di questo rinnovato scenario sono che le aziende si trovano ad avere un minor controllo sui punti di accesso alla rete

Ne deriva l'esigenza di disporre di soluzioni di sicurezza capaci di estendere la protezione oltre il perimetro della rete aziendale e di predisporre una più profonda integrazione delle soluzioni IT per difendere le interazioni degli utenti da potenziali minacce alla sicurezza.

Per stare un passo avanti rispetto all'evoluzione delle minacce servono sistemi e dispositivi di nuova generazione che sappiano intervenire in modo più mirato e dispongano del livello di "intelligenza" necessario a valutare in modo più approfondito e circostanziato i dati di sicurezza.

Con la nuova gamma di sistemi TippingPoint NGFW HP si propone di fornire una soluzione per contrastare i rischi legati a questi trend tecnologici emergenti.

L'evoluzione della network security

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 ?

L'indagine *2013 Cost of Cyber Crime Study* condotta da Ponemon Institute per conto di HP Enterprise Security Product, ha rilevato che il costo medio annuo del crimine informatico riscontrato su un campione di aziende degli Stati Uniti (in vari settori industriali, di cui molte multinazionali con oltre mille postazioni) è di11,56 milioni di dollari, con un incremento del 78% rispetto ai dati rilevati quattro anni fa nella prima edizione dell'indagine. I risultati indicano, inoltre, che il tempo necessario per risolvere un attacco informatico è aumentato di quasi il 130% nello stesso periodo e che il costo medio per la risoluzione di un singolo attacco ammonta a oltre 1 milione di dollari.

Predisporre misure efficaci di sicurezza significa anche affrontare una revisione della rete che, tuttavia, non è solo di natura tecnologica, ma anche di carattere strategico.

Un 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).

Le carenze di firewall 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". Ma

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.

I Next Generation Firewall rappresentano uno degli ultimi step di questo percorso evolutivo.

I Next Generation Firewall

La prima definizione di Next Generation Firewall si deve a Gartner che nel suo "Magic Quadrant for Enterprise Network Firewalls" del 2009 individua come requisiti caratterizzanti per questo tipo di soluzioni l'integrazione delle seguenti funzioni:

- analisi approfondita dei pacchetti (Deep Packet Inspection),
- Intrusion Detection,
- capacità di riconoscere le applicazioni,
- capacità di controllo granulare.

Inoltre i Next Generation Firewall differiscono da quelli tradizionali nella loro efficacia quando operano anche come Sistemi di Intrusion Prevention (IPS).

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

La prima riguarda la possibilità di controllo a livello di applicazione poiché oramai la stragrande maggioranza delle violazioni sfruttano le vulnerabilità collocate all'interno di applicazioni.

Si tratta, in realtà, 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.

Una seconda 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 dai ricercatori HP ha dimostrato vulnerabilità in relazione alla possibile perdita o fuoriuscita di dati.

Un risultato che non sorprende se si considera che, 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 driver 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 firewall evolute 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 definitiva, in un contesto di reti senza perimetro, minacce persistenti e utenti remoti, i Next Generation Firewall appresentano soluzioni in grado di contribuire a elevare il livello di protezione della rete senza impattare su processi e infrastruttura.

La sicurezza enterprise di HP

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), HP 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.

La famiglia HP TippingPoint NGFW

HP TippingPoint Next-Generation Firewall (NGFW) è una nuova linea di prodotto sviluppata sulla base del motore dei sistemi HP TippingPoint NGIPS.

L’introduzione di questa famiglia di dispositivi costituisce per HP una naturale estensione del proprio

portafoglio di soluzioni di rete, pensata per bloccare gli attacchi in corrispondenza di ogni singolo punto di controllo lungo la rete enterprise.

I dispositivi della gamma HP TippingPoint NGFW 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 gli NGFW 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 NGFW 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.

Uno dei punti distintivi di queste soluzioni è la loro semplicità d'uso che li rende adatti 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.

HP TippingPoint NGFW consente di creare dashboard personalizzati e funzioni di reporting automatizzato.

L'affidabilità è un altro aspetto su cui HP intende rimarcare il valore della nuova famiglia di firewall. A tale riguardo, il vendor cita uno studio interno del 2012 realizzato su un campione casuale di 100 clienti delle soluzioni TippingPoint, che evidenzia un uptime di rete su un arco di 12 mesi del 99,99999 percento.

Per quanto riguarda, invece, l'efficacia della propria tecnologa di protezione nel bloccare possibili minacce, HP mette sul piatto l'attività del team di ricerca DVLabs cha ha pubblicato a oggi oltre 7400 filtri e che è costantemente impegnato in operazioni per arrestare gli exploit e bloccare gli attacchi.

A questo si aggiungono iniziative quali il programma HP TippingPoint Zero Day Initiative e l'inserimento delle soluzioni NGFW in un contesto più ampio fatto di soluzioni di sicurezza come ArcSight o Fortify che rientrano sotto la divisione Enterprise Security Product.

Le funzionalità comuni a tutti i modelli

Il portafoglio prodotti della famiglia HP TippingPoint NGFW prevede cinque modelli.

Tra le funzionalità comuni a tutti i modelli vi è il supporto per funzionalità di rete predisposte per il protocollo IPv6 che includono "link aggregation", OSPF, RIP, supporto VLAN, BGP e routing multicast dinamico. Inoltre prevedono funzioni di alta disponibilità sia in modalità attiva sia passiva.

Questi appararti supportano connettività tramite VPN IPsec sia in modalità "site-to-site" sia "client-to-site", mentre

I Next Generation Firewall di HP prevedono anche il supporto integrato per la definizione di policy basate sull'utente con servizi di autenticazione basati su Active Directory, LDAP o RADIUS. Le funzioni di controllo d'accesso tramite ruolo (RBAC) consentono di avere sempre sotto controllo chi è in grado di intervenire sulla configurazione del dispositivi e su quali parti.

Tutti i modelli 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 presenta una porta seriale RJ-45 per la console.

La gestibilità può avvenire tramite Security Management Server (SMS), linea di comando SSH, Web browser (https) oppure utilizzando la HP TippingPoint NGFW Management Information Base (MIB).

Il consumo energetico è di 142 W per il modello entry level e di 493 W per gli altri quattro.

HP TippingPoint Next Generation Firewall 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+Application control 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 Next Generation Firewall 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+Application control 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+Application control.

HP TippingPoint Next Generation Firewall 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+Application control e 1,5 Gbps per le VPN IPsec; questi numeri raddoppiano sul modello S8010F.

HP TippingPoint Security Management System

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 (NGFW) e i sistemi IPS di nuova generazione dispositivi (NGIPS).

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.

Soluzioni per una protezione integrata

I dispositivi della gamma HP TippingPoint Next Generation Firewall si avvalgono delle avanzate ricerche sul tema della sicurezza di HP TippingPoint DVLabs e Zero Day Initiative (ZDI), del supporto di una nuova community per condividere informazioni di sicurezza nonché dei feed di HP TippingPoint RepDV, al fine di individuare in maniera proattiva le più recenti minacce e gli attacchi "command and control" centralizzati.

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 NGFW 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 NGFW 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 DVLabs 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 Threat Central

Threat Central è una piattaforma collaborativa di security intelligence per la condivisione di informazioni di sicurezza da parte di una community di utenti che operano su settori simili.

Threat Central è stata pensata da HP per creare un sistema di difesa contro le minacce informatiche più avanzate e si propone, per esempio, di fornire un valido aiuto in settori come il finance dove la stessa tipologia di attacchi viene replicata su più organizzazioni dello stesso tipo.

Questa piattaforma consente di condividere informazioni su minacce, analisi e azioni correttive e fornisce 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 della community 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, l'organizzazione che conduce ricerche e fornisce servizi di intelligence per l'intero portafoglio di soluzioni HP Enterprise Security.

HP Research Group contribuisce direttamente alla community aggiungendo best practice, risultati delle proprie indagini e suggerimenti operativi.

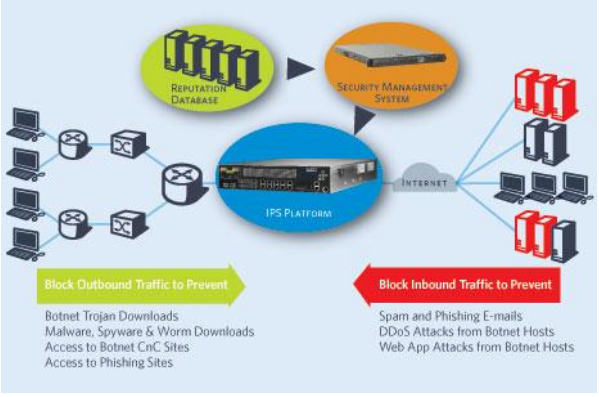
HP Reputation Digital Vaccine (RepDV)

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.