

**HP Runtime Application  
Self Protection:  
l'Application Defender  
Service di HP Enterprise  
Security Products**

**Reportec**



## HP Runtime Application Self Protection: l'Application Defender Service di HP Enterprise Security Products

*Dott. Gaetano Di Blasio,  
Vice President Reportec*

*La pressione degli attacchi che mirano al livello applicativo per sfruttarne le vulnerabilità sta portando alla realizzazione di "applicazioni blindate", che sappiano cioè resistere agli attacchi con sistemi di autoprotezione. Emergono così le soluzioni di Runtime Application Self Protection (RASP), che combinano funzionalità proprie dei Web Application Firewall con tecnologie per il test statico, dinamico e interattivo delle applicazioni. Le soluzioni RASP rappresentano per Gartner un tassello ormai imprescindibile in un sistema di sicurezza aziendale. Questo white paper illustra le caratteristiche di base delle soluzioni RASP e il loro posizionamento, soffermandosi, infine, sulla recente soluzione HP Application Defender Service.*

**I**l 24% degli attacchi informatici che si sono verificati nel 2013 e nel primo semestre del 2014 hanno sfruttato vulnerabilità note. Almeno stando al Rapporto Clusit 2014 <sup>1</sup>, che ha analizzato solo gli attacchi resi pubblici. Peraltro, altre ricerche dimostrano che non solo le vulnerabilità sono ancora al primo posto tra le "falle" preferite, ma che addirittura l'80% degli attacchi sono rivolti al layer applicativo <sup>2</sup>.

La maggior parte delle soluzioni di sicurezza sono concentrate, storicamente, sul "perimetro" aziendale. Un concetto che sta perdendo vieppiù di significato. Anche per le applicazioni i fornitori di Information Security hanno seguito questo approccio, per esempio con i Web Application Firewall e altre soluzioni un po' più sofisticate, progettate per identificare anomalie.

L'evoluzione delle minacce, però, ha reso poco efficaci le classiche tecniche per l'analisi del traffico, richiedendo

controlli "contestualizzati", al fine di comprendere la natura di determinate azioni, apparentemente maligne ma, in realtà lecitamente previste dall'applicativo.

Nelle seguenti pagine descriveremo le capacità della "Runtime Application Self Protection" (RASP): un tipo di soluzione definita dal Gartner un "must to have" per la prima volta nel 2012 <sup>3</sup>.

Ci soffermeremo, poi, sulla soluzione/servizio RASP di HP: HP Application Defender.

## Una protezione multilivello

Innanzitutto va osservato che le soluzioni RASP non sono una panacea. La sicurezza totale non esiste, ma è auspicabile raggiungere la massima sicurezza possibile compatibilmente con le attività online che il business aziendale richiede.

La sicurezza perimetrale resta fondamentale per monitorare il traffico e bloccare una gran numero di attacchi. Anche se il perimetro aziendale è sempre più "liquido", sul mercato si trovano soluzioni che sono in grado di adattarsi alle nuove architetture "aperte".

Ovviamente una soluzione preventiva efficace per mitigare il rischio derivante dagli attacchi evidenziati nel rapporto Clusit e non solo, consiste nell'application security testing, cioè nell'impedire di mettere in esercizio applicazioni che contengono vulnerabilità note.

Come abbiamo più volte osservato su queste pagine, sono veramente poche le imprese che riescono a perseguire questo obiettivo. Anche quelle che hanno un piano di patch management, faticano a starvi dietro. Senza contare le

problematiche derivante dalle nuove applicazioni.

Certamente sono stati compiuti giganteschi passi avanti rispetto al passato, quando gli editori di software trovavano "naturale" e forse divertente demandare ai clienti la bug discovery. Oggi i processi sono stati notevolmente migliorati e le applicazioni sono molto più sicure sin dalla nascita, ma le esigenze di time to market, le conoscenze non sempre approfondite sulla sicurezza e, soprattutto, le maggiori risorse di sviluppo sul fronte dei cybercriminali, rendono impossibile disporre di un'applicazione sicura al 100%. Questo non significa che non si debbano seguire processi di testing accurati per progettare le applicazioni il più sicure possibili.

Le soluzioni RASP non nascono per sostituire questi primi due livelli di protezione, ma per aumentarne l'efficacia. I Web Application Firewall, infatti, sarebbero in grado di eseguire le azioni protettive necessarie, se solo avessero le informazioni giuste e le avessero in tempo, ma in ogni caso forniscono tecnologie dedicate alla protezione delle applicazioni.

La protezione RASP è appunto capace di analizzare il codice in tempo reale e di attuare contromisure sulla base dei risultati. Punto fondamentale: l'analisi

deve avvenire nel contesto reale, direttamente nell'ambiente di produzione.

Questo perché solo il reale funzionamento, con l'utilizzo dei dati effettivi permette di portare a termine l'analisi: per capire il comportamento di una query SQL, per esempio, è necessario guardare la query completa, che si costruisce, di fatto, all'interno dell'applicazione.

Le soluzioni RASP, dunque, costituiscono una protezione essenziale per le applicazioni in produzione.

## Runtime Application Self Protection

Come accennato, il funzionamento di un'applicazione varia anche in base alla tipologia di dati che essa deve elaborare. Per verificarne il comportamento è dunque necessario osservare lo stesso nell'ambiente d'elaborazione, durante l'elaborazione stessa.

Attualmente, le soluzioni sul mercato effettuano questo tipo di controlli con dispositivi "esterni" all'ambiente di runtime, come firewall e IPS. Si tratta di soluzioni certamente valide ma la cui efficacia potrebbe essere ridotta dall'impossibilità d'entrare nella logica dell'applicazione, della sua

configurazione e delle sue relazioni con i flussi dei dati e degli eventi. Non a caso sono spesso "relegati" a una funzione di alerting, non potendo garantire l'accuratezza necessaria a evitare tassi di falsi positivi accettabili.

Secondo gli analisti di Gartner, le imprese cosiddette "pioniere" della tecnologia hanno già adottato tecnologie RASP o lo stanno facendo, mentre le altre dovrebbero comunque implementarle entro i prossimi tre anni. Un lasso di tempo durante il quale le tecnologie oggi sul mercato arriveranno a una piena maturità. Già adesso, peraltro, sono in essere soluzioni che, appoggiandosi al cloud, permettono alle imprese di utilizzare lo stato dell'arte in ambito RASP, seguendone "naturalmente" l'evoluzione e, non per ultimo, di incontrare minori difficoltà nell'implementazione, installazione e gestione delle soluzioni.

Peraltro, sempre secondo Gartner<sup>4</sup>, entro il 2017 il 25% degli ambienti di elaborazione avranno capacità di autoprotezione integrate (rispetto a meno dell'1% nel 2012).

Questa "urgenza" deriva dalla crescente pressione delle minacce sul layer applicativo. È fondamentale che le applicazioni siano in grado di "autoprottegersi": cioè disporre di funzioni che le proteggano durante

l'elaborazione. Queste devono idealmente poter osservare qualsiasi dato entri o esca dall'applicazione, tutti gli eventi che la riguardano, ogni istruzione eseguita e tutti gli accessi al database.

Una soluzione RASP possiede tutti questi requisiti e così permette all'ambiente d'elaborazione di rilevare gli attacchi e proteggere l'applicazione più a fondo.

### ***Web Application Firewall più l'Interactive Application Security Testing***

In buona sostanza, le soluzioni RASP combinano le tecnologie dei Web Application Firewall (WAF) e dell'Interactive Security Testing (IAST), mettendo insieme funzionalità di scansione, monitoraggio in real time, detection, protezione, analisi dell'esecuzione e analisi del traffico. In pratica, si tratta di una nuova tecnologia resa possibile solo grazie all'interazione di altre tecnologie. La componente IAST, di recente introduzione, è fondamentale, perché è questa che "arma" l'ambiente di runtime. Tali soluzioni di testing s'integrano per esempio in una Java Virtual Machine (JVM) o nel .NET Common Language Runtime (.NET CLR) diventando parte.

Essendo all'interno della JVM o del .NET CLR, il sistema di test riesce a "vedere" i flussi indotti da un attacco. Meglio ancora, li può simulare per prevederli.

Le soluzioni RASP prendono a prestito tale capacità dalle tecniche IAST e, contemporaneamente, utilizzano la capacità di reazione in tempo reale dei Web Application Firewall per terminare una sessione "maligna" o per lanciare un alert in caso di esecuzioni sospette rilevate dall'Interactive Application Testing.

È quindi la combinazione delle due tecnologie che rende possibile la Runtime Application Self Protection. Di fatto, la massima efficienza si ottiene combinando tutte le tipologie di application protection disponibili, dal testing statico a quello dinamico fino a quello interattivo. Non solo, perché le analisi delle vulnerabilità e quelle degli attacchi condotte da queste tecnologie sono alla base delle soluzioni RASP. Proprio la loro combinazione realizza la self protection, permettendo di superare i principali limiti. Se l'analisi statica permette di sospettare una vulnerabilità in una linea di codice, solo l'analisi in runtime consente di verificare la consistenza di un exploit che sfrutta la vulnerabilità ipotizzata. Potrebbe dunque accorgersene il test dinamico dell'applicazione. Nessun sistema di test, peraltro, è in grado di fermare un attacco. Può invece farlo il RASP, prendendo la decisione in base alle informazioni fornite dal testing

applicativo e utilizzando le capacità d'azione real time del WAF.

In effetti, può avvenire anche il contrario: la componente Web Application Firewall può rilevare traffico sospetto e "richiede" alla componente IAST di effettuare un supplemento di analisi testando il flusso d'elaborazione e di dati durante l'esecuzione.

In ogni caso, la soluzione RASP sfrutta la combinazione delle tecnologie, ma non le sostituisce. Il Web Application Firewall, infatti, ha ragione di sussistere anche a sé stante per bloccare un'azione potenzialmente dannosa, come il collegamento a un sito Web elencato in una blacklist.

Le soluzioni RASP rappresentano una prima pietra miliare di un percorso verso il cosiddetto "Application Shielding", che potremmo tradurre come la "blindatura delle applicazioni". Blindare un'applicazione per renderla resistente agli attacchi, permettendole di difendersi direttamente da sola.

Ancora una volta, sottolineiamo che non si tratta di sostituire un precedente livello di protezione, né, in realtà di aggiungerne uno nuovo, ma più semplicemente di allargare l'orizzonte di protezione, per rispondere all'espansione del fronte di attacco.

È ancora presto per capire fino in fondo come si svilupperà l'Application Shielding o quanto rapidamente si affermeranno le tecnologie RASP. Anche perché ci sono diversi fattori che intervengono nel disegnare tale scenario. Per esempio, l'adozione di soluzioni per la Runtime Application Self Protection sarebbe probabilmente accelerata dalle alleanze che i produttori di applicazioni e/o quelli del middleware per gli ambienti d'elaborazione potrebbero siglare con i vendor che sviluppano e vendono soluzioni RASP. In pratica, si potrebbero realizzare ambienti di runtime blindati alla nascita.

Questo avrebbe anche il benefico effetto di rendere meno invasiva l'analisi di sicurezza e testing, riducendo il rischio di impatti sulle capacità di elaborazione.

Un contributo ad accelerare la blindatura delle applicazioni potrebbe arrivare anche dal cloud, come precedentemente accennato. L'ambiente di runtime è pressoché totalmente controllato dal cloud provider. Per costoro è quindi logico installare soluzioni RASP che garantiscano la sicurezza dell'elaborazione. Con tale garanzia possono girare la responsabilità di eventuali attacchi alla connessione di rete utilizzata dal loro cliente.

Lasciare la gestione della soluzione RASP al provider è un vantaggio anche

per il cliente, che non si dovrà più preoccupare di installare e mantenere tali soluzioni.

In un circuito virtuoso queste soluzioni contribuiscono a sciogliere i dubbi sulla sicurezza del cloud che rimane uno dei principali ostacoli alla sua adozione.

### L'autoprotezione delle applicazioni: HP Application Defender

HP ha introdotto tecniche RASP già da qualche tempo, per esempio nelle soluzioni HP WebInspect e HP ArcSight Application View. Soprattutto la tecnologia RASP chiamata HP Fortify Real-Time Analyzer è implementata come estensione di un debugger Java o di un profiler .NET, appunto a protezione

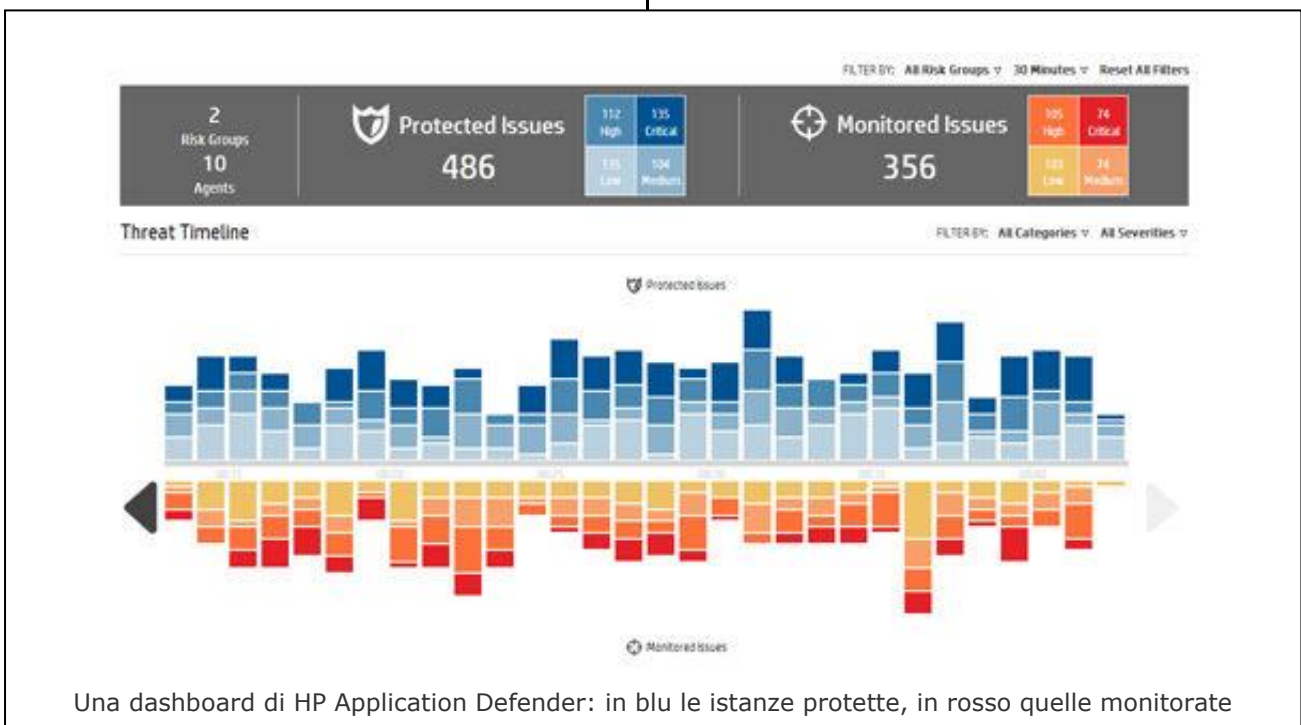
delle applicazioni Java e .NET.

A queste se ne aggiungono altre funzioni inserite nei sistemi per il monitoraggio. Insomma una base significativa, che ha permesso ad HP di maturare un consistente esperienza in materia di tecnologie RASP.

Esperienza che è stata ulteriormente messa a frutto con il servizio per la protezione delle applicazioni in cloud HP Application Defender.

Più precisamente, si tratta di un managed service per l'autoprotezione delle applicazioni, in risposta alla crescente pressione degli attacchi informatici ai servizi applicativi online.

Con l'aumentare del numero e della complessità delle applicazioni aziendali, la superficie esposta agli attacchi cresce



Una dashboard di HP Application Defender: in blu le istanze protette, in rosso quelle monitorate

considerevolmente e, come in precedenza osservato, i tradizionali metodi per proteggere le applicazioni richiedono tempi lunghi, a cominciare dall'installazione delle patch, mentre le difese perimetrali sono una protezione indiretta.

Per questo, in HP hanno progettato un sistema di autoprotezione delle applicazioni, basato sull'analisi in tempo reale dell'esecuzione stessa del codice, monitorandone così l'attività per prevenire le aggressioni dall'interno dell'applicazione.

Grazie al servizio di auto-protezione delle applicazioni, HP Application Defender consente alle aziende di identificare automaticamente le vulnerabilità del software e proteggersi in tempo reale.

Dopo il processo di configurazione, la piattaforma cloud based consente ai professionisti della sicurezza d'individuare e bloccare le aggressioni senza cambiare codice o installare altri dispositivi sulla rete.

La soluzione permette di gestire e riportare i dati di sicurezza in tempo reale, tramite dashboard interattive e alert che forniscono informazioni dettagliate sulla natura dell'attacco e sul punto in cui si è verificato. L'accuratezza è garantita dal fatto che HP Application

Defender fornisce informazioni dall'interno dell'applicazione.

Questo aiuta gli sviluppatori a risolvere il problema in via permanente nel codice sorgente, mentre lo stesso viene risolto in maniera virtuale nell'ambiente di produzione.

- 
- 1 Rapporto Clusit 2014
  - 2 Ricerca HP Security Products
  - 3 Runtime Application Self Protection: A Must Have, Emerging Security Technology (24 aprile 2012)
  - 4 Gartner Research G00229122, Joseph Feiman



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**.



**Gaetano Di Blasio** è giornalista professionista dal 1997. Da oltre 25 anni segue il settore dell'ICT e della sicurezza in particolare. Attualmente è Direttore Responsabile delle riviste SOLUTIONS e Security & Business di Reportec, di cui è socio e cofondatore.



The Reportec logo consists of the word "Reportec" in a white, bold, sans-serif font, set against a dark blue rectangular background.

**HP Runtime Application Self Protection:  
l'Application Defender Service di HP Enterprise Security Products**

© Reportec S.r.l. - Ottobre 2014 - Tutti i diritti riservati  
Reportec S.r.l. via Marco Aurelio, 8 - 20127 Milano

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

[www.reportec.it](http://www.reportec.it) - [www.tomshw.it/index/itpro.html](http://www.tomshw.it/index/itpro.html) - [www.tomshw.it/index/manager.html](http://www.tomshw.it/index/manager.html) - [www.tomshw.it/index/reseller.html](http://www.tomshw.it/index/reseller.html)

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