

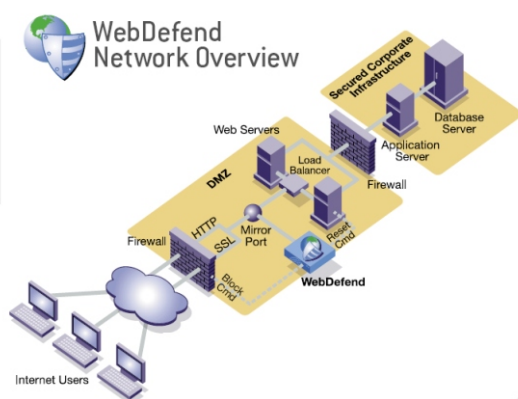
La miglior difesa contro gli attacchi alle applicazioni Web

PREVIENE IL FURTO DI IDENTITA' E DI INFORMAZIONI; METTE AL SICURO I DATI DEI CLIENTI

Nell'era di Internet, dove le applicazioni di business sono connesse ai browser in tutto il mondo, le aziende sono motivate a salvaguardare i dati di valore dei clienti, non finire sulle pagine dei giornali e assicurare la compliance con le regolamentazioni vigenti per governo e industria. *Rendere sicure le applicazioni web, e i dati dietro di esse, è oggi una parte essenziale del business sul Web.*

LA NETWORK SECURITY NON PROTEGGE DA ATTACCHI WEB MIRATI

I firewall e le soluzioni IDS/IPS non offrono nessuna protezione contro attacchi mirati alle applicazioni Web. Questi attacchi sfruttano vulnerabilità proprie dell'applicazione Web, e non possono essere protette da un IDS/IPS che non ha una completa conoscenza del comportamento dell'applicazione né può gestirne lo stato. *Ciascuna applicazione Web deve avere un profilo di sicurezza su misura, creato per proteggere le sue peculiari vulnerabilità e un meccanismo per tracciare lo stato di ciascun utente dell'applicazione.*



L'ENCRYPTION SSL NON PROTEGGE L'APPLICAZIONE WEB

L'SSL protegge i dati durante la trasmissione; tuttavia, non offre nessuna protezione dagli attacchi contro le applicazioni Web. Infatti, *gli attacchi inviati tramite SSL attraversano il firewall e bypassano la maggior parte degli IDS/IPSs, che non sono in grado di esaminare traffico criptato.*

LA SOLUZIONE WEBDEFEND

WebDefend è una soluzione per la protezione di applicazioni Web disegnata per

indirizzare le specifiche problematiche di sicurezza alle applicazioni web. WebDefend tappa i buchi della sicurezza a livello di rete, offrendo sicurezza specifica e su misura per l'applicazione, e protezione completa contro l'intera gamma di potenziali minacce Web-based.

- Protegge informazioni confidenziali, data privacy, segreti commerciali, proprietà intellettuali e copyright
- Tappa i buchi della network security per prevenire attacchi mirati alle applicazioni
- Richiede risorse di gestione limitate: genera e mantiene profili di application security su misura per ciascuna applicazione Web, grazie alla tecnologia brevettata Adaption™
- Fornisce decrittazione SSL passiva per l'analisi delle minacce criptate senza terminare la sessione SSL
- Fornisce protezione completa su tutte le minacce Web conosciute e sconosciute
- E' facile da implementare come security appliance non in linea, collegato a una porta mirro o tap
- Consente la prevenzione distribuita e flessibile delle minacce, attraverso l'architettura Distributed Detect Prevent Architecture (DDPA) che si integra con le migliori device di rete come firewall e SIM



MINACCE IDENTIFICATE E PREVENUTE

- SQL Injection
- Cross-site Scripting
- Attacchi alle applicazioni conosciuti e sconosciuti
- Zero Day Attack
- Session Hijacking
- Cookie Tampering
- Manipolazioni al Protocollo
- Worm automatici
- Attack Reconnaissance
- Data Leakage & Identity Theft
- XML Parameter Tampering
- Data Theft
- OWASP Top 10 Security Threats

ENTERPRISE MANAGEMENT ASSOCIATES

"WebDefend rappresenta la prossima generazione di sicurezza operativa sulle applicazioni: la gestione distribuita della sicurezza applicativa. Questo approccio ha il potenziale di rendere obsolete le tecniche single-point-of-protection attuali, comprendendo l'intera gamma di strumenti disponibili per proteggere le applicazioni enterprise critiche."

Scott Crawford, CISSP, Senior Security Analyst
Enterprise Management Associates

CIO, VENDOR E-COMMERCE

"Cosa non mi fa dormire? Non sapere chi sta entrando nelle mie applicazioni Web. WebDefend mi offre report on-demand sul comportamento anomalo del traffico che entra ed esce dalle nostre applicazioni Web. Scopre e blocca la perdita di informazioni sensibili."

BreachGate WebDefend™

BREACH

- Offre un'analisi dettagliata degli eventi attraverso una consolle di gestione intuitiva
- Prepara report dettagliati e generali per le esigenze di security, compliance e auditing

CONSOLE DI GESTIONE INTUITIVA

Questa consolle di gestione user-friendly facilita la predisposizione e la gestione di policy di attraverso Policy Manager, la definizione del profilo di sicurezza di ciascuna applicazione tramite Site Manager, e fornisce informazioni dettagliate sugli eventi con Event Viewer.

IL MOTORE MULTIPLE THREAT DETECTION OFFRE PROTEZIONE COMPLETA

WebDefend Protection Engine	Benefici
Behaviour	Fornisce una validazione positiva di tutto il traffico dell'applicazione confrontata con un profilo di comportamento accettabile. tutto il traffico anomalo viene passato al motore di detection per identificare qualsiasi attacco e fornire azioni da intraprendere in risposta. Assicura la protezione da tutti gli attacchi noti e ignoti verso le applicazioni Web.
Signature	Fornisce un database di attacchi per le vulnerabilità conosciute dei componenti delle applicazioni. L'analisi delle firme offre un contesto di sicurezza per le anomalie riscontrate dal motore comportamentale. Offre protezione contro attacchi noti contro le applicazioni Web, server Web, application server, componenti middleware e script.
Protocollo	Protegge contro attacchi di violazione del protocollo che utilizzano i protocolli HTTP e HTTPS per attaccare le applicazioni web. Protegge contro attacchi spesso sotto forma di denial of service (DoS) o di worm automatici.
Sessioni	Controlla le sessioni utente per attacchi che cercano di impersonare altri utenti. Offre protezione contro la manipolazione delle sessioni e hijacking così come "cookie poisoning", attacchi che permettono ai cybercriminali di assumere un'identità valida e di accedere a funzionalità e dati privati.
Analisi dell'utilizzo	Fornisce l'analisi di gruppi di eventi cercando pattern di utilizzo che indicano che un sito è sotto esame da parte di un potenziale hacker. Gli attacchi mirati necessitano che i cybercriminali ricerchino le vulnerabilità presenti su un sito per poterle utilizzare per i loro scopi. L'analisi dell'utilizzo del tempo e delle sessioni utenti offre protezione contro un attacco mirato prima che l'hacker sia pronto a lanciarlo, bloccando la ricerca sul sito richiesta dall'hacker.
ExitControl	Protegge contro gli hacker che cercano di estrarre informazioni sensibili da un database aziendale attraverso un'applicazione Web. Regole specifiche, chiamate BreachMarks™, sono predefinite per la maggior parte dei dati sensibili, come codici fiscali e carte di credito. Le aziende possono definire i loro propri BreachMark per identificare le loro informazioni privilegiate e di proprietà intellettuale.
Servizi Web	Protegge le applicazioni che implementano servizi Web da virus XML, corruzione dei dati e attacchi denial of Web service (DoS).

Come fare a sapere se un hacker sta attaccando le vostre applicazioni Web?

Come sapere se informazioni confidenziali sono uscite dalla vostra azienda?

Come scoprire se le vostre applicazioni Web sono al sicuro da attacchi mirati?

SPECIFICHE TECNICHE

- Configurazione NIC 10/100/1000 Mb/Sec
- Supporto per algoritmi RSA e key exchange
- Supporto per tutte le encryption più comuni e per gli algoritmi MAC digest:
 - DES, Triple DES, RC4, RC2, MD5, SHA, SHA1
- Tre modelli disponibili con performance differenziati
- FIPS 140-2 Livello 2 e 3 compliant key storage

BREACH

Breach Security, Inc.
Corporate Headquarters
2011 Palomar Airport Rd., Ste. 200
Carlsbad, CA 92011
Tel: 760.268.1924
Email: info@breach.com

(c) (2005) Breach Security, Inc. All Rights Reserved. 9/05

DISTRIBUITO DA

DotForce
Via Zuretti, 25
20125 Milano MI
tel.: 02-45.48.15.21
Fax: 02-670.76.111
www.dotforce.it
breach@dotforce.it

BREACH SECURITY

Breach Security, Inc. provides next-generation Web application security to protect privileged information. Breach addresses today's enterprise security needs by delivering solutions to comprehensively protect web applications against attack and resolve security challenges such as Identity Theft, Information Leakage, regulatory compliance, and insecurely coded applications. [For more information visit www.breach.com.](http://www.breach.com)