



SERVIZIO GESTITO DI  
WEB APPLICATION FIREWALL

# WAF AS A SERVICE

*Datasheet*



Le aziende del Gruppo MEET IT



Via di Corticella, 89/2  
40128 Bologna BO

+39 05 14070383

[www.3cime.com](http://www.3cime.com) | [info@3cime.com](mailto:info@3cime.com)



ntnuovetecnologie

Viale Alcide De Gasperi, 37  
33100 Udine UD

+39 0432 524001

[infoentonline.it](http://infoentonline.it) | [www.ntonline.it](http://www.ntonline.it)



**Il servizio rivoluziona l'approccio alla protezione delle applicazioni e dei siti web, grazie ad un servizio firewall dedicato che permette di risparmiare sul costo di acquisto, a favore di un servizio gestito sicuro e di alta qualità.**

La **sicurezza delle applicazioni** fornita dal cloud protegge i tuoi dati, ti aiuta a raggiungere la conformità e a mantenere la "reputation", una delle chiavi fondamentali del business presente e futuro.

L'implementazione e la configurazione dei tradizionali **firewall per applicazioni web (WAF)** può essere proibitiva e richiedere molto tempo. In effetti, alcune aziende installano semplicemente un WAF in modalità predefinita per garantire la conformità e non lo configurano quasi mai nella maniera ottimale, rendendosi così vulnerabili alle minacce basate sulle applicazioni.

Con il nostro servizio è possibile **distribuire, configurare e rendere operativo** il servizio WAF aaS in pochi minuti. I modelli precostituiti proteggono immediatamente le applicazioni e un'**interfaccia intuitiva** semplifica la messa a punto di criteri specifici. La protezione DDoS a spettro completo garantisce la disponibilità continua delle applicazioni. Inoltre, il servizio integrato di **Vulnerability Remediation Service** (opzionale) esegue automaticamente la scansione delle applicazioni e rimedia alle vulnerabilità.

Dovendo garantire una protezione continua **24 ore su 24, 7 giorni su 7**, l'adozione di un servizio è una soluzione molto più affidabile rispetto all'acquisto di un semplice prodotto.

## PREMESSA

Il servizio prende in considerazione siti e piattaforme web di qualunque tipo, **sia in ambienti cloud che on-premise**:

- **Siti vetrina**, per i quali la protezione è volta a garantire la reputation
- Servizi di **commercio elettronico**
- **Servizi al cittadino** esposti in Internet
- **Servizi di tipo B2B** per le relazioni tra operatori economici

## SITI





## Semplice e flessibile

WAF aaS offre una **procedura guidata di onboarding in cinque fasi**, facile da usare, per garantire la **protezione delle applicazioni in pochi minuti**. Efficaci modelli precostituiti forniscono una **protezione completa** per le applicazioni più utilizzate. Gli utenti avanzati possono facilmente affermare un **controllo granulare** su elementi specifici per impostare **criteri di sicurezza personalizzati**. È sufficiente aggiungere l'elemento di configurazione che si desidera perfezionare all'elenco dei componenti di configurazione e regolarli per soddisfare le proprie esigenze specifiche.



## Protegge dagli attacchi di nuova generazione

Il servizio si basa su una tecnologia collaudata a livello aziendale che difende dai rischi di sicurezza della **OWASP Top 10**, dalle **OWASP Automated Threats to Web Applications** e da molto altro, comprese le **minacce zero-day**. La **difesa bot avanzata** blocca gli attacchi automatizzati come il **web scraping**, lo **scalping**, il **carding**, lo **spam bot** e gli **attacchi di credential-stuffing/accoppiamento di account**. La **protezione DDoS** non misurata previene gli attacchi DDoS sia applicativi che volumetrici. **Ricche analisi e report intuitivi** aiutano a documentare la conformità.



## Protegge le app di nuova generazione

Indipendentemente dal luogo in cui vengono ospitate le tue applicazioni (in sede, nel cloud, in un container o in un ambiente serverless), avrai a disposizione un'**API REST** e il servizio di **Vulnerability Remediation Service**, che esegue la **scansione delle vulnerabilità delle applicazioni e le corregge con un solo clic**. Questo garantisce una **sicurezza ottimizzata e ininterrotta** anche quando aggiorni le tue applicazioni e ne distribuisce di nuove in risposta all'evoluzione delle esigenze aziendali, senza alcun costo amministrativo aggiuntivo.



## Protezione

- All OWASP risks, including "Top 10"
- Brute force attacks
- Parameter tampering
- Cookie/form manipulation
- Forceful browsing
- XML attacks
- Application tampering
- Zero-day attacks
- SQL Injection
- Cross-site scripting (XSS)
- Convalida dei meta-dati dei campi dei moduli
- Occultamento del sito web
- Controllo delle risposte
- Prevenzione del web scraping
- Criteri granulari per gli elementi HTML - Controlli dei limiti di protocollo
- Controllo del caricamento dei file
- Elenco di IP consentiti/bloccati

## Miglioramenti dell'applicazione

- Alta disponibilità
- Offloading SSL
- Bilanciamento del carico

## Protezioni avanzate

- Database di reputazione IP
- Fingerprinting euristico
- Sfide CAPTCHA
- Protezione dei client lenti
- Nodi di uscita ToR
- Elenco di blocco
- Protezione DDoS L3-L7 non misurata

## Protocolli supportati

- HTTP/S/0.9/1.0/1.1/2.0
- WebSocket
- IPv4