GIDS

De complete gids voor Web Application Firewalls

WAF-typen, kosten, OWASP-bescherming, implementatie en NIS2-compliance voor het MKB.

Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij •

Wat is een WAF? 1

Waarom is een WAF belangrijk? 2

Hoe werkt een WAF? Het proces 3

Wat kost een WAF? 4

Waar moet je op letten bij de keuze? 5

Veelgemaakte fouten 6

Compliance: NIS2 en regelgeving 7

WAF vs. traditionele firewall vs. WAAP 8

Trends 2025--2026 9

Aan de slag 10

Bronnenlijst •

Kerncijfers op een rij

Webapplicatie-aanvallen groeien explosief. Een WAF is je eerste verdedigingslinie.

311 mrd

Webapplicatie-aanvallen wereldwijd in 2024 (+33% jaar-op-jaar)

Akamai [1]

150 mrd

API-aanvallen geregistreerd van januari 2023 tot december 2024

Akamai [1]

88%

Van Basic Web Application attacks gebruikte gestolen credentials

Verizon DBIR 2025 [2]

USD 8,6 mrd

Wereldwijde WAF-markt in 2025, groeiend met 14,9% per jaar

Fortune Business Insights [3]

44%

Van alle bevestigde breaches betrof ransomware (was 32%)

Verizon DBIR 2025 [2]

4.875

Cyberincidenten in EU geanalyseerd (juli 2024 - juni 2025)

ENISA [4]

EUR 10 mln

Maximale NIS2-boete voor essentiële entiteiten bij nalatigheid

Kynexis [5]

30.000+

CVE's voor cross-site scripting (XSS), een van de meest voorkomende webaanvallen

OWASP Top 10 2025 [6]

1. Wat is een WAF?

Een Web Application Firewall (WAF) beschermt je webapplicaties door HTTP/HTTPS-verkeer te analyseren en kwaadaardig verkeer te blokkeren voordat het je applicatie bereikt.

Een WAF werkt als een schild tussen het internet en je webapplicatie. Elke HTTP-request wordt geinspecteerd op bekende aanvalspatronen zoals SQL-injectie, cross-site scripting (XSS), path traversal en andere OWASP Top 10-kwetsbaarheden [6].

Anders dan een traditionele firewall, die op netwerkniveau (Layer 3/4) werkt, opereert een WAF op applicatieniveau (Layer 7). Dit betekent dat een WAF de inhoud van HTTP-requests kan beoordelen -- niet alleen de herkomst en bestemming [7].

> **Voor wie is een WAF?** Elke organisatie met een webapplicatie, webshop, klantportaal of API die via het internet bereikbaar is. Voor MKB is een cloud-based WAF de meest praktische en betaalbare optie.

2. Waarom is een WAF belangrijk?

Het aanvalsvolume op webapplicaties groeit explosief en aanvallers richten zich steeds vaker op het MKB.

In 2024 registreerde Akamai 311 miljard webapplicatie-aanvallen wereldwijd, een stijging van 33% ten opzichte van het jaar ervoor [1]. API's zijn daarbij het primaire doelwit geworden, met 150 miljard API-aanvallen in twee jaar tijd [1].

Volgens het Verizon DBIR 2025 begon 20% van alle breaches met exploited vulnerabilities, een stijging van 34% [2]. Een WAF kan veel van deze aanvallen blokkeren voordat ze je applicatie bereiken.

Een datalek kost gemiddeld USD 4,44 miljoen [8]. Een cloud WAF kost vanaf EUR 50 per maand. De kosten-baten zijn helder.

3. Hoe werkt een WAF? Het proces

Van request tot blokkering -- hoe een WAF je webapplicatie beschermt.

1

DNS-configuratie

1 DAG

Je DNS wordt aangepast zodat verkeer eerst via de WAF loopt voordat het je webserver bereikt.

2

Verkeersinspectie

REAL-TIME

De WAF analyseert elke HTTP/HTTPS-request op bekende aanvalspatronen, anomalieen en verdacht gedrag.

3

Regelbeoordeling

MILLISECONDEN

Requests worden getoetst aan regelsets (OWASP Core Rule Set, custom regels, IP-reputatie, geo-blocking).

4

Actie: blokkeren of doorlaten

MILLISECONDEN

Kwaadaardig verkeer wordt geblokkeerd, legitiem verkeer wordt doorgelaten. Geblokkeerde requests worden gelogd.

5

Monitoring en tuning

DOORLOPEND

De WAF wordt continu gemonitord op false positives en de regelsets worden bijgewerkt voor nieuwe dreigingen.

4. Wat kost een WAF?

WAF-kosten varieren van tientallen tot duizenden euro's per maand, afhankelijk van het type en de schaal.

MODEL	PRIJSINDICATIE	GESCHIKT VOOR
Cloud WAF (basis)	EUR 50 - 250/maand [9]	MKB, 1-5 websites
Managed cloud WAF	EUR 250 - 750/maand	MKB met custom regels
Enterprise managed WAF	EUR 750 - 2.500/maand	API-bescherming, 24×7 SOC
On-premise appliance	EUR 5.000 - 50.000 eenmalig	Groot MKB, eigen datacenter

MKB-TIP

Een cloud-based WAF met CDN-integratie beschermt je webapplicatie en versnelt tegelijkertijd je website. Vanaf EUR 50/maand heb je basisbescherming tegen de OWASP Top 10.

5. Waar moet je op letten bij de keuze?

10 vragen die je moet stellen bij het selecteren van een WAF.

1. Beschermt de WAF tegen de volledige OWASP Top 10 2025?
2. Is API-bescherming inbegrepen of een aparte module?
3. Hoe wordt omgegaan met false positives?
4. Is er een learning mode voor initiële tuning?
5. Wat is het effect op de laadtijd van je website?
6. Biedt de WAF DDoS-bescherming op applicatieniveau?
7. Hoe worden regelsets bijgewerkt bij nieuwe dreigingen?
8. Is bot management inbegrepen?
9. Welke rapportage is beschikbaar voor compliance?
10. Wat is de SLA voor beschikbaarheid?

6. Veelgemaakte fouten

Deze valkuilen zien we regelmatig bij WAF-implementaties.

1. WAF als enige beveiligingsmaatregel

Een WAF is een verdedigingslaag, geen complete beveiligingsoplossing. Combineer een WAF met veilige code, penetratietesten en security monitoring.

2. Geen tuning na implementatie

Elke webapplicatie is anders. Zonder tuning genereren WAF's te veel false positives, waardoor legitiem verkeer wordt geblokkeerd of de WAF op "alert only" wordt gezet.

3. API's niet beschermen

API-aanvallen zijn met 47% gestegen [1]. Veel organisaties beschermen hun website maar laten hun API's onbeschermd.

4. Verouderde regelsets

Regelsets die niet regelmatig worden bijgewerkt, missen nieuwe aanvalspatronen. Kies een WAF met automatische regelset-updates.

5. Performance niet testen

Een slecht geconfigureerde WAF kan de laadtijd van je website significant verhogen. Test altijd de impact op performance voor en na implementatie.

7. Compliance: NIS2 en regelgeving

De Cyberbeveiligingswet maakt webapplicatiebescherming onderdeel van je zorgplicht.

Onder de NIS2-richtlijn, die in Q2 2026 als Cyberbeveiligingswet in werking treedt, zijn organisaties verplicht passende technische maatregelen te treffen [10]. Een WAF is een concrete invulling van die zorgplicht voor webapplicaties.

Boetes voor niet-naleving kunnen oplopen tot EUR 10 miljoen of 2% van de wereldwijde jaaromzet [5].

PCI DSS

PCI DSS Requirement 6.6 schrijft voor dat webapplicaties die betalingsgegevens verwerken beschermd moeten worden met een WAF of regelmatige code reviews. Een WAF is de meest praktische oplossing voor MKB.

8. WAF vs. traditionele firewall vs. WAAP

Drie beschermingslagen met verschillende functies.

ASPECT	TRADITIONELE FIREWALL	WAF	WAAP
OSI-laag	Layer 3/4	Layer 7	Layer 7+
Beschermt tegen	Netwerkscans, poortscans	SQL-injectie, XSS, OWASP Top 10	Alles van WAF + API's + bots + DDoS
API-bescherming	Nee	Beperkt	Ja, kern functie
Bot management	Nee	Basis	Geavanceerd
MKB-geschiktheid	Standaard aanwezig	Cloud WAF vanaf EUR 50/mnd	Vanaf EUR 250/mnd

9. Trends 2025--2026

WAAP vervangt traditionele WAF

Web Application and API Protection (WAAP) combineert WAF, API-bescherming, bot management en DDoS-mitigatie in een platform.

AI-gestuurde detectie

Machine learning detecteert zero-day aanvallen door afwijkend gedrag te herkennen. 54% van WAF-leveranciers biedt inmiddels behavioral analytics [3].

API-first security

Met 150 miljard API-aanvallen in twee jaar is API-bescherming de belangrijkste uitbreiding van WAF-platforms [1].

10. Aan de slag

Bescherm je webapplicaties vandaag nog. Zo begin je.

1. **Inventariseer:** Welke webapplicaties, portalen en API's zijn via internet bereikbaar?
2. **Prioriteer:** Welke applicaties verwerken gevoelige data of betalingen?
3. **Kies je model:** Cloud WAF, managed WAF of on-premise?
4. **Implementeer stapsgewijs:** Begin in monitoring mode, tune, schakel dan naar blocking.
5. **Monitor continu:** Analyseer geblokkeerd verkeer en pas regelsets aan.

Bronnenlijst

[1] **Akamai** -- Web Attacks Research 2024 -- akamai.com/newsroom/press-release/akamai-research-web-attacks-up-33-apis-emerge-as-primary-targets

[2] **Verizon** -- DBIR 2025 -- verizon.com/business/resources/reports/dbir/

[3] **Fortune Business Insights** -- WAF Market 2026-2034 -- fortunebusinessinsights.com/web-application-firewall-market-108841

[4] **ENISA** -- Threat Landscape 2025 -- enisa.europa.eu/publications/enisa-threat-landscape-2025

[5] **Kynexis** -- NIS2 boetes -- kynexis.nl/nis2-boetes-cyberbeveiligingswet-uitgelegd/

[6] **OWASP** -- Top 10 2025 Injection -- owasp.org/Top10/2025/A05_2025-Injection/

[7] **Cyso** -- WAF uitleg -- cyso.com/stories/web-application-firewall-waf-wat-is-het-en-wat-zijn-de-voordelen/

[8] **IBM** -- Cost of a Data Breach 2025 -- ibm.com/reports/data-breach

[9] **Indusface** -- Cloud WAF Pricing -- indusface.com/blog/cloud-waf-pricing-all-you-need-to-know/

[10] **Digitale Overheid** -- Cyberbeveiligingswet -- digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cyberbeveiligingswet/

[11] **CBS** -- Cybersecuritymonitor 2024 -- cbs.nl/nl-nl/longread/aanvullende-statistische-diensten/2025/cybersecuritymonitor-2024?onepage=true

[12] **IMARC Group** -- WAF Market 2034 -- imarcgroup.com/web-application-firewall-market

[13] **Cloudflare** -- WAF -- cloudflare.com/application-services/products/waf/

[14] **AWS** -- WAF Pricing -- aws.amazon.com/waf/pricing/

[15] **OWASP** -- Web Application Firewall -- owasp.org/www-community/Web_Application_Firewall