

# **Sunray Zero Trust ([sunray-zero-trust.eu](http://sunray-zero-trust.eu))**

**Solution Européenne et Open Source de Contrôle d'Accès Zero Trust Web**

**Protection moderne, souveraine et économique pour vos applications internes et extranets**

 Sécurité sans complexité • Souveraineté sans compromis • Performance native

# La Réalité des Cybermenaces en 2025

## Toute application exposée sur Internet est une cible

- **Attaques automatisées 24/7** : Bots scannent en permanence — centaines à milliers de tentatives/jour
- **Exploitation immédiate des CVE** : Les failles sont exploitées dans les heures suivant leur publication
- **Sophistication croissante** : IA générative utilisée pour créer des attaques personnalisées

### En chiffres :

- **56%** des organisations compromises via une app web sur 12 mois
- **25%** des violations de sécurité proviennent de failles applicatives

 Les applications à accès nominatif mal protégées sont devenues les portes d'entrée privilégiées

# Le Coût Réel d'un WAF Efficace

## Protection Enterprise : Un investissement conséquent

**WAF SaaS/CDN** (Cloudflare, Akamai, AWS, Azure)

- **Business** : 3 000-10 000€/mois — **Enterprise** : >10 000€/mois

**Appliances/VM** (Fortinet, F5, Barracuda)

- **TCO annuel** : 15 000-50 000€

**Open Source** (ModSecurity)

- **Coût réel** : 35 000-40 000€/an (expertise interne requise)

**⚠ Réalité** : Protection WAF efficace = minimum 15 000€/an par application

... et vos données transitent par des infrastructures soumises au Cloud Act américain

# Le Dilemme des DSIs

**Protéger sans se ruiner — sans perdre le contrôle de ses données**

**Applications critiques mais à faible valeur ajoutée directe :**

- Portails fournisseurs
- Outils de reporting interne
- Applications métier WEB
- Interfaces de gestion WEB
- Extranets partenaires
- Applications soumises au RGPD et à la conformité NIS2

*"Ces applications ont une audience nominative et connue — ont-elles vraiment besoin d'un WAF enterprise américain ?"*

# Repenser l'Exposition des Applications Web

## Deux catégories, deux stratégies de protection

### Applications Publiques

- Sites vitrines, e-commerce, portails grand public
- **Tout le monde** doit pouvoir y accéder
- → Nécessitent un **WAF très sophistiqué** (idéalement basé sur l'IA)
- Sans cela, toujours à la merci d'un exploit zero-day

### Applications à Accès Nominatif

- Portails fournisseurs, ERP, extranets, outils métier
- Seule une **liste définie d'utilisateurs** doit y accéder
- → Doivent être protégées par une **solution Zero Trust souveraine**
- **C'est pour cela que Sunray a été conçu — en Europe, en Open Source**

 **Conclusion :** Pourquoi payer un WAF Enterprise pour des applications dont on connaît chaque utilisateur par son nom ?

# Sunray — La Solution Zero Trust

## Protection Enterprise Souveraine à Prix Accessible

*Pour vos applications à accès nominatif, une approche Zero Trust est plus efficace et plus économique qu'un WAF*

**Notre approche :**

- Open Source** : Transparence totale, pas de vendor lock-in
- Souveraineté européenne** : Conçu en Europe, hébergé où vous le décidez
- Surface d'attaque minimale** : Architecture coupe-circuit — Sunray ne voit jamais le trafic applicatif
- Authentification moderne** : Passkeys/WebAuthn (biométrie)
- Scalabilité native** : De 10 à "x millions" d'utilisateurs
- Déploiement sans modification** : Vos applications restent intactes

**Résultat :**

**Division des coûts par 10** tout en maintenant un niveau de sécurité enterprise

# Souveraineté Numérique : Un Impératif Européen

## Vos données, vos règles, votre infrastructure

### ⚠ Contexte réglementaire européen

- **RGPD** : Amendes jusqu'à 4% du CA mondial
- **Directive NIS2** (oct. 2024) : Obligations de cybersécurité renforcées
- **Arrêt Schrems II** : Transferts UE → US remis en question

### ⚠ Le problème des solutions US

- **Cloud Act / FISA 702** : Accès aux données exigible par les autorités US, même en Europe
- Cloudflare Access, Zscaler, Okta, Auth0 : juridiction américaine

### 🌐 Sunray : la réponse européenne

- **Conçu et développé en Europe**
- **Code source ouvert** : Auditabilité totale, aucune porte dérobée possible
- **Déploiement souverain** : Vos données ne quittent jamais votre infrastructure
- **Aucune dépendance envers un fournisseur non-européen**

💡 "La souveraineté numérique n'est pas un luxe — c'est une responsabilité."

# Deux Modèles d'Architecture

## Un coupe-circuit souverain — ou un proxy serverless global

### Modèle principal — Worker FastAPI

*Middleware ForwardAuth (coupe-circuit)*

Sunray **ne voit jamais le trafic applicatif**. Votre reverse proxy interroge Sunray avant chaque requête → autorisé ou bloqué.

- **Filtre sans encaisser le trafic** — performances intactes
- Référence : **Traefik** ; compatible Nginx, Caddy, HAProxy, Envoy
- **Souveraineté totale** : on-premise ou cloud européen
- Idéal : secteur public, banque, santé, RGPD/NIS2

📍 **Principes communs** : Serveur isolé (jamais exposé) • Workers stateless • Authentification forte (Passkeys) • Souveraineté architecturale

### Alternative — Worker Cloudflare

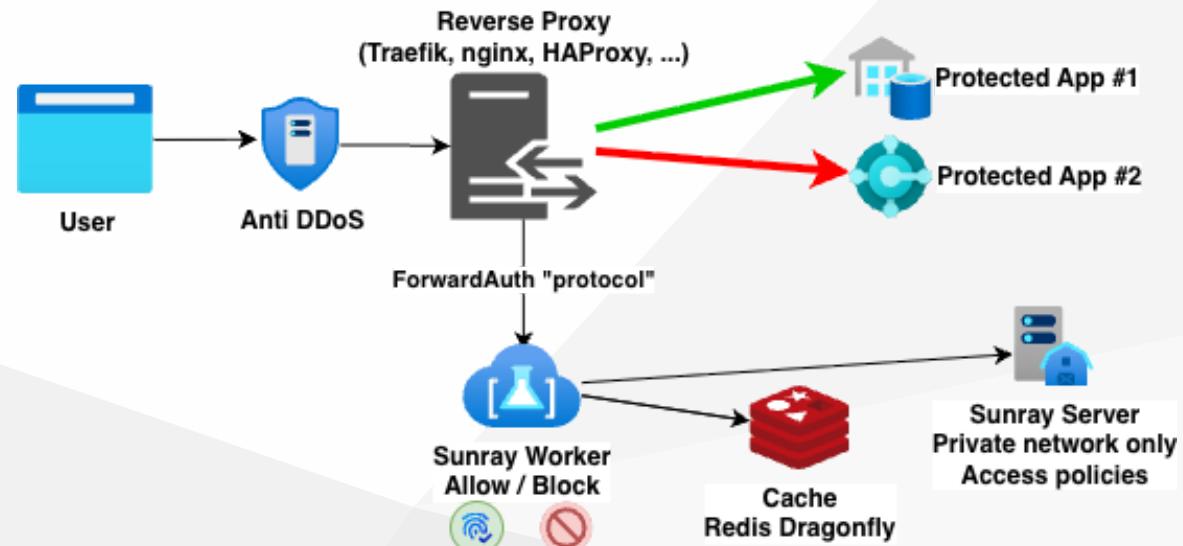
*Reverse Proxy Serverless*

Pour les applications à **audience mondiale** ou sans reverse proxy existant.

- Reverse proxy sur réseau Cloudflare (300+ PoP)
- Intercepte **tout le trafic** — scaling auto, DDoS inclus
- Le serveur Sunray reste sous votre contrôle

# Architecture Zero Trust — Mode ForwardAuth (principal)

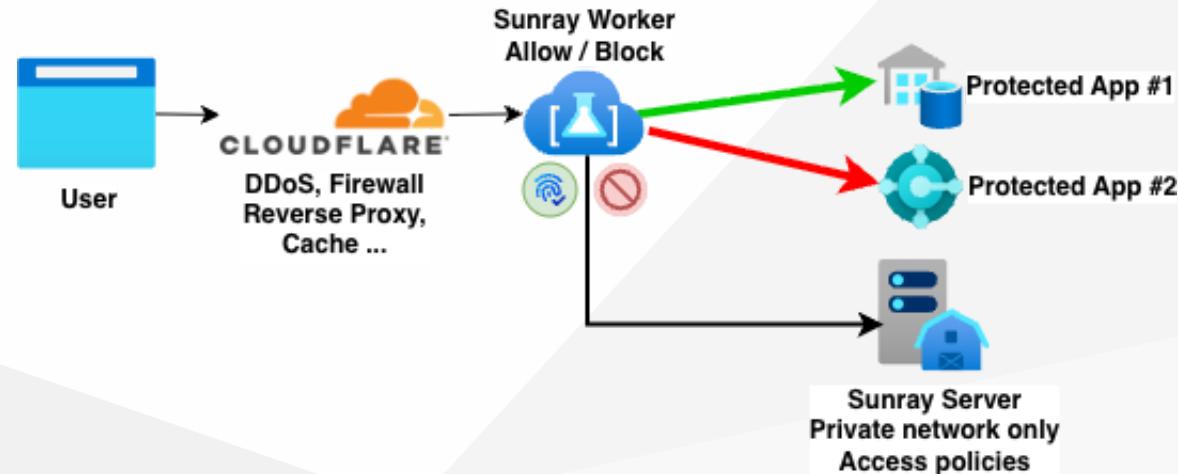
Le coupe-circuit : Sunray filtre, votre proxy route



- Le worker est un **agent de décision** — il répond autorisé/refusé, c'est tout
- Le **trafic applicatif ne passe jamais par Sunray** : zéro impact sur les performances
- Le reverse proxy reste maître du routage, du TLS, du load balancing

# Architecture Zero Trust — Mode Proxy Serverless (alternative)

Le proxy edge : Sunray intercepte et transmet tout le trafic



- Le worker **EST** intégré dans le pipeline Cloudflare — il reçoit, authentifie et transmet chaque requête
- Scaling automatique sur 300+ points de présence Cloudflare
- Protection DDoS native incluse
- Pour les cas sans reverse proxy ForwardAuth, ou pour des **applications à audience mondiale**

# Fonctionnalités Clés

## Tout ce dont vous avez besoin

### Contrôle d'accès

- Authentification sans mot de passe (Passkeys)
- Règles d'accès granulaires
- Support API/Webhooks natif

### Sécurité

- Protection Zero-Day complète
- Audit trail complet

### Simplicité

- Interface graphique évoluée
- Configuration centralisée
- Aucune modification des applications

### Conformité

- Compatible RGPD et NIS2
- Audit trail complet
- Déploiement souverain on-premise

# Cas d'Usage Typiques

## Parfait pour vos applications à accès nominatif :

- **Portails clients/fournisseurs** : Accès sécurisé sans VPN
- **Applications métier** : ERP, CRM, outils internes exposés
- **APIs et webhooks** : Protection transparente des échanges M2M
- **Sites de staging** : Sécurisation des environnements de test
- **Extranets** : Collaboration sécurisée avec les partenaires
- **Applications réglementées** : Santé, finance, secteur public — conformité RGPD/NIS2 native

## ROI immédiat :

- Réduction de 90% des coûts vs WAF traditionnel
- Déploiement en moins de 2 heures, Zéro modification du code existant

# Comparaison avec la Concurrence

Critère	WAF Enterprise	VPN	Sunray
<b>Coût mensuel</b>	5000-15000€	500-2000€	<b>50-500€</b>
<b>Complexité</b>	Élevée	Moyenne	<b>Faible</b>
<b>Modification apps</b>	Parfois	Non	<b>Jamais</b>
<b>Protection Zero-Day</b>	✓	✗	✓
<b>Expérience utilisateur</b>	Transparente	Contraignante	<b>Transparente</b>
<b>Scalabilité</b>	Coûteuse	Limitée	<b>Native</b>
<b>Open Source</b>	✗	Parfois	✓
<b>Souveraineté données</b>	✗ (US)	Partielle	✓
<b>Conformité RGPD/NIS2</b>	Complexe	Partielle	<b>Native</b>

📍 Sunray ne remplace pas un WAF pour les applications publiques — il élimine le besoin d'un WAF pour les applications à accès nominatif, tout en garantissant la souveraineté de vos données

# Architecture Technique

## Simple mais Puissant

### Sunray Server

- Gestion centralisée des politiques
- Interface d'administration web
- API REST complète
- Déploiement on-premise ou cloud souverain
- basé sur le Framework Odoo community 18

### Sunray Worker FastAPI (principal)

#### *Middleware ForwardAuth*

- Décision d'accès (autorise / refuse / redirige)
- Compatible : Traefik, Nginx, Caddy, HAProxy, Envoy
- Cache Redis/DragonflyDB — Docker/Kubernetes

### Sunray Worker Cloudflare (alternative)

#### *Reverse Proxy Serverless*

- Proxy serverless sur réseau edge Cloudflare
- Intercepte et route toutes les requêtes
- Cache Cloudflare KV — Scaling mondial auto

# Modèle de Licence

## Choisissez votre niveau de support

### Sunray Core (Open Source)

- Fonctionnalités de base, Authentification Passkeys, Community support

### Sunray Advanced (Licence)

- Règles d'accès avancées, Audit log complet, Support professionnel

### Sunray Enterprise (Package complet)

- Services professionnels, Formation et onboarding, Support dédié

# Roadmap Produit 2025-2026

## Notre Vision

### Disponible aujourd'hui

- Sunray Worker FASTAPI, Sunray Worker for Cloudflare, Authentification Passkeys et Mail, Multi hosts, API REST

### T2 2026

- Analytics dashboard

### T3-T4 2026

- Certifications de conformité (SOC2, ISO27001)
- Qualification SecNumCloud (ANSSI)

# Protégez vos Applications dès Aujourd'hui

 **Essai Gratuit 30 jours**

 **Contact**

**Email** : [cmorisse@oursbl.eu](mailto:cmorisse@oursbl.eu)

**Source** : [gitlab.com/cmorisse/sunray-server](https://gitlab.com/cmorisse/sunray-server), [gitlab.com/cmorisse/sunray-worker-fastapi](https://gitlab.com/cmorisse/sunray-worker-fastapi),  
[gitlab.com/cmorisse/sunray-worker-cloudflare](https://gitlab.com/cmorisse/sunray-worker-cloudflare)

 **Prochaines étapes**

1. Proof of Concept sur application pilote
2. Déploiement en production
3. Évaluation de conformité RGPD/NIS2

*"Security is a pain, not a feature — so let's make it affordable, sovereign, and invisible."*