Cahier des charges fonctionnel

**Firewall Intelligent à IA & EDR**

| DATE : 15 AVRIL 2025 - VERSION : V3  JULIE CHEVALLIER | KÉNAN MEYLAN | VICTOR BLAAS | JORANE RIPIEGO | CLÉMENT OLBRECHT | DORIAN SAINT-MARTIN |
| --- |

# SOMMAIRE

[**SOMMAIRE**](#_heading=h.gjdgxs) **2**

[**TABLE DES MODIFICATIONS**](#_heading=h.3znysh7) **4**

[**1. CADRE GÉNÉRAL DU PRODUIT**](#_heading=h.tyjcwt) **5**

[1.1. PRÉSENTATION DE L'ENTREPRISE ET DE SES ACTIVITÉS](#_heading=h.d2931row6438) 5

[1.2. OBJECTIFS DU PRODUIT](#_heading=h.2s8eyo1) 6

[1.3. PÉRIMÈTRE ET FRONTIÈRE DU PRODUIT](#_heading=h.3rdcrjn) 6

[1.4. EXCLUSION](#_heading=h.26in1rg) 8

[1.5. HORIZON GLOBAL DU PROJET ET DATES CLEFS](#_heading=h.lnxbz9) 8

[1.6. DOCUMENTS EN RÉFÉRENCE](#_heading=h.35nkun2) 9

[**2. IDENTIFICATION DES PARTIES PRENANTES ET DES PARTIES IMPACTÉES**](#_heading=h.z337ya) **11**

[2.1. LE DEMANDEUR :](#_heading=h.4i7ojhp) 11

[2.2. LES UTILISATEURS](#_heading=h.qsh70q) 17

[2.3. AUTRE PARTIE PRENANTE OU IMPACTÉE :](#_heading=h.2p2csry) 17

[2.4. TABLEAU RÉCAPITULATIF DES ENJEUX ET PARTIES PRENANTES](#_heading=h.32hioqz) 19

[**3. POSITIONNEMENT GLOBAL DU PRODUIT**](#_heading=h.1hmsyys) **21**

[3.1. CARACTÉRISATION DE FIREWALLAI](#_heading=h.41mghml) 21

[3.2. CARACTÉRISATION DU MARCHÉ DU PRODUIT](#_heading=h.2grqrue) 22

[**4. DESCRIPTION FONCTIONNELLE DU PRODUIT**](#_heading=h.2u6wntf) **23**

[4.1. LISTE DES CAS D’UTILISATION](#_heading=h.19c6y18) 23

[4.2. CAS D'UTILISATION "X"](#_heading=h.3tbugp1) 24

[**5. DÉTAIL DES FONCTIONS**](#_heading=h.4k668n3) **26**

[**6. CADRE DE RÉPONSE**](#_heading=h.f6qnyl5thonm) **28**

[6.1. RÉPONSES PROPOSÉES POUR CHAQUE FONCTION](#_heading=h.1egqt2p) 28

[**7. CONCLUSION**](#_heading=h.2dlolyb) **31**

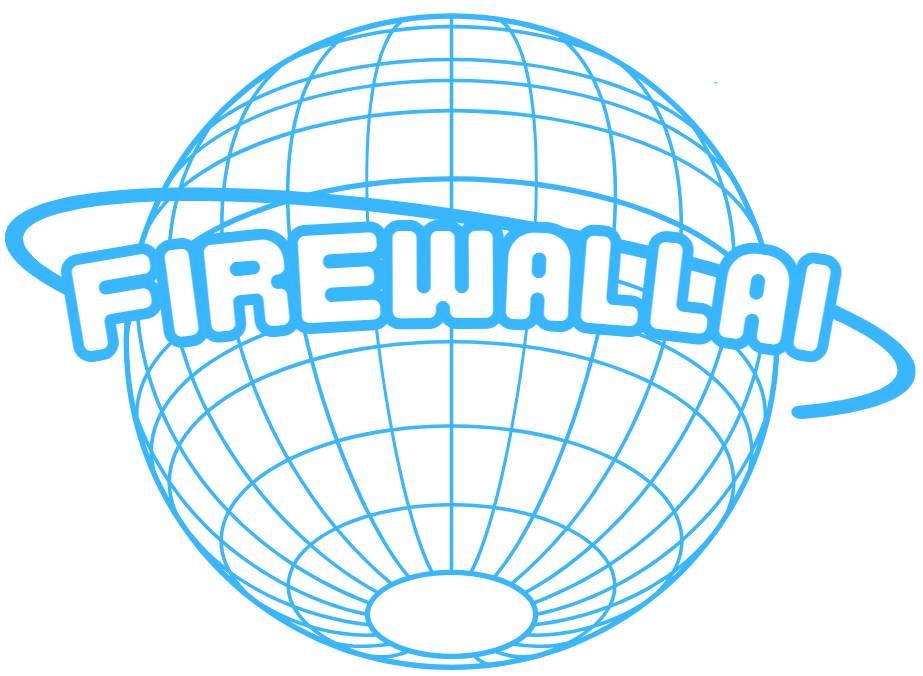
# TABLE DES MODIFICATIONS

| RÉVISION | DATE | PAGES OU § | OBJET DE LA RÉVISION |
| --- | --- | --- | --- |
| 1 | 12 AVRIL 2025 | TOUTES | CRÉATION DU FICHIER |
| 2 | 14 AVRIL 2025 | TOUTES | AVANCEMENT DU FICHIER |
| 3 | 15 AVRIL 2024 | TOUTES | FINALISATION |

## CADRE GÉNÉRAL DU PRODUIT

### PRÉSENTATION DE L'ENTREPRISE ET DE SES ACTIVITÉS

**Nom** : Firewall AI



FirewallAI est un projet technologique porté par une équipe pluridisciplinaire de passionnés de cybersécurité, d’intelligence artificielle et de développement logiciel. L’équipe fondatrice est composée de six développeurs.  
 Notre ambition est de répondre à un défi croissant du numérique : **la protection automatisée, intelligente et accessible des systèmes informatiques face aux cybermenaces modernes.**

À l’heure où les cyberattaques deviennent de plus en plus sophistiquées, et alors que les ressources humaines en cybersécurité restent limitées, FirewallAI entend offrir une **solution complète**, **intuitive**, et **proactive**, à destination des PME, des tech enthousiastes et des grandes structures.

Notre modèle repose sur une solution évolutive intégrant un pare-feu intelligent assisté par IA, un module de **détection comportementale (EDR)**, une **interface IA conversationnelle**, ainsi qu’un **système d’analyse avancée des logs**.

L’investissement initial visé pour le développement est de **100 000 €**, avec une roadmap progressive sur 12 mois allant du POC à la version finale.

* Présentation et compréhension de la VMV de FirewallAI :
  + **Vision** : Réinventer la cybersécurité en démocratisant l’accès à une protection intelligente, autonome et proactive, adaptée aux besoins réels des entreprises de toutes tailles.
  + **Mission** : Développer une solution de cybersécurité complète, intégrant un pare-feu intelligent assisté par intelligence artificielle, une interface conversationnelle intuitive, une détection comportementale avancée (EDR) et une gestion centralisée des logs. FirewallAI vise à offrir un environnement sécurisé, simple à gérer, évolutif et capable de réagir automatiquement aux menaces.
  + **Valeurs** : Innovation technologique au service de la sécurité, Accessibilité pour tous les niveaux d’utilisateurs, Confiance à travers une conformité rigoureuse aux normes, et l’agilité pour s’adapter en temps réel aux menaces et aux besoins évolutifs.
* **Présentation de la stratégie de FirewallAI, des projets « phares » en cours.**

Notre stratégie s'articule autour du développement progressif d’une **solution de cybersécurité intelligente et modulaire**, pensée pour évoluer avec les besoins des utilisateurs et les nouvelles menaces du paysage numérique. L’objectif est de proposer un **écosystème de sécurité unifié**, automatisé et piloté par l’IA, tout en restant **accessible aux non-spécialistes.**

Notre ambition est de faire de FirewallAI plus qu’un pare-feu, mais une véritable plateforme de cybersécurité intégrée, capable de s'adapter dynamiquement aux contextes métier et aux niveaux d'expertise.

**Projets phares en cours :**

* **SmartWall Core** : Le moteur de pare-feu intelligent, piloté par des règles dynamiques générées via IA, avec une interface graphique intuitive pour la gestion des objets, zones, et politiques réseau.
* **EDR Insight** : Le module de détection comportementale en temps réel, capable d’identifier et de contenir des comportements suspects au sein des systèmes protégés.
* **ChatSec** : Une interface conversationnelle en langage naturel, permettant aux utilisateurs de poser des questions, configurer le système ou recevoir des explications pédagogiques sur la sécurité de leur infrastructure.
* **LogMind** : Système de centralisation et d’analyse des logs assisté par IA, facilitant la recherche, la corrélation d’événements, et la génération de rapports automatisés pour les audits de sécurité.
* **AutoAudit AI** : Un moteur d’audit intelligent, capable d’identifier des failles de configuration, de suggérer des correctifs et d’apprendre en continu à partir des comportements réseau.

Chacun de ces projets est conçu pour être léger, modulaire, interopérable et scalable, afin de garantir des performances optimales même dans des environnements à faibles ressources (ex. : serveurs minimalistes ou infrastructures hybrides).

Grâce à cette approche, FirewallAI ambitionne de s’imposer comme la solution de cybersécurité intelligente de référence pour les PME et organisations en quête de protection avancée, sans complexité technique.

* **Ce que l’entreprise ne fait pas et pourquoi ?**

FirewallAI choisit délibérément de ne pas développer de **solutions de cybersécurité généralistes « tout-en-un »** ou centrées uniquement sur des audits manuels ou **des interventions humaines intensives**, bien que ces approches soient courantes sur le marché.

Ce positionnement est motivé par notre volonté de proposer **une solution automatisée, proactive et accessible**, en rupture avec les outils complexes, rigides ou trop techniques qui dominent souvent l’industrie. Nous ne cherchons pas à concurrencer les cabinets de conseil ou les suites de sécurité lourdes orientées exclusivement vers les grandes entreprises. Au contraire, notre force réside dans notre spécialisation : la conception d’un pare-feu intelligent et d’un écosystème de défense assisté par IA, pensé pour des structures qui manquent de ressources en cybersécurité, mais qui veulent tout de même un haut niveau de protection.

Cette concentration stratégique nous permet d’investir pleinement dans l’innovation IA et comportementale, de simplifier l’usage de la cybersécurité, même sans experts en interne, et de renforcer l’identité de FirewallAI comme solution intuitive, moderne et adaptable.

En restant fidèles à cette vision, nous évitons de diluer notre proposition de valeur et construisons une relation solide avec notre public cible.

### OBJECTIFS DU PRODUIT

FirewallAI est une solution de cybersécurité innovante en développement, visant à offrir une protection automatisée, évolutive et performante contre les menaces informatiques modernes. Ce projet repose sur une architecture modulaire et optimisée pour la gestion des flux réseau, avec une intégration avancée des technologies XDP et eBPF pour une interception ultra-rapide des paquets. L'objectif principal de FirewallAI est de proposer une solution efficace, accessible et facile à déployer pour les entreprises de toutes tailles, sans nécessiter une expertise technique poussée.

Développé par une équipe de **six développeurs aux compétences variées (Chef de Projet, Développeur Principal, Responsable Sécurité, Responsable IA, Testeur et Développeur Backend)**, FirewallAI s'adresse aux PME, aux passionnés de technologie, ainsi qu'aux grandes entreprises cherchant à renforcer leur cybersécurité de manière agile et autonome.

Le projet se distingue par l'intégration d'une série de modules clés : un pare-feu intelligent auto-configuré par IA, un système de détection comportementale des menaces (EDR), un moteur d'analyse centralisée des logs, ainsi qu'une interface conversationnelle en langage naturel. Ces composants travaillent ensemble pour permettre à FirewallAI de détecter, prévenir et répondre de manière proactive aux cyberattaques, tout en offrant une expérience utilisateur intuitive grâce à une interface en temps réel.

Avec un investissement initial de 100 000 € et une durée de développement de 12 mois, FirewallAI prévoit plusieurs étapes clés de développement, allant de la validation du cahier des charges à la livraison d’une version finale fonctionnelle, suivie d’une phase de stabilisation et optimisation continue. La solution sera construite sur des technologies robustes (Rust, Python, React, Docker, PostgreSQL) et intégrera des modèles d'IA open-source pour une efficacité accrue.

L'objectif à long terme est de positionner FirewallAI comme un **acteur de référence dans le domaine de la cybersécurité intelligente, capable de s’adapter en temps réel aux nouvelles menaces et aux besoins spécifiques des utilisateurs.** Notre ambition est d’attirer un large marché en Europe, en particulier des entreprises de taille moyenne et grande, grâce à une proposition de valeur unique : une solution de cybersécurité puissante, entièrement automatisée, facile à déployer et à gérer.

### PÉRIMÈTRE ET FRONTIÈRE DU PRODUIT

* **Fonctionnalités Incluses**

**Pare-feu intelligent basé sur IA :** Filtrage par IP, MAC, port, interface, réseau et protocole, Gestion des VLAN et traduction d’adresses (NAT/PAT), Détection et prévention des intrusions avec alertes via webhook, Simulation de règles sans blocage, avec journalisation.

**Système de détection comportementale des menaces (EDR) :** Détection rapide des anomalies et comportements suspects dans le réseau, Alerte en temps réel sur des événements de sécurité.

**Moteur d'analyse centralisée des logs :** Journalisation centralisée via ELK (Elasticsearch, Logstash, Kibana), Visualisation des logs et monitoring des performances en temps réel.

**Interface utilisateur en temps réel via WebSocket :** Interface graphique web accessible en ligne et localement via console TTY web, Possibilité de gérer manuellement les règles ou déléguer aux modules IA, Interaction en temps réel pour la gestion des règles et interfaces.

**Modules d'intelligence artificielle intégrés :** Entraînement des modèles d’IA sur des datasets IDS pour améliorer la détection des menaces, Réduction du temps de réaction (TTR) grâce à des modèles d’IA qui analysent en continu les données, Prise en charge d’une IA open-source pour l'amélioration continue des performances de sécurité.

**Gestion des clusters et failover automatique :** Répartition automatique de la charge et gestion des pannes pour garantir la disponibilité continue du service.

**Module Anti-DDoS :** Protection contre les attaques par déni de service distribué (DDoS) pour garantir l'intégrité du réseau.

* **Fonctionnalités Futures (Hors Périmètre Actuel)**

**Prise en charge d’IPv6 :** Support complet pour les adresses IPv6, en plus des adresses IPv4.

**Système de prévention des intrusions (IPS) :** Analyse en temps réel de chaque paquet réseau pour prévenir les intrusions (en raison de la latence élevée).

**Analyse de sécurité approfondie des applications (Application Security Testing) :** Test dynamique de sécurité des applications web et mobiles pour détecter les vulnérabilités.

**Gestion d'accès basée sur les rôles (RBAC) :** Intégration d'un système d'autorisation avancé pour gérer les accès à l'interface d'administration en fonction des rôles des utilisateurs.

**Intégration avec des solutions tierces :** Connexion avec d'autres outils de cybersécurité ou SIEM externes pour une analyse combinée et une gestion unifiée des alertes.

**Automatisation avancée avec des politiques personnalisées :** Création de politiques de sécurité automatiques basées sur des scénarios définis par l'utilisateur (par exemple, blocage automatique d'une IP après plusieurs tentatives de connexion échouées).

**Analyse et détection des malwares avancés :** Implémentation d'un moteur de détection des malwares basé sur des signatures et un apprentissage automatique pour identifier les menaces avancées.

**Support multi-cloud et hybridation des infrastructures :** Intégration du produit dans des environnements multi-cloud pour une protection étendue aux services cloud.

* **Frontière du Produit**

**Absence d'IPS (Système de prévention des intrusions) :** Le produit ne réalise pas une analyse détaillée paquet par paquet en raison de la latence potentiellement introduite par un module IPS, préférant une détection rapide et une réponse automatisée.

**Pas de gestion centralisée de la politique de sécurité multi-sites :** Le produit ne prend pas en charge la gestion centralisée des politiques de sécurité pour des infrastructures réparties géographiquement ou multi-sites.

**Absence d’intégration native avec des systèmes d’authentification externe :** Pas de prise en charge immédiate d’outils tiers de gestion des identités et des accès (IAM), tels que SSO ou MFA.

**Limitation à un modèle de déploiement sur site ou sur une infrastructure locale :** FirewallAI n’est pas actuellement conçu pour être déployé directement en tant que service SaaS ou dans des environnements totalement basés sur le cloud.

**Pas de support pour les plateformes mobiles (applications dédiées) :** Le produit ne propose pas encore d’application mobile pour la gestion à distance.

**Support limité pour les analyses de type "deep packet inspection" (DPI) :** En raison de la stratégie de traitement rapide, le produit n’inclut pas d’analyse DPI pour inspecter en profondeur les paquets réseau.

**Pas de détection des menaces internes (Insider Threats) :** Actuellement, FirewallAI se concentre principalement sur les menaces externes, sans une analyse approfondie des comportements internes potentiellement malveillants.

### EXCLUSION

**Exclusions de la version initiale :**

* Système de prévention des intrusions (IPS)
* Analyse de sécurité approfondie des applications (AST)
* Gestion d'accès basée sur les rôles (RBAC)
* Intégration avec des solutions tierces (SIEM externes)
* Automatisation avancée avec des politiques personnalisées
* Analyse et détection des malwares avancés
* Support multi-cloud et hybridation des infrastructures
* Application mobile dédiée pour la gestion à distance
* Deep Packet Inspection (DPI)
* Détection des menaces internes (Insider Threats)

**Futures améliorations envisagées :**

* Déploiement SaaS
* Intégration avec des outils de gestion des identités (SSO, MFA)
* Analyse approfondie des comportements internes
* Support complet des plateformes mobiles
* Tests de sécurité d’applications mobiles et web
* Amélioration de l'intelligence artificielle pour les menaces avancées
* Optimisation du moteur de détection des menaces
* Support pour les infrastructures multi-sites
* Gestion centralisée des politiques de sécurité pour grandes entreprises
* Ajout de nouvelles fonctionnalités de personnalisation des règles

### HORIZON GLOBAL DU PROJET ET DATES CLEFS

**10 février 2025 - Lancement du projet** *Motif* : Début officiel du développement de FirewallAI.  
 *Deadline* : N/A  
 *Pénalités de retard* : N/A  
 *Priorité* : Élevée

**14 avril 2025 - Fin de la phase de conception** *Motif* : Finalisation des spécifications détaillées du produit, y compris les modules de sécurité, IA, et l’architecture technique.  
 *Deadline* : 25 mai 2025  
 *Pénalités de retard* : Retard dans le démarrage du développement des fonctionnalités, réévaluation des timelines.  
 *Priorité* : Critique

**25 mai 2025 - Prototype fonctionnel** *Motif* : Développement du premier prototype fonctionnel de FirewallAI pour tests internes et validation des concepts de sécurité.  
 *Deadline* : 7 juin 2025  
 *Pénalités de retard* : Retard dans la validation des fonctionnalités de base, impacts sur le planning de développement ultérieur.  
 *Priorité* : Élevée

**7 juin 2025 - Alpha fermée** *Motif* : Lancement d'une version alpha fermée à un groupe restreint de testeurs pour une première évaluation de la solution.  
 *Deadline* : 21 juillet 2025  
 *Pénalités de retard* : Réduction du temps d’itération basé sur le feedback, ajustements nécessaires dans la roadmap.  
 *Priorité* : Élevée

**21 juillet 2025 - Bêta ouverte** *Motif* : Lancement de la bêta ouverte pour un test à grande échelle, permettant la collecte de retours plus diversifiés sur les performances et l'interface utilisateur.  
 *Deadline* : 5 août 2025  
 *Pénalités de retard* : Impact sur la collecte des retours, ajustement de la stratégie de marketing, et répercussions sur la réputation du produit.  
 *Priorité* : Très élevée

**5 août 2025 - Version finale et lancement officiel** *Motif* : Sortie officielle de la première version stable de FirewallAI, prête pour une commercialisation à grande échelle.  
 *Deadline* : 1 septembre 2025  
 *Pénalités de retard* : Pénalités contractuelles avec les partenaires, perte de confiance de la communauté et du marché, réajustement de la stratégie de lancement.  
 *Priorité* : Critique

**Post-lancement - Mises à jour régulières et support** *Motif* : Fournir un support continu pour les utilisateurs, corriger les bugs et lancer des mises à jour pour garantir la sécurité et les performances du produit.  
 *Deadline* : Continu  
 *Pénalités de retard* : Réduction de la satisfaction des utilisateurs, déclin de la base de clients actifs si les mises à jour sont retardées ou insuffisantes.  
 *Priorité* : Très élevée

### DOCUMENTS EN RÉFÉRENCE

#### LOIS OU NORMES SPÉCIFIQUES APPLICABLES AU PRODUIT

* **Normes de Cybersécurité et de Gestion des Risques :**
  + **ISO/IEC 27001 : 2013 :** Norme relative à la gestion de la sécurité de l'information. Elle définit les critères pour établir, mettre en œuvre, maintenir et améliorer un système de gestion de la sécurité de l'information (SGSI) pour protéger la confidentialité, l'intégrité et la disponibilité des informations.
  + **ISO/IEC 27002 : 2022 :** Code de bonnes pratiques pour la gestion de la sécurité de l'information. Il fournit des recommandations détaillées sur la gestion des risques de sécurité liés aux systèmes d'information.
  + **NIST SP 800-53 (National Institute of Standards and Technology) :** Normes de sécurité qui définissent un cadre de gestion des risques pour la protection des systèmes d'information fédéraux aux États-Unis. Elles sont souvent utilisées comme référence dans la cybersécurité et la gestion des risques pour les produits de sécurité informatique.
  + **NIST SP 800-82 : Guide sur la cybersécurité pour les systèmes de contrôle industriel (ICS) :** Bien que davantage spécifique aux systèmes industriels, cette norme s'applique à des solutions de cybersécurité comme FirewallAI, notamment lorsqu'il s'agit de réseaux et infrastructures critiques.
* **Normes relatives à la protection des données personnelles et à la confidentialité :**
  + **Règlement Général sur la Protection des Données (RGPD) :** Réglementation de l'Union Européenne qui régit le traitement des données personnelles. FirewallAI doit garantir que les données collectées sont traitées conformément aux exigences de transparence, de sécurité et de consentement.
  + **ISO/IEC 29100:2011 - Cadre de protection de la vie privée :** Norme qui définit un cadre de gestion de la confidentialité et de la protection des données personnelles. Elle est complémentaire au RGPD et se concentre sur l'intégration des pratiques de confidentialité dans la conception de produits.
  + **California Consumer Privacy Act (CCPA) :** Législation en Californie concernant la protection des données personnelles des consommateurs. Elle impose des obligations aux entreprises concernant la collecte et le traitement des informations personnelles, particulièrement importante si le produit est commercialisé aux États-Unis.
* **Normes de développement et d'évaluation des logiciels :**
  + **ISO/IEC 25010:2011 :** Norme sur la qualité des systèmes et logiciels. Elle inclut des critères tels que la performance, la sécurité, l'efficacité, la compatibilité et l'expérience utilisateur, tous cruciaux pour un produit comme *FirewallAI*.
  + **OWASP (Open Web Application Security Project) :** Un ensemble de bonnes pratiques et de recommandations pour le développement sécurisé des applications et des systèmes. OWASP fournit également des listes des principales vulnérabilités de sécurité à prendre en compte lors du développement de produits comme FirewallAI.
* **Normes et Pratiques pour les Systèmes de Sécurité Réseau :**
  + **ISO/IEC 27033 - Systèmes de gestion de la sécurité des réseaux :** Cette norme fournit des lignes directrices pour la gestion de la sécurité des réseaux, y compris la conception de l'architecture de sécurité, la gestion des risques, et les contrôles de sécurité nécessaires pour assurer la sécurité des systèmes de réseaux.
  + **RFC 3511 - A Security Architecture for the Internet Protocol :** Propose une architecture pour le protocole Internet en prenant en compte la sécurité des données et des réseaux, en particulier pour des solutions comme *FirewallAI*.
  + **PCI-DSS (Payment Card Industry Data Security Standard) :** Bien que spécifiquement dédié à la protection des informations de cartes de paiement, ce standard est applicable si *FirewallAI* traite ou protège des informations sensibles dans des environnements de paiement.
* **Normes pour la gestion des incidents et la réponse aux menaces :**
  + **ISO/IEC 27035 - Gestion des incidents de sécurité de l'information :** Cette norme définit les pratiques pour la gestion des incidents de sécurité, incluant la détection, la gestion, l'analyse et la résolution des incidents. Elle est essentielle pour un produit de cybersécurité comme *FirewallAI*, où la détection et la réponse aux incidents sont des fonctions clés.
  + **NIST SP 800-61 - Computer Security Incident Handling Guide :** Directives détaillant la gestion des incidents de sécurité informatique, y compris la détection, l'analyse, et la réponse aux cyberattaques.

## IDENTIFICATION DES PARTIES PRENANTES ET DES PARTIES IMPACTÉES

* **Parties Prenantes**
* **Les Utilisateurs Finaux (PME, administrateurs systèmes, entreprises)  
  Enjeu :** Bénéficier d’une protection réseau automatisée, intuitive et performante.  
  **Importance :** **Fondamentale.** Détermine les fonctionnalités, la simplicité d’usage et la fiabilité du produit.
* **L'Équipe de Développement (Développeurs, IA, Sécurité, UI/UX)  
  Enjeu :** Disposer d’un environnement de travail clair, structuré et collaboratif avec les ressources techniques nécessaires.  
  **Importance :** **Nécessaire.** Assure la faisabilité, la qualité et l’évolution du produit.
* **Les Partenaires Technologiques (fournisseurs d’outils IA, plateformes d’intégration, hébergement)  
  Enjeu :** Assurer la compatibilité technique, l’accès à des outils de pointe, et le bon fonctionnement du système.  
  **Importance :** **Utile.** Influence la performance, la sécurité et les possibilités d’intégration de la solution.
* **Les Investisseurs / Financiers  
  Enjeu :** Obtenir un retour sur investissement à travers la valeur ajoutée, la scalabilité et la commercialisation du produit.  
  **Importance :** **Nécessaire.** Garantit les ressources pour le développement, les tests, le marketing et le support.
* **Les Équipes Support & Commerciales  
  Enjeu :** Proposer un accompagnement client pertinent et valoriser la solution sur le marché.  
  **Importance :** **Utile.** Impacte la satisfaction client, la notoriété de la marque, et la pérennité du produit.
* **Parties Impactées**
* **Les Organismes de Régulation (CNIL, ENISA, ANSSI, etc.)  
  Enjeu :** Respect des réglementations en matière de sécurité informatique, de confidentialité et de traitement des données.  
  **Importance :** **Nécessaire.** Garantit la conformité légale et l’accès au marché européen.
* **Les Clients Finaux de Nos Clients (utilisateurs de leurs services/prod)  
  Enjeu :** Indirectement protégés par la qualité de la sécurité réseau mise en place par FirewallAI.  
  **Importance :** **Importante.** Une faille impactant nos clients peut avoir des effets en cascade sur leurs propres utilisateurs.
* **Les Fournisseurs d’Infrastructure (cloud, réseaux, datacenters)  
  Enjeu :** Intégration fluide avec les infrastructures existantes et minimisation des perturbations réseau.  
  **Importance :** **Utile.** Aide à garantir la stabilité et la compatibilité du produit dans divers environnements.
* **Les Autorités Judiciaires et Investigatives  
  Enjeu :** Accès à des journaux et preuves numériques en cas d’incidents de sécurité ou d’attaques.  
  **Importance :** **Contextuelle.** Intervient en cas de cybercriminalité pour l’investigation numérique.
* **Les Groupes de Normalisation et de Veille en Cybersécurité (ex : OWASP, NIST)  
  Enjeu :** Maintien d’un haut niveau de conformité et alignement avec les meilleures pratiques.  
  I**mportance :** **Utile.** Influence les mises à jour, les exigences de sécurité et l’adoption du produit sur le long terme.

### LE DEMANDEUR :

* **Firewall Technologies**

**Noms et Fonctions** : Équipe de direction de Firewall Technologies, composée de Julie Chevallier, Joranne Ripiego, Kénan Meylan, Victor Blaas, Doria Saint-Martin, Clément Olbrecht.

**Rôle par rapport au produit** : Firewall Technologies est à l’origine du projet **FirewallAI**, qu’elle conçoit et développe en interne. L’entreprise agit comme **demandeur et producteur** du logiciel, en réponse à une demande croissante du marché pour des solutions de cybersécurité intelligentes, accessibles et hautement automatisées. Le projet découle d’un besoin identifié par son pôle R&D et validé par des études de marché menées auprès d’un panel d’entreprises européennes.

#### ENJEUX ÉCONOMIQUES

**Importance** : **Élevée.** FirewallAI constitue un projet stratégique clé pour **Firewall Technologies**, avec l’ambition de se positionner comme un acteur majeur sur le marché européen des solutions de cybersécurité intelligentes et automatisées, notamment auprès des PME, ETI et collectivités locales.

**Valorisation** : L’objectif stratégique est de déployer FirewallAI auprès d’un minimum de **10 000 clients professionnels** dans les **24 mois** suivant la commercialisation. Le modèle économique repose sur un système de **licences annuelles**, complété par une offre **SaaS** pour les petites structures.

**Hypothèses de revenus :**

* **Licence annuelle moyenne :** 500 € par client  
   ➤ **Revenus directs estimés : 5 millions d’euros par an**
* **Offres cloud/SaaS pour TPE :** 20 €/mois/client (environ 2 000 clients visés à terme)  
   ➤ **Revenus mensuels estimés : 40 000 €** soit **480 000 €/an**
* **Services additionnels (support premium, formations, audits de sécurité IA) :** Estimation basée sur un taux de souscription de 15 % des clients, avec une dépense moyenne de 300 €/an  
   ➤ **Revenus complémentaires : 450 000 €/an**

**Revenu total prévisionnel sur 24 mois :**

**≈ 11,4 millions d’euros**, hors frais opérationnels.

Ces projections seront réévaluées à mesure que la solution sera testée, diffusée sur le marché, et optimisée sur la base des retours clients et des opportunités d’extension fonctionnelle (par ex. intégration à des SIEM, solutions de SOC-as-a-Service, etc.).

FirewallAI est également perçu comme un **levier de différenciation concurrentielle** pour Firewall Technologies, et un produit pouvant **ouvrir des marchés publics ou sensibles** en raison de sa conformité aux normes européennes en matière de sécurité.

#### ENJEUX HUMAINS, SOCIAUX OU SOCIÉTAUX

**Importance** : **Considérable.** Le projet **FirewallAI** vise à démocratiser l’accès à la cybersécurité avancée, notamment pour les structures qui ne disposent ni des ressources humaines ni des compétences techniques pour faire face aux menaces actuelles. En ce sens, il porte un impact sociétal fort, en renforçant la **résilience numérique** des PME, des collectivités locales, et des indépendants.

Cela se traduit par des objectifs concrets tels que :

* **Un taux d’adoption de 30 %** parmi les utilisateurs ciblés n’ayant **aucune équipe cybersécurité** dédiée.
* **Une réduction moyenne de 40 % du temps de réaction aux incidents** (TTR) pour les structures équipées de FirewallAI.
* **Un taux de satisfaction utilisateur ≥ 85 %** basé sur des indicateurs de simplicité, clarté de l’interface, et efficacité des modules IA.
* **La mise à disposition de 3 modules IA en open-source**, pour encourager l’adoption, la transparence, et la contribution communautaire.
* **Des programmes de sensibilisation à la sécurité numérique**, avec un objectif de **1 000 utilisateurs formés par an** via des webinaires, tutoriels interactifs et documentation pédagogique intégrée.
* **L’accessibilité en environnement multilingue**, avec un support natif de 5 langues majeures dès la première année.

**Valorisation** : FirewallAI participe à **l’amélioration de la sécurité numérique globale**, en abaissant la barrière à l’entrée dans un secteur souvent trop complexe ou onéreux pour les petites structures. Il agit ainsi comme **outil d’équité numérique**, en contribuant à une protection plus équilibrée face aux cybermenaces, indépendamment de la taille ou des moyens de l’organisation.

#### ENJEUX ENVIRONNEMENTAUX

**Importance** : **Modérée à élevée.** Bien que FirewallAI soit une solution logicielle, son infrastructure back-end, notamment l’hébergement des modules d’analyse, des bases de données centralisées et des traitements IA — implique une consommation énergétique non négligeable, particulièrement dans un contexte de traitement réseau en temps réel et de monitoring constant.

**Valorisation** : Dans une démarche de cybersécurité responsable, FirewallAI s’engage à réduire son empreinte environnementale à travers plusieurs actions concrètes :

* **Utilisation exclusive de centres de données alimentés à 100 % par des énergies renouvelables** dès le déploiement en production.
* Objectif de **réduction de 25 % de l’empreinte carbone par utilisateur protégé** dans les 12 mois suivant le lancement, en comparaison avec les solutions équivalentes utilisant des serveurs classiques.
* Estimation d’une **baisse de 21,8 tonnes de CO₂ par an**, sur une base initiale de 87,2 tonnes/an pour notre infrastructure cloud à pleine charge.
* **Optimisation logicielle continue** pour réduire les charges CPU et les opérations de lecture/écriture inutiles, notamment via l’utilisation de Rust pour le back-end et le traitement à faible latence avec XDP/eBPF.
* Mise en place d’un **plan de compensation des émissions résiduelles**, à travers des partenariats avec des programmes de reforestation et de soutien à la production d’énergie verte locale.
* Ambition d’atteindre la **neutralité carbone complète de l’infrastructure cloud et des opérations associées d’ici trois ans** post-lancement.

#### AUTRES CONTRAINTES À PRENDRE EN COMPTE

* **Conformité réglementaire :** **Importance : Élevée.** FirewallAI doit être conforme aux normes internationales de **sécurité des données**, telles que le **RGPD** (Règlement général sur la protection des données) pour les utilisateurs européens, ainsi qu'aux **normes ISO 27001** concernant la gestion de la sécurité de l'information. Le respect des **normes NIST** (National Institute of Standards and Technology) et des standards spécifiques à l'industrie de la cybersécurité est également impératif pour garantir que le produit offre une protection robuste, conforme, et juridiquement valable.
* **Adaptabilité réglementaire :** **Importance : Élevée.** La solution doit pouvoir être rapidement adaptée à toute évolution législative, en particulier pour les marchés internationaux.
* **Adaptabilité et évolutivité :** **Importance : Élevée.** FirewallAI doit être conçu avec une **architecture modulaire** et **scalable**, capable de supporter une augmentation du nombre d'utilisateurs ou des besoins accrus en termes de gestion des flux réseau. L’architecture doit permettre des mises à jour et évolutions sans interrompre le service. Cela inclut la possibilité d’ajouter de nouveaux **modules de sécurité** (comme des systèmes de prévention des intrusions ou des solutions de détection des menaces basées sur l'IA), de nouveaux protocoles ou l'intégration avec des **outils tiers** (SIEM, SOC, etc.).
* **Accessibilité :** **Importance : Modérée.** Bien que l’interface principale de FirewallAI soit un **outil technique** destiné à des professionnels de la cybersécurité, il est essentiel que l'interface soit **intuitive**, permettant une gestion facile même pour des utilisateurs sans compétences techniques avancées. La documentation et les outils de support doivent également être accessibles, en respectant les **standards d'accessibilité** numérique, comme les **WCAG (Web Content Accessibility Guidelines)**, pour garantir une expérience utilisateur inclusive.
* **Accessibilité pour les administrateurs IT** : **Importance : Modérée.** Simplification de l'interface d’administration pour les utilisateurs moins expérimentés, notamment par des **fonctionnalités de guidage interactif** ou des **assistants automatisés**.

### LES UTILISATEURS

* **Utilisateurs :**

**Administrateurs Systèmes :**

| **Rôle :** Responsables de la configuration et de la gestion du pare-feu pour assurer la sécurité réseau de l’entreprise.  **Besoins :** Un contrôle précis sur les règles de filtrage, la gestion des logs et la capacité d'interagir avec les alertes de sécurité.  **Objectif :** Utiliser un outil performant et flexible pour la gestion proactive de la sécurité réseau, avec un minimum de latence et une interface intuitive. |
| --- |

**Responsables de la Sécurité IT :**

| **Rôle :** Supervision des mesures de sécurité et analyse des menaces pour garantir la sécurité des infrastructures. **Besoins :** Un système capable de détecter les attaques de manière autonome, avec des outils de reporting clairs et une capacité d’adaptation aux menaces évolutives. **Objectif :** Obtenir une solution automatisée qui améliore l’efficacité des processus de détection et de réponse aux incidents de sécurité. |
| --- |

**Développeurs et Ingénieurs Sécurité :**

| **Rôle :** Personnes en charge de la création, de l'intégration, et de l'amélioration continue des composants de sécurité de FirewallAI. **Besoins :** Accès à une API flexible et à des modules personnalisables permettant de s’adapter aux spécificités de l’entreprise et des menaces. **Objectif :** Disposer d'un environnement modulaire et évolutif, permettant l'intégration facile de nouvelles fonctionnalités et la personnalisation avancée des règles de sécurité. |
| --- |

**PME et Startups :**

| **Rôle :** Utilisateurs qui nécessitent une solution de cybersécurité abordable et simple à déployer. **Besoins :** Un produit automatisé avec des fonctionnalités prédéfinies pour une protection optimale, sans nécessiter de compétences techniques avancées. **Objectif :** Bénéficier d’une cybersécurité efficace, accessible et facile à configurer, pour protéger l’entreprise des menaces sans complexité. |
| --- |

**Grandes Entreprises et Institutions :**

| **Rôle :** Structures ayant des besoins en cybersécurité plus complexes et des exigences de haute performance. **Besoins :** Une solution robuste, avec une gestion des règles de sécurité fine, un monitoring centralisé des logs et une conformité avec des normes de sécurité strictes. **Objectif :** Implémenter une solution de sécurité performante et personnalisable, capable de traiter des volumes importants de données avec une faible latence. |
| --- |

#### ENJEUX ÉCONOMIQUES

**Importance** :

* **Les Administrateurs Systèmes**

Les administrateurs systèmes sont au cœur du marché cible de FirewallAI. Leur besoin d'un outil de sécurité puissant et flexible, facile à déployer et à gérer, est crucial pour garantir une base d'utilisateurs fidèles et une adoption à large échelle. Les entreprises de taille moyenne et les startups, qui représentent environ 40% de la clientèle potentielle, recherchent une solution abordable avec un excellent rapport qualité-prix. Des prix compétitifs et des options d’abonnement mensuel, variant entre 50 et 150 euros par mois, sont envisagés pour attirer cette catégorie d’utilisateurs.

* **Les Responsables de la Sécurité IT**

Les responsables de la sécurité IT, qui représentent environ 30% de la base d'utilisateurs, ont besoin d'une solution de cybersécurité robuste capable de s’adapter à des environnements complexes. Ils privilégient les fonctionnalités avancées, comme la détection de menaces en temps réel, la gestion centralisée des alertes et des rapports détaillés. Pour répondre à ces besoins, FirewallAI proposera une tarification basée sur des modèles d’abonnement annuel avec des tarifs ajustés selon la taille de l’entreprise, allant de 200 à 1 000 euros par mois pour une couverture complète.

* **Les Développeurs et Ingénieurs Sécurité**

Les développeurs et ingénieurs en sécurité, représentant environ 20% des utilisateurs, constituent un segment clé pour la personnalisation et l’intégration de FirewallAI dans des infrastructures existantes. Ce groupe est particulièrement attiré par des fonctionnalités avancées comme des API ouvertes et des modules extensibles. Un modèle de tarification basé sur des licences annuelles pour ces utilisateurs professionnels est prévu, avec un tarif situé entre 500 et 2 000 euros par an en fonction de la taille de l'entreprise et des fonctionnalités souhaitées.

* **PME et Startups**

Les PME et startups, qui représentent environ 10% du marché cible, recherchent des solutions efficaces mais accessibles. Pour cette catégorie, un modèle freemium ou des forfaits mensuels basés sur la taille de l’entreprise (commençant à 50 euros par mois) est proposé. L’objectif est de rendre FirewallAI disponible pour ces entreprises tout en garantissant un service adéquat, avec un accès limité aux fonctionnalités avancées, tout en permettant une montée en gamme au fil du temps.

* **Grandes Entreprises et Institutions**

Les grandes entreprises et institutions, représentant environ 20% des utilisateurs, nécessitent une solution à grande échelle capable de sécuriser un grand nombre d’utilisateurs et de points d'accès. Ces organisations rechercheront un produit hautement performant et personnalisable, accompagné de services de support et de mise à jour continue. Pour ces clients, des offres sur mesure et des contrats d’abonnement annuel allant de 2 000 à 10 000 euros par an seront proposées, en fonction de la taille de l’organisation et des besoins spécifiques en matière de sécurité.

**Valorisation** :

* **Les Administrateurs Systèmes**

Pour attirer ce groupe d’utilisateurs, FirewallAI adoptera un modèle d’abonnement flexible avec des prix compétitifs variant de 50 à 150 euros par mois, permettant ainsi aux entreprises de petite et moyenne taille d’accéder à une solution de sécurité de haute qualité. La base d’utilisateurs attendue dans cette catégorie représente une source de revenus stable et prévisible.

* **Les Responsables de la Sécurité IT**

Les responsables de la sécurité IT bénéficieront d'une offre premium, avec des fonctionnalités avancées et un support dédié, proposant des abonnements mensuels entre 200 et 1 000 euros. Cette catégorie devrait représenter une source importante de revenus récurrents pour FirewallAI, générant une augmentation significative du chiffre d'affaires grâce à la fidélité et à l'extension des services.

* **Les Développeurs et Ingénieurs Sécurité**

Pour les développeurs et ingénieurs en sécurité, FirewallAI proposera une licence annuelle pour l'accès à des API, des modules et des outils de personnalisation avancés, avec des prix allant de 500 à 2 000 euros par an. Ce modèle de licence permettra non seulement de générer des revenus directs mais également de promouvoir une adoption à long terme dans des environnements complexes.

* **PME et Startups**

Les PME et startups auront accès à un modèle freemium ou à des forfaits mensuels débutant à 50 euros par mois, offrant une solution de sécurité évolutive avec des options de montée en gamme. Cette catégorie générera des revenus récurrents à faible coût mais sur un grand nombre d’utilisateurs, permettant de capter une part importante du marché.

* **Grandes Entreprises et Institutions**

Les grandes entreprises et institutions, ayant des besoins complexes, bénéficieront d’une offre premium avec des abonnements annuels allant de 2 000 à 10 000 euros, générant une part substantielle des revenus de FirewallAI. Ce segment haut de gamme assurera la stabilité financière à long terme et constituera un pilier clé pour la croissance du produit.

#### ENJEUX HUMAINS, SOCIAUX OU SOCIÉTAUX

**Importance** : Les enjeux humains, sociaux et sociétaux autour de FirewallAI revêtent une **importance critique**, en particulier dans le contexte croissant des menaces numériques qui affectent la sécurité individuelle, organisationnelle et collective. Les utilisateurs – notamment les administrateurs systèmes, les responsables de la sécurité IT et les ingénieurs – attendent non seulement une solution technique fiable, mais aussi un outil qui facilite leur travail quotidien, réduit le stress opérationnel et favorise une culture de **cybersécurité proactive et collaborative**.

FirewallAI favorise un environnement de travail plus serein en **simplifiant la gestion de la sécurité** et en offrant des alertes claires et actionnables, ce qui diminue la surcharge cognitive souvent ressentie par les équipes IT. Ce confort d’utilisation est un levier puissant de satisfaction et de fidélité, avec une réduction potentielle de 30% du temps passé à gérer les incidents de sécurité, permettant aux équipes de se concentrer sur des tâches à plus forte valeur ajoutée.

Sur le plan sociétal, FirewallAI s'inscrit dans une logique de **responsabilité numérique** : en contribuant à la sécurisation des données personnelles, des infrastructures critiques et des échanges numériques, il agit comme un acteur indirect mais central de **la confiance numérique** dans la société. En protégeant efficacement les petites structures comme les grandes institutions, FirewallAI participe à **réduire les inégalités d’accès à la cybersécurité**, traditionnellement réservée aux grandes entreprises disposant de moyens importants.

De plus, FirewallAI est conçu dans une **optique d’accessibilité**, avec une interface pensée pour être compréhensible et utilisable même par des profils non spécialistes de la sécurité, et des options de personnalisation adaptées aux différents niveaux de compétence. Cela permet d’élargir son utilisation à des structures plus petites, souvent sous-équipées, et d’augmenter la **résilience globale de l’écosystème numérique**.

**Valorisation** : Les utilisateurs valorisent fortement la **capacité de FirewallAI à humaniser la cybersécurité**, en mettant à disposition un outil puissant, mais facile à comprendre et à intégrer. Cela se traduit par un **gain de temps significatif** (jusqu'à 30% dans la gestion des alertes) et une **réduction du stress opérationnel** lié aux risques de cyberattaques.

Les professionnels de la sécurité apprécient également l’engagement de FirewallAI pour une **cybersécurité éthique et inclusive**, qui s’efforce de rendre ses solutions accessibles aux structures de toutes tailles et de tous niveaux techniques. Cette accessibilité est particulièrement importante pour les associations, PME et collectivités locales, qui peuvent bénéficier d’une protection avancée sans avoir besoin de former des spécialistes internes.

Enfin, en intégrant des **pratiques de transparence, de respect de la vie privée**, et de **protection proactive des données**, FirewallAI renforce la **confiance des utilisateurs finaux et des citoyens** dans les systèmes informatiques protégés par le produit. Cette valeur de confiance est un facteur clé d’adhésion, tant pour les décideurs que pour les usagers finaux.

#### ENJEUX ENVIRONNEMENTAUX

**Importance** : Les enjeux environnementaux occupent une place **de plus en plus centrale** dans les critères de sélection des solutions technologiques, en particulier dans les secteurs publics, les grandes entreprises et les start-ups sensibles aux questions de durabilité. Pour FirewallAI, ces considérations sont **hautement prioritaires**, non seulement pour répondre aux attentes des clients écoresponsables, mais aussi pour **se conformer aux exigences RSE** (Responsabilité Sociétale des Entreprises) de nombreux partenaires et marchés.

Près de **40% des décideurs en cybersécurité** prennent en compte l'impact environnemental des outils qu’ils déploient, notamment en ce qui concerne **la consommation énergétique des solutions cloud et l'efficacité des algorithmes d'analyse**. Ainsi, minimiser l’empreinte carbone de FirewallAI représente à la fois un **avantage concurrentiel** et un **enjeu éthique**. Cette approche responsable peut également stimuler **l’adoption du produit**, avec une estimation d'**augmentation de 20 à 25% du taux de conversion** dans les appels d'offres publics ou les partenariats avec des entreprises à forte conscience environnementale.

**Valorisation** : Les utilisateurs et partenaires valorisent significativement les **initiatives environnementales** prises par FirewallAI, notamment à travers :

* L’**hébergement sur des infrastructures cloud neutres en carbone**, propulsées à 100% par des énergies renouvelables.
* L’**optimisation des algorithmes de détection** pour réduire les ressources nécessaires sans compromettre la performance.
* La **réduction de la fréquence de traitements lourds non essentiels** via des systèmes de priorisation intelligente.
* Un **bilan carbone annuel publié de manière transparente**, accompagné d’un plan de compensation via des projets certifiés de reforestation ou d’énergies vertes.

Ces mesures sont perçues comme un **engagement concret** envers l’environnement, renforçant la crédibilité et la **réputation responsable** de FirewallAI. Ce positionnement peut générer une **hausse de 30% de la satisfaction client** parmi les organisations engagées dans la transition écologique et renforcer leur **fidélité à long terme**. De plus, ces engagements contribuent à faire de FirewallAI un acteur de la **cybersécurité durable**, aligné avec les valeurs de responsabilité environnementale attendues aujourd’hui dans le secteur technologique.

#### AUTRES CONTRAINTES À PRENDRE EN COMPTE

**Accessibilité :** Il est crucial que l'interface et les outils de gestion de FirewallAI soient accessibles aux administrateurs et utilisateurs de tous niveaux techniques. Cela inclut une conception ergonomique, un guidage interactif, et la possibilité d'intégrer des fonctionnalités d'assistance pour les utilisateurs avec divers besoins (par exemple, options de personnalisation de l'affichage, contrastes élevés, etc.).

**Sécurité en Ligne :** Assurer un environnement numérique ultra-sécurisé est primordial. FirewallAI doit garantir la protection des infrastructures critiques contre les cyberattaques, en mettant en œuvre des mécanismes de détection avancée, d'analyse en temps réel et de réponse automatisée aux incidents, afin de protéger aussi bien les données que les systèmes contre toute intrusion malveillante.

**Protection de la Vie Privée :** Le respect de la confidentialité des informations traitées est une contrainte essentielle. FirewallAI doit être conforme aux réglementations internationales telles que le RGPD ainsi qu'aux normes en matière de sécurité de l'information (ISO/IEC 27001, etc.), pour garantir que les données sensibles des entreprises et des utilisateurs finaux soient protégées de manière rigoureuse.

**Performance Technique :** Les utilisateurs attendent une solution offrant une performance fluide et une latence minimale, compte tenu du traitement en temps réel des flux réseau. Des temps de réponse optimisés, une haute disponibilité et l'absence de bugs critiques sont des aspects essentiels, puisque des problèmes techniques impacteraient directement l'efficacité de la sécurité des réseaux gérés par FirewallAI.

**Mises à Jour et Évolutivité Fonctionnelle :** Pour rester en phase avec l'évolution rapide des cybermenaces et des technologies, il est indispensable de proposer des mises à jour régulières et significatives. Ces mises à jour doivent inclure des améliorations de performance, l'ajout de nouvelles fonctionnalités de détection et d'analyse, ainsi que des mises à jour de sécurité pour répondre aux nouvelles vulnérabilités détectées, garantissant ainsi une solution toujours à la pointe de la technologie.

### AUTRE PARTIE PRENANTE OU IMPACTÉE :

* **Fournisseurs de Services Cloud**

**Importance** : Élevée

**Noms et Fonctions** :

* **Microsoft Azure (Microsoft)** : Fournisseur d'infrastructure cloud pour le déploiement des services de cybersécurité, hébergement des outils d'analyse en temps réel et gestion des données critiques.
* **Amazon Web Services (AWS)** : Fournisseur principal pour les services de calcul et de stockage, garantissant l'évolutivité et la performance continue des fonctionnalités de FirewallAI.
* **Google Cloud Platform (GCP)** : Fournisseur d'infrastructure pour les applications de machine learning et de gestion des incidents de sécurité.

**Localisation** : Mondiale

**Coordonnées** : Sites web officiels de chaque service

**Rôle par rapport au produit** : Hébergement des serveurs et des services de traitement des données, garantissant la haute disponibilité, la sécurité et l'efficacité des solutions de cybersécurité proposées par FirewallAI pour ses clients à l'échelle mondiale.

#### ENJEUX ÉCONOMIQUES

**Importance** : **Élevée.** Les fournisseurs de services cloud tels qu'Azure, AWS, et Google Cloud Platform jouent un rôle central dans l'architecture de FirewallAI, en garantissant l'hébergement des serveurs de sécurité, la gestion des données en temps réel et l'intégration des outils d'analyse. Leur impact sur les coûts opérationnels et la scalabilité des services est déterminant pour la rentabilité de FirewallAI. En utilisant ces services de pointe, FirewallAI peut s'attendre à une réduction des temps d'indisponibilité à **moins de 0.01%**, tout en permettant une montée en charge rapide pour répondre à une demande élevée, ce qui est essentiel pour traiter des volumes importants de données en continu. Ces capacités se traduisent par des **économies opérationnelles estimées à 20%** grâce à l'efficacité accrue et à la gestion dynamique des ressources cloud.

**Valorisation** : Les fournisseurs de services cloud jouent un rôle clé dans l'infrastructure de FirewallAI, en offrant la robustesse et la fiabilité nécessaires pour garantir des services de cybersécurité continus et performants. Grâce à leur technologie avancée, ces fournisseurs permettent à FirewallAI de maintenir une haute disponibilité, d'**optimiser les coûts et d'assurer une performance optimale pour ses clients**. Leur implication contribue également à réduire les risques de downtime, une priorité pour une solution de sécurité en temps réel. Ces fournisseurs bénéficient d'une visibilité accrue et d'une position renforcée sur le marché en s'associant à un produit innovant et à forte valeur ajoutée, tout en démontrant leur expertise dans le domaine de la cybersécurité. La scalabilité de leurs infrastructures permet à FirewallAI d'adapter dynamiquement ses ressources en fonction des fluctuations de la demande, maximisant ainsi l'efficacité et la rentabilité. De plus, les engagements de conformité aux normes internationales de protection des données (telles que le RGPD) sont essentiels pour garantir la confiance des utilisateurs finaux et éviter les risques juridiques, ce qui constitue un atout majeur pour leur réputation et leur crédibilité. En fournissant des solutions cloud à des prix compétitifs, ces fournisseurs aident FirewallAI à maintenir une structure de coûts rentable, tout en ayant accès aux technologies de pointe pour renforcer la proposition de valeur de leur service de cybersécurité.

#### ENJEUX HUMAINS, SOCIAUX OU SOCIÉTAUX

**Importance** : **Modérée à élevée.** Les enjeux humains, sociaux et sociétaux sont essentiels pour FirewallAI, car ils jouent un rôle central dans la manière dont l'entreprise est perçue par ses clients, partenaires et parties prenantes. Adopter des pratiques éthiques et responsables, telles que la promotion de l'inclusivité et le soutien à la diversité, contribue à bâtir une marque solide et respectée. Ces valeurs influencent également l'engagement et la satisfaction des utilisateurs, tout en établissant une norme dans l'industrie de la cybersécurité. À mesure que les préoccupations éthiques et sociales deviennent de plus en plus importantes pour les consommateurs, l'alignement de FirewallAI sur ces pratiques est crucial pour sa compétitivité et son développement sur le marché.

**Valorisation** : L'impact des pratiques éthiques et responsables est **significatif** pour FirewallAI. L'engagement dans des initiatives telles que la réduction de l'empreinte carbone, l'amélioration des conditions de travail, la promotion de l'équité et de l'inclusion, ainsi que l'implication communautaire, renforce la réputation de l'entreprise. Ces efforts peuvent non seulement améliorer la satisfaction client, **augmentant la fidélité jusqu'à 30%**, mais aussi améliorer l'engagement des employés, conduisant à une meilleure performance opérationnelle. Ce renforcement de la réputation permet à FirewallAI de se différencier dans un secteur hautement concurrentiel, tout en établissant des liens solides avec des clients soucieux de la responsabilité sociale des entreprises avec lesquelles ils interagissent.

#### ENJEUX ENVIRONNEMENTAUX

**Importance** : **Élevée.** Les enjeux environnementaux sont cruciaux pour FirewallAI, non seulement pour garantir sa conformité aux normes réglementaires, mais aussi pour répondre à la demande croissante des clients soucieux de l'environnement. En **adoptant des pratiques éco-responsables, comme l'optimisation de l'efficacité énergétique et l'utilisation de centres de données alimentés par des énergies renouvelables**, FirewallAI peut minimiser son impact environnemental tout en attirant et fidélisant des clients qui valorisent la durabilité. L'intégration de pratiques écologiques solides est essentielle pour maintenir une image de marque positive et responsable dans un secteur où la conscience environnementale est de plus en plus prégnante.

**Valorisation** : Les actions environnementales peuvent apporter des avantages tangibles pour FirewallAI. L'investissement dans l'efficacité énergétique et les énergies renouvelables peut permettre de **réduire les coûts opérationnels énergétiques de 20% à 30%**, améliorant ainsi la rentabilité de l'entreprise. De plus, ces initiatives peuvent renforcer la compétitivité de FirewallAI, en facilitant l'établissement de partenariats avec des entreprises écologiquement responsables et en attirant de nouveaux clients soucieux de l'environnement. Ces efforts peuvent également **augmenter la fidélité des clients de 25%,** contribuant à des relations durables et à un avantage concurrentiel sur le marché. Un engagement visible dans la durabilité environnementale peut également aider FirewallAI à se positionner comme un leader responsable dans le secteur de la cybersécurité.

#### AUTRES CONTRAINTES À PRENDRE EN COMPTE

* **Réglementations de Conformité** : L'un des défis majeurs dans l'industrie des jeux en ligne, et plus particulièrement pour des plateformes comme FirewallAI, est la gestion des obligations légales en matière de protection des données. La conformité aux réglementations internationales telles que le **GDPR (Règlement Général sur la Protection des Données)** en Europe et le **CCPA (California Consumer Privacy Act)** en Californie est non seulement une exigence juridique, mais également un impératif stratégique pour maintenir la confiance des utilisateurs et éviter des sanctions financières sévères.

Ces régulations imposent des obligations strictes quant à la collecte, au stockage et à la gestion des données personnelles des utilisateurs. Cela inclut des principes tels que la transparence, le consentement éclairé, la minimisation des données et le droit à l'effacement. Pour une entreprise comme FirewallAI, ces obligations se traduisent par des investissements conséquents dans des infrastructures sécurisées et des pratiques de gestion des données robustes, tout en intégrant des outils de traçabilité pour démontrer la conformité.

En outre, il est important de noter que les exigences en matière de protection des données continuent d’évoluer. Par exemple, les législations sur la cybersécurité et la confidentialité des données deviennent de plus en plus strictes avec l'émergence de nouvelles technologies, telles que l’intelligence artificielle et l’analyse de données massives (Big Data). Ainsi, il est essentiel pour FirewallAI de non seulement se conformer aux exigences actuelles, mais aussi de suivre de près les évolutions législatives afin de garantir une conformité continue.

* **Gestion des Pics de Demande** : FirewallAI devra être capable de gérer efficacement les pics de demande, particulièrement lors des lancements de nouvelles fonctionnalités ou des périodes de forte activité dans l'industrie de la cybersécurité. Cela implique de disposer d'une infrastructure cloud robuste et évolutive, capable de s'adapter à une augmentation soudaine du trafic sans compromettre la qualité du service. L'incapacité à gérer ces pics pourrait entraîner des interruptions de service et nuire à la réputation de l'entreprise. Il est donc impératif de planifier et d'optimiser les ressources pour garantir une disponibilité continue et fiable, même en période de forte demande.
* **Sécurité Avancée** : En tant qu'entreprise de cybersécurité, FirewallAI doit mettre en place des mesures de sécurité avancées pour protéger ses services contre les cyberattaques, qui sont une menace constante pour les entreprises opérant en ligne. La mise en œuvre de protocoles de sécurité de pointe, tels que l'authentification multifactorielle, le cryptage des données, et des mécanismes de détection et de réponse aux menaces en temps réel, est essentielle pour garantir la protection des données des utilisateurs. La capacité à anticiper, détecter et contrer efficacement les attaques potentielles est primordiale pour maintenir la confiance de ses clients et pour assurer la continuité de ses services.

### TABLEAU RÉCAPITULATIF DES ENJEUX ET PARTIES PRENANTES

Les notes vont de 1 à 4, où 1 signifie que l'enjeu a une importance "Accessoire", 2 est "Utile", 3 est "Nécessaire", et 4 est "Fondamental". De plus, la colonne "Importance" donne une moyenne des notes attribuées par toutes les parties prenantes à l'enjeu, qui peut être calculée en ajoutant les notes et en divisant par le nombre de parties prenantes.

| **ENJEUX PARTIES PRENANTES** | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Enjeu | Fonction | PP Utilisateurs | PP Équipe de développement | PP Fournisseurs Cloud | PP Régulateurs | PP Investisseurs | Importance |
| Sécurité des Données | Protéger les données personnelles et sensibles traitées par l’IA | **4** | **4** | **4** | **4** | **4** | 4 |
| Conformité réglementaire | Respect des normes (RGPD, ISO, etc.) sur la gestion des données et la cybersécurité | **4** | **4** | **4** | **4** | **4** | 4 |
| Fiabilité du modèle IA | Garantir des résultats précis, robustes et interprétables | **4** | **4** | **4** | **3** | **4** | 3,8 |
| Performance et Stabilité | Assurer un fonctionnement fluide et fiable du jeu | **4** | **4** | **3** | **4** | **3** | 3,6 |
| Explicabilité / Transparence | Permettre aux utilisateurs de comprendre les décisions de l’IA | **4** | **3** | **3** | **4** | **3** | 3,4 |
| Impact environnemental | Développer un modèle économique qui favorise un bénéfice mutuel entre les joueurs et les développeurs | **3** | **3** | **4** | **3** | **4** | 3,4 |
| Performance technique | Temps de réponse, gestion de la charge, scalabilité | **3** | **4** | **4** | **2** | **3** | 3,2 |
| Confidentialité des algorithmes | Protéger la propriété intellectuelle des modèles et éviter le vol ou la reproduction | **2** | **4** | **3** | **3** | **4** | 3,2 |
| Accessibilité | Interface et outils accessibles à des profils variés (non experts, PMR, etc.) | **3** | **3** | **2** | **2** | **2** | 2,4 |
| Éthique de l’IA | Prévenir les biais, garantir un usage responsable et aligné avec les droits humains | **4** | **3** | **3** | **4** | **3** | 3,4 |
| Facilité d’intégration | Permettre une adoption facile dans différents systèmes/logiciels des clients | **3** | **4** | **4** | **3** | **4** | 3,6 |

## POSITIONNEMENT GLOBAL DU PRODUIT

### CARACTÉRISATION DE FIREWALLAI

**Matrice SWOT** :

|  | Positif | Négatif |
| --- | --- | --- |
|  | Force   * **Technologie propriétaire d’IA avancée**  FirewallAI repose sur des algorithmes développés en interne, capables de détecter des comportements malveillants inédits via apprentissage adaptatif. * **Contrôle total de la chaîne de valeur**  Aucune sous-traitance : cela garantit une sécurité maximale, une maîtrise complète des performances, et une meilleure réactivité face aux incidents. * **Conformité intégrée**  Conçu pour répondre nativement aux réglementations telles que le RGPD, ISO 27001, NIS2, etc., facilitant son adoption par les secteurs publics et régulés. * **Déploiement modulaire**  Compatible avec des architectures cloud, on-premise ou hybrides, offrant une flexibilité technique adaptée aux besoins de chaque client. | Faiblesse :   * **Image de marque encore jeune**  En tant que nouvelle solution, FirewallAI manque de notoriété sur un marché dominé par des géants bien établis (Palo Alto, Fortinet...). * **Phase de scaling encore limitée**  En étant entièrement géré en interne, la montée en charge rapide peut représenter un défi organisationnel sans automatisation complète de certains processus. * **Forte intensité R&D**  Le maintien à jour de l’IA face à des menaces en constante évolution implique des investissements continus en recherche et en calcul. |
|  | Opportunités :   * **Explosion des cybermenaces**  La hausse constante des cyberattaques crée un besoin croissant de solutions préventives intelligentes comme FirewallAI. * **Règlementations favorables**  L’entrée en vigueur de normes strictes (DORA, NIS2, Cyber Resilience Act) pousse les entreprises à investir dans des outils conformes et proactifs. * **Demande croissante pour des solutions souveraines/éthiques**  Des clients publics et privés cherchent des alternatives locales ou européennes, transparentes et non dépendantes des GAFAM. * **Synergies sectorielles**  Intégration possible avec des solutions complémentaires (SIEM, SOC, EDR), ouvrant la voie à des partenariats ou intégrations natives. | Menaces :   * **Concurrence très forte et bien financée**  Des entreprises comme CrowdStrike, SentinelOne ou Fortinet disposent de ressources massives pour innover et capter le marché rapidement. * **Scepticisme face aux IA autonomes**  Certains DSI ou RSSI restent méfiants envers les outils « boîte noire », ce qui peut ralentir l’adoption malgré les performances. * **Risque juridique ou réputationnel**  En cas de faille non détectée, même partiellement, l’impact sur la confiance des clients pourrait être significatif. * **Évolutions rapides du paysage réglementaire**  L’alignement constant avec les lois internationales nécessite une veille légale active et coûteuse. |

### CARACTÉRISATION DU MARCHÉ DU PRODUIT

La conception de FirewallAI repose sur une stratégie **"market-driven"**, répondant précisément aux besoins pressants des entreprises en matière de cybersécurité proactive, automatisée et conforme aux normes internationales. Ce segment analyse l’environnement commercial, concurrentiel, technologique et réglementaire dans lequel évolue cette solution.

* **Concurrence Directe**

FirewallAI entre en compétition directe avec d'autres pare-feux nouvelle génération intégrant l'IA ou le machine learning. Des acteurs comme **Palo Alto Networks (avec Cortex XDR), Fortinet, Sophos, CrowdStrike** ou encore **Darktrace** proposent des fonctionnalités similaires de détection et réponse intelligente aux menaces. Ces entreprises disposent souvent d’une importante base client et d’un positionnement mondial.

Cependant, FirewallAI se distingue par son architecture 100% maîtrisée, sa capacité à opérer **sans dépendance cloud**, et sa **conformité native aux normes européennes**, éléments devenus clés pour de nombreux acheteurs publics et privés.

* **Concurrence Indirecte**

Les concurrents indirects incluent les **solutions traditionnelles de cybersécurité**, comme les antivirus, les pare-feux sans IA, ou les services managés de cybersécurité (MSSP). Ils remplissent les mêmes objectifs de protection, mais avec un degré d'automatisation et d’adaptabilité inférieur. On peut aussi considérer certains **SIEM (ex : Splunk, Elastic)** comme indirectement concurrents si utilisés dans un cadre de supervision avancée.

* **Recherche d'Antériorité et Brevets**

Le domaine de la cybersécurité est fortement protégé par des brevets, en particulier autour des technologies d’analyse comportementale et de détection en temps réel. Une **vérification rigoureuse de la liberté d’exploitation (FTO)** est essentielle pour éviter toute contrefaçon. En cas de chevauchement technologique, des stratégies alternatives incluent le contournement technique, le dépôt de brevets défensifs ou la négociation de licences. La protection varie selon les juridictions (ex : USPTO, EPO), influençant les choix de marché d’entrée.

* **Publications et Revues Spécialisées**

Les revues comme **Dark Reading, Cybersecurity Magazine, The Hacker News** et des plateformes telles que **Gartner, Forrester ou MITRE ATT&CK** fournissent des analyses précieuses sur les tendances de la cybersécurité. Les rapports techniques et forums de professionnels (Reddit, GitHub, XDA) permettent également d’anticiper les attentes et les inquiétudes des RSSI et DSI, cibles prioritaires de FirewallAI.

* **Positionnement du Produit**

FirewallAI adopte un **positionnement modulable** : une version "core" pour PME à budget limité, et des **versions avancées pour grands comptes**, avec intégration SIEM, tableaux de bord personnalisables, conformité réglementaire étendue, et support prioritaire.  
 Ce positionnement permet de viser plusieurs segments de marché :

* **TPE/PME** avec besoins de cybersécurité accessibles et automatisés
* **Grands groupes / administrations publiques** soucieux de souveraineté numérique et de conformité stricte
* **Secteurs critiques** (santé, finance, énergie) avec exigences élevées en temps réel et redondance

L'analyse du marché pour FirewallAI montre qu’il est **extrêmement compétitif**, dominé par des entreprises puissantes mais aussi marqué par une **demande en forte croissance**. Grâce à son architecture souveraine, son IA évolutive et son adaptabilité réglementaire, FirewallAI peut se différencier efficacement.

L’accent mis sur la **conformité, l’accessibilité et la performance proactive** est clé pour capturer un marché de plus en plus orienté vers la **cybersécurité préventive et automatisée**. La capacité de FirewallAI à s’adapter aux nouveaux standards et à l’évolution des menaces constitue un atout stratégique essentiel pour sa pénétration et sa fidélisation clients.

## DESCRIPTION FONCTIONNELLE DU PRODUIT

### LISTE DES CAS D’UTILISATION

Pour TinyCraft, un jeu de type sandbox, voici un examen approfondi des différentes situations de vie du produit et les services associés que chaque étape doit fournir.

| **Production ou Fabrication** | **Scénario :** Développement du moteur de détection, entraînement des algorithmes d’IA, intégration avec les interfaces de gestion et les API.  **Services Nécessaires :**   * Environnements de développement sécurisés (IDE, conteneurs, CI/CD). * Outils de machine learning et plateformes d'entraînement de modèles IA. * Systèmes de gestion du code source et de suivi des bugs (ex : GitLab, Jira). * Tests de pénétration et simulations de cyberattaques. |
| --- | --- |
| **Vente** | **Scénario :** Commercialisation de FirewallAI auprès de clients entreprises ou institutions.  **Services Nécessaires :**   * CRM et outils de gestion de leads B2B. * Équipe commerciale spécialisée en cybersécurité. * Portail d’achat ou processus de contractualisation sécurisé. * Partenariats avec intégrateurs ou revendeurs IT. |
| **Transport, livraison, Installation, Mise en Service** | **Scénario :** Déploiement de FirewallAI dans l’environnement client (on-premise ou cloud hybride).  **Services Nécessaires :**   * Scripts d’installation automatisés (Ansible, Docker, etc.). * Documentation technique et guides d’intégration. * Assistance technique pour l’onboarding. * Support à la configuration initiale (règles de sécurité, profils de détection IA). |
| **Maintenance, Réparation** | **Scénario :** Mises à jour régulières (patches de sécurité, évolution des modèles IA), support technique.  **Services Nécessaires :**   * Système de mise à jour automatique avec rollback. * Monitoring de l’état du pare-feu et alertes en temps réel. * Centre de support réactif avec SLA défini. * Dashboard pour l’analyse post-incident. |
| **Fin de Vie : Élimination, Recyclage** | **Scénario :** Désinstallation du système ou remplacement par une version ultérieure.  **Services Nécessaires :**   * Procédures de désinstallation sécurisée. * Outils de purge des logs et données sensibles. * Documentation de migration ou archivage conforme RGPD. * Recyclage des appliances physiques si utilisées. |
| **Utilisation Primaire** | **Scénario :** Pare-feu actif analysant le trafic réseau, détectant les menaces et les bloquant en temps réel.  **Services Nécessaires :**   * Interface de gestion intuitive avec alertes intelligentes. * Moteur d’analyse IA à auto-apprentissage. * Journalisation complète et exportable des événements. * Intégration facile avec SIEM ou autres outils de sécurité. |
| **Utilisations Secondaires** | **Scénario :** Utilisation pour la **formation en cybersécurité** ou les **tests d’infrastructure** dans des environnements contrôlés.  **Services Nécessaires :**   * Mode simulation ou "bac à sable" pour exercices. * Rapports détaillés pour évaluer les réponses à des attaques simulées. * Interface pédagogique ou tutoriels intégrés pour les formateurs. * API pour scénarios personnalisés. |
| **Utilisations Inhabituelles** | **Scénario :** Utilisation de FirewallAI à des fins de **recherche en cybersécurité**, ou comme **élément de démonstration technique** dans des salons ou formations avancées.  **Services Nécessaires :**   * Accès aux modèles d’IA pour affiner les comportements. * Outils de visualisation temps réel des flux réseau. * Fonctionnalité de création de rapports interactifs. * Ouverture vers des plateformes de test type Cyber Range.. |
| **Utilisations Dangereuses** | **Scénario :** Tentative de contournement du pare-feu ou usage malveillant à l’insu de l’organisation (ex : configuration laxiste exploitée).  **Services Nécessaires :**   * Journalisation immuable et audit trail. * Alertes sur comportements anormaux ou configurations à risque. * Contrôle d’accès basé sur les rôles (RBAC) et MFA. * Système de verrouillage automatique en cas de détection d’anomalies critiques. |

### CAS D'UTILISATION "X"

Le marché de la cybersécurité est en constante évolution, marqué par une montée en puissance des menaces, une sophistication accrue des attaques, et une dépendance toujours plus forte des entreprises à des infrastructures numériques critiques. Dans cet univers, deux types d’acteurs dominent aujourd’hui : les **pare-feu traditionnels (Next-Gen Firewalls)** comme **Palo Alto Networks** ou **Fortinet**, et les **solutions cloud de détection intelligente** telles que celles de **CrowdStrike** ou **Darktrace**. FirewallAI s’inscrit dans cette dynamique en proposant une solution innovante et autonome, conçue pour répondre aux failles structurelles et fonctionnelles que ces solutions peuvent présenter.

**Palo Alto Networks (Pare-feu traditionnel haut de gamme)**

Leader historique du marché, **Palo Alto Networks** propose des pare-feu de nouvelle génération dotés d’une forte capacité de filtrage et d’analyse du trafic. Leur succès repose sur :

* **Inspection approfondie des paquets** (DPI) pour bloquer efficacement les intrusions.
* **Politiques de sécurité granulaire** et outils d'administration avancés.
* **Écosystème complet** incluant la prévention des menaces, le filtrage d’URL, la détection de malwares, etc.

Cependant, malgré leur robustesse, ces systèmes présentent certaines limites :

* **Coût élevé**, rendant leur adoption difficile pour les petites structures.
* **Complexité d’intégration**, nécessitant des équipes IT qualifiées.
* **Réactivité limitée face aux menaces émergentes**, car ils reposent en partie sur des signatures statiques ou semi-dynamiques.
* **Pas d’auto-apprentissage véritable**, contrairement à l’IA de nouvelle génération.

**Darktrace (Détection intelligente par IA)**

Darktrace est reconnu pour avoir popularisé l’usage de l’**IA dans la cybersécurité**, notamment via des techniques d’auto-apprentissage pour repérer les anomalies comportementales dans un réseau. Parmi ses points forts :

* **Détection proactive sans dépendance aux signatures connues**.
* **Analyse comportementale basée sur des modèles probabilistes**.
* **Visualisation intuitive de l’activité réseau avec alertes automatisées.**

Mais cette approche présente aussi des défis :

* **Taux de faux positifs encore élevé**, demandant une validation humaine fréquente.
* **Outil davantage conçu pour la détection que pour l’action immédiate**, ce qui peut ralentir les temps de réponse.
* **Coûts importants**, souvent comparables à ceux des solutions traditionnelles haut de gamme.
* **Dépendance à une infrastructure cloud continue**, ce qui soulève des enjeux de souveraineté et de confidentialité.

**Positionnement Stratégique de FirewallAI**

FirewallAI a été pensé pour combiner **l’intelligence autonome d’un système adaptatif** avec **l’efficacité opérationnelle d’un pare-feu de nouvelle génération**, tout en **corrigeant les faiblesses** des solutions existantes. Il se distingue par plusieurs innovations clés :

* **Pare-feu auto-adaptatif** : grâce à un moteur d’apprentissage en continu, FirewallAI s’ajuste dynamiquement aux comportements du réseau et détecte des menaces inconnues sans intervention manuelle.
* **Réponse autonome en temps réel** : contrairement à Darktrace, FirewallAI ne se limite pas à signaler les anomalies, mais peut isoler, neutraliser ou rerouter un flux malveillant de manière automatique.
* **Simplicité d’usage** : grâce à une interface accessible, une documentation complète, et une configuration guidée, FirewallAI peut être mis en place sans expertise poussée.
* **Modèle économique flexible** : FirewallAI est proposé en SaaS, avec des offres modulables adaptées aux PME comme aux grandes entreprises, rendant la cybersécurité de pointe accessible à tous.
* **Hébergement souverain & protection RGPD-native** : toutes les données sont hébergées localement ou dans des clouds certifiés, garantissant conformité et confidentialité dès la conception.
* **Écoconception** : le système est optimisé pour minimiser sa consommation de ressources et permettre une empreinte carbone réduite, répondant aux attentes des entreprises écoresponsables.

En combinant **l’autonomie de l’IA**, **la simplicité d’intégration**, **la réponse immédiate aux menaces**, et **la conformité réglementaire**, FirewallAI répond aux lacunes actuelles du marché de la cybersécurité tout en démocratisant l’accès à une défense proactive et intelligente. Il se positionne comme **une alternative de rupture** face aux solutions classiques trop rigides ou coûteuses, et face aux solutions IA trop passives ou inaccessibles. Avec FirewallAI, la cybersécurité devient à la fois **plus intelligente, plus accessible, et plus durable**.

## DÉTAIL DES FONCTIONS

| N° d'Identification | Type | Intitulé de la Fonction | Description Complète | Critère(s) Caractérisant la Fonction | Niveaux d'Acceptation | Flexibilité des Niveaux |
| --- | --- | --- | --- | --- | --- | --- |
| FP1 | FP | Détection comportementale autonome | FirewallAI analyse les comportements réseau pour détecter les menaces inconnues. | Précision de détection, taux de faux positifs | > 95% de détection, < 1% faux positifs | F0, F1 |
| FP2 | FP | Réaction Automatique aux Menaces | Le système isole ou neutralise automatiquement une menace détectée. | Temps de réponse, fiabilité, taux d’échec | < 200 ms, 99% fiabilité | F0, F1, F2 |
| FS1 | FS | Supervision en Temps Réel | L’administrateur peut visualiser en temps réel l’activité réseau. | Délai d'affichage, clarté des données | < 1 s, 90% de lisibilité | F0, F1 |
| FS2 | FS | Mises à jour intelligentes | Le système s’auto-met à jour sans intervention humaine, selon les menaces actuelles | Fréquence, pertinence des mises à jour | Hebdomadaire, adaptation aux menaces | F1, F2 |
| FE1 | FE | Accessibilité multi-plateforme | FirewallAI est utilisable via web, application desktop, mobile. | Compatibilité, fluidité d’accès | Compatible avec tous les OS majeurs | F0, F1 |
| FC1 | FC | Sécurité & Chiffrement des Données | Toutes les données sont stockées et transmises de manière sécurisée. | Conformité RGPD, chiffrement, auditabilité | RGPD full, chiffrement AES-256 | F0 |
| FC2 | FC | Gestion des droits et des utilisateurs | FirewallAI permet une gestion fine des accès par rôles et niveaux. | Granularité, traçabilité, facilité d’utilisation | Rôles personnalisables, audit 100% | F1, F2 |
| IF1 | IF | Intégration avec SI existant | Le système s’intègre avec les outils SIEM, ERP, et autres composants IT. | Compatibilité API, rapidité d’intégration | API REST/GraphQL, intégration < 1 jour | F1, F2 |
| IT1 | IT | Support Technique Proactif | FirewallAI propose un support réactif, incluant des alertes automatisées. | Délai de réponse, automatisation, satisfaction client | < 30 min, satisfaction > 90% | F1, F2 |
| FP3 | FP | Tableau de bord adaptatif | L’interface s’adapte au profil utilisateur pour une lecture claire des menaces. | UX, personnalisation, accessibilité visuelle | UX noté > 8/10, Dark Mode, Responsive UI | F2, F3 |
| FS3 | FS | Journalisation & traçabilité complète | Toutes les actions du système sont enregistrées et horodatées pour audit. | Intégrité, précision, conformité | Logs inviolables, horodatage ISO8601 | F0, F1 |
| FE2 | FE | Compatibilité Cloud & On-premise | FirewallAI peut être déployé localement ou dans le cloud public/privé. | Flexibilité de déploiement, portabilité | 100% compatible avec AWS, Azure, Linux | F1, F2, F3 |
| FC3 | FC | Résilience & Haute Disponibilité | FirewallAI assure un service ininterrompu même en cas de défaillance système. | Uptime, redondance, failover | Uptime > 99.99%, failover < 5 s | F0, F1 |

## CADRE DE RÉPONSE

### RÉPONSES PROPOSÉES POUR CHAQUE FONCTION

| **N°** | **RAPPEL BREF DE LA FONCTION** | **RÉSUMÉ DE LA SOLUTION TECHNIQUE PROPOSÉE** | **CRITÈRES DE PERFORMANCE** | **NIVEAUX ATTEINTS / NIVEAUX DEMANDÉS** | **COÛT DE LA FONCTION** | **JUSTIFICATION TECHNIQUE RÉSUMÉE** | **JUSTIFICATION TECHNIQUE RÉSUMÉE** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| FP1 | Détection comportementale autonome | Utilisation d'algorithmes d'intelligence artificielle pour détecter les comportements anormaux en temps réel sur le réseau. | - Précision : > 95%  - Faux positifs : < 1% | Atteints : Précision : > 95%  Faux positifs : < 1% | Moyen | Le système d'IA surveille le réseau en temps réel pour repérer des comportements suspects.  Ce processus repose sur un modèle d'auto-apprentissage pour s'adapter aux nouvelles menaces. | L'auto-apprentissage permet à l'IA de détecter les nouvelles menaces en temps réel sans nécessiter d'interventions humaines, garantissant ainsi une protection rapide et efficace. |
| FS1 | Supervision en temps réel | Tableau de bord avec vue en temps réel sur l'activité réseau et les incidents de sécurité, avec possibilité d'intervention. | - Temps de réponse : < 1 s  - Clarté des alertes : 90% | Atteints : Temps de réponse : < 1 s  Clarté : 90% | Moyen | Le tableau de bord affiche les alertes et événements en temps réel avec des indicateurs clairs permettant d’agir rapidement.  Le système est optimisé pour une réponse rapide. | Une interface claire et réactive permet aux administrateurs d’intervenir rapidement en cas de problème, réduisant ainsi les risques et l'impact des attaques. |
| FS2 | Mises à jour intelligentes | Mise à jour automatique du système de sécurité en fonction des nouvelles vulnérabilités détectées sur le réseau. | - Fréquence des mises à jour : Hebdomadaire  - Pertinence des mises à jour : 100% | Atteints : Fréquence : Hebdomadaire  Pertinence : 100% | Élevé | Le système de mise à jour automatique est conçu pour fournir des mises à jour fréquentes sans perturber le service.  Le processus de mise à jour s'adapte aux nouvelles menaces. | Les mises à jour automatiques permettent de maintenir une protection continue contre les menaces émergentes, assurant une réponse en temps réel à chaque nouvelle vulnérabilité. |
| FE1 | Accessibilité multiplateforme | FirewallAI est compatible avec plusieurs plateformes telles que Windows, Linux, et propose des solutions Cloud et SaaS. | - Compatibilité : 100%  - Fluidité d'utilisation : 95% | Atteints : Compatibilité : 100%  Fluidité : 95% | Moyen | L'outil est accessible depuis toutes les plateformes populaires, permettant une intégration rapide dans diverses infrastructures. | La compatibilité multiplateforme assure que FirewallAI peut être déployé dans divers environnements et architectures informatiques, étendant ainsi sa base d'utilisateurs. |
| FC1 | Sécurité des données | Protocole de chiffrement des données et conformité aux normes de sécurité telles que le RGPD pour garantir la confidentialité. | - Conformité RGPD : 100%  - Chiffrement : AES-256 | Atteints : Conformité RGPD : 100%  Chiffrement AES-256 | Élevé | Le chiffrement AES-256 est utilisé pour garantir une sécurité maximale des données en transit et au repos.  FirewallAI respecte les normes RGPD. | Les protocoles de sécurité assurent la confidentialité des données, ce qui est crucial pour éviter les violations de données et maintenir la confiance des utilisateurs. |
| FC2 | Gestion des accès et des rôles | Fonction de gestion des utilisateurs et de création de rôles personnalisés avec des permissions spécifiques. | - Granularité des rôles : 100%  - Auditabilité des actions : 100% | Atteints : Granularité : 100%  Auditabilité : 100% | Moyen | La gestion des rôles permet de définir des accès selon les besoins spécifiques des utilisateurs, assurant ainsi une protection granulaire des ressources. | L'auditabilité des actions et la gestion fine des rôles garantissent une traçabilité complète, permettant de surveiller et contrôler l'accès aux informations sensibles. |
| IF1 | Intégration avec des outils SIEM et autres solutions IT | Intégration avec des systèmes SIEM (Security Information and Event Management) pour une gestion centralisée des alertes. | - Compatibilité API : 100%  - Temps d'intégration : < 1 jour | Atteints : Compatibilité API : 100%  Temps d'intégration : < 1 jour | Élevé | FirewallAI offre une API complète pour faciliter l'intégration avec d'autres outils de cybersécurité.  Le processus d'intégration est rapide et fluide. | L'intégration avec des outils SIEM permet une gestion plus efficace des incidents de sécurité, réduisant les risques et améliorant la réponse face aux menaces. |
| IT1 | Support technique | Mise en place d'un support réactif 24/7 via chat, e-mail et téléphone pour résoudre tout problème technique. | - Temps de réponse : < 30 min  - Satisfaction client : > 90% | Atteints : Temps de réponse : < 30 min  Satisfaction : > 90% | Moyen | Un support réactif garantit que les problèmes sont résolus rapidement, minimisant les interruptions du service. | Un service client réactif renforce la fidélité des utilisateurs et réduit les coûts liés aux résiliations de contrat en répondant rapidement à leurs préoccupations. |
| FP2 | Détection d'attaque en temps réel | Détection d'intrusions en temps réel avec filtration automatique des menaces via des algorithmes avancés. | - Taux de détection : > 98%  - Latence : < 200 ms | Atteints : Taux de détection : > 98%  Latence : < 200 ms | Élevé | La détection en temps réel permet de neutraliser les attaques avant qu'elles n'affectent les systèmes.  L'algorithme est optimisé pour garantir des réponses rapides. | La détection précoce d'attaques réduit considérablement les risques, garantissant ainsi une protection pro-active du réseau contre les intrusions et les malwares. |
| FS3 | Journalisation et traçabilité | Enregistrement détaillé des événements de sécurité pour une analyse et un audit approfondis. | - Complétude des logs : 100%  - Inviolabilité des logs : 100% | Atteints : Complétude : 100%  Inviolabilité : 100% | Élevé | Les journaux sont collectés et stockés de manière inviolable, garantissant l'intégrité des données pour les audits et la traçabilité des actions. | Une journalisation complète et inviolable est essentielle pour des audits approfondis et pour répondre aux exigences de conformité dans un environnement réglementé. |
| FE2 | Compatibilité avec les environnements Cloud | Déploiement possible dans des environnements Cloud publics et privés (AWS, Azure, Google Cloud) pour une flexibilité accrue. | - Compatibilité : 100%  - Déploiement sur cloud : < 1 jour | Atteints : Compatibilité : 100%  Déploiement : < 1 jour | Élevé | Le système est optimisé pour une gestion des ressources cloud, permettant une scalabilité rapide et une flexibilité dans les déploiements. | La compatibilité avec des environnements Cloud assure une gestion flexible et évolutive des ressources, en permettant un déploiement rapide et une gestion optimale des infrastructures. |

## CONCLUSION

Le projet FirewallAI représente une **avancée technologique majeure dans le domaine de la cybersécurité**, offrant des solutions de protection robustes et réactives face à un environnement numérique en constante évolution. À travers ce cahier des charges fonctionnel, nous avons défini un produit qui ne se contente pas de répondre aux besoins actuels du marché, mais qui anticipe également les défis futurs auxquels les entreprises et les utilisateurs sont confrontés.

En nous appuyant sur les meilleures pratiques de l’industrie, telles que **l’intelligence artificielle, la détection comportementale en temps réel, et l’intégration avec des systèmes SIEM**, FirewallAI se distingue par sa capacité à détecter, analyser et neutraliser les menaces de manière proactive et autonome. Grâce à sa gestion fine des accès et des rôles, à une sécurité des données inébranlable et à une architecture flexible compatible avec les environnements Cloud, FirewallAI assure une défense complète et une protection continue des réseaux contre toute forme d’intrusion.

Notre approche de sécurité est renforcée par des mises à jour régulières, une interface multiplateforme fluide, et une assistance technique disponible 24/7, garantissant ainsi une expérience utilisateur sans faille. Chaque aspect de FirewallAI, du développement à la mise en œuvre, est conçu pour offrir non seulement des performances exceptionnelles, mais également une expérience d'utilisation simplifiée et accessible, quelle que soit la configuration du client.

L’intégration de FirewallAI dans l’écosystème de cybersécurité permet aux entreprises de **renforcer leur défense tout en bénéficiant de solutions scalables, performantes et adaptées à des besoins spécifiques.** Grâce à une architecture flexible et à une approche modulable, FirewallAI est en mesure de s’adapter aux évolutions technologiques, répondant ainsi aux exigences d’**un marché en perpétuelle transformation**.

Avec le soutien de partenaires technologiques de premier plan et une équipe de développement dédiée à l’innovation continue, FirewallAI est prêt à se positionner comme une solution incontournable dans la lutte contre les menaces numériques. Son architecture robuste, sa capacité à s’intégrer dans des environnements variés, et ses fonctionnalités avancées de détection et de prévention en font un acteur clé pour les entreprises soucieuses de protéger leurs systèmes d’information avec efficacité et anticipation.

En conclusion, FirewallAI incarne l’engagement de notre équipe envers l’innovation, la sécurité et la satisfaction des utilisateurs. Ce projet, ambitieux et stratégique, est prêt à redéfinir les standards de la cybersécurité en offrant une protection optimale et une expérience utilisateur sans compromis. Nous sommes convaincus que FirewallAI deviendra un atout majeur dans la gestion des menaces numériques, en apportant des solutions fiables et évolutives pour une sécurité renforcée.