CRYPTOWEB

Documentation Technique

28 juin 2016

Nos coordonnées

contact@cryptoweb.com

+33 (0) 2 78 77 51 18

Niveau de confidentialité

Diffusion non restreinte

Sommaire

1 - Correspondance des niveaux avec les packs

1.1 - Niveaux dans l'offre de base

Produit	Pack START	Pack EVOLUTION	Pack BUSINESS
Centre de Sécurité et Assistance	Niveau 1	Niveau 2	Niveau 3
Supervision de sécurité	Niveau 1	Niveau 2	Niveau 3
Test de vulnérabilité automatique		Niveau 1	Niveau 1
Pare feu applicatif et réseau de diffusion			Niveau 1

1.2 - Niveaux atteints avec les options

Produit	Pack START	Pack EVOLUTION	Pack BUSINESS
Centre de Sécurité et Assistance	Niveau 2	Niveau 3	Niveau 4
Supervision de sécurité			
Test de vulnérabilité automatique	Niveau 1	Niveau 2	Niveau 2
Pare feu applicatif et réseau de diffusion	Niveau 1	Niveau 1	Niveau 2

2 - Produit : Centre de Sécurité et Assistance

Le cœur de CryptoWeb se trouve dans son Centre de Sécurité où des experts en cybersécurité hautement qualifiés surveillent en permanence vos sites et vous préviennent en cas d'événements suspects.

2.1 - Fonctionnalités clés

Rapports de sécurité mensuels
Un rapport est remis mensuellement, celui-ci présente le niveau de sécurité de l'application web, un résumé des événements de sécurité et une analyse des performances.

Conseil en sécurité web
Le centre de sécurité peut vous conseiller sur vos interrogations en matière de sécurité de vos applications web.

Alertes de sécurité temps réel
Lorsqu'un ou plusieurs événements de sécurité demandent une attention particulière, une alerte est créee dans le centre de sécurité, vous pouvez en être informé en temps réel.

Assistance solutions CryptoWeb
Les demandes concernant l'utilisation des solutions CryptoWeb ou les incidents techniques sur ceux-ci, sont pris en charge par le centre de sécurité.

Analyse des événements de sécurité
Le centre de sécurité synchronise et corrèle les événements de sécurité depuis les solutions de CryptoWeb compatibles.

Réponse à incident de sécurité
Lorsqu'un incident de sécurité est ouvert, le centre de sécurité peut intervenir pour mettre en place des mesures immédiates pour limiter l'impact de l'attaque.

2.2 - Services

Fonctionnalités	Description
Collecte des événements de sécurité	Les évènements de sécurité en provenance des solutions CryptoWeb compatibles, sont synchronisées avec le centre de sécurité.
Corrélation d'événements de sécurité	Les évènements de sécurité synchronisés sont analysés, et si le risque est considéré comme suffisamment important, une alerte est déclenchée.
Levées de doute	Lorsqu'une alerte de sécurité est déclenchée, le centre de sécurité peut réaliser une analyse de celle-ci. L'analyse consiste à vérifier que l'alerte est justifiée par une réelle menace. En fonction du type d'alerte, cette analyse peut se faire de façon externe ou peut nécessiter des accès prilivégiés sur le serveur ou l'application. La levée de doute donne lieu à l'ouverture d'un incident de sécurité si nécessaire.
Mesures de réponses immédiates suite à incident de sécurité	Elles consistent à limiter l'impact de l'incident de sécurité en déclenchant des actions palliatives. Ces actions sont différentes en fonction du type d'incident.
Investigations et Traitements suite à incident de sécurité	Ils consistent à analyser l'incident de sécurité afin de préciser la nature de l'incident, le fait générateur, le périmètre concerné et l'impact de celui-ci. La préservation des traces de l'incident sera effectuée si nécessaire.

2.3 Engagements

2.3.1 Temps de réponse

CryptoWeb s'engage sur le temps de réponse aux demandes d'assistance sur les produits CryptoWeb suite à des incidents :

	Niveau 1	Niveau 2	Niveau 3	Niveau 4
Temps de réponse Incident P1	8 heures	4 heures	2 heures	30 minutes
Temps de réponse Incident P2	16 heures	8 heures	4 heures	2 heures
Temps de réponse Incident P3	24 heures	16 heures	8 heures	2 heures

Le temps de réponse est décompté sur les Horaires ouvrés du centre de sécurité, à partir du moment où le problème est signalé au support technique par l'ouverture d'un ticket. Le ticket peut être ouvert directement par l'envoi d'un e-mail à l'Adresse E-mail de contact de l'assistance ou par l'intermédiaire d'un agent via la Ligne téléphonique de l'assistance. Dans les deux cas, l'horaire pris en compte est celui de la réception de l'email de confirmation. Pour que la demande soit prise en compte, la demande doit être suffisamment détaillée pour permettre au support technique de constater et reproduire le problème.

Les pénalités sont calculées mensuellement. Elles sont de 5 % le montant de l'abonnement mensuel pour chaque heure de retard. Le total des pénalités annuelle (12 mois) ne peut en aucun cas dépasser le montant d'un (1) mois d'abonnement. Les pénalités sont remises sous forme d'un crédit de service.

2.3.2 - Disponibilité de la Console d'administration CryptoWeb

CryptoWeb s'efforce, dans la mesure du possible, d'assurer un taux de disponibilité de 99,9 % par mois, et d'effectuer les maintenances ponctuelles planifiées dans les plages horaires où la console est la moins utilisée.

Cette disponibilité est donnée à titre indicatif et ne donne pas lieu à un engagement. En cas d'indisponibilité de la Console d'administration, les opérations pourront être demandées directement au support technique.

2.4 - Quotas

2.4.1 - Ressources allouées par année

	Niveau 1	Niveau 2	Niveau 3	Niveau 4
Nombre de Levées de doute	5	15	25	30
Nombre de Mesures de réponses immédiates suite à incident de sécurité	1	5	9	15
Nombre d'Investigations et Traitements suite à incident de sécurité	0	3	6	9
Nombre d'heures de Conseil en sécurité web et assistance aux produits CryptoWeb	0	1	12	24

2.4.2 - Tarifs pour quotas supplémentaires

	Niveau 1	Niveau 2	Niveau 3	Niveau 4
Levée de doute	40 € / occurrence	35 € / occurrence		
Mesure de réponse immédiate suite à incident de sécurité	90 € / occurrence	75 € / occurrence		
Investigation et Traitement suite à incident de sécurité	460 € / occurrence	380 € / occurrence		
Conseil en sécurité web et assistance aux produits CryptoWeb	2 € / min	1,5 € / min		

3- Produit : Supervision de sécurité

Malgré toutes les précautions prises, une intrusion peut toujours subvenir, par exemple simplement par le vol des identifiants d'administration d'un Wordpress. Il convient de mettre en place une solution de surveillance des applications Web qui permet de détecter rapidement toute intrusion sur ces applications. Une solution de ce type permet également de nettoyer plus facilement les applications qui pourraient déjà être compromises.

3.1 - Fonctionnalités clés

Protection de la réputation
Nous aidons votre entreprise à détecter toute modification sur vos sites Web avant que vos clients le remarquent. La détection précoce d'une intrusion permet de limiter la portée de l'attaque.

Déploiement simple dans le Cloud
La solution tire parti du Cloud pour permettre une mise en place simple et en rendant facultatif tout ce qui nécessite une intervention sur le serveur.

Vérification des configurations
La solution scanne les espaces Web dans le but de détecter des configurations impactant la sécurité des applications. Par exemple simplement des fichiers oubliés sur le serveur (index.php.txt) ou des options dans les fichiers .htaccess.

Détection des programmes espions
L'agent installé sur le serveur procède à une analyse des applications Web. La technologie utilisée garantit une confidentialité totale des données tout en étant couplée avec une analyse tirant parti de l'intelligence du Cloud. Celui-ci supporte les langages PHP et ASP.

Surveillance des fichiers
La solution réalise un suivi des fichiers sur le serveur : leur ajout, modification, suppression ou changement de permissions. Un moteur d'analyse permet de déterminer un niveau de risque sur chacune de ces modifications et ainsi lancer une alerte si une modification est suspecte.

Détection des programmes de SPAM
Les Webshell de SPAM sont sujets à une forte mutation et sont plus difficiles à détecter par les solutions traditionnelles. La solution permet néanmoins de les détecter grâce à une méthode d'analyse comportementaliste du code source.

3.2 - Fonctionnement

La solution est basée sur 3 composants différents :

- Le robot visiteur
- Le robot réputation
- L'agent de serveur

3.2.1 - Robot Visiteur

Il visite le site internet comme le ferait un visiteur classique. Pendant cette visite, il compare le site avec sa dernière visite et détecte les modifications suspectes. Il analyse également le contenu des pages pour détecter les programmes malveillants.

Il ne requiert pas d'installation ni de configuration sur le serveur.

3.2.2 - Robot Réputation

Il interroge les moteurs de recherche, les antivirus et les listes de réputation pour détecter les baisses anormales de la réputation du site internet.

Il ne requiert pas d'installation ni de configuration sur le serveur.

3.2.3 - Agent de Serveur

Il analyse les fichiers de l'application web sur le serveur, pour détecter les programmes malveillants et les modifications de fichiers suspectes.

Il requiert l'installation d'un programme sur le serveur mais est facultatif.
Sans l'installation de cet agent, toutes les fonctionnalités du produit ne peuvent être assurées.

3.3 - Fonctionnalités

Fonctionnalités	Description
Détection des Web Shell et Backdoor	● Si l'agent de serveur est installé, il analyse les fichiers présents dans l'espace de stockage de l'application web pour détecter les programmes malveillants.
Détection des Web Shell 0-Day	● Un algorithme d'intelligence artificiel est capable de détecter les programmes malveillants, avant même qu'ils soient connus par les antivirus.
Détection des Web Shell de SPAM	● L'agent détecte les Web Shell qui profitent du serveur pour envoyer des e-mails indésirables.
Détection des problèmes de configuration	● La solution analyse le site Internet pour trouver les configurations qui présentent un risque pour la sécurité. Par exemple : du code source non protégé ou des fichiers avec des attributs suspects.
Suivi des modifications de fichiers	● L'agent surveille les modifications sur les fichiers et évalue un risque pour chacune de ces modifications afin de déterminer si elle peut avoir un impact sur la sécurité.
Suivi des versions de CMS	● La solution détecte les systèmes de gestion de contenu (CMS) les plus connus ainsi que les vulnérabilités connues.
Détection des défacements	● Un algorithme de reconnaissance d'image, détecte les modifications suspectes sur le site.
Surveillance des listes noires	● La solution surveille les listes noires afin de déterminer l'application web s'y retrouve.

3.4 - Fréquence d'analyse en fonction de l'offre

	Niveau 1	Niveau 2	Niveau 3
Analyse du site	1 fois par jour	4 fois par jour	8 fois par jour
Analyse en profondeur du site	1 fois par semaine	2 fois par semaine	3 fois par semaine

3.5 - Confidentialité et vie privée

Les robots “Visiteur” et “Réputation” parcourent l’application web comme le ferait n’importe quel visiteur. Ils n’accéderont pas à d’autres informations que celles accessibles publiquement. Les seules informations stockées sont des captures d’écran des pages de l’application.

L’agent quand il est installé sur le serveur, accède aux fichiers présents sur l’espace de stockage de l’application. Il analyse le contenu de ces fichiers mais ne le transmet pas à l’extérieur du serveur, seule une empreinte des fichiers le sera.

3.6 - Propriété du contenu

Des captures d’écran de l’application pourront être stockées dans le système d’information de CryptoWeb ou de ses partenaires mais vous conservez tous les droits sur le contenu de l’application.

3.7 - Responsabilités de CryptoWeb

CryptoWeb s’efforce rigoureusement de fournir un niveau de détection important, cependant, en raison de la nature des menaces nous ne pouvons garantir un taux de détection de 100%. CryptoWeb s’engage donc à mettre en place des mesures raisonnables et propose un service en adéquation avec le niveau de la prestation souscrit.

3.8 - Responsabilités du Client

Le client s’engage à commander la supervision de sécurité uniquement sur les applications web et infrastructures informatiques et réseaux sur lesquels il possède toutes les autorisations, pouvoirs et droits nécessaires.

3.9 - Prérequis techniques et mise en place

La solution requiert que l’application soit accessible via le réseau Internet, en HTTP ou HTTPS, sans authentification.

L’agent facultatif supporte les systèmes d’exploitation suivants :

- Linux 32-bit et 64-bit
- Windows 32-bit et 64-bit

Il se présente sous la forme d'un exécutable qui devra être exécuté avec les droits suffisants pour accéder aux fichiers de l'application, écrire dans un fichier temporaire et communiquer avec son serveur de contrôle via le réseau Internet. Cet exécutable devra être exécuté à intervalles réguliers grâce au système de planification de tâche du système.

La mise en place de l'agent pourra être effectuée par CryptoWeb sans coûts supplémentaires dans les conditions suivantes :

- Un accord est trouvé sur la date d'installation et le moyen de donner la possibilité à CryptoWeb d'obtenir les accès privilégiés sur le serveur
- CryptoWeb valide que les caractéristiques du serveur (logicielles et matérielles) sont prises en charge

4 - Produit : Test de vulnérabilité automatique

Les tests de vulnérabilité automatiques permettent d'identifier les problèmes de sécurité présents dans une application web ou un site Internet. Ils sont réalisés par un robot qui parcours l'application et teste les différents points d'entrées pour détecter les bugs ou les problèmes de configuration qui peuvent avoir des impacts sur la sécurité.

4.1 - Fonctionnalités clés

Identifier les vulnérabilités
La solution identifie les vulnérabilités présentes dans l'application web. Le moteur d'analyse prend en charge les vulnérabilités connues dans une version spécifique d'un logiciel, ou celles inconnues grâce une analyse par fuzzing.

Priorisation par niveau de risque
Les vulnérabilités identifiées sont classées par niveau de risque. Ce classement permet d'identifier celles qui présentent un risque important et de planifier les corrections par niveau d'importance.

Informations détaillées
À chaque vulnérabilité est associée une description de la menace, de l'impact sur l'application et une solution pour la corriger. Des références externes permettent d'obtenir plus d'informations sur ces vulnérabilités.

Rapport de sécurité
À la suite de l'analyse, un rapport récapitulatif est généré. Il est constitué d'une partie synthétique et d'une partie qui détaille les vulnérabilités.

Informations techniques
Le détail de la requête HTTP et la réponse qui ont permis de mettre en évidence la vulnérabilité sont inclus dans le rapport. Ils permettent de pouvoir reproduire l'attaque et de mieux comprendre son fonctionnement.

Analyse du site paramétrable
Le parcours de l'application web peut être paramétré pour répondre aux particularités de celle-ci. Un compte utilisateur peut par exemple être configuré pour permettre l'analyse d'une section du site protégée par mot de passe.

4.2 - Fonctionnalités

Fonctionnalités	Description
Parcours automatique de l'application web	● Le moteur de parcours automatique d'application web va parcourir l'application web afin de couvrir le plus possible les pages du site. Cette analyse est réalisée avec différentes techniques, comme par exemple : La reconnaissance de gabarit, l'observation de comportement, ...
Support du JavaScript	● Le moteur de parcours automatique d'application web supporte le JavaScript ce qui permet de maximiser la surface de couverture de l'analyse.
Liste d'exclusion d'URL	● Certaines parties de l'application web peuvent être évitées grâce une liste d'exclusion d'URL de l'application.
Utilisation d'un compte utilisateur	● Un compte utilisateur peut être configuré afin de parcourir une section de l'application web qui requiert une authentification. Le moteur supporte les modes d'authentification les plus courants.
Rapport récapitulatif	● Le rapport montre à l'aide de schémas synthétiques et de texte détaillé toutes les vulnérabilités qui ont été découvertes à la suite d'un scan de l'application web.
Planification du test	● Le test peut être planifié à un jour et une heure spécifique pour correspondre aux exigences métiers et celles de l'application.
Personnalisation du niveau d'intensité	● Le niveau d'intensité du test peut être personnalisé pour limiter l'impact sur les performances de l'application web.
Pas d'installation	● Le test de vulnérabilité ne demande pas d'installation ou de configuration sur le serveur. Si le site est protégé par un pare-feu applicatif, une configuration de celui-ci peut être utile pour maximiser le niveau de détail des résultats.

4.3 - Responsabilités et engagements de CryptoWeb

4.3.1 - Risques spécifiques au test

CryptoWeb s'interdit de réaliser volontairement des actions dangereuses pour le système d'information du client. Cependant, de par sa nature, le test de vulnérabilité présente des risques tels que, de façon non exclusive :

- Indisponibilité d'une partie ou de la totalité du système d'information suite à une saturation du réseau, un bouclage logiciel ou une anomalie dans un système
- Divulgation d'une information confidentielle à CryptoWeb suite à un accès involontaire

Pour réduire ces risques, le client est fortement incité à réaliser les tests sur un serveur de test ou de préproduction pour limiter l'impact de tout dommage qui pourrait subvenir.

4.4 - Responsabilités du Client

Le client s'engage à commander les tests de vulnérabilité uniquement sur les applications web et infrastructures informatiques et réseaux au sein des quels il possède toutes les autorisations, pouvoirs et droits nécessaires.

Le client reconnaît que le test de vulnérabilité présente des risques pour le système d'information audité, et qu'il possède en conséquence toutes les ressources nécessaires pour remettre en état le système d'information en cas d'incident. Ce qui inclus de façon non exhaustive : des jeux de sauvegarde, des ressources correctement dimensionnées, du matériel de rechange.

4.5 - Fréquences en fonction du niveau

Lorsque que le test de vulnérabilité est inclus dans un pack CryptoWeb, celui-ci est réalisé avec une certaine fréquence telle que décrite dans le tableau ci-dessous :

	Niveau 1	**Niveau 2**
Fréquence de l'analyse	Mensuel	Hebdomadaire

En dehors d'un pack CryptoWeb, le test de vulnérabilité est réalisé de façon ponctuelle.

5 - Produit : Pare feu applicatif et réseau de diffusion

Chaque jour les applications web sont la cible de nombreuses attaques informatiques qu'elles soient ciblées ou non. Elles peuvent avoir un impact important sur la disponibilité du site ou l'image de l'entreprise, causant de grave pertes financières. Le pare-feu applicatif protège les applications web contre ces menaces en bloquant les requêtes illégitimes.

La disponibilité et le temps de chargement des ces applications est également un facteur important dans le taux de transformation et la satisfaction client. Le réseau de diffusion de contenu (CDN), permet d'améliorer la réactivité des applications web en copiant les données sur des serveurs proches des visiteurs.

5.1 - Fonctionnalités clés

Pare-feu applicatif
Un moteur d'analyse des requêtes des visiteurs vers votre serveur permet d'identifier les utilisateurs malveillants et ainsi bloquer leurs attaques. Ces attaques peuvent par exemple être : Injection SQL, XSS (Cross-Site scripting), ...

Déploiement simple dans le Cloud
La solution tire parti du Cloud pour permettre une mise en place simple, sans matériel ni logiciel à installer, tout en offrant des performances et une disponibilité exemplaire.

Protection Anti-DDoS
Un algorithme de détection et de mitigation analyse le trafic réseau vers le serveur et met à l'abri l'application web contre les attaques de type déni de service.

Optimisation du contenu
Les ressources statiques comme les images, le JavaScript ou les CSS peuvent être minifiées et compressées, réduisant le temps de chargement et la consommation de bande passante.

Sécurisation HTTPS
La solution intègre un certificat TLS/SSL qui permet de protéger les échanges avec vos visiteurs en les chiffrant. Le HTTPS améliore également votre référencement et augmente la confiance de vos visiteurs.

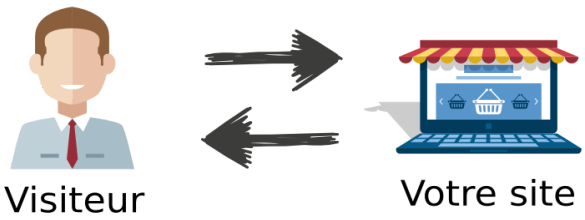
Mise en cache
Les ressources statiques peuvent être mises en cache automatiquement. Réduisant le temps de chargement et la charge sur le serveur.

5.2 - Fonctionnement

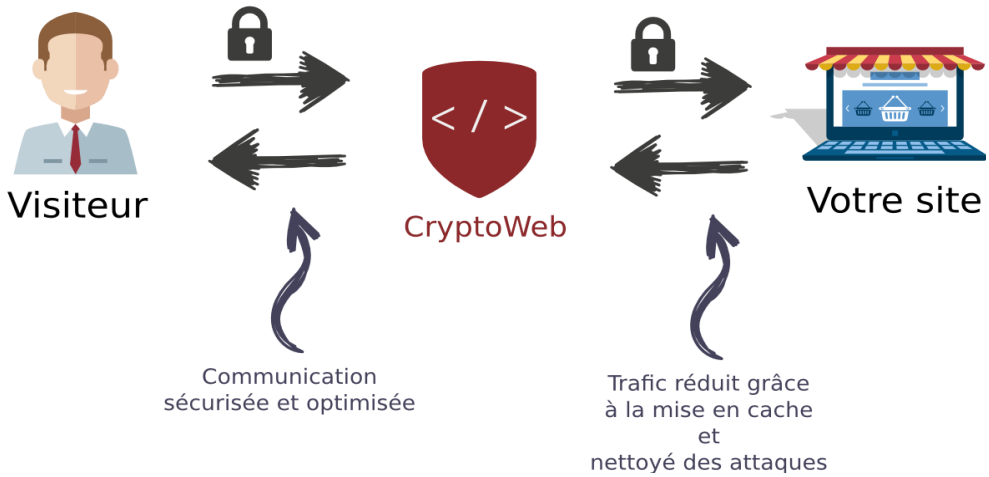
Dans les architectures classiques, vos visiteurs communiquent directement avec le serveur qui héberge votre application web ou site Internet. Il est alors exposé aux attaques.

La solution pare-feu applicatif et CDN de CryptoWeb vient se positionner devant le site Internet pour le protéger. Le trafic de vos visiteurs passe alors à travers un réseau sécurisé avant d'atteindre votre serveur.

Sans CryptoWeb :



Avec CryptoWeb :



Cette solution se base sur une architecture Cloud qui permet une mise en place simple sans modifications de la configuration de votre serveur, ni d'installation sur celui-ci.
La mise en place se fait grâce à la modification des enregistrements DNS du nom de domaine.

Des modifications supplémentaires pourront êtres effectuée sur le serveur si vous souhaitez augmenter le niveau de sécurité de celui-ci. Un certain nombre de ces modifications est pris en charge dans l'abonnement.

5.3 - Fonctionnalités du Pare-feu applicatif

Fonctionnalités	Description
Inspection des Paquets HTTP en Profondeur (DPI)	● Détecte et bloque les attaques web telles que les Injections SQL (SQLi), Cross-Site scripting (XSS), et les autres attaques parmi les plus courantes ● Possibilité de configuration en mode"blocage" ou "avertissement" pour tester les faux positifs avant la mise en place
Mitigation DDoS	● Protection contre les attaques de type DDoS
Réputation IP	● Intégration à une base de données de réputation des adresses IP pour bloquer le trafic connu comme malveillant
Défi pour les utilisateurs suspects	● Lorsqu'un utilisateur est suspect mais non confirmé comme malveillant, une page lui demande de saisir un CAPTCHA
Réglage du niveau de sensibilité	● Le niveau de sensibilité du moteur de détection peut être réglé en fonction du niveau de menace
Personnalisation des pages d'erreur	● Les pages d'erreur lors des blocages peuvent être personnalisées pour correspondre à l'image de l'entreprise

5.4 - Fonctionnalités du CDN

Fonctionnalités	Description
Mise en cache du contenu	● Le contenu statique (Images, JavaScript, CSS, …) est mis cache par défaut ● Le contenu dynamique (HTML, …) peut être mis en cache via la création de règles spécifiques
Toujours en ligne	● Si le serveur d'origine devient indisponible, une copie limitée du site peut être présentée aux visiteurs
Protection contre les pics de trafic	● La mise en cache d'une partie du contenu fait que le serveur origine aura en moyenne 65% de requêtes en moins à traiter. Cette baisse de la charge sur le serveur permet d'absorber les pics de trafic

HTTP/2 et SPDY	● Les protocoles les plus récents comme HTTP/2 et SPDY sont proposés aux visiteurs de l'application web sans avoir à modifier la configuration du serveur. Le CDN réalise une traduction de protocole et intérroge le serveur d'origine avec un protocole qu'il supporte.
IPv6	● Le CDN offre une connectivité IPv6 aux visiteurs si ceux-ci la supporte

5.5 - Fonctionnalités spécifiques par offre

	Niveau 1	**Niveau 2**
Taille maximale des upload	100 Mo	200 Mo
Règles de pare-feu personnalisées	Non	Jusqu'à 25
Protection Anti-DDOS	Oui	Oui avec protection avancée
Règles de contenu	20	50

5.6 - Hébergement des données

5.6.1 - Partenariat

CryptoWeb travaille avec la société CloudFlare Inc à travers un partenariat afin de vous proposer une solution facile à mettre en place, rapide et sécurisée.
Nous apportons un soin particulier à choisir nos partenaires, CloudFlare est aujourd'hui une référence dans ce domaine en proposant une infrastructure à haute disponibilité, de grande capacité et avec des fonctionnalités innovantes.

Conditions et politiques de CloudFlare :

- Conditions d'utilisation : https://www.cloudflare.com/terms/
- Politique de sécurité : https://www.cloudflare.com/security-policy/
- Politique contre les abus : https://www.cloudflare.com/abuse/

5.6.2 - Hébergement et circulation des données

Le trafic du site web circule par l'intermédiaire du réseau de CloudFlare. En fonction du type et des règles de mise en cache configuré, les données peuvent également être recopiées à des fn de mise en cache.

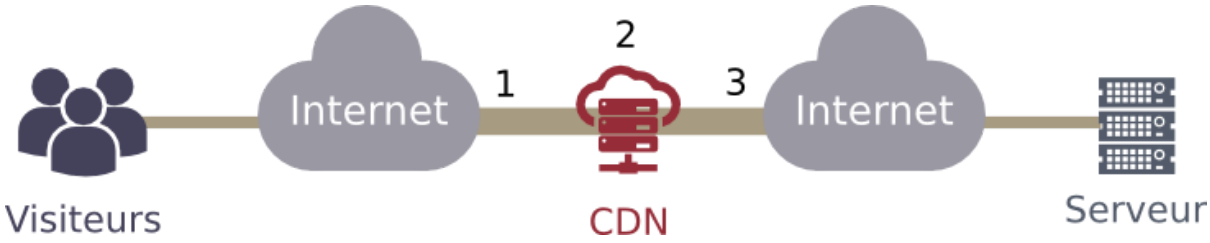
Le principe de fonctionnement est le suivant :

1. Le visiteur interroge le centre de données le plus proche et rapide de sa localisation.

2. Si le centre de données n'a pas déjà la ressource demandée en mémoire, il interroge le Serveur origine via une connexion ultra rapide, puis l'enregistre en cache.
3. La ressource est retournée au visiteur.

Le trafic est routé à travers 76 centres de données autour du monde, ce qui permet de proposer une réactivité exemplaire, quelque soit l'origine des visiteurs.

5.7 - Confidentialité et vie privée



5.7.1 - Confidentialité entre le visiteur et le CDN (1)

En fonction de la demande au moment de l'installation, le SSL/TLS peut être mis en place sur le CDN et ainsi proposer le HTTPS aux visiteurs et utilisateurs de l'application web.
Le SSL/TLS permet d'authentifier et chiffrer le CDN auprès de l'utilisateur. La confidentialité est donc assurée entre l'utilisateur et le CDN avec un niveau équivalent à celui des sites bancaires.
Sans le HTTPS, les données échangées entre le visiteur et le CDN transitent en clair sur le réseau Internet et peuvent êtres interceptées par un tiers.

5.7.2 - Confidentialité dans le centre de données du CDN (2)

Dans ses centres de données, CloudFlare s'engage à prendre toutes les mesures raisonnables permettant de protéger les informations des utilisateurs contre la perte, la mauvaise utilisation, les accès non autorisés, la divulgation, l'altération et la destruction.

Les données de ces centres pourront cependant être consultés par les forces de l'ordre avec ordonnance de tribunal ou autre procédure juridique avec un aspect obligatoire. Dans la mesure du possible, vous serez informé de cette procédure juridique.

Dans le cas où des données personnelles sont mises en cache dans le CDN, leur suppression peut être demandée directement à CryptoWeb. Cette demande se fait via une demande de support technique en précisant les URL des pages contenant les informations devant être supprimées.

5.7.3 - Confidentialité entre le CDN et le serveur origine (3)

La communication entre le serveur CDN et le serveur est réalisée en HTTP ou HTTPS en fonction de la configuration et des capacités du serveur origine.

Le tableau ci-dessous présente le niveau de sécurité possible en fonction des caractéristiques et des possibilités du serveur racine.

Type de sécurité	Chiffrement	Authentification serveur origine	Authentification client CDN	Prérequis
Sans				Aucun
Niveau 1	✓			Certificat HTTPS auto-signé et possibilité de le configurer sur le serveur origine
Niveau 2	✓	✓		Certificat HTTPS signé par une autorité de confiance et possibilité de le configurer sur le serveur origine
Niveau 3	✓	✓	✓	Certificat HTTPS signé par une autorité de confiance et possibilité de le configurer sur le serveur origine ainsi qu'une authentification client par certificat

5.8 - Engagements de disponibilité et de service

5.8.1 - Disponibilité de l'infrastructure CloudFlare

L'infrastructure du CDN est conçue sur un modèle de Haute-Disponibilité pour réduire au maximum les risques d'interruption de service ou de ralentissement. Cependant, de par la nature du réseau Internet, la disponibilité et les performances de celui-ci ne peut être garantie contractuellement.

5.8.2 - Interruption du service

CryptoWeb se réserve le droit de suspendre le service, sans préavis, notamment dans les cas suivants :

- Plainte ou réclamation par un tiers relative à une atteinte à l'ordre public, tout usage illicite ou préjudiciable
- Usage perturbant la disponibilité, les performances ou le fonctionnement global de l'infrastructure
- Non-paiement des factures

5.9 - Propriété du contenu

Vous conservez tous les droits sur le contenu de votre site internet. En fonction de la configuration de la solution, le contenu pourra éventuellement être modifié avant d'être présenté au visiteur dans les cas suivants :

- Pour bloquer les demandes des visiteurs qui sont considérés comme malveillants, une page d'erreur ou de défi pourra être présentée en lieu et place du contenu.
- Ajouter des cookies ou des scripts pour assurer des fonctionnalités de sécurité ou de performance
- Autres modifications pour améliorer la performance et la sécurité, comme cacher les adresses e-mail si la fonctionnalité est activée

5.10 - Prérequis techniques et mise en place

La solution requiert que le serveur origine soit accessible via le réseau Internet, en HTTP ou HTTPS.

La version supportée de HTTP est 1.1.

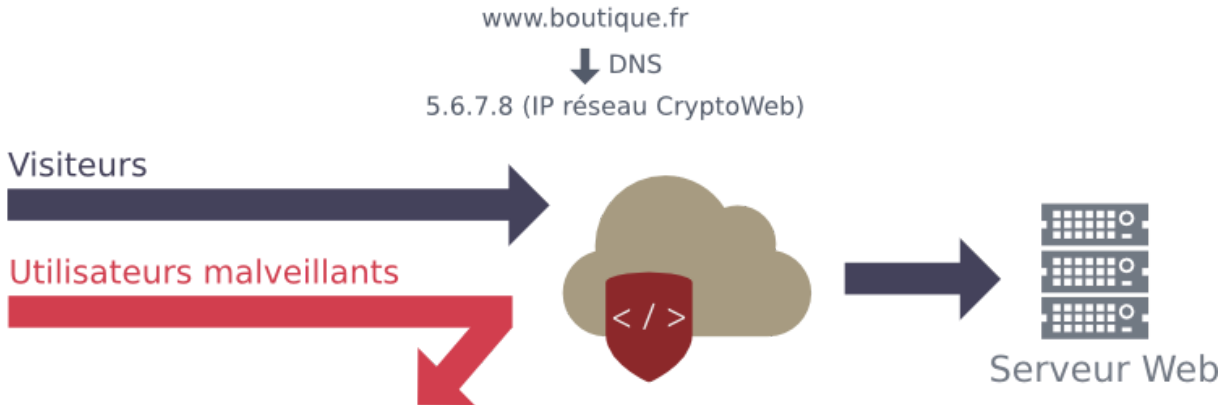
En HTTPS, les modes de chiffrements proposés et les tailles de clés doivent correspondre aux standards actuels. Ces prérequis sont susceptibles d'évoluer en même temps que la pratique, notamment les modes ou tailles de clés n'étant plus considérés comme sécurisés peuvent être abandonnés.

5.10.1 - Configuration requise : DNS

Pour mettre en place la solution, les DNS doivent êtres configurés pour faire passer le trafic à travers le réseau de protection.

Configuration Initiale :

Configuration Visée :



La configuration des DNS peut être réalisée de deux façons différentes :

- Utilisation d'enregistrements CNAME
- Migration des DNS vers les serveurs DNS distribués CloudFlare

Si l'application web est disponible à la racine du nom de domaine, par exemple https://boutique.fr (sans www), la migration des DNS sera obligatoire car les DNS ne peuvent pas être utilisés sur la racine.

Vous devez posséder les accès et les autorisations pour effectuer les modifications requises pour la solution technique correspondant à votre situation, sans cela, la solution ne pourra pas être mise en place.

5.10.2 - Configuration facultative : restaurer les IP des visiteurs

Le trafic web passant par le CDN avant d'atteindre l'application web, l'IP du CDN apparaîtra dans les journaux du serveur web et de l'application à la place de celle du visiteur.

L'IP originale du visiteur est cependant accessible dans une entête HTTP rajoutée à la requête, celle-ci est nommée CF-Connecting-IP.

Il existe différentes solutions pour restaurer l'adresse IP en fonction du serveur web et de l'application web.

Solution officielle

La solution officielle est d'utiliser le module apache mod_cloudflare qui est compatible avec Apache HTTPD 2.2.x et 2.4.x, installé avec les paquets officiels sur les distributions suivantes :

- RHEL / CentOS / CloudLinux 6 (32 et 64 bit)

- RHEL / CentOS / CloudLinux 5 (32 et 64 bit)
- Debian 7 (32 et 64 bit)
- Debian 6 (32 et 64 bit)
- Ubuntu 12.04 (32 et 64 bit)
- Ubuntu 10.04 (32 et 64 bit)

Pour cette installation, l'accès SSH et les droits administrateur (root) sont nécessaires. L'installation est comprise dans l'abonnement sans surcoût.

Solutions alternatives
Dans les autres configurations, bien que de nombreuses solutions existent, la restauration de l'IP des visiteurs ne peut pas être garantie sans une analyse technique. En fonction de la complexité de la solution induite par les besoins techniques, l'installation pourra être comprise dans l'abonnement ou nécessiter des frais d'installation.

5.10.3 - Configuration facultative : limiter l'accès au CDN

Une fois que le trafic de l'application passe par le réseau CDN, il est préférable de bloquer les connexions à l'application web depuis les adresses IP qui ne sont pas celles du CDN.

Pour cela plusieurs solutions sont possibles :
- Liste blanche d'IP dans le pare-feu
- Liste blanche d'IP dans la configuration du serveur web (par exemple .htaccess)
- Utilisation de l'authentification par certificat client du CDN

Sans ce type de configuration, un attaquant qui connaît l'adresse IP du serveur peut contourner la protection.

5.10.3 - Configurations incompatibles

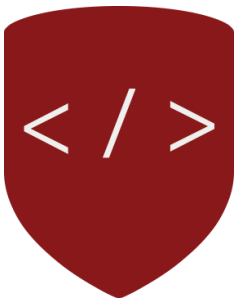
Le trafic provenant du CDN, il faut veiller qu'aucun système de prévention d'intrusion ou solution de protection contre la force brute ne bloque l'adresse IP ou le trafic provenant du CDN.

6 - Définitions

Incident	Dysfonctionnement de la solution, non imputable à une mauvaise utilisation, ni une anomalie de l'application web ou du serveur origine ou du réseau de celui-ci.
Incident P1 (Priorité 1)	Incident rendant impossible l'accès à la totalité du site web pour tous les utilisateurs.
Incident P2 (Priorité 2)	Incident rendant impossible l'accès à une partie du site web pour tous les utilisateurs ou totalité du site web pour une partie des utilisateurs.
Incident P3 (Priorité 3)	Incident qui est autre que Incident P1 et Incident P2
Horaires ouvrés du centre de sécurité	Entre 9h00 et 18h00 CET, du lundi au vendredi, sauf les jours fériés définis dans le code du travail, et fermetures exceptionnelles signalées sur le site www.cryptoweb.com.
Console d'administration	Interface web permettant de configurer la solution. Elle est accessible grâce à une authentification par identifiant et mot de passe.
Adresse E-mail de contact de l'assistance	Adresse E-mail permettant de contacter l'assistance de CryptoWeb : support@cryptoweb.com
Ligne téléphonique de l'assistance	Ligne téléphonique permettant de contacter l'assistance de CryptoWeb : +33 (0) 2.78.77.51.28
Fuzzing	Méthode de test d'une application qui consiste à envoyer des données aléatoires ou spécialement conçues dans les entrées de celle-ci pour mettre en évidence des anomalies.
Serveur Origine	Serveur qui héberge l'application web à protéger.

7 - Plus d'informations

Pour en savoir plus sur les solutions CryptoWeb, visitez cryptoweb.com ou contactez-nous :



Centre de Sécurité et Assistance Technique

Téléphone : +33 (0) 2 78 77 51 28
E-mail : support@cryptoweb.com

Standard

Téléphone : +33 (0) 2 78 77 51 18
E-mail : contact@cryptoweb.com