Sécurité de la Smartbox

Aperçu de l'architecture de sécurité Keycafe

Introduction

Keycafe offre aux entreprises un moyen pratique de gérer à distance les clés tout en maintenant un niveau de sécurité acceptable pour la majorité des cas d'utilisation. De la conception des produits à l'architecture des systèmes en passant par la construction solide des SmartBox, nos solutions sont conçues dès le départ avec un équilibre entre sécurité, commodité et convivialité. Cet aperçu décrit les fonctions de sécurité essentielles intégrées à la plateforme Keycafe Smart Key Management.

Meilleure architecture de serveur, d'application et de base de données

Service et sécurité de pointe

Keycafe s'intègre aux meilleurs fournisseurs de logiciels pour offrir une sécurité de haut niveau sur le back-end. La sécurité de la couche de transport, la protection contre les attaques par déni de service et les pare-feu gérés font partie intégrante de notre architecture de serveur de données. Keycafe observe les meilleures pratiques de sécurité telles que les hachages de mot de passe, la journalisation des accès, les révisions du code source et les tests d'intrusion.

Sécurité de la couche de transport

TLS chiffre, authentifie et vérifie l'intégrité des données contre la falsification. Un canal de communication privé entre votre ordinateur et Keycafe garantit que lorsque vous gérez votre compte, toutes les informations sont transmises en toute sécurité.

Déni de service

L'accès à Keycafe est sécurisé contre les attaques par déni de service (DDOS) par un partenaire CDN de premier ordre. Avec plus de 67 Tbps de capacité réseau, Cloudflare bloque en moyenne 70 milliards de menaces par jour pour vous protéger contre les attaques les plus importantes et les plus sophistiquées.

Pare-feu gérés

Vos données sont sécurisées derrière plusieurs pare-feu à la pointe de la technologie. Les pare-feu sont essentiels pour protéger le trafic réseau, y compris le flux de données sensibles. Ils sont nécessaires pour la conformité aux mandats tels que PCI DSS, HIPAA et GDPR.

Traitement des paiements conforme à la norme PCI

Vos informations de paiement sont cryptées par un processeur de paiement conforme à la norme PCI certifié PCI Service Provider Niveau 1, le niveau de certification le plus strict disponible dans l'industrie des paiements.

Tests de pénétration

Keycafe effectue périodiquement des tests de pénétration automatisés pour trouver les vulnérabilités avant qu'elles ne puissent être exploitées. Ces tests, conçus par des experts en sécurité, simulent les activités de vrais pirates pour signaler des problèmes tels que des serveurs mal configurés, des injections SQL, des scripts intersites, des fichiers/répertoires exposés, des protocoles de cryptage ou des chiffrements faibles, et bien d'autres. Ils testent également les vulnérabilités connues dans les logiciels et protocoles populaires ("Heartbleed", etc.).

Nos fournisseurs de logiciels équipent Keycafe d'une surveillance constante des menaces à la pointe de l'industrie et d'un correctif automatique des vulnérabilités du système d'exploitation. Les fournisseurs de logiciels Keycafe sélectionnés incluent :

Cloudflare

Leader mondial de la protection DDoS, de la limitation de débit, du proxy pour l'amélioration des performances CDN et de la gestion DNS. Cloudflare est approuvé par 25 millions de propriétés Internet.

Heroku

Sécurité hautement avancée pour l'hébergement Web, l'administration des systèmes, les mises à jour de sécurité Linux, les mises à jour de sécurité des bases de données, le pare-feu et la détection des intrusions logicielles. Heroku est conforme aux normes ISO 27001, 27017, 27108 avec les rapports SOC 1, 2, 3. Voir plus.

Intruder.io

Intruder est un scanner de vulnérabilité basé sur le cloud qui détecte les faiblesses de la cybersécurité dans l'infrastructure numérique en recherchant 10 000 vecteurs d'attaque courants.

Particle

Le fournisseur leader d'IoT à grande échelle du secteur permet la gestion d'un réseau hautement sécurisé d'appareils distants, de matériel et de services cloud.

Stripe

La première plateforme de facturation en ligne. Des millions d'entreprises de toutes tailles, des startups aux grandes entreprises, utilisent le logiciel et les API conformes à la norme PCI de Stripe pour accepter des paiements, envoyer des paiements et gérer leurs activités en ligne.

Keycafe a obtenu un A+ avec un score d'efficacité de la sécurité de 99,98 % sur une analyse Intruder.io de plus de 10 000 vecteurs d'attaque.

Authentifications et autorisations des utilisateurs

Authentification d'accès sur mesure

L'authentification des utilisateurs Keycafe offre un certain nombre d'options pour vous permettre de contrôler qui accède à la clé de votre entreprise pour les propriétés de location, les véhicules et les installations de l'entreprise. Par défaut, l'authentification à deux facteurs est activée, ce qui oblige les utilisateurs finaux à saisir un numéro d'identification ainsi qu'un code d'accès envoyé par SMS.

En fonction de votre plan d'abonnement, une variété d'autorisations personnalisées supplémentaires peuvent être superposées pour l'authentification, telles que des contrôles administratifs, des autorisations planifiées, des analyses de badges, etc. L'utilisation de toute l'étendue de nos options d'authentification face à l'utilisateur et l'adaptation de l'accès à chaque utilisateur de vos SmartBox est un moyen de dissuasion important contre l'accès non autorisé aux clés.

Vous trouverez ci-dessous un tableau des types d'objets accessibles et des options d'autorisations pouvant être accordées et gérées.

Type d'objet / d'autorisation	Description	Qui peut accéder	Exigence d'authentification
Codes des clés	Un code simple qui peut être créé pour n'importe quelle clé qui, une fois entré dans la SmartBox, révèle la clé. Le code de la clé est valable jusqu'à ce qu'elle soit retirée.	Toute personne à qui vous donnez le code de la clé	Saisie du code de la clé sur la SmartBox
Réservations planifiées	Un accès à une clé qui est valide dans un laps de temps spécifique où le tiers n'est pas tenu d'être un utilisateur enregistré.	Toute personne à qui vous donnez les détails de la réservation	Saisie du code de réservation sur la SmartBox ou utiliser l'URL unique pour une expérience mobile conviviale.
Autorisation de clé unique	Autorisation dans la base de données permettant à un utilisateur ou à un groupe d'utilisateurs d'accéder à une clé spécifique.	Tout utilisateur disposant d'autorisations d'échange ou d'administrateur sur la clé, ou tout utilisateur d'un groupe d'utilisateurs disposant d'autorisations d'échange ou d'administrateur sur la clé	Utilisation de l'application Keycafe iOS ou Android, ou saisie du code d'identification sur la SmartBox plus le code 2FA si requis par les paramètres
Autorisation de toutes les clés	Autorisation dans la base de données permettant à un utilisateur ou à un groupe d'utilisateurs d'accéder à toutes les clés appartenant à votre compte.	Tout utilisateur disposant d'autorisations d'échange ou d'administrateur sur le groupe toutes les clés, ou tout utilisateur d'un groupe d'utilisateurs disposant d'autorisations d'échange ou d'administrateur sur le groupe toutes les clés	Utilisation de l'application Keycafe iOS ou Android, ou saisie du code d'identification sur la SmartBox plus le code 2FA si requis par les paramètres.
Groupe personnalisé de clés	Autorisation dans la base de données permettant à un utilisateur ou à un groupe d'utilisateurs d'accéder à un groupe de clés que vous avez désigné.	Tout utilisateur ayant reçu des autorisations d'échange, utilisateur ayant reçu des autorisations d'administrateur sur le groupe de clés personnalisé, groupe d'utilisateurs disposant d'autorisations d'échange ou d'administrateur sur le groupe de clés personnalisé	Utilisation de l'application Keycafe iOS ou Android, ou saisie du code d'identification sur la SmartBox plus le code 2FA si requis par les paramètres.
Casier à clés	Possibilité pour un utilisateur d'ouvrir à distance n'importe quel casier à clés sur la SmartBox, quelles que soient les autorisations de clé.	Tout utilisateur disposant d'autorisations d'administrateur pour l'emplacement d'échange de clés	Utilisation de l'application Web Keycafe, de l'application iOS ou Android.
Serrure principale de la SmartBox	Une possibilité pour un utilisateur de déverrouiller à distance depuis le mur l'intégralité de la SmartBox, quelles que soient les autorisations de clés	Tout utilisateur disposant d'autorisations d'administrateur pour l'emplacement d'échange de clés	Utilisation de l'application Web Keycafe, de l'application iOS ou Android.

Communication entre serveur IoT et la SmartBox

Robuste, dynamique & informatif

En s'intégrant au Device Cloud de Particle, la sécurité Keycafe IoT est soutenue par un hébergement de première qualité avec une sécurité physique et une gestion des risques ISO 27001, 27017 et 27018 qui minimise la surface d'attaque à la fois dans la couche de service et dans les données.

Sécurité IoT avancée

Toutes les communications entre la SmartBox et nos serveurs sont cryptées et sécurisées. Ne laissant aucun port entrant ouvert, notre service déjoue les scanners de ports et les attaques secondaires. Chaque appareil porte une clé de cryptage unique et la surveillance continue du paysage de sécurité protège les serveurs contre les menaces potentielles.

Connexions radio cryptées

La communication BLE avec la SmartBox est entièrement cryptée en transit. Les connexions WiFi sont sécurisées à l'aide de WPA2, la norme de l'industrie. Les connexions cellulaires utilisent le cryptage standard de l'industrie pour garantir la sécurité de toutes les données en transit.

Alertes d'activité de l'appareil

Avec la connectivité cloud de la SmartBox 24h/24 et 7j/7, les échanges de clés déclenchent automatiquement des notifications détaillées en temps réel via e-mail, notifications mobiles ou webhook. Étant donné que l'authentification se produit en direct dans la communication avec notre serveur, Keycafe fournit un contrôle en temps réel sur l'accès à vos clés.

Mises à jour OTA

Chaque SmartBox reçoit des mises à jour en direct, ce qui signifie que le micrologiciel et les fonctionnalités de sécurité sont toujours à jour pour garder une longueur d'avance sur les menaces émergentes.

Données sensibles hors site

Aucune donnée sensible n'est stockée localement sur la Keycafe SmartBox. Pendant ce temps, les protocoles de cryptage ajoutent une autre couche de protection essentielle.

Politique de confidentialité et traitement des données

Conforme au RGPD

La politique de confidentialité de Keycafe, axée sur le client, décrit quelles informations sont collectées et comment elles sont utilisées, partagées, sécurisées et stockées. Keycafe a son siège social à Vancouver, au Canada, et les données des clients ne sont pas traitées sur place. Nous comptons sur les meilleurs fournisseurs de services cloud pour traiter et stocker vos informations en notre nom et ces fournisseurs peuvent traiter et stocker vos informations aux États-Unis, au Canada, dans l'Union européenne et dans d'autres pays. Nous avons vérifié que ces fournisseurs ont mis en place des programmes de conformité au RGPD et ont conclu des accords de traitement de données avec nos fournisseurs de services qui restreignent et réglementent leur traitement de vos données en notre nom.

Nos systèmes contiennent des règles et des garanties relatives aux données qui sont présentées aux autres utilisateurs en fonction de leurs autorisations et de la relation implicite entre les parties. De plus, nous allons au-delà des contrôles internes typiques en n'affichant pas les PII utilisateur par défaut aux membres de notre propre équipe et en limitant le nombre de vues PII que chaque membre de l'équipe est autorisé sans réauthentification. Vous pouvez accéder à notre politique de confidentialité complète **ici**.

La SmartBox

Dissuasion solide de la plupart des falsifications

Notre SmartBox montée sur plaque d'acier est dotée d'un cadre en acier robuste à revêtement en poudre de calibre 16. À l'intérieur, chaque bac à clés individuel est construit avec un boîtier séparé en métal moulé sous pression. La serrure principale électronique est inaccessible et entièrement cachée à la vue. La SmartBox devrait dissuader la plupart des altérations occasionnelles par des tiers non autorisés compte tenu de sa construction en métal solide, des verrous sur chaque bac à clés individuel et de l'absence de serrure principale orientée vers l'extérieur.

La SmartBox Keycafe est conçue pour avoir un niveau de sécurité similaire, par exemple, aux casiers d'une gare ou aux cadenas pour vélos utilisés en ville. Elle n'est pas conçue pour résister aux cambrioleurs équipés d'outils. Il convient de noter que les coffres-forts qui ont des certifications antivol officielles pour la protection des objets de valeur mesurent leur dureté en nombre de minutes pendant lesquelles ils peuvent résister à un vol, généralement 10 minutes ou moins, de sorte que même les coffres-forts les plus sûrs ne résisteront en pratique à un tiers à l'intention malveillante que pour une période de temps limitée. Notre produit n'est pas un coffre-fort et est conçu pour offrir une facilité d'utilisation et une commodité associées à une construction solide. La SmartBox ne doit être utilisée que dans des environnements bien éclairés et surveillés qui, selon vous, sont peu susceptibles d'attirer les vols. Vous devriez vérifier auprès de votre compagnie d'assurance comment l'utilisation et le placement de la SmartBox peuvent avoir un impact sur les réclamations.

Caractéristiques de la SmartBox:

- Support de plaque en acier à 15 vis
- Cadre robuste en acier laminé à froid de calibre 16
- Casiers à clés en métal moulé sous pression en alliage A383
- Accès principal inaccessible et contrôlé électroniquement
- Revêtement en poudre résistant aux intempéries

Chaque SmartBox est en outre protégée par une sécurité IoT de pointe, une authentification sur mesure et des intégrations logicielles de pointe, comme décrit ci-dessus.

Informations complémentaires

Bien que nos équipes d'assistance et de vente fassent de leur mieux pour communiquer sur un large éventail de sujets techniques liés à nos produits, leurs réponses ne sont pas toujours entièrement nuancées ou à jour. Ce document fournit un résumé de haut niveau de notre architecture de sécurité, de nos pratiques et de nos principaux fournisseurs. Si vous avez une question de sécurité non abordée par ce document et que vous souhaitez une réponse définitive, veuillez contacter security@keycafe.com et nous consulterons nos chefs de produit et nos ingénieurs pour vous fournir des informations supplémentaires.