

Paxton Solo – Présentation de la sécurité

Présentation

Paxton Solo a été conçu pour rendre le contrôle d'accès simple à utiliser tout en maintenant un haut niveau de sécurité dans tout le système. La sécurité est intégrée à chaque étape de la communication et de l'administration entre le téléphone de l'utilisateur et le contrôleur de porte, ainsi que dans les services cloud qui soutiennent le système.

Ce document fournit une vue d'ensemble des principales mesures de sécurité incluses dans Paxton Solo.

Communication téléphone-contrôleur

Paxton Solo utilise Bluetooth Low Energy (BLE) pour la communication directe entre le téléphone de l'utilisateur et le contrôleur Solo.

Pour protéger cette connexion, à la fois le contrôleur et le dispositif mobile utilisent du matériel sécurisé et des processus sécurisés conçus pour empêcher la copie ou l'interception des identifiants.

Un élément sécurisé au sein du contrôleur offre un environnement protégé pour stocker des informations de sécurité sensibles. Sur les appareils mobiles pris en charge, les fonctionnalités de sécurité intégrées au téléphone offrent une protection similaire pour les identifiants numériques.

Cela signifie que les informations d'accès ne sont pas stockées ou échangées de manière visible, ce qui pourrait facilement être extrait, cloné ou réutilisé par des utilisateurs non autorisés. Comme la communication s'effectue directement entre le téléphone et le contrôleur Solo, le matériel Solo n'a pas besoin de se connecter au réseau local du client pour un fonctionnement normal.

Cryptographie asymétrique

La communication entre l'application mobile Paxton Solo et le contrôleur Solo est protégée par cryptographie asymétrique.

En termes simples, cela signifie que le système utilise une paire de clés numériques, une publique et une privée. Ces clés fonctionnent ensemble pour confirmer l'identité et protéger les informations pendant la communication.

Comme la clé privée n'est jamais partagée, le système peut vérifier que les deux appareils sont authentiques sans exposer d'informations sensibles. Cette approche réduit le risque de copie d'identifiants, d'attaques par rejeu et de tentatives d'accès par des appareils non autorisés.

Chaque interaction est conçue pour confirmer que le téléphone et le contrôleur Solo sont dignes de confiance avant qu'un accès ne soit accordé, sans nécessiter que le contrôleur Solo communique sur le réseau local du client.

Communication téléphone-cloud

Le matériel Paxton Solo ne se connecte pas directement au réseau du client ni à Internet. Lorsque la communication cloud est requise, l'application mobile de l'utilisateur agit comme canal de communication vers les services cloud de Paxton.

La communication entre l'application et les services cloud s'effectue sur des connexions HTTPS standard utilisant le port 443 et est protégée par un chiffrement SSL/TLS.

Cette approche réduit la complexité du réseau sur site, évite d'ouvrir des connexions entrantes dans l'infrastructure du client et maintient la communication dans le trafic Internet sécurisé standard. Les données transmises entre l'application et les services cloud sont protégées durant le transit et prennent en charge la gestion sécurisée des utilisateurs et des autorisations.

Connexion sécurisée avec Passkeys (Optionnel)

La connexion utilisateur peut être protégée en utilisant des passkeys, qui sont largement reconnues comme l'une des approches les plus sûres et conviviales pour l'authentification multi-facteurs.

Contrairement aux mots de passe traditionnels, les passkeys utilisent des identifiants cryptographiques stockés en toute sécurité sur un appareil de l'utilisateur et peuvent être combinés avec des méthodes d'authentification de l'appareil telles que l'authentification biométrique ou les codes PIN de l'appareil.

Cela réduit les risques associés aux mots de passe faibles, à la réutilisation de mots de passe et aux attaques par hameçonnage. Les passkeys sont facultatives, permettant aux organisations de choisir l'approche qui correspond le mieux à leurs politiques de sécurité et aux besoins des utilisateurs.

Administration contrôlée par niveaux d'autorisations

L'accès administratif au sein de Paxton Solo est contrôlé par des niveaux d'autorisation dans l'application. Cela permet aux organisations d'attribuer aux utilisateurs uniquement l'accès dont ils ont besoin pour leur rôle.

Par exemple, certains utilisateurs ne peuvent gérer que l'administration quotidienne, tandis que d'autres peuvent configurer les paramètres du système ou des appareils.

En limitant l'accès en fonction des responsabilités, les organisations peuvent réduire le risque de modifications accidentelles et maintenir un contrôle plus clair sur l'administration du système.

Accès aux portes géré par niveaux d'accès personnalisables

Paxton Solo permet aux organisations de contrôler qui peut accéder à des portes spécifiques et quand.

Les niveaux d'accès personnalisables permettent de définir des autorisations basées sur les utilisateurs, les équipes, les emplacements, les horaires ou les exigences opérationnelles. Cela donne aux organisations la flexibilité nécessaire pour s'adapter à différents modes de travail tout en maintenant un contrôle sécurisé des points d'accès.

Les changements d'autorisations d'accès peuvent être gérés de manière centralisée, aidant à s'assurer que les droits d'accès restent alignés avec les besoins de l'entreprise.

Sécurité qui soutient l'utilisation quotidienne

Paxton Solo combine des pratiques de sécurité modernes avec une exploitation quotidienne simplifiée.

En sécurisant la communication téléphone-contrôleur, en protégeant les identifiants, en séparant le matériel des réseaux sur site, en contrôlant l'administration, et en permettant une gestion flexible de l'accès, le système est conçu pour aider les organisations à gérer l'accès en toute confiance.

Identifiants de sécurité

Les contrôles de sécurité de Paxton Solo sont soutenus par des évaluations indépendantes reconnues en cybersécurité.

Niveau 2 d'Assurance Cyber IoT de l'IASME

Paxton Solo a obtenu l'accréditation Niveau 2 d'Assurance Cyber IoT de l'IASME.

Cette certification est spécifiquement conçue pour les produits connectés et évalue si des contrôles de sécurité ont été mis en œuvre et vérifiés de manière indépendante. Elle couvre des domaines tels que les pratiques de développement sécurisées, la protection des appareils, la gestion des vulnérabilités, le traitement des données, et les processus de sécurité en cours.

Le niveau 2 inclut une évaluation technique indépendante pour fournir une confiance supplémentaire quant à la bonne opération des mesures de sécurité.

Pour les utilisateurs finaux, cela offre l'assurance que la sécurité a été prise en compte à la fois dans la conception du produit et dans sa gestion continue.

UL Cybersecurity Diamond Rating

Paxton Solo a également obtenu la UL Cybersecurity Diamond rating.

Cette notation reconnaît les produits démontrant une approche large et mature de la cybersécurité dans plusieurs domaines, y compris les contrôles de sécurité des produits, les processus logiciels, la gestion des vulnérabilités et la gestion du cycle de vie.

Le niveau Diamant représente le niveau le plus élevé au sein du programme et reflète un engagement à construire et maintenir des produits connectés sécurisés.

Pour les organisations sélectionnant une solution de contrôle d'accès, l'accréditation indépendante offre une assurance supplémentaire que les mesures de sécurité ont été examinées selon les normes reconnues de l'industrie.

Secured by Design (SBD)

Paxton Solo est également accrédité dans le cadre du programme Secured by Design, l'initiative officielle de sécurité de la police britannique gérée par le College of Policing du Royaume-Uni.

Cette accréditation Secured by Design (SBD) reconnaît les produits qui répondent à des normes et exigences de sécurité reconnues, conçues pour contribuer à réduire la criminalité et à renforcer la sécurité. Pour les organisations qui sélectionnent une solution de contrôle d'accès, elle offre une assurance supplémentaire que la sécurité a été évaluée de manière indépendante selon les normes établies par l'industrie et les services de police.