

Paxton Solo – Säkerhetsöversikt

Allmänt

Paxton Solo är utformat för att göra passerkontroll enkel att använda samtidigt som stark säkerhet upprätthålls i hela systemet. Säkerhet är inbyggd i varje steg av kommunikation och administration från användarens telefon till dörrkontrollen och in i de molntjänster som stödjer systemet.

Detta dokument ger en översikt över de viktigaste säkerhetsåtgärderna som ingår i Paxton Solo.

Kommunikation mellan telefon och kontroller

Paxton Solo använder Bluetooth Low Energy (BLE) för kommunikation direkt mellan användarens telefon och Solo Controller.

För att skydda denna uppkoppling använder både kontrollern och mobiltelefonen säker hårdvara och säkra processer som är utformade för att förhindra att legitimation kopieras eller avlyssnas.

Ett säkert element inom kontrollern ger en skyddad miljö för lagring av känslig säkerhetsinformation. På stödda mobila enheter säkerställer inbyggda säkerhetsfunktioner i telefonen liknande skydd för digitala legitimationer.

Detta innebär att åtkomstinformation inte lagras eller byts öppet på ett sätt som lätt kan extraheras, klonas eller återanvändas av obehöriga användare. Eftersom kommunikationen sker direkt mellan telefonen och Solo Controller, behöver Solo-hårdvaran inte vara ansluten till kundens lokala nätverk under normal drift.

Asymmetrisk kryptografi

Kommunikation mellan Paxton Solo-mobilappen och Solo Controller skyddas med asymmetrisk kryptografi.

Enkelt uttryckt innebär detta att systemet använder ett par digitala nycklar, en offentlig och en privat. Dessa nycklar samarbetar för att bekräfta identitet och skydda information under kommunikation.

Eftersom den privata nyckeln aldrig delas, kan systemet verifiera att båda enheterna är äkta utan att avslöja känslig information. Detta tillvägagångssätt minskar risken för att legitimation kopieras, attacker med återspelning och att obehöriga enheter försöker få åtkomst.

Varje interaktion är utformad för att bekräfta att telefonen och Solo Controller är betrodda innan åtkomst beviljas, utan att kräva att Solo Controller kommunicerar över kundens lokala nätverk.

Kommunikation mellan telefon och moln

Paxton Solo-hårdvaran ansluter inte direkt till kundens nätverk eller internet. När molnkommunikation krävs fungerar användarens mobilapp som kommunikationslänk till Paxtons molntjänster.

Kommunikation mellan appen och molntjänsterna sker över standard-HTTPS-anslutningar med port 443 och skyddas med SSL/TLS-kryptering.

Detta tillvägagångssätt minskar nätverkskomplexiteten på plats, undviker att öppna inkommande anslutningar i kundens infrastruktur och håller kommunikationen inom vanlig säker internettrafik. Data som överförs mellan appen och molntjänsterna skyddas under transport och stöder säker hantering av användare och behörigheter.

Säker inloggning med passkeys (valfritt)

Användarinloggning kan skyddas med passkeys, som är allmänt erkända som en av de starkaste och mest användarvänliga metoderna för multifaktorsautentisering.

Till skillnad från traditionella lösenord använder passkeys kryptografiska legitimationer som lagras säkert på användarens enhet och kan kombineras med enhetsautentiseringsmetoder som biometri eller enhetens PIN-koder.

Detta minskar riskerna med svaga lösenord, återanvändning av lösenord och nätfiskeattacker. Passkeys är valfria, vilket möjliggör för organisationer att välja det tillvägagångssätt som bäst passar deras säkerhetspolicyer och användarkrav.

Kontrollerad administration genom behörighetsnivåer

Administrativ åtkomst i Paxton Solo styrs genom appens behörighetsnivåer. Detta gör det möjligt för organisationer att endast tilldela användare den åtkomst som de behöver för sin roll.

Till exempel kan vissa användare endast hantera den dagliga administrationen, medan andra kan konfigurera systeminställningar eller enhetsinställningar.

Genom att begränsa åtkomsten utifrån ansvar kan organisationer minska risken för oavsiktliga förändringar och bibehålla tydligare kontroll över systemadministrationen.

Dörråtkomst hanteras genom anpassningsbara åtkomstnivåer

Paxton Solo gör det möjligt för organisationer att styra vem som kan få åtkomst till specifika dörrar och när.

Anpassningsbara åtkomstnivåer gör det möjligt att definiera behörigheter baserat på användare, team, plats, tidsscheman eller operativa behov. Detta ger organisationer flexibilitet att stödja olika arbetsmönster samtidigt som de bibehåller säker kontroll över åtkomstpunkter.

Förändringar av åtkomstbehörigheter kan hanteras centralt, vilket hjälper till att säkerställa att åtkomsträttigheter förblir i linje med affärsbehov.

Säkerhet som stöder vardaglig användning

Paxton Solo kombinerar moderna säkerhetspraxis med enkel daglig drift.

Genom att säkra kommunikation från telefon till kontroller, skydda legitimationer, separera hårdvara från lokala nätverk, kontrollera administration och möjliggöra flexibel åtkomsthantering är systemet utformat för att hjälpa organisationer att hantera åtkomst med förtroende.

Säkerhetslegitimation

Paxton Solo-säkerhetskontroller stöds av erkända oberoende cybersäkerhetsbedömningar.

IASME IoT Cyber Assurance Level 2

Paxton Solo har uppnått IASME IoT Cyber Assurance Level 2-ackreditering.

Denna certifiering är specifikt utformad för anslutna produkter och bedömer om säkerhetskontroller har implementerats och verifierats oberoende. Det täcker områden som säker utvecklingspraxis, enhetsskydd, sårbarhetshantering, datahantering och pågående säkerhetsprocesser.

Nivå 2 inkluderar oberoende teknisk bedömning för att ge ytterligare förtroende för att säkerhetsåtgärder fungerar som avsett.

För slutanvändare erbjuder detta trygghet att säkerhet har beaktats som en del av både produktdesign och löpande produktförvaltning.

UL Cybersecurity Diamond Rating

Paxton Solo har också uppnått UL Cybersecurity Diamond rating.

Denna klassificering erkänner produkter som visar ett brett och moget förhållningssätt till cybersäkerhet inom flera områden, inklusive produktsäkerhetskontroller, mjukvaruprocessteg, sårbarhetshantering och livscykelhantering.

Diamantnivån representerar den högsta nivån inom programmet och speglar ett åtagande att bygga och upprätthålla säkra anslutna produkter.

För organisationer som väljer en passerkontrollösning ger oberoende ackreditering ytterligare säkerhet att säkerhetsåtgärder har granskats mot erkända branschstandarder.

Secured by Design (SBD)

Paxton Solo är också ackrediterat under Secured by Design-programmet, det officiella polisiära säkerhetsinitiativet som ägs av Storbritanniens College of Policing.

Secured by Design (SBD) ackreditering erkänner produkter som uppfyller erkända säkerhetsstandarder och krav som är utformade för att hjälpa till att minska brott och förbättra säkerheten. För organisationer som väljer en passerkontrollösning ger detta ytterligare säkerhet att säkerheten har bedömts oberoende mot etablerade bransch- och polisiära standarder.