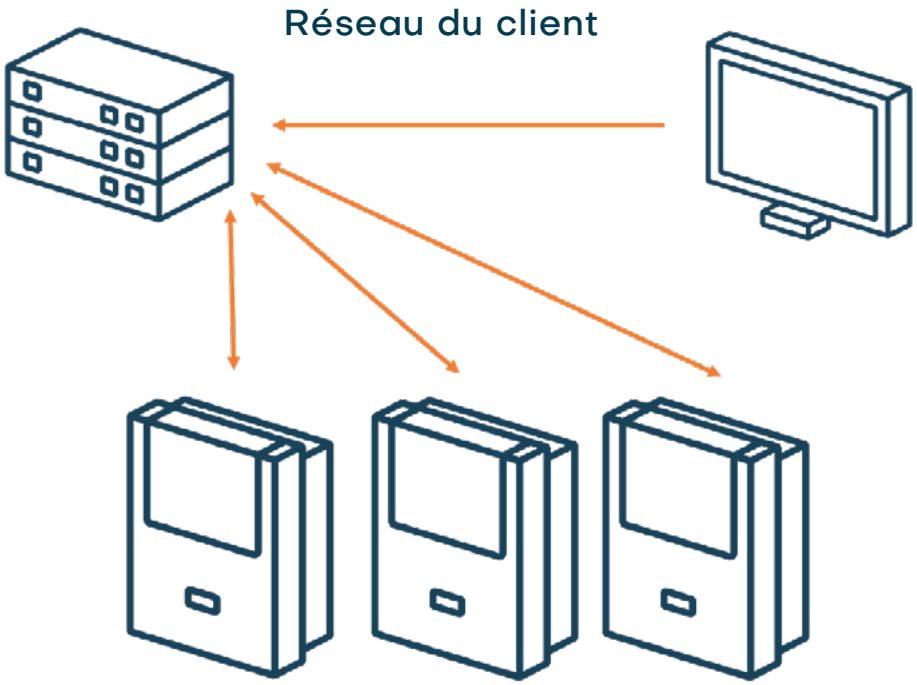
Solution avec serveur local ou dans le Cloud ?

Quelle est la meilleure solution pour le contrôle d'accès physique ?

Aujourd'hui, il existe de nombreuses solutions différentes pour le contrôle d'accès physique. La plupart sont proposées sous forme de solution locale, mais de plus en plus de solutions sont maintenant proposées sous forme de service ou de solution native basée sur le cloud.

La confusion autour des distinctions entre ces modèles est fréquente. Par conséquent, dans ce livre blanc, nous allons examiner en détail les trois principaux modèles disponibles, en mettant en évidence les avantages et les inconvénients de chacun.



Solutions sur site

Un système de contrôle d'accès physique local implique l'installation de logiciels sur les serveurs du client et une gestion interne du système. Cela permet une personnalisation et un contrôle accrus, mais nécessite également des ressources et une expertise plus importantes pour assurer la maintenance.

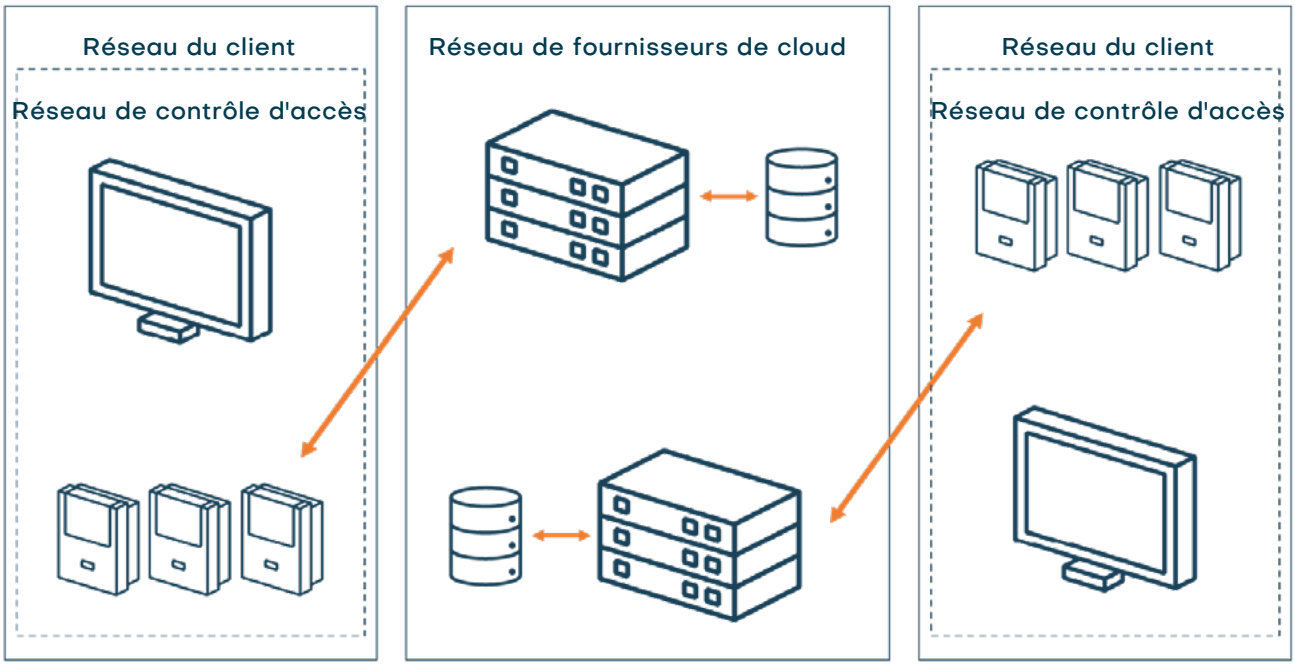
Toutes les communications entre le serveur, les contrôleurs et les clients restent internes, sans connexion vers l'extérieur.

Dans ce cas de figure, le serveur de contrôle d'accès est souvent une application monolithique unique avec une grande base de données connectée pour le stockage.

Les différents éléments de cette solution sont étroitement interconnectés, tous les processus étant gérés par le même code source. Ainsi, pour mettre à jour le système, il est nécessaire de mettre à jour l'ensemble du code source.

Le principal avantage d'une application monolithique sur site avec une base de données unique est la facilité de développement et la cohérence de l'accès aux données et de la logique métier ; comme tout est centralisé en un seul endroit.

Cependant, à mesure que l'application devient plus grande et complexe, la mise à l'échelle et la maintenance deviennent plus compliquées.



Solutions en pseudo-Cloud

Pour les produits de contrôle d'accès pseudo-cloud, une solution locale est installée dans un environnement cloud et est hébergée séparément pour chaque client. Cela convient aux clients qui ont besoin de flexibilité et de commodité, car la plus grosse partie de l'installation et de la maintenance est prise en charge par le fournisseur de la solution, qui s'occupe également des mises à jour et des sauvegardes. Cependant, étant donné que le fournisseur est responsable de la maintenance de toutes les installations, ainsi que de l'infrastructure réseau et des connexions avec les clients, cela peut être un défi.

L'architecture d'une solution pseudo-cloud est quasiment identique à celle d'une solution sur site - le fournisseur installe simplement la même solution, mais dans un environnement cloud. Cela signifie que chaque client dispose de sa propre installation autonome, avec sa propre base de données. La mise à jour d'une telle solution implique la réinstallation du logiciel pour chaque client, ce qui peut être long et fastidieux..

Solutions basées sur le cloud

Les produits conçus pour le cloud sont hébergés et gérés par un fournisseur de services tiers, ce qui permet aux clients d'accéder à la solution de contrôle d'accès physique via Internet. Cette approche est rentable et évolutive, car le fournisseur prend en charge l'infrastructure, la maintenance et les mises à jour, et le système peut être accessible de n'importe où avec une connexion Internet. Un autre avantage est la possibilité d'intégrer la solution cloud avec d'autres technologies natives du cloud telles que les systèmes RH, les systèmes de gestion des visiteurs et d'autres services liés à la sécurité. Une solution native du cloud s'appuie fortement sur des contrôleurs sur site pour garantir la continuité des activités en cas de panne réseau.

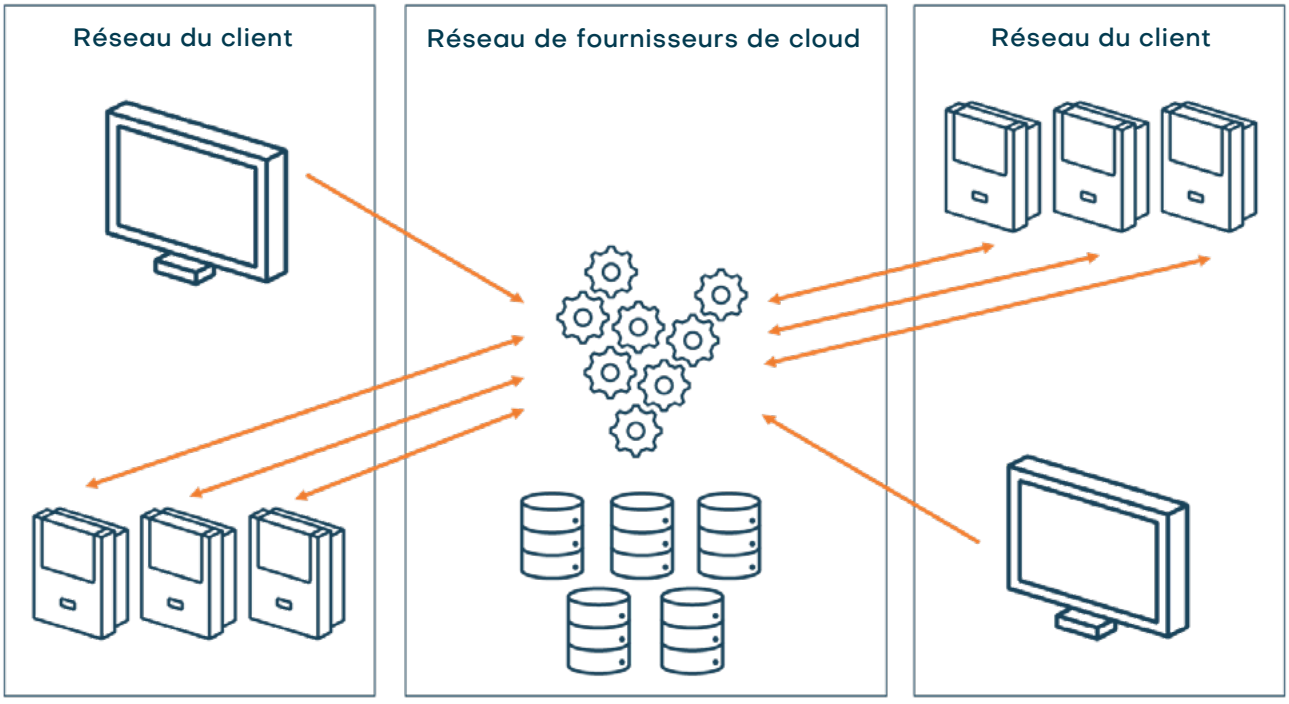
En règle générale, l'architecture des solutions natives du cloud repose sur l'utilisation de microservices, où les processus sont fragmentés en petits services autonomes, chacun pouvant être déployé indépendamment. Ces services interagissent entre eux via des interfaces clairement définies.

Avec cette méthode, chaque client tire parti des mêmes ressources et infrastructures, ce qui simplifie la mise à jour autonome des services sans provoquer d'interruption. De plus, les services sont généralement élaborés de manière à s'adapter aisément aux exigences changeantes. Par exemple, vous pouvez avoir une instance d'un service en fonctionnement pendant les heures de bureau classiques, puis augmenter le nombre d'instances le reste du temps.

Cette architecture propose trois alternatives pour le stockage des données. La première implique la création d'un nouveau serveur de base de données pour chaque client, de manière similaire à une solution sur site. Bien que cette méthode assure l'isolement des données entre les clients, elle peut poser des défis en termes de maintenance et de mise à l'échelle en raison de la nécessité de dédier des ressources spécifiques à chaque client.

La deuxième possibilité consiste à utiliser un schéma de base de données distinct pour chaque client sur le même serveur. Cette approche offre toujours une certaine séparation des données, mais elle permet au fournisseur de ne maintenir qu'un seul serveur.

La troisième option regroupe toutes le données dans une seule base de données, simplifiant ainsi la liaison des données et la mise à jour globale. Cependant, cette option comporte le risque qu'un client puisse accéder aux données d'un autre client, ce qui pourrait avoir des conséquences graves. Atténuer ce risque peut s'avérer complexe.



Quels sont les avantages et les inconvénients de chaque approche ?

Ces trois solutions présentent des variations en termes de degré de contrôle, de capacité de mise à l'échelle et d'entretien requis. Par conséquent, il est crucial pour les entreprises d'examiner attentivement les options disponibles et de choisir celle qui correspond le mieux à leurs besoins.

Les systèmes de contrôle d'accès physique sur site sont installés et gérés localement. Les clients ont la possibilité d'exercer un contrôle total sur leur système et leurs données, de personnaliser le système pour répondre à leurs besoins spécifiques, et de déterminer comment les données sont stockées et traitées. Cette option convient aux entreprises qui exigent un niveau élevé de contrôle.

Les systèmes sur site nécessitent en effet davantage de ressources et d'infrastructures à gérer, ce qui entraîne des coûts d'exploitation élevés. En raison de leur conception principalement monolithique, les adapter à l'évolution des besoins de l'entreprise, que ce soit pour les mettre à l'échelle ou les mettre à jour, peut s'avérer complexe.

Les solutions pseudo-cloud intègrent certaines fonctionnalités propres aux systèmes natifs du cloud, mais requièrent toujours la même infrastructure et les mêmes ressources que les solutions sur site. Elles peuvent être une option intéressante pour les entreprises désireuses de profiter de certains avantages des systèmes natifs du cloud, tels que l'accès à distance et l'allégement de la charge de travail, sans pour autant être prêtes à effectuer une transition complète vers une solution nativement cloud. Les solutions pseudo-cloud offrent davantage de souplesse en matière de personnalisation et de contrôle par rapport aux systèmes natifs du cloud. Cependant, étant donné que leur architecture ressemble à celle des solutions sur site, la mise à jour et la mise à l'échelle peuvent encore représenter un défi pour le fournisseur.

Les systèmes de contrôle d'accès physique natifs du cloud sont gérés et entretenus par un prestataire tiers, ce qui offre une évolutivité et une flexibilité accrues. Ils peuvent être accessibles et administrés depuis n'importe quel endroit disposant d'une connexion Internet, offrant ainsi une plus grande commodité et simplicité d'utilisation. Du fait que ces systèmes natifs du cloud reposent sur des technologies et des architectures modernes, il est également plus aisé d'ajuster les ressources en fonction des besoins des clients. Cependant, les clients doivent accorder leur confiance à l'expertise du fournisseur et compter sur lui pour la maintenance et la sécurité, ce qui implique une perte de contrôle direct pour les clients.

Lorsque vous optez pour une solution native du cloud, il est essentiel de prendre en compte la protection de la vie privée et la sécurité des données, car le fournisseur a un contrôle total sur ces éléments. La manière dont les données sont stockées, par exemple, peut varier considérablement. Il est également important de vérifier où les données sont stockées et si des procédures de sauvegarde et/ou de redondance efficaces sont en place. Étant donné que le client n'a pas le contrôle direct, il dépendra de l'expertise et de la maturité du fournisseur et de son infrastructure.

Les exigences en matière de maintenance diffèrent également en fonction du type de solution. Les systèmes de contrôle d'accès physique sur site nécessitent du personnel informatique dédié pour les entretenir et les mettre à jour, ce qui peut être coûteux. En revanche, les systèmes de contrôle d'accès physique pseudo-cloud et natifs du cloud sont gérés et entretenus par le fournisseur tiers, ce qui peut être un avantage pour les entreprises qui ne disposent pas des ressources ou de l'expertise nécessaires pour gérer leur propre système.

Qu'est-ce qui est le mieux pour vos clients ?

Le choix du système de contrôle d'accès physique le plus adapté à une entreprise nécessite une réflexion approfondie sur les options disponibles, ainsi que sur les besoins spécifiques, les ressources disponibles et les préférences de l'organisation concernée. Le processus de prise de décision doit inclure une évaluation des avantages et des inconvénients de chaque option, la prise en compte des exigences en matière de mise à l'échelle et de maintenance, et la détermination du niveau de contrôle souhaité par l'entreprise sur son système de sécurité et ses données.

De plus, il est essentiel que les entreprises accordent une attention particulière à la sécurité, car la protection des employés, des visiteurs et des actifs constitue une priorité absolue.

À propos de Nedap

Pour nous, la sécurité ne se limite pas uniquement à la technologie. Elle englobe les individus et leur mode de vie au quotidien. Elle vise à satisfaire leur besoin fondamental de sécurité, afin qu'ils se sentent en confiance pour profiter pleinement de la vie et du travail. En réalité, une véritable sécurité se traduit par l'absence de préoccupation à ce sujet.

Nedap France

8 chemin d'Andrésy
95610 Eragny sur Oise

contact.ca@nedap.fr
01 61 03 03 01