voicepoint | CLOUD

Voicepoint Cloud

Security Factsheet

Dictée intelligente, basée sur le cloud

Voicepoint Cloud offre une solution sûre, basée sur le cloud, de gestion de dictée et de reconnaissance vocale, qui permet aux médecins et aux avocats de documenter l'historique des patients et les cas juridiques par la voix. Il n'est pas nécessaire de mettre en place et d'exploiter une infrastructure interne, car les applications sont directement prêtes à être utilisées immédiatement, ce qui permet de gagner du temps pour le personnel informatique et d'accroître la productivité et l'efficacité du corps médical et du corps juridique. Vous trouverez de plus amples informations sur notre Voicepoint Cloud dans notre Factsheet Voicepoint Cloud ou sur notre Site web.

Fournisseur de cloud Premium sécurisé

Voicepoint exploite ses solutions dans le centre de données suisse Microsoft Azure et a été étroitement soutenu par les spécialistes de Microsoft pendant la conception, l'architecture et la mise en œuvre.

Les services Microsoft Azure requis par Voicepoint Cloud depuis le centre de données de Zürich et de Genève sont hautement disponibles et offrent des durées de fonctionnement constantes avec une très haute disponibilité.

Microsoft Azure répond à un large éventail de normes de conformité internationales et spécifiques à l'industrie. Vous pouvez trouver une présentation détaillée et des informations supplémentaires sur la Microsoft Compliance-Azure ici.

Certification ISO 27001

Les principales normes de l'industrie sont respectées par notre certification ISO 27001, constamment renouvelées et offrent un niveau de protection plus élevé pour la sécurité de l'information.

Une offre cloud sécurisée et solide

Nos pratiques en matière de sécurité, associées à notre infrastructure hautement disponible et redondante, garantissent que nos solutions performantes et sécurisées sont mises à la disposition des utilisateurs avec un maximum de confort, quel que soit le lieu.

Sécurité du centre de données

En plus de la sécurité de base du centre de données Microsoft Azure, Voicepoint applique de nombreuses Best Practices de l'industrie pour mieux protéger les données des clients et pour augmenter la sécurité globale des solutions proposées.

Accès physique : L'accès physique au centre de données est sécurisé par de nombreuses techniques de sécurité avancées. Les collaborateurs de Voicepoint n'ont pas d'accès physique aux centres de données Microsoft Azure, ce qui renforce encore la sécurité.

Accès électronique : Voicepoint adhère à l'exigence du « Minimum Need », lorsqu'elle accorde un accès électronique au centre de données à des fins de support.

Authentification multi-facteurs/Jumphost : Pour accéder au portail Microsoft Azure Management, une authentification multi-facteurs (MFA) est nécessaire, et disponible que pour certains collaborateurs sélectionnés. Les serveurs d'applications respectifs sont strictement protégés et ne permettent un accès indirect aux systèmes, que par l'intermédiaire de serveurs Jumphosts via un VPN spécial.

Patches et Updates : Les collaborateurs de Voicepoint autorisés pour l'infrastructure Cloud Voicepoint effectuent des mises à jour Windows mensuelles de l'environnement. Les mises à jour des applications utilisées ou de l'infrastructure sont réalisées indépendamment des mises à jour mensuelles et sont planifiées à l'avance. Les utilisateurs sont ainsi informés à l'avance des créneaux de maintenance planifiés. Voicepoint se réserve le droit d'effectuer des mises à jour urgentes de Windows et des mises à jour d'applications urgentes en dehors des créneaux de maintenance mensuels prévus afin d'augmenter encore la sécurité.

Cryptage de la transmission des données

La communication entre les applications Client utilisées et les services Voicepoint Cloud est cryptée à tout moment. Cela s'applique au flux de données audio pendant la reconnaissance vocale ainsi qu'à la transmission de toute donnée au sein des applications. Les données sont transmises via HTTPS en utilisant TLS 1.3 avec un algorithme de chiffrement AES 128/256 bits. Les anciens algorithmes ou versions TLS définis comme non sécurisés ont été désactivés.

Les normes de sécurité et les protocoles de transmission évoluent constamment en fonction des nouvelles menaces de sécurité. C'est pourquoi nous contrôlons régulièrement nos services pour nous assurer qu'ils répondent aux normes les plus strictes en matière de transmission sécurisée des données. Les applications web de Voicepoint Cloud reçoivent régulièrement la note « A+ » de Qualys SSL Labs, qui effectue une analyse approfondie des points de terminaison TLS. Le test vérifie, entre autres, la solidité des certificats, les versions du protocole TLS prises en charge, les chiffrements pris en charge et les vulnérabilités de la configuration.

Stockage des données et utilisation ultérieure

Les données de l'application sont stockées dans ce que l'on appelle des « Storage Accounts » qui ne sont pas accessibles via internet et qui sont cryptés et protégés contre tout accès non autorisé.

Les dictées du système de gestion des dictées « Winscribe » sont stockées sous forme cryptée et sont requises par les utilisateurs des applications Client pour la transcription des dictées. Dans Winscribe, les dictées sont conservées jusqu'à ce qu'elles soient transcrites. Les dictées sont ensuite supprimées dans un délai personnalisable.

Par défaut, les données de la solution de reconnaissance vocale « Dragon Medical One » sont conservées jusqu'à un total de 50 heures de dictée par utilisateur. Dès que cette limite est atteinte, les enregistrements les plus anciens sont automatiquement supprimés. Les données audio et textuelles reconnues de la solution de reconnaissance vocale sont utilisées pour le processus d'adaptation à des fins de comparaison. Cela inclut les corrections du texte effectuées par l'utilisateur. Le système utilise uniquement les données présentes dans le fichier audio et le texte pour effectuer des ajustements acoustiques et vocaux dans le profil vocal de l'utilisateur.

Ceux-ci contribuent à améliorer la qualité de la reconnaissance vocale. Par exemple, si un utilisateur en environnement médical dicte : <Le patient a des troubles du rythme cardiaque>, il n'y a pas d'informations audio stockées qui pourraient associer cette information à un patient individuel. La transmission des données via Internet est cryptée.

Haute disponibilité et continuité de service

Les services Microsoft Azure utilisés sont mis à disposition dans différentes zones de disponibilité (« Availability Zones »). Certains services plus anciens utilisent encore les « Availability Sets ». Cela permet d'atteindre une haute disponibilité, car un service est réparti dans plusieurs zones de disponibilité et peut donc se trouver dans différents sites et installations physiques. Chacune de ces zones est dotée de sa propre source d'alimentation et de réseau, ce qui réduit l'impact des pannes matérielles potentielles ou des perturbations du site. Les mises à jour de Microsoft Azure ne sont appliquées que dans une zone de disponibilité à la fois et n'affectent donc pas la disponibilité des services dans les autres zones.

L'architecture système de Voicepoint Cloud dans Microsoft Azure offre les caractéristiques de haute disponibilité suivantes sur l'ensemble des zones de disponibilité :

- Infrastructure réseau entièrement redondante, y compris Loadbalancer et Switches
- Plusieurs serveurs d'applications redondants
- Stockage de données hautement disponible et sécurisé
- Clusters de serveurs de base de données SQL redondants

Voicepoint s'engage à maintenir un haut niveau de continuité de service et à revoir, mettre à niveau et améliorer régulièrement la haute disponibilité selon les besoins.

Traiter le US CLOUD Act

Le CLOUD Act est une loi américaine qui permet aux autorités américaines d'accéder aux données stockées des entreprises américaines, même si ces données ne sont pas situées aux États-Unis. Pour de plus amples informations et sur la manière de traiter le US CLOUD Act, Voicepoint vous invite à lire cet article « US CLOUD Act : Pourquoi il ne devrait pas empêcher les projets cloud » de David Rosenthal, avocat et partenaire du cabinet d'avocats VISCHER AG.

Voicepoint fait également référence au « Microsoft Commitment Summary ». En avril 2023, Microsoft a complété ses « Online Service Terms » par un « Data Protection Addendum (DPA) ». Microsoft s›engage ainsi à respecter dans ses contrats les exigences de la loi suisse sur la protection des données, le secret professionnel et le secret de fonction concernant les produits et les services. De plus amples informations à ce sujet peuvent être fournies par Voicepoint sur demande.

Engagement suisse

En tant qu'entreprise suisse, Voicepoint AG intègre les valeurs suisses et prête également attention au facteur « Swiss-made » lors de la mise à disposition de ses services. Depuis l'introduction des centres de données suisses, la succursale suisse de Microsoft (Microsoft Schweiz GmbH) peut également compter parmi les hébergeurs suisses, ce qui signifie que Voicepoint peut continuer à proposer le facteur « Swiss made ». En tant que fournisseur de solutions suisse, Voicepoint assure l'installation, la maintenance et le support de manière indépendante, sans influence directe ni accès de tiers.

Présentation de la sécurité des données Microsoft Azure

Sécurité du réseau

Des Firewalls conformes aux normes industrielles sont-ils déployés ? Où sont-ils déployés ? Comment sont-ils maintenus à jour ? L'accès administratif au Firewall et aux autres dispositifs n'est-il autorisé que par des canaux sécurisés ou un accès direct ?	Voicepoint utilise des VMs Linux redondantes et ininterrompues de la société loadbalancer.org avec un Firewall intégré. Les VMs sont exploitées au sein du centre de données Microsoft Azure dans un « Availability Set », dont les mises à jour logicielles et les directives de sécurité sont entièrement automatisées. Ces VMs Loadbalancer sont le pivot de la connexion entre l'accès externe et les réseaux internes au Cloud. Une interface web avec authentification séparée est disponible pour l'administration, à laquelle le personnel autorisé ne peut accéder que via une connexion VPN sécurisée par MFA.
Quels protocoles et ports sont autorisés pour la communication ?	Toutes les applications Client et les applications pour smartphone transmettent les données via le port HTTPS 443, sécurisé par TLS 1.3 avec un cryptage AES 128/256 bits.
Existe-t-il des procédures formelles pour répondre aux incidents ? Sont-ils testés régulièrement ?	Les procédures relatives aux incidents sont mises en œuvre et comprennent des procédures spécifiques de classification de la gravité et de traitement des incidents concernant la disponibilité ou la sécurité des solutions.

Sécurité physique

Quelles sont les caractéristiques de sécurité physique et de Business-Continuity de votre centre de données ?	Le Datacenter Microsoft Azure propose de nombreuses mesures de sécurité électroniques et physiques. Notre configuration de Datacenter est préparée avec des « Availability Sets », ce qui garantit une disponibilité constamment élevée du matériel.
Qui a un accès physique aux serveurs (y compris les collaborateurs du Datacenter, les collaborateurs Voicepoint ou les fournisseurs) ?	Seul le personnel autorisé a accès à l'installation physique, qui est strictement limitée et contrôlée régulièrement.

Sécurité du système

Les autorisations de fichiers sont-elles définies uniquement sur la base du « Minimum Need » ?	L'accès aux fichiers est conçu sur la base d'un « Minimum Need » et est limité aux comptes de service concernés et aux collaborateurs autorisés qui ont besoin d'y accéder.
Tous les systèmes qui stockent ou traitent des informations critiques sont-ils dotés de Logs d'audit ? Les commandes Root sont-elles enregistrées ? Quels sont les processus utilisés pour contrôler l'accès aux appareils et aux proto-coles ?	Toutes les applications utilisées contiennent des mécanismes d'enregistrement Log ou Audit indépendants. La journalisation du système s'effectue via l'affichage d'événements Windows, qui permet l'enregistrement d'événements de sécurité, de système et d'application. Les accès sont contrôlés régulièrement et adaptés en cas de besoin. De plus, les accès et les modifications sont enregistrés dans le portail Microsoft Azure.
Comment l'intégrité et la disponibilité des services et du serveur d'applications sont-elles surveillées ?	La surveillance du système est en place et utilise des outils développés en interne et conformes aux normes industrielles. Les services spécifiques à Microsoft Azure sont notamment utilisés pour les alertes et la surveillance.
Les services et applications inutiles ont-ils été désactivés sur les serveurs d'applications ?	Oui, seuls les services et applications nécessaires sont installés et exploités sur les serveurs.
D'autres mécanismes de sécurité sont-ils utilisés ?	Oui, Microsoft Azure Security Center est également utilisé pour la sécurité globale de l'infrastructure, qui vérifie les dernières connaissances en matière de sécurité et mesures de sécurité et évalue la gravité de la situation. Celles-ci sont régulièrement vérifiées par Voicepoint et appliquées si nécessaire. Windows Defender, qui agit comme un antivirus et envoie des commentaires à Microsoft Azure Defender, est également disponible sur les serveurs d'applications.

Sécurité du web

Des modules ou extensions HTTP inutiles ont-ils été désactivés sur les serveurs d'applications ?	Oui, seuls les modules et extensions HTTP requis sont utilisés sur nos serveurs d'applications.
Le compte sous lequel les services web sont exécutés a-t-il des droits d'administrateur sur les serveurs d'applications ?	Un compte de service distinct est disponible pour chaque application proposée. Chaque service web fonctionne donc sous son propre compte de service. Les droits du compte de service sont réduits au minimum nécessaire.
Les versions et les chiffrements TLS non sécurisés ont-ils été désactivés ?	Oui, les versions TLS (<TLS 1.3) et les chiffrements plus anciens et non sécurisés ont été désactivés sur les serveurs d'application ainsi que sur l'ensemble de l'environnement. Les nouvelles versions de chiffrement ou de TLS non sécurisées sont régulièrement vérifiées avec l'aide de Qualys SSL Labs et désactivées si nécessaire.

Sécurité des personnes autorisées

Comment sont traitées les données d'inscription des personnes autorisées ?	Chaque collaborateur Voicepoint autorisé utilise un utilisateur personnel, protégé par un code d'authentification (MFA), pour l'ensemble du système. Les collaborateurs sont répartis entre différents rôles administratifs. Les collaborateurs autorisés à assurer un soutien purement applicatif n'ont pas d'accès direct aux serveurs d'applications individuels ou aux composants de l'infrastructure. Un concept spécial « Joiners-Movers-Leavers » est en place et appliqué. Voicepoint peut ainsi garantir que seuls les collaborateurs autorisés peuvent accéder aux services mis à leur disposition. Le rôle de l'administrateur système est réduit au minimum afin que les opérations puissent être garanties en cas d'absence des collaborateurs.

Sécurité des applications

Les données sont-elles cryptées lorsqu'elles sont transmises via des connexions de réseau public ?	Toutes les communications entre les applications Client et les services Voicepoint Cloud sont transmises par HTTPS, sécurisé par TLS 1.3 avec un cryptage AES 128/256 bits.
Des données sont-elles stockées localement sur l'appareil ou l'ordinateur (gestion des dictées) ?	Lors de l'utilisation des applications Client pour la solution de gestion de dictée, des dossiers pour les paramètres spécifiques à l'application et les fichiers journaux sont créés dans les données d'application locales de l'utilisateur. Un « UserWorkingDirectory » est également utilisé pour le stockage intermédiaire, l'accès temporaire aux données du serveur et aux projets de dictée, qui peuvent être configurés localement pour chaque utilisateur ou sur un emplacement de stockage central pour le client en standard. Les dictées originales des appareils de dictée mobiles sont stockées localement chez le client après le téléchargement jusqu'à ce qu'elles soient supprimées par le cycle d'archivage automatique. Une sauvegarde des données souhaitée de ces fichiers est de la responsabilité du client.
Des données sont-elles stockées localement sur le smartphone ?	Lors de l'utilisation de l'application smartphone pour la solution de gestion de dictée, les données de dictée temporaires sont enregistrées sur l'appareil. Les fichiers audio sont cryptés avec une clé de sécurité générée automatiquement sur le smartphone. De plus amples informations concernant la sécurité dans l'application Winscribe Professional Smartphone peuvent être fournies sur demande. Aucune donnée de dictée n'est enregistrée avec la solution pour smartphone PowerMic Mobile, car cette application ne sert qu'à remplacer le microphone.
Des données sont-elles stockées localement sur l'appareil ou l'ordinateur (reconnaissance vocale) ?	Les clients de reconnaissance vocale concernés transmettent les données audio en temps réel à l'environnement sécurisé du serveur pour le traitement de la reconnaissance vocale. La conservation du texte reconnu renvoyé par le serveur de reconnaissance vocale relève de la responsabilité de l'application cible et de l'utilisateur.

Informations complémentaires

Vous trouverez de plus amples informations sur Voicepoint Cloud sur notre Site web. L'équipe Voicepoint se tient à votre entière disposition via le Formulaire de contact ou par tél. au 022 994 39 99 pour vous conseiller.

Version : septembre 2023