voicepoint | CLOUD

Voicepoint Cloud

Security Factsheet

Intelligent, cloud-based dictation

Voicepoint Cloud offers a secure, cloud-based dictation management and speech recognition solution that enables doctors and lawyers to record patient histories and legal cases using their voice. Minimal time and effort is required to implement and run your own infrastructure and the applications are ready to use immediately, which saves time for IT staff and increases the productivity and efficiency of medical and legal staff. For more information including the advantages and disadvantages of the Voicepoint Cloud, please consult our Voicepoint Cloud factsheet or visit our website.

Secure premium cloud provider

Voicepoint operates its solutions in the Swiss data center of Microsoft Azure and was closely supported by Microsoft specialists during the conception, architecture, and implementation phases.

The Microsoft Azure services required by the Voicepoint Cloud in the Zurich data center are highly available, providing consistent uptime with very high availability.

Microsoft Azure complies with a wide range of international and industry-specific compliance standards. For a detailed overview and further information on Microsoft Azure compliance, you can find it here.

ISO 27001 Certification

Our ISO 27001 certification ensures compliance with the most important industry standards, continuously renewed, and provides a higher level of protection for information security.

Secure and robust cloud offering

Our security practices, in combination with our highly available and redundant infrastructure, ensure that users have access to our high-performance, secure solutions with maximum convenience and location independence.

Datacenter security

Voicepoint also applies many industry-standard best practices to further protect customer data and to increase the security of the solutions as a whole.

Physical access: Physical access to the datacenter is secured using numerous advanced security technologies. Voicepoint staff have no physical access to Microsoft Azure's datacenters, increasing security even further.

Electronic access: Voicepoint adheres to the "minimum need" requirement when granting electronic access to the datacenter for support purposes.

Multi-factor authentication / jump host: Multi-factor authentication (MFA), which is only available to selected employees, is required to access the Microsoft Azure management portal. The application servers are strictly protected, enabling indirect access to the systems by jump hosts via a special VPN.

Patches and updates: Voicepoint staff entitled to use the Voicepoint Cloud infrastructure perform Windows Updates on a monthly basis. Updates to applications or the infrastructure are performed independently of monthly updates and are planned in advance. As a result, users are informed about maintenance windows in good time. Voicepoint reserves the right to perform urgent Windows Updates and urgent application updates outside of the planned monthly maintenance window in order to increase security even further.

Encryption of data transmission

All communication between client applications and Voicepoint Cloud services is encrypted at all times. This applies to the steaming of audio data during speech recognition as well as the transmission of any data within applications. Data is transmitted via HTTPS using TLS 1.3 with an AES 128/256-bit cipher algorithm. Older algorithms and TLS versions that are defined as insecure have been disabled.

Security standards and transmission protocols are constantly undergoing development in response to new security threats. For this reason, we review our services on a regular basis to ensure they meet the highest standards for secure transmission. Voicepoint Cloud's web-based applications are routinely awarded an "A+" rating from Qualys SSL Labs, which performs a detailed analysis of TLS endpoints. Besides other things, the test checks the strength of certificates, supported TLS protocol versions, supported ciphers and weak points in the configuration.

Data storage and subsequent use

The application data is stored in so-called «Storage Accounts» that are not accessible via the internet and are encrypted to protect against unauthorized access.

Dictations from the dictation management system «Winscribe» are stored in encrypted form and are required by users of the client applications for transcription. In Winscribe, dictations are retained until they have been transcribed, after which they are deleted within a customizable timeframe.

By default, data from the speech recognition solution «Dragon Medical One» is retained for a total duration of up to 50 dictation hours per user. Once this limit is reached, the oldest recordings are automatically deleted. The recognized audio and text data from the speech recognition solution are used for the adaptation process to align with the user. This includes text corrections made by the user. The system only uses data present in the audio file and text to make acoustic and linguistic adjustments to the user›s speech profile.

This contributes to the improvement of speech recognition quality. For example, when a medical user dictates, «The patient has arrhythmias,» there are no stored audio data that could link this information to a specific patient. The transfer of data over the internet is encrypted.

High availability and service continuity

The utilized Microsoft Azure services are deployed in different Availability Zones. Some older services still make use of Availability Sets. This enables achieving high availability, as a service is distributed across multiple Availability Zones, which means it can be located in different physical locations and facilities. Each of these zones is equipped with its own power and network source, reducing the impact of potential hardware failures or site disruptions. Updates to Microsoft Azure are applied in one Availability Zone at a time, thus not affecting the availability of services in other zones.

The system architecture of the Voicepoint Cloud in Microsoft Azure offers the following high availability features across Availability Zones:

- Fully redundant network infrastructure, including load balancers and switches.
- Multiple redundant application servers.
- Highly available and secure data storage.
- Redundant SQL database server clusters.

Voicepoint is committed to maintaining service continuity and regularly reviewing and enhancing high availability as needed.

The US CLOUD Act

The CLOUD Act is an American law that grants U.S. authorities access to stored data held by American companies, even if that data is not located within the United States. For further information and guidance on dealing with the U.S. CLOUD Act, Voicepoint refers you to the article «US CLOUD Act: Why It Shouldn›t Hinder Cloud Projects» by David Rosenthal, an attorney and partner at the VISCHER AG law firm.

Furthermore, Voicepoint also highlights the «Microsoft Commitment Summary.» Microsoft expanded its «Online Service Terms» in April 2023 with a «Data Protection Addendum (DPA).» Microsoft commits to complying with the requirements of the Swiss Data Protection Act, professional secrecy, and official secrecy in its contracts for products and services. Additional information on this matter can be provided by Voicepoint upon request.

Swiss commitment

As a Swiss company, Voicepoint AG embraces Swiss values and pays attention to the «swiss-made» factor in the provision of its services. Since the introduction of Swiss data centers, the Swiss branch of Microsoft (Microsoft Schweiz GmbH) can also be considered one of the Swiss hosting providers, allowing Voicepoint to continue offering the «swiss-made» factor. As a Swiss solutions provider, Voicepoint independently handles the installation, maintenance, and support without direct influence and access from third parties.

Overview of Microsoft Azure's data security

Network security

Are industry-standard firewalls deployed? Where are they deployed? How are they kept up to date? Is administrative access to the firewall and other devices only permitted through secure channels or direct access?	Voicepoint utilizes redundant and uninterrupted Linux-based load balancer virtual machines (VMs) from loadbalancer.org, which come with an integrated Web Application Firewall. These VMs are operated within the Microsoft Azure Datacenters in an „Availability Set," and their software updates and security policies are fully automated. These load balancer VMs serve as the central point of connection between external access and the cloud's internal networks. For management, there is a web interface with separate authentication available, accessible for authorized personnel only through an MFA-secured VPN connection.
What protocols and ports are allowed for communication?	All client applications and smartphone apps transmit data via HTTPS port 443, secured by TLS 1.3 with a 128/256-bit AES encryption.
Are there formal incident-response procedures in place? Are they tested regularly?	Incident processes are implemented and include specific procedures to classify the level and handling of incidents, which relates to the availability or security of the solutions.

Physical security

What are the primary physical security and business continuity features of your datacenter?	The Microsoft Azure datacenter provides extensive electronic and physical security measures. Our datacenter configuration is provided with “availability sets”, guaranteeing the consistently high availability of hardware.
Who (including datacenter staff, Voicepoint staff and suppliers) has physical access to the servers?	Only authorised personnel have access to the physical facility, which is strictly limited and monitored on a regular basis.

System security

Are file permissions set on a “minimum need” basis?	Access to files is set on a “minimum need” basis and is restricted to the relevant service accounts and authorised staff who require access to them.
Are audit logs implemented on all systems that store or process critical information? Are root commands logged? What processes are used to control access to devices and logs?	All applications contain independent log or audit mechanisms. System logging is performed via Windows Event Viewer, which allows security, system and application events to be logged. Access is monitored regularly and adjusted if necessary. Access and amendments are also logged in the Microsoft Azure portal.
How is the integrity and availability of services and application servers monitored?	System monitoring is in place and uses internally developed and industry-standard tools. Microsoft Azure-specific services are used for alerts and monitoring.
Have unnecessary services and applications been disabled on the application servers?	Yes, only necessary services and applications are installed and operated on the servers.
Are other security mechanisms used?	Yes, the Microsoft Azure Security Center is also used for the overall safety of the infrastructure, monitoring current security-related findings and measures and assessing severity. These are reviewed by Voicepoint on a regular basis and applied when necessary. Windows Defender is also available on application servers, acting as an antivirus and sending feedback to Microsoft Azure Defender.

Web security

Have unnecessary HTTP modules or extensions been disabled on the application servers?	Yes, only the necessary HTTP modules and extensions are used on our application servers.
Does the account, under which the web services are conducted, have administrator rights to the application server?	A separate service account is available for each application offered. Each web service is therefore implemented under its own service account. The rights of the service account are reduced to the minimum necessary.
Have insecure TLS versions and ciphers been disabled?	Yes, older and insecure TLS versions (<TLS 1.2) and ciphers have been disabled on the application servers as well as on the whole environment. New, insecure ciphers and TLS versions are regularly checked using Qualys SSL Labs and disabled as necessary.

Staff security

How are the credentials of staff handled?	Every authorised Voicepoint employee uses a personal, MFA-protected, system-wide user. Employees are divided into different administrative roles. For application support, authorised employees have no direct access to the individual application servers or components of the infrastructure. A special "joiners movers leavers" concept is in place and in use. Thus, Voicepoint can ensure that only authorized employees can access the services released for them. The role of the system administrator is kept to a minimum so that operations can be guaranteed in the event of staff absences.

Security of applications

Is data encrypted when it is transmitted using public network connections?	The communication between client applications and Voicepoint Cloud services is transmitted over HTTPS, secured by TLS 1.3 with 128/256-bit AES encryption.
Is any data stored locally on the device or computer (dictation management)?	When using client applications for the dictation management solution, folders for application-specific settings and log files are set up in the user's local application data. A "UserWorkingDirectory" is also used for intermediate storage, temporary access to server data and draft jobs, which can be set up either locally for each user or on a customer's central storage location. Original jobs from mobile dictation devices are filed locally under the customer after downloading until they are removed by the automatic archiving cycle. The customer is responsible for backing up these files.
Is any data stored locally on the smartphone?	Temporary job data is saved on the device when using the smartphone app for the dictation management solution. Audio files are encrypted on the smartphone with an automatically generated security key. Further information regarding security in the Winscribe Professional smartphone app can be provided on request. No dictation data is saved with the smartphone solution PowerMic Mobile, as this app only serves as a microphone replacement.
Is any data stored locally on the device or computer (speech recognition)?	Speech recognition clients stream audio data in real time to the secure server environment for processing speech recognition. The target application and user are responsible for the safekeeping of the text that is returned by the speech recognition server.

Further information

For more information about the Voicepoint Cloud, please visit our website.
The Voicepoint team will also be happy to provide personal advice either through the contact form or by telephone on 044 933 39 39.

Version as of September 2023.

Voicepoint AG Schellerstrasse 14 CH-8620 Wetzikon
044 933 39 39 info@voicepoint.ch www.voicepoint.ch