



## ORdigiNAL Cloud Services APAC/EU/UK/NORWAY

Powered by Microsoft Azure

Version : 1.4  
Date : December 2021

*Optimising Together*

Data security is a key focus to ORDigiNAL; we are dedicated to meeting the highest security standards while guaranteeing a level of continuity that today's professionals demand.

In partnership with Microsoft® we utilise Azure as our cloud platform for solutions including Dragon® Professional Anywhere, Dragon® Legal Anywhere and Dragon® Anywhere Mobile among many other solutions. This partnership ensures the ORDigiNAL cloud platform complies with some of the broadest international level, industry-specific, compliance standards and security standards in the world. For more information, please visit the Microsoft Trust Center.

<https://www.microsoft.com/en-us/trustcenter/compliance/complianceofferings>

## Streaming and data storage

Data protection is at the heart of the ORDigiNAL cloud platform; such data is protected with end to end encryption using a combination of HTTPS & Transport Layer Security (TLS 1.2 Minimum) with 256-bit AES cypher algorithms. With security implemented as a core element; both local and international regulations covering data storage and data streaming are regularly assessed and adhered to, this ensures your users can enjoy a fast, secure and timely service while staying safe doing so.

Conforming to internationally recognized security standards; the ORDigiNAL cloud platform streams data in real-time while ensuring no such data is stored on the client machine, and any such data stored on the cloud platform is both encrypted and periodically deleted.

Where audio is streamed for voice to text applications; stored audio and text are used to “train” and optimize the speech engine for individual user-profiles and to improve speech recognition accuracy for every user. Such audio and text are anonymous, in that respect, ORDigiNAL Cloud Services do not have direct access to the data dictated. For example, if a client dictates, “The defendant claims to be not guilty concerning the felonies mentioned in point 3.1 and 3.2”, there is no stored information that associates that information with an individual person.

## Application security

It is of utmost importance for your organization to understand the protection measures used to secure the ORDigiNAL Cloud Services infrastructure.

Qualys® SSL Labs rated “A+”

ORDigiNAL monitors security standards continuously and performs audits to ensure that the provided cloud infrastructure meets the highest standards for secure data transmission. To that end, our hosting environment has received an “A+” rating from Qualys SSL Labs; this rating is a security test representation which tests for common vulnerabilities. Such infrastructure at the time of writing applies: SSL certificate (256-bit, trusted), protocol support (TLS 1.2 Minimum, HTTP Strict Transport Security (HSTS), Secure Renegotiation,

Forward Secrecy (ROBUST), OSCP Stapling, Downgrade Attack Prevention (mitigated), among many other continually evolving changes.

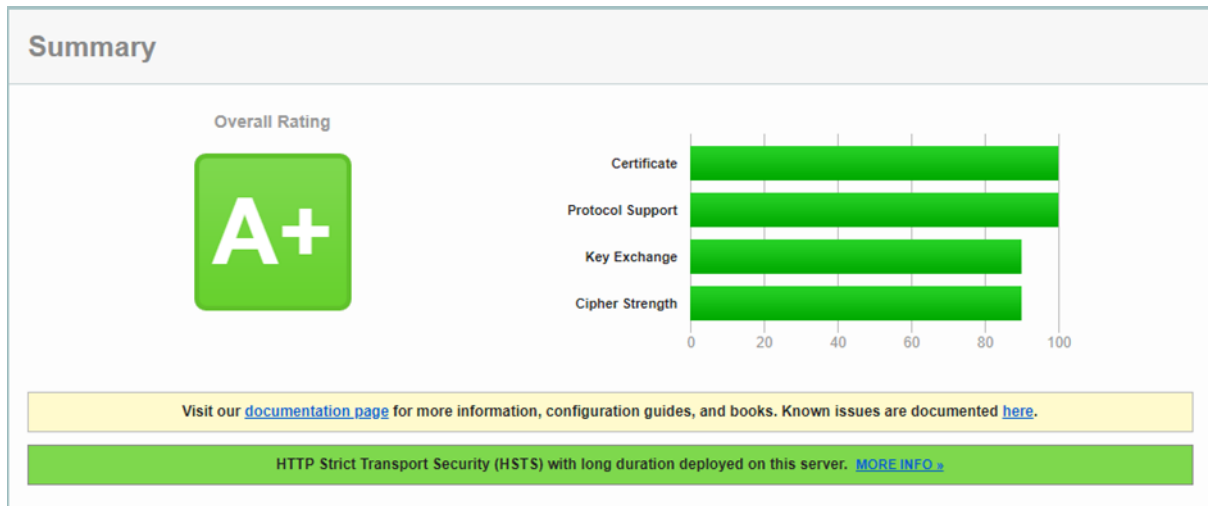


Figure 1: An SSL Labs security check of an ORdigiNAL regional offering (<https://sas-uk.ordiginal.com>)

\*This is an example; ORdigiNAL provide multiple regional offerings of which all conform to the above

## Microsoft Azure Security Standards

As a leading cloud provider that serves multiple industries including 95% of the companies in the fortune 500 list and many others in the healthcare, government and financial sectors, Microsoft has 3500 global cybersecurity experts delivering state-of-art security in Azure data centers globally. Rely on a cloud that is built with customized hardware, has security controls integrated into the hardware and firmware components, and added protections against threats. Microsoft provides denial of service, intrusion detection, and performs routine penetration testing. As a direct result of these security measures, Microsoft data centres are ISO27001, SOC I Type 1 SOC 2 Type 2 compliant. Further information concerning the certifications can be found here: <https://docs.microsoft.com/en-us/azure/compliance/>

## Customer responsibility “Utilising a secured cloud environment”

Security and compliance is a shared responsibility between ORdigiNAL and the Reseller and/or End-user. Because you are using applications that utilise ORdigiNAL Cloud Services, the security responsibilities are shared by both you and ORdigiNAL, with both parties having security and privacy policies and procedures in place. ORdigiNAL is responsible for protecting the infrastructure that runs all of the services offered in the ORdigiNAL Service Cloud; this infrastructure is composed of the hardware, software, networking, and facilities that run ORdigiNAL Cloud Services while the customer is responsible for securing the environments that utilize or consume those services.

## High availability

Refers to a set of technologies that minimise IT disruptions by providing business continuity of IT services through redundant, fault-tolerant, or failover-protected components inside the data center

Microsoft Azure cloud is designed to be highly available 24x7 and deliver consistent uptimes of 99.95%;

Microsoft has leveraged its constantly expanding worldwide network of data centers to create Azure, a cloud platform for building, deploying, and managing services and applications, anywhere. Entrust Microsoft with all of your computing and network needs with Infrastructure as a Service (IaaS). Azure provides secure, reliable access to your cloud-hosted data—one built on Microsoft's proven architecture.

Below are just some of the numbers concerning the Microsoft Azure platform.

- 15 billion dollar investment in a worldwide footprint
- We utilize multiple data center-pairs across multiple regions such as North Europe/West Europe/UK South/UK West/Germany West Central/France Central/Australia East/ Norway
- World's largest multi-terabit global network with extensive dark fiber footprint

From an installation perspective, the hosted ORdigiNAL Cloud services cluster provides the following high availability features:

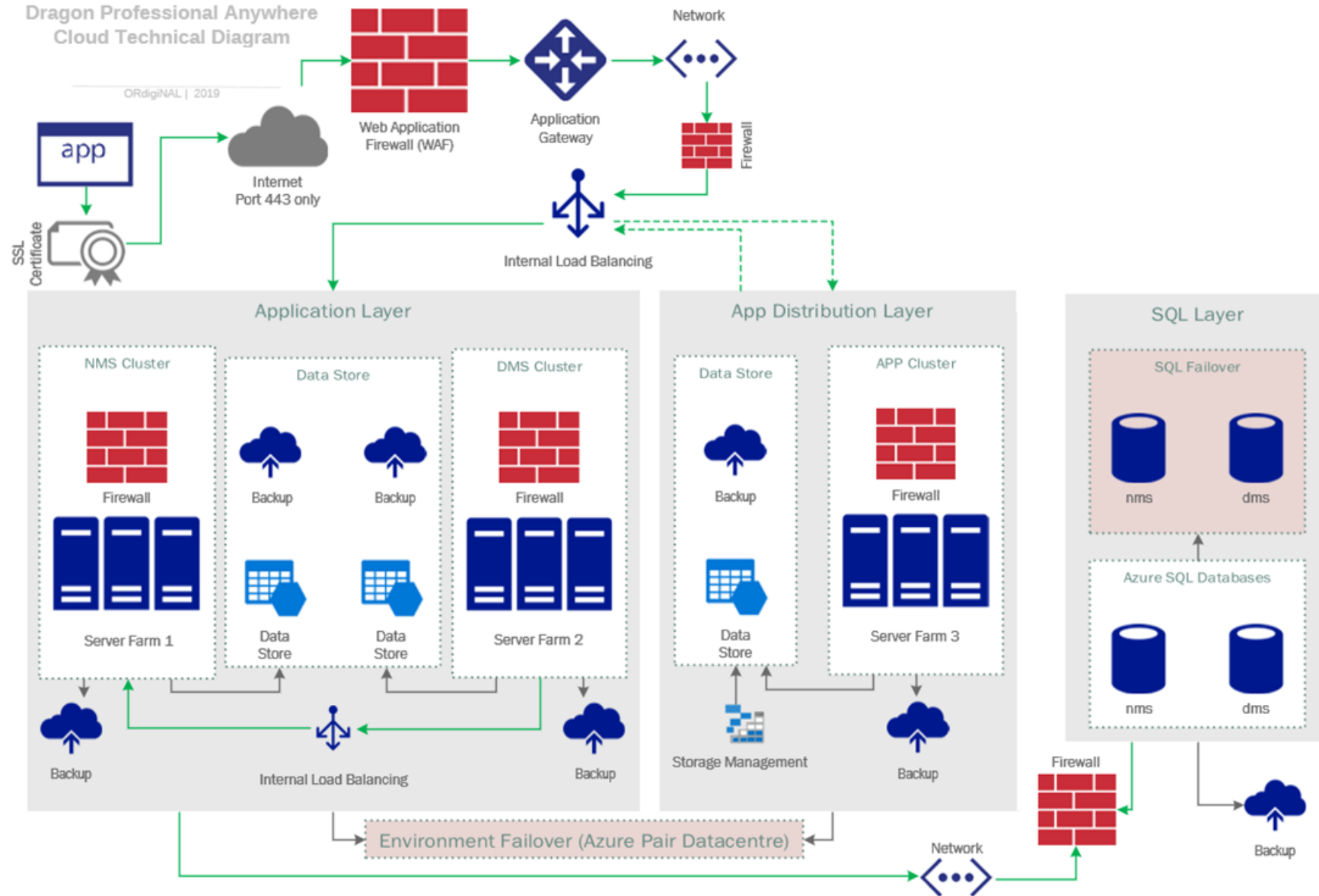
- Fully redundant network infrastructure, including load balancers and switches
- Multiple clustered application servers – High availability network storage with fiber-optic connections
- Clustered and backed-up databases
- Clustered and extensible server “farms”
- Secure and robust cloud offering utilizing a multitude of firewalls and security analytics solutions

See the cloud diagram for an example on the next page

## Overview

Our best in class security practices, combined with our highly available and redundant infrastructure, help ensure that your customers will enjoy fast, secure and uninterrupted clinical speech recognition.

# Dragon Professional Anywhere Cloud Technical Diagram



## Physical security

Microsoft Azure datacentre locations are not disclosed they however provide extensive electronic and physical security measurements as required by the certifications and accreditations they employ.

The configuration of the ORdigiNAL Cloud Service provides automatic failover in case of server outage to guarantee business continuity.

Additional security is provided by only allowing Microsoft Azure certified staff to enter the datacentres, our non-certified staff/clients and suppliers are prohibited from accessing such facilities.

## Network security

Network security is a priority at ORdigiNAL and Microsoft; firewalls are deployed at the datacentre across multiple layers to provide optimal security. Such layers include; Application layer, Network layer, Storage Layer, Machine Layer and SQL layer. Microsoft regularly employs updates to such layers and are deployed according to their internal change management processes. Access to these resources is only possible through secure connections or on exception through serial port interfaces.

All communication to and from the servers is encrypted and transported through HTTPS; only necessary ports are open for communication for both inbound and outbound traffic. Additionally, 'where possible', traffic is routed through the Microsoft internal backbone where web routes are avoided for further and more robust security.

Our network is monitored by a network analysis tool, that monitors all public elements of our infrastructure and alerts ORdigiNAL Azure team of any suspicious behaviour. This type of analytical monitoring includes a large range of different scans across a multitude of Azure resources to provide the greatest level of security possible.

In case of incidents, we have Incident Management Processes in place, which includes specific procedures to classify the level of impact and the handling of fore mentioned incidents. These procedures are reviewed and tested regularly across our organisation.

## Application security

To prevent any abuse of data, we do not store any data on the local machine or device. All streams are real-time and utilize encrypted transmissions over an encrypted https connection to our secure ORDigiNAL Cloud Platform for processing. All data is then returned by our cloud platform over a secured connection. Tools such as HP fortify among others are used to test our applications against known security vulnerabilities.

## System Security

To provide optimal system security, Microsoft performs continuous tests, including penetration testing and has measurements in place to prevent Distributed Denial of Service (DDoS) and intrusion detection. ORDigiNAL additionally implement gateway-layered security to mitigate DDoS attacks.

Access to our resources within our infrastructure are on a need to access basis and is restricted to our Azure operations teams only through secure Microsoft Bastions services with 2 step authentication in place.

Our platform applications log relevant information on data access within the platform. Internal windows tooling is used to keep track of system logging which keeps track of applications, system and security events. For changes on our platform, we use change management procedures, which provide guidelines for various changes and management approval levels to implement them.

Monitoring of our cloud platform is preformed using the monitoring tools supplied by Microsoft Azure; we also utilize a set of tooling provided by the manufacturer of the speech solution, a dedicated team monitors the alerts 24/7 to ensure continuity.

## Local Rules and regulations

The General Data Protection Regulation (EU-GDPR) & (UK-GDPR) is a European & British privacy law that became effective in May 2018. It imposes new rules on organizations that offer goods and services to people in the European Union (EU), European Economic Area & The United Kingdom or that collect and analyze data belonging to individuals from the forementioned areas. We maintain the same high standards across our other geographical regions to secure privacy sensitive information. The GDPR requires that data controllers (such as organizations using Azure) only use data processors (such as Microsoft) that provide sufficient guarantees to meet critical requirements of the GDPR.

Microsoft Azure has been granted a multitude of region-specific certifications, to view these please visit:

<https://docs.microsoft.com/en-us/azure/compliance/>