Trust Dragon with your data

Security with Dragon® cloud and hosted solutions

Nuance understands the importance of security and data privacy with customers of our new products that take advantage of the cloud and externally hosted data services. While our traditional desktop products have always worked locally with very minimal data sent back to our servers (and only if the user opted in), new products such as Dragon® Anywhere or Nuance® User Management Center work reliably in the cloud in order to provide customers with its features advantages. We outline in this document how we address data privacy and security for enterprise customers who may be concerned with their data transmitted and processed by externally hosted servers.

Dragon Anywhere and Nuance User Management Center are hosted by HP Helion Managed Virtual Private Cloud (VPC). We selected HP as one of the leaders in enterprise cloud services and evaluated them as a partner from all security aspects including data center and network security, reliability, authentication and encryption capabilities and access, maintenance and enforcement policies. We feel confident that HP is a reliable and secure partner to host our solutions and are committed to ensuring that our customers are satisfied with our choice.

Dragon Anywhere and Nuance User Management Center security

– All speech-related transactions between the Dragon Anywhere mobile client and the speech recognition servers in our data center are conducted over HTTPS using 256-bit encryption channels for bi-directional, end-to-end security

Security measures for client data or confidential information used in Dragon cloud based products, such as Dragon Anywhere or Nuance User Management Center, include:

– Any synchronization of Dragon Anywhere with the central server, for all communication is over HTTPS using 256-bit encryption
– All user accounts are password protected
– Dragon Anywhere does not access content on your device such as contacts or your location
– The Nuance User Management Center database stores no recognition data in the database
– Each corporate customer's recognition data is partitioned from our other customers in the data center
– Dragon solutions are backed by HP Helion Managed Virtual Private Cloud's proven and comprehensive security policies.

NUANCE

– All user accounts on desktops or devices are password protected
– Dragon Anywhere does not access content on your device such as contacts or your location
– The Nuance User Management Center database stores user authentication information specific to the Nuance system. The system does not store credentials valid for a customer's network. The database also stores product license grant information, custom words, auto-texts, and usage metrics. No recognition data, such as dictation data that Dragon has converted to text, resides in the database.
– Each corporate customer's recognition data is partitioned from our other customers in the data center in a Virtual Private Cloud (VPC) environment that reduces network security risks and enables customer-defined parameters targeted to specific security requirements
– Dragon solutions adhere to HP Helion Managed Virtual Private Cloud services' proven and comprehensive security policies. If needed, customers can contact Nuance or a Nuance partner directly for any customer-specific data retention and processing policies that need to be further implemented.

HP security policies

Data center security

HP data centers are operated in accordance with HP's best practices, hardened against both physical and electronic intrusion, including:

– Access control by key card or biometric scanner
– Site monitoring includes indoor/outdoor video surveillance and on-site security personnel on a 24 by 7 basis
– Redundant power and cooling infrastructure, for high reliability
– Diverse network access points, for optimum network connectivity and flexibility
– ITIL (Information Technology Infrastructure Library)-based operations ensure predictable, maintainable service levels using guidelines and best practices that align IT infrastructure management to business needs
– Data center physical security reviewed at least annually

Network security

HP's Virtual Private Cloud environment provides network security through various means, including:

– Network compartments will be provided for each customer with a customer-dedicated perimeter virtual firewall. Customers define their own firewall rules for their compartment and are subject to HP review and approval. Customer firewall rules will be implemented by HP except where HP determines they pose a security risk for HP or other tenants. If there is a security risk posed by the customer proposed firewall rule, HP will meet with the customer to determine if an alternative solution can be implemented.
– Logical separation and isolation of individual customers' network traffic reduces the risk that customer data could be subject to unauthorized exposure during transport across the Managed VPC network infrastructure
– Customer dedicated server operating system instances within customer dedicated virtual networks separate customer environments from other customers' environments
– Security events from the VMware Hypervisor virtualization layer are collected and stored so that security logs would be available for forensic analysis by HP if such analysis were determined to be necessary.

Customers work with Nuance or a Nuance partner directly for access to security logs or if any action is required.
- Industry standard storage strategies and controls are used to secure data in the Storage Area Network so that customers are restricted to their allocated storage
- Network Intrusion Detection and Network Intrusion Prevention (NIDS/NIPS) services inspect all public Internet traffic to the Managed VPC network. Industry-standard attack filters are deployed in order to detect, report and block known network security threats before they can harm the Managed VPC network or Managed VPC infrastructure.

Authentication and encryption
- Default passwords on HP managed systems and equipment used to provide services are changed when placed into production
- Data stored on tape media is encrypted
- Unique IDs are required for all HP personnel where technology permits

Access, maintenance and enforcement
- HP support personnel access through the HP management infrastructure is logged
- Periodic penetration testing of the Managed VPC management infrastructure (not including customer dedicated systems) is performed.
- Periodic assessments or audits of the HP Managed VPC environment are performed
- Policies and standards applicable to HP personnel and HP managed servers are maintained
- Restricted administrative access to the Managed VPC management network and servers is accomplished by verifying authorized users' identities with multi-factor authentication to reduce the risk of inappropriate access
- Patches are applied for systems managed by HP, as deemed necessary by HP
- HP will perform security incident response, consisting of investigation and resolution of incidents in accordance with HP standard procedures. This service is limited to the extent that security incidents are external to a customer's operation and use of the servers (such as incidents concerning physical or logical security at HP's data center) that are detected by HP or reported to HP by the customer. Customers can work directly with Nuance or a Nuance partner for this service.

Regulatory compliance
If there is a particular regulatory compliance requirement that you need, please inquire with a Nuance representative. If a specific set of security requirements are needed, Nuance or a Nuance partner will work with you and HP to analyze the compliance level and take any steps needed to achieve compliance.

Additional resources

To learn more about Dragon Anywhere, Nuance User Management Center as well as the complete line of Dragon speech recognition products, visit: http://www.nuance.com/dragon-anywhere/ or http://www.nuance.com/dragon/

Contact your local Dragon speech recognition sales representative for more details.

For more information about HP Helion Virtual Private Cloud, please refer to the following resources:

http://www8.hp.com/us/en/cloud/helion-overview.html

http://www8.hp.com/us/en/cloud/hphelion-openstack-overview.html

http://www.networkworld.com/article/2172203/cloud-computing/hp-private-cloud-service-leads-the-pack--followed-by-cisco-and-microsoft--forrester-.html

HP Helion

About Nuance Communications, Inc.
Nuance Communications is reinventing the relationship between people and technology. Through its voice and language offerings, the company is creating a more human conversation with the many systems, devices, electronics, apps and services around us. Every day, millions of people and thousands of businesses experience Nuance through intelligent systems that can listen, understand, learn and adapt to your life and your work. For more information, please visit nuance.com.

NUANCE

August 2015