Nuance OnDemand provides security and reliablity.

Achieving the highest level of security within IVR, Web and mobile customer service applications while meeting the challenges of security certification, compliance and ongoing auditing.

NUANCE®

Table of contents

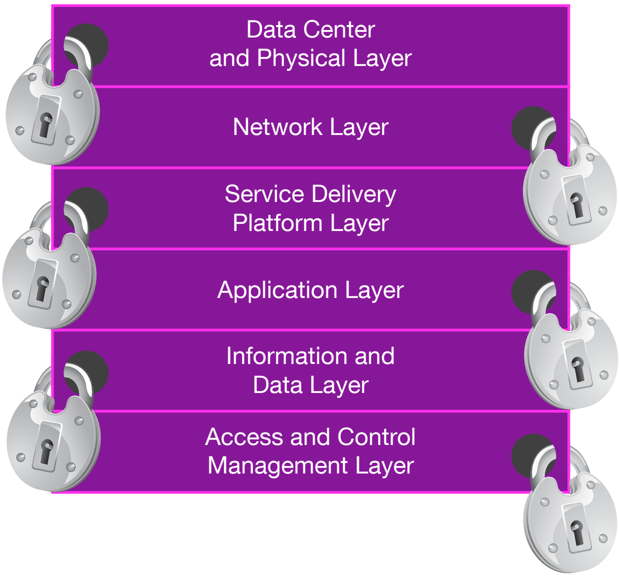
Introduction

Each year, Enterprise applications handle billions of transactions that include confidential and sensitive consumer data, such as credit card numbers, healthcare information, and passwords. Evolving internet technologies, customer service channels, and deployment options have increased the chances for successful malicious attacks. More than ever before, consumers are aware of and concerned with fraud and privacy issues. As a result, many regulations and standards have been put into place to protect consumer data. It is essential for companies to demonstrate compliance with current legislation, and to be prepared for the barrage of new legislations being considered. Recent laws such as HIPAA (Health Insurance Portability and Accountability Act), Privacy Legislations, and Sarbanes-Oxley have had major implications for businesses. To maintain the highest levels of security within their IVR, Web and mobile customer care applications, many enterprises are turning to hosted solutions where they can rely on vendor experts to meet the difficult challenge of security certification, compliance and ongoing auditing.

Nuance has been providing secure, hosted customer care solutions for over 10 years. Nuance's hosted customer care offer, Nuance OnDemand (NOD), includes sophisticated security architecture, policies, guidelines, and best practices. The multi-layered implementation of physical and network infrastructure, management access and controls, and application security framework ensures robust protection for our customers' sensitive data. Today, Nuance technology securely handles over 2B customer contacts annually.

As the largest hosted speech automation platform in the world, Nuance OnDemand takes security to a whole new level to address privacy, data confidentiality, authentication, integrity, non-repudiation, access control, and communication security. Operating 24x7, 365 days a year, Nuance OnDemand's multi-layer security mitigates many levels of threats to your customers' information so that your business consistently provides quality customer care.

Nuance On Demand Multi-Layer Security



Enterprises using Nuance's multi-tenant service platform include the largest U.S. retail banks, insurance, mobile service providers, and travel companies. And, as such, Nuance incorporates stringent security requirements for hosted services. Nuance OnDemand has been designed from the ground up to handle Fortune 1000 enterprise security requirements and has incorporated many controls that meet compliance requirements. This document discusses the measures implemented within Nuance OnDemand to secure every interaction with your most valuable assets–your customers–thus guaranteeing the confidentiality, integrity and security of their sensitive data.

Nuance OnDemand Security Overview

Security from the ground up

To adequately protect Personally Identifiable Information (PII), Nuance Enterprise Network Services has established a security management framework and team. The framework provides structure for information security within the organization. Within the framework, management approves the information security policy, assigns security roles, and co-ordinates and reviews the implementation of security across the organization. The team's information security advisors communicate regularly with external security specialists or groups, including relevant authorities, to keep up with industry trends, monitor standards and assessment methods, and provide suitable liaison points when handling information security incidents.

The Nuance OnDemand system is a Customer Care computing platform hosted in three geographically distributed locations within the continental US. Nuance partners with highly trusted SAS 70 Certified data centers (Internap, Qwest, CoreSite) which adhere to and are in compliance to and or certified according to stringent security standards, inclusive of SOX, ISO 27k, PCI DSS, and HIPAA (WIP). Nuance has worked closely on the architecture and design of our platform with internal and external security experts, ensuring compliance with Nuance's high standards for availability, security and integrity of customer data. User data is processed within the borders of the United States only.

Security Framework

PHYSICAL SECURITY

Nuance OnDemand systems are housed in isolated segments within SAS 70 Certified data center locations. Data Center physical security employs four broad categories:

- **Confidentiality** – Ensure that only authorized users can access any physical layer of our hosted infrastructure.
- **Integrity** – Ensure access approval policy is continuously monitored and executed.
- **Authentication** – Ensure multiple levels of authentication in the system.
- **Audit Trail** – Ensure full historical reporting of any physical access.

Requests for access require a service ticket for official review, acknowledgement, approval or rejection and historical tracking. Access is approved on a need-to-have basis only. Furthermore, all platform servers are stored in secured cages and are password protected.

Data centers are operated around the clock with onsite personnel. All persons must identify themselves with a data center provided or governmental approved picture ID (driver's license or passport). All Nuance employees must be on an approved data center list, and visitors must be matched to a Nuance-approved visitor request. All critical building areas are monitored via 24x7 security cameras and compartmentalized with steel high-security portals. Depending on the data center entry in the secured zones requires the use of biometric authentication. Data centers are operated 24x7 with onsite personnel. Maintenance personnel and personnel without regular established access require an approved data center escort while in the building. Other physical security characteristics include motion sensors, secure building entrances, exits and fire routes. Automatic fire extinguishing systems, redundant power distribution systems with independent backup generators and flood protection systems reside in certain locations.

NETWORK SECURITY

Information and the systems on which it resides interconnected by networks are important business assets. Maintaining, and ensuring network security at all levels is essential. Nuance OnDemand achieves this network security through both technical means and administrative level controls. Nuance OnDemand network security includes the following:

- Firewalls
- Network Address Translation
- Network Segmentation
- Data Encryption
- Intrusion Detection
- Security Events Monitoring
- System Authentication

The Nuance OnDemand security management team determines the security features, service levels, and management requirements of all network services. The team manages and controls the networks, not only to protect them from threats, but also to maintain security for the systems and applications using the network, including information in transit. Detective, preventive, and corrective controls, along with appropriate user awareness procedures, protect against malicious code. Audit logs record all user activities, exceptions, and information security events. The Nuance OnDemand security team preserves these logs to assist in future investigations and access control monitoring. Independent reviews are conducted on a regular basis to ensure that information security processes are adequate, complete, fit-for-purpose and enforced.

PLATFORM SECURITY

Nuance network services engineers harden the operating systems and infrastructure to protect its systems from various security vulnerabilities. Servers must deliver data in a secure, reliable fashion. Operating system, middleware and application hardening involves:

- Security sensitive installations
- Implementations and configurations of robust logging
- Encryption of sensitive communications
- Prudent configuration of access controls, “least privilege” and “need-to-know”
- Strong authentication

Hardened platforms further restrict system capabilities to only those that are explicitly required and tolerated for expected system functionality. Systems and software versions and upgrades are cross-checked and undergo suitable testing in a staging environment prior to acceptance for production deployment and use. Technical vulnerabilities of information systems are monitored and assessed by the security team. The team evaluates any exposures to such vulnerabilities and takes appropriate measures to address any associated risk. Procedures monitor the use of information processing facilities, and the team regularly reviews these activities.

ADMINISTRATION SECURITY

Nuance ensures segregation of duties as a method for reducing the risk of accidental or deliberate system misuse. Due diligence with policies, process and procedures prevents any single person from accessing, modifying or using assets without authorization or detection. The initiation of an event is separate from its authorization. The design of these controls considers the possibility of collusion. Development, test and production environments for IT Infrastructure and Applications are segregated to reduce the risk of unauthorized access or changes to operational systems. The team establishes, documents, and reviews an access control procedure based on business and security requirements for access.

Sensitive data at rest is not permitted, unless encrypted. Data in transmission is encrypted or otherwise protected via a dedicated link. Customer session data is normally accessed and transactions can be completed through a dedicated connection to customer backend systems. Each link is dedicated to a single customer and often encrypted (MPLS/SSL), further reducing risk of data exposure through strong technical controls. Nuance supports and recommends private data links for transmission over public Internet for data access but can also optionally provision a secure VPN tunnel.

ACCESS AND CONTROL SECURITY

Nuance employees' access to sensitive data is granted on a need-to-have basis only, considering an employee's job role and the problem at hand. Each username is uniquely assigned to a person and assigned to a centrally defined role with associated privileges. Access roles might be elevated on a temporary basis but only after a security committee has determined the validity of a written request. Each elevation, system or data access request is logged in a separate audit system for later retrieval and analysis. Nuance's Business Continuity Plan outlines emergency access to the platform in case of disaster and highlights contact information for mission-critical personnel and their substitutes. The Nuance OnDemand platform stores logs for each call for diagnostic and reporting purposes. Nuance's policy prevents any sensitive application data (account, PIN number input etc.) from being written to the logs. Instead, sensitive data is stored in-memory only and is masked in stored log files. The platform also provides a mechanism to mask or encrypt callers' audio data. Nuance clients provide a public key and determine the encryption scheme for audio data. Only the client can decrypt the caller audio utterances and play them using the decryption key and a tool provided.

All Nuance computers and terminals auto-lock after 15 minutes. Nuance employees manually lock or logout of systems before they leave their work place. User access roles are reviewed on a quarterly basis. Upon an employee's voluntary or involuntary job termination, electronic access to systems is immediately terminated, the user's badge is collected, and building access is granted only with escorts.

APPLICATION SECURITY

Nuance Products and Professional Services organizations adopted the Open Web Application Security Project (OWASP) as our framework for security standards in software and application development. Product design documents and customer application statements of work specify the security framework requirements as defined in OWASP guidelines. The design documents are translated to an agile development methodology as tasked for development and QA efforts. Nuance's Software Development Lifecycle (SDLC) ensures for the implementation of Open Web Application Security Project (OWASP) as part of its application software security development framework.

Management Security

Information, information systems, and all related assets are critical and vitally important to Nuance's business processes. Nuance takes appropriate steps to guard its assets from threats such as error, fraud, sabotage, terrorism, extortion, industrial espionage, privacy violation, service interruption, theft, and natural disaster. Nuance protects information assets in a manner commensurate with their sensitivity, value, and criticality. Security measures are employed regardless of the media on which information is stored, the systems that process information or the methods used to transport information. Such protection includes restricting access to information based on the two security principles of “least privilege” and “need-to-know.” Nuance management ensures that all assets, including information and information systems, are protected in a manner that is at least as secure as that required by our clients and other organizations in the same industry handling similar types of information. To achieve this objective, Nuance conducts annual reviews of the risks to its collective. Similarly, whenever a major security incident indicates that the lifecycle protection of these assets is insufficient, management takes prompt remedial action to reduce Nuance's exposure and thus mitigate the risk of harm to an asset. Information security training, guidance, direction, and authority are centralized in the Nuance Security Organization, which is responsible for establishing, maintaining and monitoring the enterprise information security policies, standards, guidelines, and procedures.

Nuance employs a corporate security officer (CSO) overseeing implementation and compliance to all published security standards, business continuity planning, loss prevention and fraud prevention, and privacy. In addition, divisional security manager roles are assigned to control divisional compliance and adherence to Nuance OnDemand's security certifications and standards. Nuance is annually audited for security and privacy compliance. Nuance OnDemand includes a set of 15 policies detailing corporate and divisional requirements for handling PII and sensitive data.

Every Nuance employee is annually trained and mandated to maintain and practice a working knowledge of security, privacy and ethics rules according to their job role. Nuance's Learning and Development team monitors employees' progress with Nuance-provided security, privacy and ethics material and initiates sanctions in cases of non-compliance. Exhaustive legal contracts and stringent NDA's ensure Nuance's service partners obligation to protect Nuance information assets. As a solutions provider, Nuance's use of outside services is limited to exceptional cases and access to protected data is not granted to external personnel. Nuance uses critical judgment and a chain of policies before exposing sensitive information, even within the corporation, as a first method of protection. All employees must undergo background checks before receiving an offer of employment.

Nuance's systems security performance is evaluated on a quarterly basis by various external 3rd party security firms specializing in domain specific security standards. Nuance's security policies are reviewed and revised at least once annually.

Data Security
Client data reports and other tracking tool— such as using our advanced reporting system, OnDemand Insight (ODI)—are available through a secure OWASP compliant Web interface. Depending on the nature of the voice application and the security policy applied during application development, certain reports might contain individually identifiable or protected information by design. ODI access is secured via role-based username and password combinations. Web access is tunneled through https with at least 128-bit encryption and at least 1024-bit authentication key agreement. The server is authenticated with a X.509 certificate. Nuance can restrict access to the Web portal to a set of trusted IP addresses.

Each Nuance OnDemand client operates within its own Web tool domain, virtually eliminating any risk of contaminating data with other enterprise applications or leaking of confidential information into other accounts. Only a manually configured super user can designate second tier users and their role for reporting access within their company. ODI facilitates large-scale business metric and diagnostic analysis while adhering to an enterprise's security standards. Each role is defined as a subset of over 50 selectable criteria, with each user assigned to a specific role. Each client maintains reporting accounts and purges reporting data. The ODI reporting console provides an extensive audit trail of user interactions with the reporting system. ODI keeps detailed report data for about 3 days after the end-user's interaction with the system has ended, and it preserves aggregated data for 13 months before automatic purging.

Certification Achievements
The Nuance OnDemand system is PCI DSS certified. PCI DSS provides an actionable framework for developing a robust payment card data security process — including prevention, detection and appropriate reaction to security incidents

Nuance OnDemand Reliability

Monitoring
The Nuance operations team has extensive operational processes to support high availability. These processes include the selection of key human resources, support and contact processes, system monitoring processes, and system testing processes. For example, the network operations team uses HP Open View as the primary production monitoring system with agents that track performance of production servers and monitor health of the components in the system. Should an alarm trigger, the system notifies operations personnel and Nuance OnDemand customers. Nuance operations staff will immediately begin to investigate and resolve the issue. As a result, in the event of a server, network, or site failure (or even latency issues), our 24x7 NOC will be alerted and can take immediate preventative actions to minimize any adverse effects. Nuance continuously monitors all servers, Internet connectivity, latency, availability, and bandwidth, maintaining these server and network performance logs for up to one year. The network operations team regularly reviews these logs as part of capacity planning.

Business Continuity

The Nuance OnDemand platform is stable, secure, and highly available. All platform components are deployed in a redundant architecture with no single point of failure. These hardened datacenter sites feature fully redundant fiber optic network access, power grid access, power generation and air handling, and are protected by a dry fire suppression system and state-of-the-art physical and electronic security systems.

The data centers are located in three geographic regions within the US. All data centers operate in active/active mode with real-time application replication across the regions. Sites share normal call handling load. In the unlikely scenario of a data center disaster, the remaining datacenters are still capable of handling of planned daily traffic. Nuance's Business Continuity Plan mandates a complete switchover of traffic between data centers within minutes.

Customer Support

To maximize network reliability and availability, the Nuance OnDemand support organization includes 3 tiers of support experts. With rigorous monitoring and testing procedures, the Nuance Network Operations Center (NOC) is the first line of defense. The NOC includes a full-time staff located in geographically distributed 24x7 centers with locations in Sunnyvale, California and Chenai, India. NOC engineers ensure that all Nuance OnDemand systems and client applications are up and running around-the-clock. NOC engineers use tools that continuously monitor the health of every system component. These tools can alert personnel at the first sign of any problem so that potential issues can be resolved even before they impact the operations of the network. These tools can also initiate automated problem resolution procedures (such as running diagnostics). NOC engineers not only monitor network operation and respond to network emergencies but also provide a critical communication link between Nuance and its clients. NOC engineers record customer-reported problems in an automated problem-tracking system, and coordinate the on-going work necessary to quickly resolve them to the client's satisfaction.

Nuance Technical Account Managers provide a second level of customer support and are dedicated representatives for each client. The Technical Account Manager is familiar with each client's personnel, applications, and operating procedures. They work closely with the client and with the Nuance engineering team (tier 3 support) to resolve complex issues.

Nuance disallows support directly to end users, (i.e callers into our customers' IVR application, or end users of a mobile application). Instead, the Service Level Agreement specifies the client's personnel who are authorized for support. This policy, together with the tiered support structure, ensures that a support incident will never reveal private data to an unauthorized person.

Summary

Protecting sensitive customer information and keeping up with the increasing number of security standards is expensive and can become overwhelming for any Enterprise IT organization. Nuance not only has expertise in customer care, but also guarantees robust levels of security inclusive of the overall hosting package. Nuance OnDemand is the largest enterprise-grade on-demand speech IVR, Web and mobile self-service platform.

It provides stringent security and high availability at no additional cost, saving our clients millions of dollars on security alone. Our dedicated staff of security experts ensures adherence to the highest ethical, privacy and confidentiality standards. Nuance maintains PCI DSS certification and is working on implementation of HIPAA compliance and certifications. Our customers include some of the largest financial, transportation, entertainment, and mobile carriers in the world. More than ten years ago, the platform took its first call. Since then, Nuance has successfully operated a highly secure, highly available on-demand customer care data center earning the trust, respect and confidence of our customers.