Nuance Global Security

White Paper

Security at Nuance

Our foundation for trust and resiliency

NUANCE®

Table of contents

2 Introduction

3 Our Global Security team

4 Our five-point security strategy

5 Our security program in action
- Physical security
- Product security
- Operational security
- Data security
- Converged security operations
- Employee security awareness and training

8 Resiliancy through business continuity and disaster recovery

9 Regulatory compliance and data privacy

Introduction

Earning your trust through security vigilance is our top priority.

Our ever-advancing, defense-in-depth security strategy and corresponding controls are designed to ensure that the data you entrust to us is kept private and protected.

We monitor and analyze security intelligence from global sources to protect our networks and applications against both physical and online threats. The combined impact of our security infrastructure, advanced technology tools, and trained, certified security professionals helps to keep your and your customers' data safe, and our networks and systems up and running.

Inside Nuance, we work to instill a security-aware employee culture through engagement across our employee base to encourage their support in doing their part to diligently protect the systems and the data we maintain.

Finally, we have made, and are continuing to make, significant investments in the security of our operations and platforms, security-intelligence capabilities, and ongoing partnerships with outside security experts.

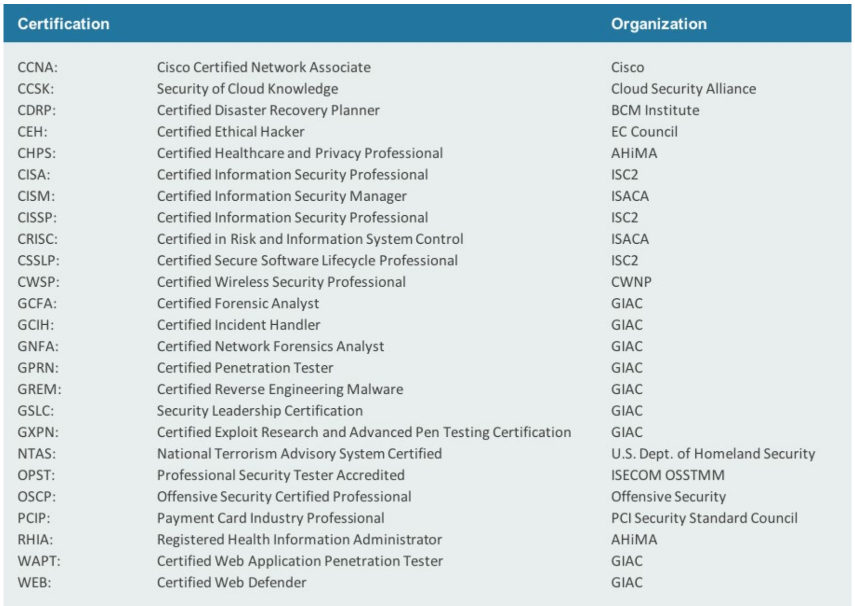
Our Global Security team

The Nuance Global Security team is staffed by trained and certified security professionals who all share a common commitment to innovation, continuous learning, and process improvement.

Nuance Global Security is led by Chief Security Officer Doug Graham, who has over two decades of global security experience spanning IT security, cybersecurity, and physical security disciplines. Before joining Nuance in 2015, Doug served in several security leadership roles at EMC and RSA Security.

Doug's team of security professionals range from security researchers to former military and law enforcement personnel, including tenured Information Security Officers who focus on and represent security for each of the company's four divisions.

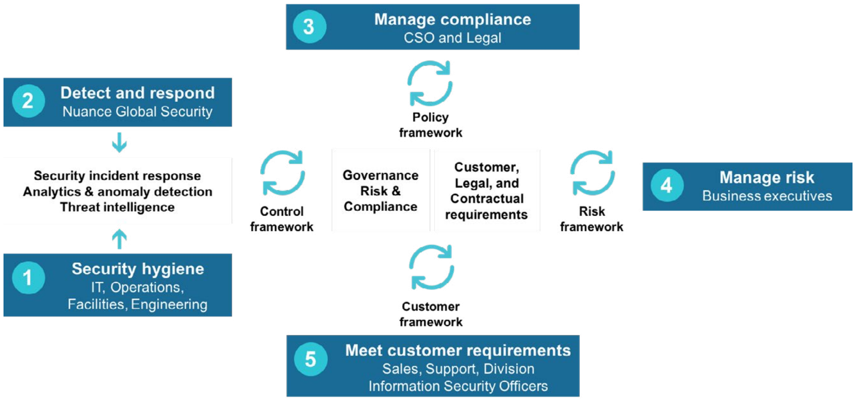
Each member of our security staff is certified by one or more security industry-recognized programs, including:



Certification		Organization
CCNA:	Cisco Certified Network Associate	Cisco
CCSK:	Security of Cloud Knowledge	Cloud Security Alliance
CDRP:	Certified Disaster Recovery Planner	BCM Institute
CEH:	Certified Ethical Hacker	EC Council
CHPS:	Certified Healthcare and Privacy Professional	AHiMA
CISA:	Certified Information Security Professional	ISC2
CISM:	Certified Information Security Manager	ISACA
CISSP:	Certified Information Security Professional	ISC2
CRISC:	Certified in Risk and Information System Control	ISACA
CSSLP:	Certified Secure Software Lifecycle Professional	ISC2
CWSP:	Certified Wireless Security Professional	CWNP
GCFA:	Certified Forensic Analyst	GIAC
GCIH:	Certified Incident Handler	GIAC
GNFA:	Certified Network Forensics Analyst	GIAC
GPRN:	Certified Penetration Tester	GIAC
GREM:	Certified Reverse Engineering Malware	GIAC
GSLC:	Security Leadership Certification	GIAC
GXPN:	Certified Exploit Research and Advanced Pen Testing Certification	GIAC
NTAS:	National Terrorism Advisory System Certified	U.S. Dept. of Homeland Security
OPST:	Professional Security Tester Accredited	ISECOM OSSTMM
OSCP:	Offensive Security Certified Professional	Offensive Security
PCIP:	Payment Card Industry Professional	PCI Security Standard Council
RHIA:	Registered Health Information Administrator	AHiMA
WAPT:	Certified Web Application Penetration Tester	GIAC
WEB:	Certified Web Defender	GIAC

Our five-point security strategy

Achieving our security strategy for defense-in-depth involves a combination of tools, attended by trained and certified security professionals, who follow established policies and protocols based on industry best practices to implement our five-point security strategy.


3 Manage compliance
CSO and Legal
Policy framework
2 Detect and respond
Nuance Global Security
Security incident response
Analytics & anomaly detection
Threat intelligence
1 Security hygiene
IT, Operations, Facilities, Engineering
Control framework
Governance Risk & Compliance
Customer, Legal, and Contractual requirements
Risk framework
4 Manage risk
Business executives
Customer framework
5 Meet customer requirements
Sales, Support, Division Information Security Officers

Our strategy represents our key principles and approaches:

1. Security hygiene
Our security control framework is built into our operations, IT and development functions, leveraging security controls including each of the Center for Internet Security's (CIS) top 20 Critical Security Controls (the "CSC 20")

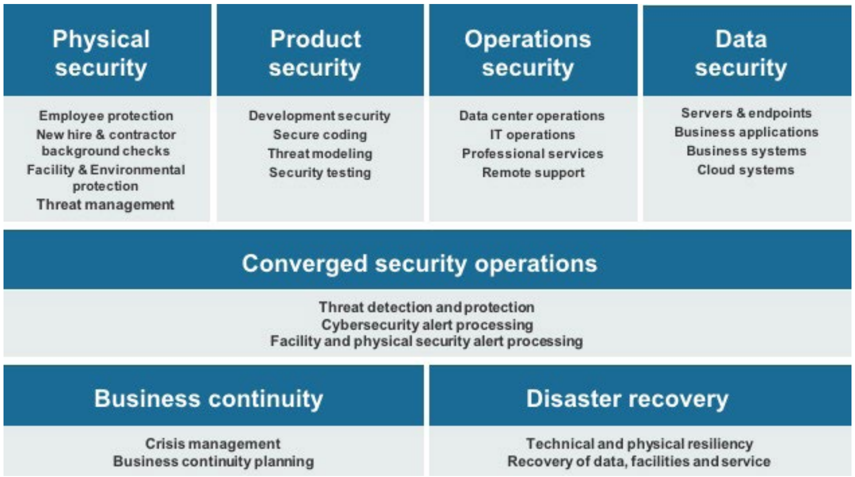
2. Detect and respond
We monitor, detect, and respond to malicious or abnormal online activity. This includes mitigating possible adverse effects using evolving processes, procedures, tools, and controls.

3. Manage compliance
Our compliance and governance initiatives set pre-defined requirements for certain products and solutions to meet compliance obligations like the Healthcare Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standard (PCI-DSS).

4. Manage risks
Our approach to risk management focuses upon policy, procedures, controls, governance, and assessments across the business.

5. Meet customer requirements
Our divisional Information Security Officers and their teams work within our business divisions to get a clear understanding of each division's unique security control requirements, and to focus on compliance at the divisional and product levels.

Our security controls in action



Physical security
Employee protection
New hire & contractor background checks
Facility & Environmental protection
Threat management

Product security
Development security
Secure coding
Threat modeling
Security testing

Operations security
Data center operations
IT operations
Professional services
Remote support

Data security
Servers & endpoints
Business applications
Business systems
Cloud systems

Converged security operations
Threat detection and protection
Cybersecurity alert processing
Facility and physical security alert processing

Business continuity
Crisis management
Business continuity planning

Disaster recovery
Technical and physical resiliency
Recovery of data, facilities and service

Physical security

Information security relies on secure facilities. We approach physical security with rigor and have measures in place to prevent unauthorized access to sensitive data, no matter what form it takes or where it lives.

Our physical security staff and associated controls safeguard our facilities and offsite activities with capabilities such as:

- Personal identification badge and access control
- Workplace safety and security guards
- Crisis, incident, and insider threat management
- Access control and video monitoring
- Travel and event security

Product security

Nuance Global Security drives a coordinated company-wide program to instill, manage, measure, and continuously improve secure software development lifecycle (SDLC) practices.

Creating secure products requires security analysis, review, and testing at every stage of the product lifecycle, from requirements through retirement.

- Secure design and implementation governance
- Identifcation and remediation of any security issues before new products are released
- Rapid response by development teams should there be security issues discovered after release

Based on industry standard frameworks such as the Microsoft Security Development Lifecycle (Microsoft SDL) and the Building Security in Maturity Model (BSIMM), we set standards and assist product teams to meet them across key domains including:

Governance	Secure development
Strategy and metrics Training and onboarding Compliance and policy	Architecture review Code review Security testing
Intelligence	**Deployment**
Attack models and threat intelligence Security features and design Standards and requirements	Software environment Configuration management & vulnerability management Penetration testing

Operations security

Our security measures are designed to protect product support functions, professional services engagements, and data center operations. Data centers hosting Nuance solutions offer resilient environments with failover and redundancy capabilities to help protect information and systems from physical and environmental threats.

Data security

To assist in keeping information private and secure we take a layered approach to securing servers, endpoints (laptops and desktops), and business applications against outside threats. Through ongoing security procedures – including server and endpoint hardening, network segmentation, vulnerability testing, and identity and access controls – we work to protect the systems that generate, move, and store sensitive business and personal information.

Our baseline to protect and govern data, and assess the “organizational security maturity” leverages the Center for Internet Security’s (CIS) twenty Critical Security Controls (the “CSC 20”).

The CSC 20 (see below) prescribes an appropriate technical security baseline to support data privacy and securitiy practices that helps protect customer and company data is any place where it is processed, transmitted, or stored.

1. **Inventory of authorized and unauthorized devices**
2. **Inventory of authorized and unauthorized software**
3. **Secure configurations for hardware and software**
4. **Continuous vulnerability assessment and remediation**
5. **Controlled use of administrative privileges**
6. **Maintenance, monitoring and analysis of audit logs**
7. **Email and web browser protections**
8. **Malware defenses**
9. **Limitation and control of network ports**
10. **Data recovery capabilities**
11. **Secure configurations for network devices**
12. **Boundary defenses**
13. **Data protection**
14. **Controlled access based on the need to know**
15. **Wireless access control**
16. **Account monitoring and control**
17. **Security skills assessment and appropriate training to fill gaps**
18. **Application software security**
19. **Incident response and management**
20. **Penetration tests and red team exercises**

Converged security operations
Our 24 x 7 x 365 Global Operations Centers are augmented by our Security Operations Center (SOC) whose staff of analysts monitor, analyze, and rapidly respond to alerts and incidents detected within our environment.

Our SOC ingests well over one million events per second (EPS) from log sources across Nuance and utilizes advanced threat intelligence, intrusion prevention systems (IPS), intrusion detection systems (IDS), and anti-virus technologies to help protect our networks and systems.

Employee security awareness and training
Our employee security awareness and education programs are foundational to our ability to protect the systems and data we maintain. These programs help employees learn about evolving online and physical threats, and their role in protecting against them, including the reporting of any suspicious activity to Nuance Security.

We provide regular, mandatory security training and provide online resources and e-learning courses to help our employees remain current and diligent about security matters.

Resilliancy through business continuity and disaster recovery

At Nuance, we realize that business continuity and disaster recovery processes are important to help us withstand adverse conditions and quickly recover from unplanned incidents.

Our goal is to maintain service continuity and availability through adverse conditions and probable incident scenarios. When necessary, Nuance-hosted services* are deployed in multiple, geographically dispersed data centers to provide high-availability, failover and redundancy, while achieving recovery time and recovery point objectives. In the unlikely event of a data center failure or other service outage, traffic is rerouted through secondary channels.

Typical features offered by our data centers*

- Tethered to regional communications hubs
- Redundant UPS feeds and backup power
- Physical security maintained by 24x7x365 security officers and cameras
- Routine risk assessments including automated vulnerability scanning on production servers and continuously updated anti-virus software
- Active network monitoring with secure firewalls and TLS-encrypted VPNs
- Proven procedures for incident response
- Climate controls and cooling systems
- Fire detection and suppression systems

*Does not entirely apply to every Nuance and/or third party facility. Some Nuance services are hosted within Nuance data centers while others may be hosted through third-party, secure cloud-computing platforms like Microsoft Azure.

Regulatory compliance and data privacy

Our approach to achieving and maintaining regulatory compliance requires diligence and staying current with relevant laws, polices, and regulations that apply to key areas of our business, while applying the proper controls through people, process, and technology.

With regulations driving operational transparency, Nuance drives compliance against consolidated and harmonized sets of compliance controls to meet all necessary governance requirements.

Standards and regulations that are important to our customers include*:

– Health Information Trust Alliance (HITRUST) Common Security Framework
– Health Insurance Portability and Accountability Act (HIPAA)
– Payment Card Industry Data Security Standard (PCI DSS)
– EU General Data Protection Regulation (GDPR) and ePrivacy Regulation

Our policies and tools that support governance and risk and compliance help manage risk and compliance issues. Our internal GRC committee provides cross-functional collaboration and alignment with business users across IT, finance, operations, and legal domains. In tandem, our GRC technology platform provides a common foundation to manage policies, controls, risks, assessments, and deficiencies across our business.

For more information about Nuance Global Security and its mission to protect our physical and information assets, visit https://www.nuance.com/about-us/security.html.

*Compliance with these regulations and others not included varies depending on Nuance product, service, industry, and geography.

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®

March 2018