

# Data security and service **continuity.**

Nuance Healthcare Solutions

## Secure and resilient networks and systems

Nuance® Healthcare customers understandably place a great deal of trust in us, and we are dedicated to earning it.

Our focus is to expand customer confidence in the integrity of our solutions, whether it be a HITRUST® certified environment, solutions with service-level guarantees, or product features that help meet Health Insurance Portability and Accountability Act (HIPAA) requirements.

Our team of certified, trained security professionals works hard to continuously enhance our security infrastructure and posture. We have made technology investments across network and IT security, including a Security Operations Center that supports Global Operations with continuous monitoring for online cyber threats.

When it comes to healthcare, we appreciate that any breach or disruption can have serious consequences. Our healthcare solutions are designed to support care teams 24x7x365, allowing them to capture, use, and share information critical to delivering the highest-quality care possible. In today's mobile-oriented environment, that means letting them use their device of choice—anywhere and at any time—without worrying about service uptimes or jeopardizing patient privacy.

### Comprehensive risk management strategy

Our approach to risk management focuses on policy, procedures, controls, governance, and assessments across the business. Our strategy is built on a foundation of best practices, proven controls, and extensive reviews such as penetration testing, scans, static and dynamic analyses, and architectural reviews. Additionally, we manage risk to protect product support functions, professional services engagements, and data center operations.

We apply specific security and privacy frameworks to ensure patient health information is treated properly. As threats become more sophisticated and our clients' demands evolve, we remain focused on improving service integrity and data security.

### Committed to a high security standard

Nuance Healthcare's policies and processes in security are based on industry standards and best practices, including the HITRUST Common Security Framework (CSF) and Center for Internet Security's CIS Controls™, and are engineered to protect against known cyber attack vectors.

We employ extensive security controls and work with outside experts to assist and augment periodic in-house risk analysis of flagship products.

To demonstrate our commitment to security, we plan to continue expanding third-party certifications across our solutions, including HITRUST CSF®, SOC I, and SOC II.

---

### Defense-in-depth approach to security

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.

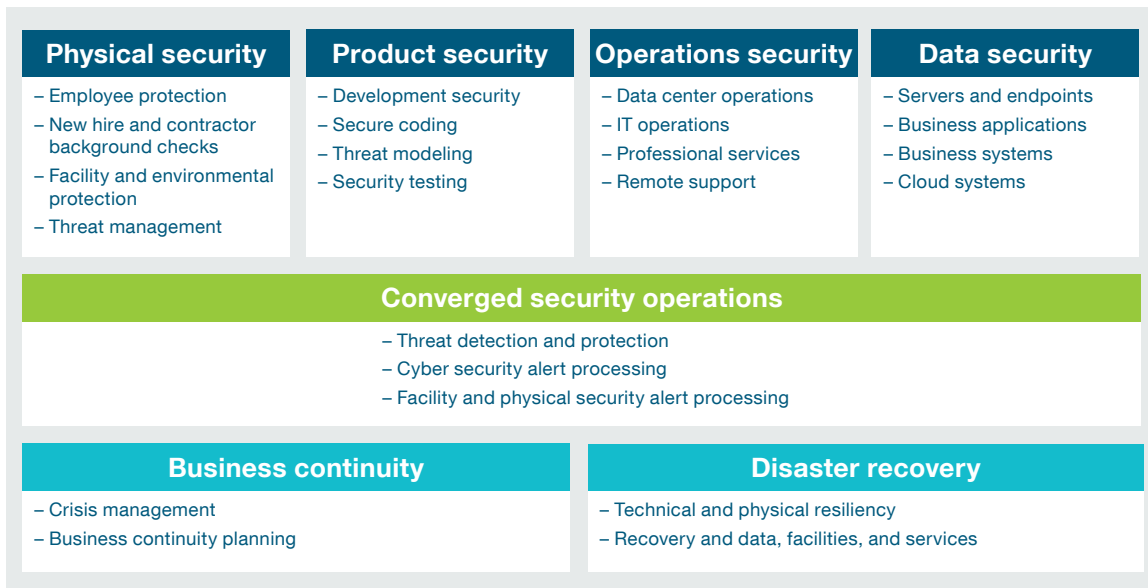
---

## The Nuance approach to security

The Nuance Global Security Office includes a chief security officer and a healthcare information security officer with teams that possess a wide spectrum of security expertise spanning IT, cyber, physical, and product. Additionally, the Nuance Privacy Office works to achieve compliance with regulations including HIPAA, GDPR, and e-Privacy.

Collectively, we are fully committed to an ever-advancing, defense-in-depth security strategy with corresponding controls intended to ensure that the healthcare data you entrust to us is kept private and protected.

Nuance will continue to invest in technologies and resources such as network and application security, security operations, data centers, and personnel to help ensure security is always job one.



### 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. Included in our physical security controls are employee background checks, mandatory security awareness training, site security guards, and video monitoring.

### Product security

The Nuance Product Security Office drives a coordinated company-wide program to instill, manage, measure, and continuously improve secure software development lifecycle (SDLC) practices. Based on industry standard frameworks such as the Microsoft® Security Development Lifecycle (Microsoft SDL) and the Building Security in Maturity Model (BSIMM), Nuance's security team sets standards and assists product teams in meeting them across key domains.

### Operations security

Maintaining open channels of communication with our customers is critical. Our security measures are designed to cover product support functions, professional services engagements, and data center operations. Our team is prepared to maintain service continuity and availability through adverse conditions and probable incident scenarios through increased network segmentation, secure credential management, enhanced security for privileged identity and access management, and critical incident process and response procedures.

### Data security

To assist in keeping information private and secure, we take a multitiered 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 authorization and access controls—we work to protect the systems that generate, move, and store sensitive business and personal information.

### Converged security operations

Our 24x7x365 Global Operations Center is augmented by our Security Operations Center (SOC), whose staff of analysts monitor, detect, analyze, and rapidly respond to malicious or abnormal online activity detected within our environment. Our SOC processes more than one million events per second from log sources across the company and utilizes advanced threat intelligence, intrusion prevention systems (IPS), intrusion detection systems (IDS), and antivirus technologies to protect our networks and systems.

### Governance, risk, and compliance

Our governance, risk, and compliance (GRC) policies and tools, along with cross-functional collaboration and alignment, provide an integrated framework using common processes and data. Our GRC platform provides a common foundation to manage policies, controls, risks, assessments, and potential deficiencies across our business.

### Conclusion

For Nuance Healthcare Solutions, the strength of our security lies in our contemporary, never-satisfied approach. We are dedicated to continuous security improvement; security is a journey with no finish line.

We know the very nature of cyber attacks is changing. They will continue to become faster, more sophisticated, and potentially more destructive. While cyber security remains a top priority for organizations across all sectors, it is especially critical for health systems to maintain the continuity and quality of patient care.

We have enhanced our network security, user and endpoint security, application and server security, and security operations and response. But we will not stop. We will continue to fortify our portfolio against threats, review policies, invest in new prevention and mitigation efforts, and certify all go-forward solutions against rigorous standards.

As part of our security strategy, we will work with our clients, share hard-won lessons learned, and explore how healthcare organizations can stand together to protect patient records, data, and information systems from large-scale, systematic disruption.

---

### Business continuity and disaster recovery

At Nuance, our goal is to maintain service continuity and availability through adverse conditions and incident scenarios. We are dedicated to applying leading industry practices to promote efficient and cost-effective response and recovery strategies that enhance business services and component resiliency. Elements of our business continuity and disaster recovery plans include:

- Defined, documented, and tested critical incident processes
- Documented solution recovery critical incident guidelines
- Defined customer communication standards and procedures
- Established and published Recovery Time (RTO) and Recovery Point (RPO) Objectives for each product

---

To learn more about Nuance Healthcare solutions, please call 1-877-805-5902 or visit [nuance.com/healthcare](http://nuance.com/healthcare).

---

---

### About Nuance Communications, Inc.

Nuance Communications, Inc. is a leading provider of voice and language solutions for businesses and consumers around the world. Its technologies, applications and services make the user experience more compelling by transforming the way people interact with devices and systems. Every day, millions of users and thousands of businesses experience Nuance's proven applications. For more information, visit [www.nuance.com/healthcare](http://www.nuance.com/healthcare) or call 1-877-805-5902. Connect with us through the healthcare blog, [What's next](#), [Twitter](#), [LinkedIn](#) and [Facebook](#).

---