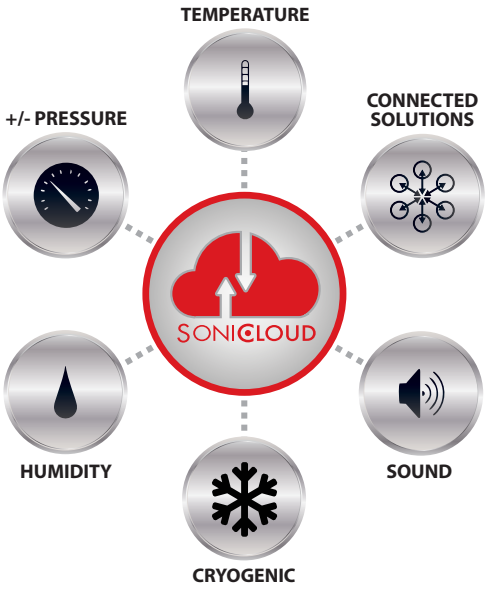
SONICU™
Monitoring Measured

www.sonicu.com

SoniCloud / AWS Technical Overview

The **Smart Choice** for remote wireless monitoring.



THE SYSTEM GOES WITH YOU

SUPERIOR ASSET PROTECTION • ELIMINATE MANUAL PROCESSES • SIMPLIFY REGULATORY COMPLIANCE

1. Sonicu Overview

Sonicu, a leader in wireless monitoring technology, offers a scalable environmental monitoring platform built for regulatory compliance. Sonicu works with hundreds of organizations across the country including many leading hospitals, manufacturing companies, universities, distribution, pharmaceutical and research companies that rely on Sonicu to help safely store food, drugs and valuable research materials. Sonicu offers a wide array of monitoring applications including temperature, humidity, pressure, sound and custom IoT applications for organizations across a broad spectrum of industries.

Specific to the platform are wireless sensors for temperature, humidity, air pressure, sound levels, and a host of other applications that transmit data via WiFi, Ethernet or Cellular to SoniCloud, our cloud-hosted monitoring platform. Sonicloud is hosted on **Amazon Web Services** (AWS) US East, which is a FedRAMP authorized system. AWS provides multi-regional failover, security controls, and maintains continuous platform monitoring.

SoniCloud is a SaaS-based platform that requires no server or software maintenance by the client. Sonicu periodically updates Sonicloud, allowing clients to benefit from the most recent system improvements.

2. Protected Health Information (PHI) and HIPAA Statement

Sonicu monitors and records environmental data such as the temperature of cold storage equipment, room temperature and humidity, sound, air pressure, etc. This is the only data that is transmitted to AWS. To that end, there is **no PHI or other HIPAA related information transmitted by Sonicu devices.**

3. System Access and User Credentialing

Clients access the SoniCloud platform by logging into **https://www.sonicumonitoring.com**. This website can be accessed on desktops, tablets, and phones. Users log in with their own unique credentials and are limited to only the sites and areas that are required for their job functions. All user interaction happens with the sonicumonitoring.com domain and subdomains hosted with AWS.

Sonicu credentials users at two levels: Admin and View. Our clients may have as many users as needed at either level. Creating users is simple from within SoniCloud's web-based user interface: Admin level users can create, edit, and remove other users as needed. At a minimum, Sonicu will collect users' email address, name, and a Sonicu-specific password for authentication.

Users may choose to receive alarm notifications via text, email or phone calls. If users opt-in to these features, Sonicu will also collect phone numbers and other information as needed to deliver alarms. Reports are available to users on-demand by logging into the system; individual users can also elect to receive auto-generated reports via email.

Sonicu's password policy system is configurable by the client and includes the ability to force password minimum length as well as password complexity (requiring numbers, uppercase letters, lowercase letters, symbols, passwords cannot match previous passwords, etc.). Sonicu also has a client-configurable password reset feature that requires passwords to be reset on a client-defined interval of days. All passwords in the Sonicu system are salted and stored encrypted (via the Blowfish encryption cypher) in the Sonicu database, ensuring that passwords are secure and cannot be easily decrypted in the unlikely event of a data breach.

4. Data Transmission and Network Topology

Sonicu offers a number of deployment options to best meet clients' security requirements, physical layout and budget. The table below highlights Sonicu deployment strategies for your facility.

		Network Placement	
		OFF Your Network	ON Your Network
Device Communication Method	Sensor to Mesh to Cloud	Example: 900 MHz to Cellular Section 4.1	Example: 900 MHz to Ethernet Section 4.3
	Sensor to Cloud	Example: Direct Cellular Section 4.2	Example: Ethernet and WiFi Section 4.4

4.1. Sensor to Mesh to Cloud: Off Your Network

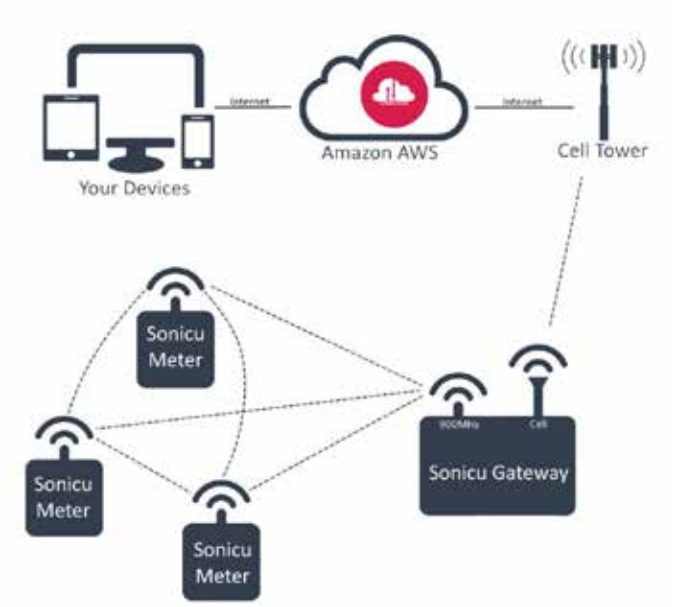
Example Topology: 900 MHz to Cellular

Sonicu's sensors sit in the client facility and never touch the client's internal network. Sensor data is transmitted via 900 MHz radios (internal to the sensors) to a central cellular gateway and then to Sonicu's AWS platform.

900 MHz radios typically provide superior radio signal compared to WiFi and Cellular and are cost effective. Furthermore, 900 MHz radios have the ability to "Mesh," providing a self-healing, reliable network. This is an ideal option for clients with many sensors in one area that can share a single cellular data plan.

SoniCloud / AWS Topology – OFF Network

The gateway utilizes a cellular modem to send data packets to SoniCloud. All traffic sent from the cellular modem is encrypted via a VPN and decrypted by Sonicu at AWS, ensuring data remains protected as it travels over the internet.



4.2. Sensor to Cloud: Off Your Network
Example Topology: Cellular

Most Sonicu sensors have the ability to serve both as a sensor and a data gateway by using a cellular modem internal to the sensor. This is an ideal option for locations that wish to use cellular transmission option and have a small number of sensors in each location.

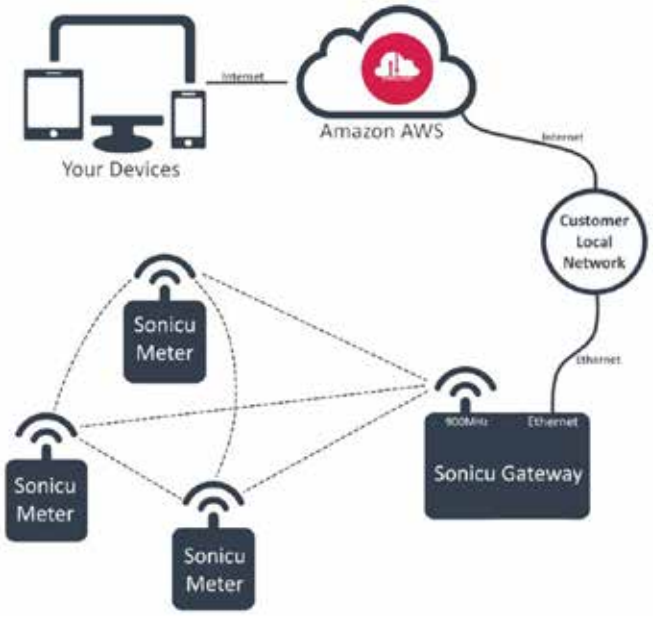
Sonicu's sensors sit in the client facility and never touch the client's internal network. All traffic sent from the cellular modem is encrypted over a VPN and decrypted by Sonicu at AWS, ensuring data remains protected as it travels over the internet.

SoniCloud / AWS Topology – ON Network

4.3. Sensor to Mesh to Cloud: On Your Network

Example Topology: 900 MHz to Ethernet

Data is transmitted via 900 MHz radios (internal to the sensors) to central gateway(s) that are connected via Ethernet. The gateway utilizes the client network to send data packets to Sonicloud.



900 MHz radios typically provide superior radio signal compared to WiFi and Cellular and are cost effective. Furthermore, 900 MHz radios have the ability to "Mesh," providing a self-healing, reliable network. This is an ideal option for clients with many sensors in one area who want to use their network for data transmission.

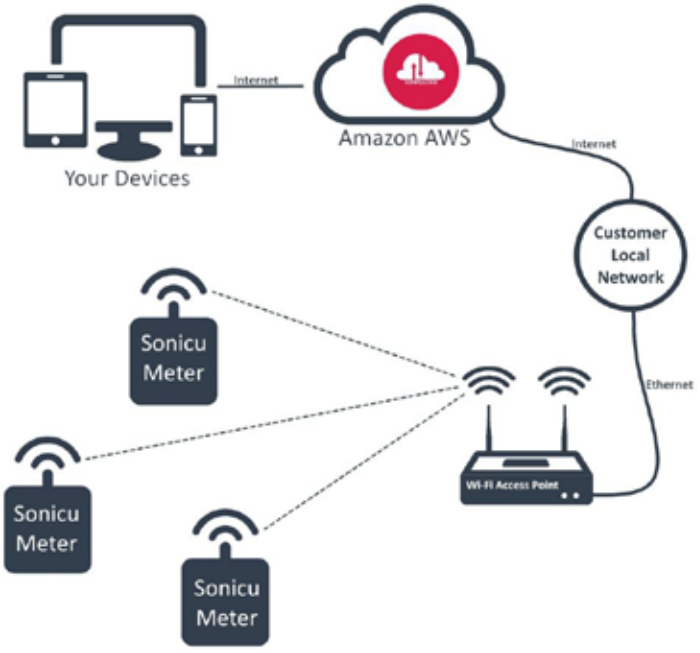
An Ethernet with cell failover option is available for customer applications that cannot afford temporary service interruptions.

Sensor data can be transmitted in a variety of ways; further transmission protocol information can be found in Section 4.5.

4.4. Sensor to Cloud: On Your Network

Example Topology: WiFi

Sonicu sensors can be equipped with WiFi radios configured to communicate with the client's WiFi network. This option allows the client to leverage an existing WiFi infrastructure to add sensors anywhere the WiFi network is accessible.



Sensor data can be transmitted in a variety of ways; further transmission protocol information can be found in Section 4.5.

4.5. Network Transmission

Cellular (click for radio data sheet)

Sonicu maintains a VPN between Verizon and Amazon Web Services (AWS). Cellular configuration offers additional advantages in that the system can be fully configured prior to shipping for simple implementation. Sonicu is a Verizon Vertical Partner (VPP) and uses Verizon 4G LTE network.

900 MHz (click for radio data sheet)

High performance radio with frequency-hopping spread spectrum and self-healing meshing networking. Used when the client's internal WiFi network cannot be used. The powerful radio allows for longer distance communication than WiFi.

WiFi (click for radio data sheet)

Standard 2.4 GHz WiFi with b/g/n network compatibility and WPA2 security.

4.6. Network Requirements

WiFiThe following requirements pertain to ALL Sonicu topology options (Cellular, WiFi, Ethernet):

- Our server will send your users' emails from both @sonicu.com and @sonicumonitoring.com addresses. Please white list both of these in your mail server.
- Web clients communicate with our monitoring site via https://www.sonicumonitoring.com. All web assets will come from this address.

Ethernet and WiFi network topologies require additional input from your IT department. For these types of networks, Sonicu has a Network Questionnaire that clients complete and send to Sonicu. The information below pertains to Sonicu devices that transmit on your network (WiFi or Ethernet).

5. Data Storage Information

Sonicu is hosted on Amazon Web Services (AWS). Data is stored long-term with AWS. AWS was chosen by Sonicu for its security, redundancy and scalability.

Below are some links related to AWS security.

Security - Overview of Amazon's security benefits, including redundancy.

Resources - List of white papers, articles, etc. regarding AWS security.

Fortune Article - Describes the physical security and requirements needed to access the servers.

Security Whitepaper - PDF detailing security benefits to clients.

FedRAMP - AWS information related to FedRAMP.

6. Device Security

In order to provide extremely long battery life, Sonicu uses low voltage microprocessors with minimal computing ability. Sonicu's devices feature an Atmel ATX Mega microprocessor, a 16-bit microcontroller with only 16KB RAM. The extremely small technical capabilities of the microprocessor, combined with the fact that Sonicu has a custom firmware solution running on the device, effectively reduce the potential for any type of network attack to zero. More technical details can be provided upon request.

7. Sonicu's Cloud Infrastructure

Sonicu utilizes Amazon Web Services (AWS) technologies to provide reliable, scalable solutions for our clients. Sonicu's internal AWS network credentials are based upon the principle of least privilege, ensuring that each service can only access what is required. Sonicu uses the AWS Relational Database Service (RDS) to host its MySQL database in multiple regions with duplication and immediate failover to ensure high levels of quality. Sonicu routinely patches its servers on a weekly basis, with more pressing industry-wide security threats (e.g., Heartbleed) being patched as soon as possible. As Sonicu's platform is web-based, no patches need to be provided to the client directly.

SoniCloud / AWS FAQs

8. FAQs

1. **Does Sonicu store or transmit any Protected Health Information (PHI)?**
   Absolutely not. Sonicu monitors and records environmental data such as the temperature of cold storage equipment, room temperature and humidity, sound, air pressure, etc. This is the only data that is transmitted to AWS.

2. **Can Sonicu meet our password access control requirements?**
   Yes! Sonicu has a large range of password control requirements that are configurable. Please see Section 3 for more details.

3. **Does Sonicu reside on our local network?**
   All of Sonicu's software, including the SoniCloud web interface, are located on AWS, not on the client's network. Sonicu's physical devices can, if chosen by the client, be located on the client's network; other options exist to physically separate Sonicu devices from a client's network if required.

4. **Does Sonicu provide auditing capabilities?**
   Yes! Sonicu's SoniCloud software provides logs of important user actions, such as clearing alarms and changing alarm thresholds. These audit logs can be provided to the user as requested.

5. **What software does the customer need to use the Sonicu platform?**
   Sonicu relies on the customer having a standard, current generation web browser installed. There is nothing else needed -- no plug-ins, no software, nothing!

6. **What data transmission options does Sonicu employ to ensure data security?**
   Sonicu provides encryption options over the cellular network (if the devices are located off of the client network) or offers a B2B IPSec VPN as required (if the devices are located on the client network) for device data transmission to AWS. Sonicu forces HTTPS for all web connections.

Sonicu Wireless Remote Monitoring
19 West Main Street, Greenfield, IN 46140
Toll-Free: 844-4SONICU • Direct: 317.468.2345
Fax: 317.586.4804 • Email: info@sonicu.com