Protecting Patient Information and Your Network

Connex® vital signs devices and connectivity solutions now include DoD RMF Approved security features

We understand that data security is a top healthcare concern, especially as data breaches and cyberattacks continue to make headlines. That's why our vital signs devices are built with tested and DoD-approved security features. Your clinicians can take advantage of connected workflows that help improve patient care and information access while still protecting patient privacy and data integrity and helping to safeguard your network.

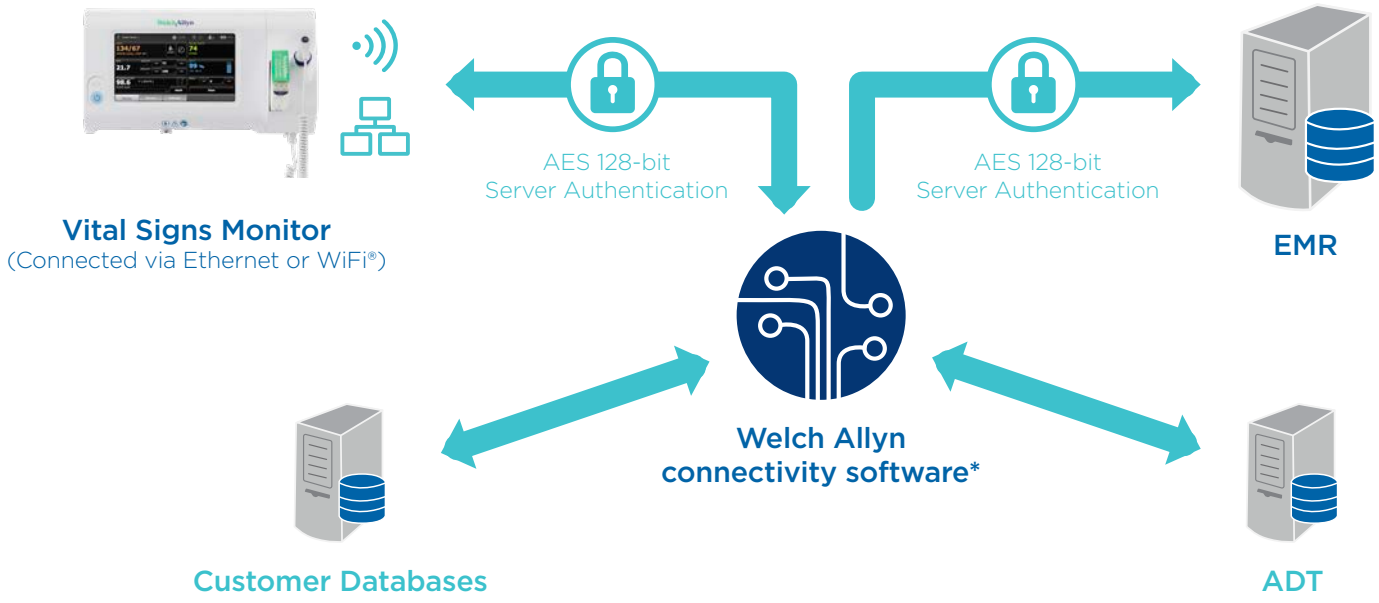
Secure Solutions

The Welch Allyn Connex family of vital signs devices feature DoD Risk Management Framework (RMF) Approved security features to help you protect your patients and your infrastructure.

Connex Vital Signs Monitor

Connex Spot Monitor

Connex Integrated Wall System



*Welch Allyn Connex Server Application Software (CSAS) or Network Connectivity Engine (NCE)

Protect What Matters.

Enhanced security features throughout the Connex family of devices and connectivity solutions can help you protect the information that matters most. We are helping to keep your data safe where it is, and when it moves, with the following features:

- FIPS-approved encryption of transmitted data
- More secure inter-network communication with device and server authentication
- Protection of devices from unauthorized changes with digitally signed software images and configuration files
- Single sign-on options, including integration with Imprivata, for quick, secure clinician login
- Screen lock function protects idle devices from unauthorized access
- Automated deletion of patient data after sending to the EMR clears information from the device

Contact your Welch Allyn representative or visit **www.welchallyn.com** to learn more.

www.welchallyn.com

Welch Allyn®