COVID-19 CONTACT TRACING

PROTECTING CRITICAL HEALTHCARE ORGANIZATIONS AND THEIR STAFF

COVID-19 infections of medical staff pose a major concern for hospitals. Besides the health risks to staff members, infections can lead to the quarantine of entire teams and shortage of available staff. It's critical to identify any staff members who have been exposed to an infected individual and trace their contacts including with other team members in order to control and reduce the risk of additional infection.

FASTER AND EFFECTIVE CONTACT TRACING

Unlike traditional manual processes, Armis can process the location information of potentially exposed medical staff and trace their whereabouts within the hospital faster. We do this by tracking the devices of the staff members - most notably devices like Vocera badges widely used in hospitals today.

Armis can passively collect and identify connections and activities of the device on the network - including their locations at given points in time based on data obtained from the network's access points (AP). Using this information, Armis can provide location data relevant to contact tracing based on defined steps.

THE ARMIS PLATFORM

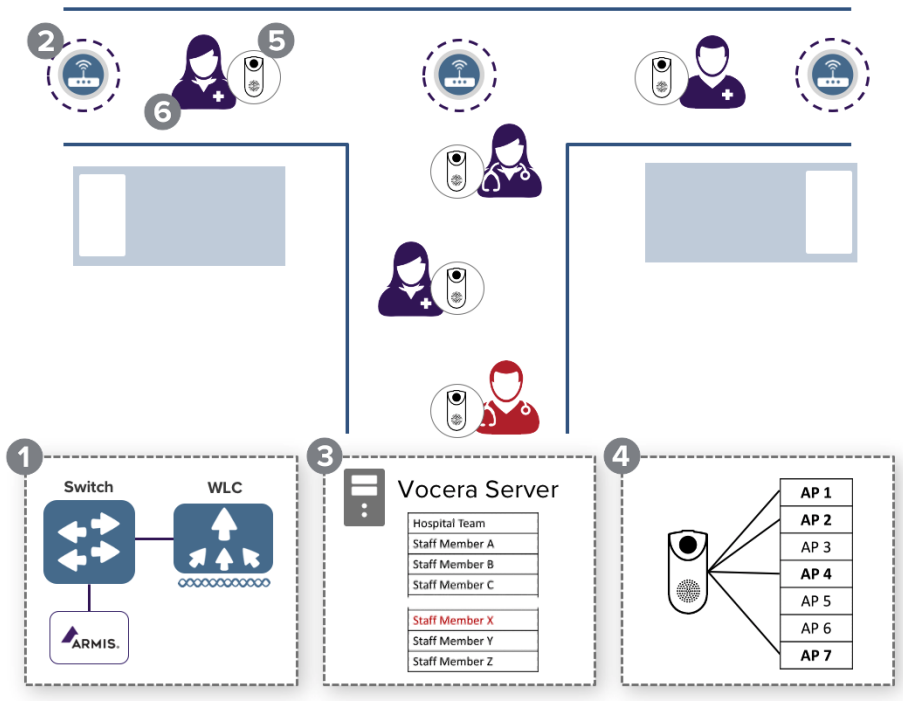
COMPREHENSIVE
Discover & classify all medical devices in your environment, on or off your network.

AGENTLESS
Nothing to install on devices, no configuration, no device disruption.

PASSIVE
No impact on your organization's network. No device scanning.

FRICTIONLESS
Installs in minutes using the infrastructure you already have.

HOW ARMIS WORKS



1. Armis connects easily to WLC.
2. Tracks all devices via WiFi connection to nearest Access Point (AP).
3. If infected staff member X is identified, the hospital identifies the ID of the Vocera Badge that X was using during a relevant timeframe.
4. A simple search query in Armis for the connections of the badge ID in a specific time frame yields those APs to which the badge was connected.
5. A search of all connections to that AP in Armis will reveal other badge IDs which were registered by that AP at the same time.
6. A reverse look up - from badge IDs back to staff members - will provide the list of potentially infected members who were in close contact with team member X.

AGENTLESS, NON-DISRUPTIVE, SOC COMPLIANT

Armis is a completely agentless solution, so there is no software to install or update on individual devices. We are also 100% passive - so we do not disrupt any device's operations.

Also, Armis is SOC2 compliant and adheres to guidelines regarding data protection. We do not collect content, just network parameters. Data is stored on a dedicated and private cloud accessible only to the hospital.

TRACKS DEVICES, NOT PEOPLE

Armis only track devices. We don't map devices to individuals - this can be done by the hospital. Additionally, Armis provides control over who can view Personally Identifiable Information in our console.

ARMIS.

1.888.452.4011
armis.com

CONTACT TRACING CHALLENGES

Traditional contact tracing is a completely manual process which can take too much time and result in inaccurate information.

- Interviews with infected staff member requiring recall of whereabouts and contacts with other staff
- Interviews with other staff who were potentially in contact including their own whereabouts
- Analysis of patient records to correlate staff who have treated and/or had contact with infected patient
- Random encounters do not show up in medical records of staff

ABOUT ARMIS

Armis is the first agentless, enterprise-class security platform to address the new threat landscape of unmanaged and IoT devices. Fortune 1000 companies trust our unique out-of-band sensing technology to discover and analyze all managed, unmanaged, and IoT devices—from traditional devices like laptops and smartphones to new unmanaged smart devices like smart TVs, webcams, printers, HVAC systems, industrial robots, medical devices and more. Armis discovers devices on and off the network, continuously analyzes endpoint behavior to identify risks and attacks, and protects critical information and systems by identifying suspicious or malicious devices and quarantining them. Armis is a privately held company and headquartered in Palo Alto, California.

20200617-1