FORTINET | PULSE

# Cybersecurity of web-connected medical devices

The internet-of-things is expanding into healthcare with a variety of web-connected medical devices. These devices introduce great potential for advances in healthcare, but they also create additional attack surfaces that tech leaders must address.

Pulse and Fortinet surveyed 125 tech leaders in healthcare whose organizations have web connected medical devices to find out how these leaders are approaching the security of these devices.

Data collected from May 27 - July 19, 2021

Respondents: 125 tech leaders in healthcare

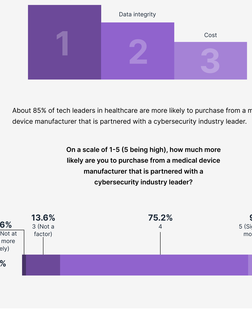
## Healthcare organizations are increasing their fleet of web-connected medical devices and prioritizing cybersecurity

Healthcare companies with web-connected medical devices are purchasing new devices frequently. 86.4% of respondents expect to make their next purchase within 2-7 months.

**When do you plan to make your next purchase of web-connected medical devices?**


Improving the cybersecurity posture of their web-connected devices is a priority for 91% of respondents.

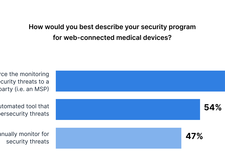
**How high a priority is improving the cybersecurity posture of your web-connected medical devices in 2021?**




## Tech leaders seek web-connected medical devices with strong protections against cybersecurity attacks

When considering the cybersecurity of their web-connected medical devices, healthcare tech leaders are most concerned about cybersecurity attacks, data integrity, and costs.

**Please rank the 3 most significant cybersecurity concerns your organization is currently experiencing with regards to your web-connected medical devices.**




About 85% of tech leaders in healthcare are more likely to purchase from a medical device manufacturer that is partnered with a cybersecurity industry leader.

**On a scale of 1-5 (5 being high), how much more likely are you to purchase from a medical device manufacturer that is partnered with a cybersecurity industry leader?**


## Good cybersecurity will also require the right security program and tools

Although all respondents have plans for or have adopted a security program for their web-connected medical devices, 44% of respondents are still in the early stages of either active research or broad future plans.

**Which of the following best describes the status of your organization's security program for web-connected medical devices?**




Most respondents (64%) describe their security program for web-connected medical devices as being outsourced to a third party.

**How would you best describe your security program for web-connected medical devices?**




More than 1 in 15 respondents (8.8%) rely solely on manual monitoring to detect security threats to their web-connected medical devices.

Tech leaders in healthcare value cybersecurity tools that offer centralized control of physical and virtual security, easy integrations (API, fabric connectors), and high performance processing.

**Which 3 of the following cybersecurity tool features would be most attractive or beneficial to your organization?**




## Respondent Breakdown




Insights powered by PULSE