Cybersecurity of web-connected medical devices

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.

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.

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?
- 2–4 months: 48.8%
- 4–7 months: 4%
- 7–12 months: 9.6%
- Over 12 months: 0%

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?
- High priority: 18%
- Medium priority: 70%
- Low priority: 9%
- Not at all a priority: 3%

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.

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.

Please rank the 3 most significant cybersecurity concerns your organization is currently experiencing with regards to your web-connected medical devices.
- 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?
- Cybersecurity attacks: 13.6%
- Costs: 75.2%
- Data integrity: 9.6%
- Other: 4%

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.

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

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 of the following best describes the status of your organization’s security program for web-connected medical devices?
- Actively researching: 38%
- Installed or in production (active program): 27%
- Piloting: 29%
- On the radar: 6%
- No plans for a security program: 0%

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

- Centralized control of physical and virtual security: We outsource the monitoring of cybersecurity threats to a third party (i.e. an MSP): 64%
- Easy integrations (API, fabric connectors): We have an automated tool that detects cybersecurity threats: 54%
- High performance processing: We manually monitor for security threats: 47%

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