

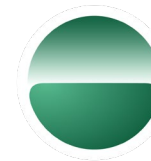


12TH ANNUAL LEADERSHIP EVENT

CYBER SECURITY SUMMIT

Security solutions through collaboration.™

TITLE SPONSOR



Island

EYES WIDE OPEN



CYBER SECURITY SUMMIT
Security solutions through collaboration.™

12th Annual Cyber Security Summit | October 24-26, 2022

cybersecuritysummit.org

Medical Device Software End of Life Planning

Every medical device company has products running code not written by them. That software ranges from components like a small software bridge that enables Bluetooth connectivity to an entire Windows operating system that runs underneath our clinical applications. As that software ages, there are inevitably vulnerabilities that introduce new risks. If they doesn't control that software, how can we control these risks? This makes supporting our medical devices...tricky.

Medical Device Software End of Life Planning

Medtronic

Engineering the extraordinary

EoL Group Therapy

2022-10-20

Judd Larson

EoL Stages of Grief

Denial
Anger
Bargaining
Depression
Acceptance

About me

At Medtronic for 4 years

Before that, at Fairview Health Services in MN

Currently focus on post-market product cybersecurity activities with the Enterprise Quality, Product Security Office, but also dabble in other things.

My Goal: Help you leave with better questions to ask than when you arrived and *maybe* a few answers.

ASK: Bring your own cases and situations up for discussion.

Buts and What Ifs are encouraged

About you

**What products are you
thinking about?**



What is EoL

The background of the image is a dense field of tall, dry grass. The grass blades are long and thin, with a mix of golden-brown and reddish-brown hues. Several large, fluffy white seed heads are visible, adding texture to the scene. A dark blue horizontal band is superimposed across the middle of the image, containing the text.

What is unsupported software?



What is can we do about EoL
software? (Today)



What is EoL

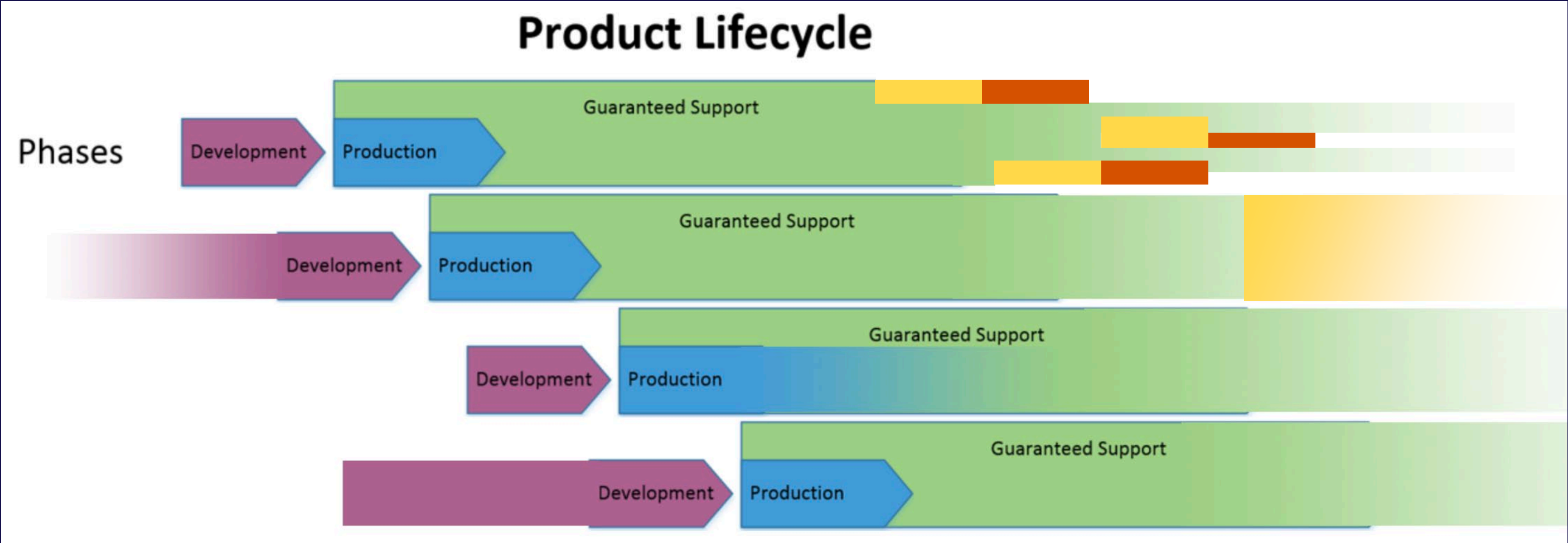
& Why can lack of software support drive it?

Terms



Any other terms?

My understanding of reality



Why does a software vulnerability influence EoL of an otherwise useful device?

- 1 • Your product is made up of physical and software components.
 - Without both, your product will not function.
- 2 • If a component has a flaw that introduces risk, that risk needs to be mitigated.
 - Controls must be scientifically provable
 - For cybersecurity issues, the attacker controls the odds of occurrence.
- 3 • If that risk cannot be mitigated, Medtronic needs to end its liability



Safety is keeping bad products from harming good people

Security is keeping bad people from harming good products

Certainties

Patients and other users don't want to trust insecure products

FDA postmarket cybersecurity guidance has directional requirements

TIR97 is recognized as an FDA consensus standard that provides more detail on how to meet their expectations

The need to EoL a product for security reasons is a combination of the need to mitigate vulnerabilities along with the inability to actually mitigate the vulnerability in a product

More?

Uncomfortable Uncertainties

Post-market enforcement is currently unclear

Different business functions have very different thoughts on EoL timing

Global implications of EoL vary

More?

The background of the image is a close-up, top-down view of a dense patch of tall grass. The grass blades are long, thin, and have a mix of colors, including golden-brown, tan, and some green, suggesting they are in a late stage of growth or beginning to dry. Several large, fluffy white seed heads are visible, rising from the blades. A dark blue, semi-transparent rectangular banner is positioned horizontally across the middle of the image, containing the text "What is unsupported software?".

What is unsupported software?

Analogies are crucial: What is software?

Instructions for carefully directing electricity

What is **unsupported** software?

If flying cars were invented and no one makes laws and stoplights and defines traffic patterns, our existing infrastructure would be unsupported.

For those unfamiliar with software development

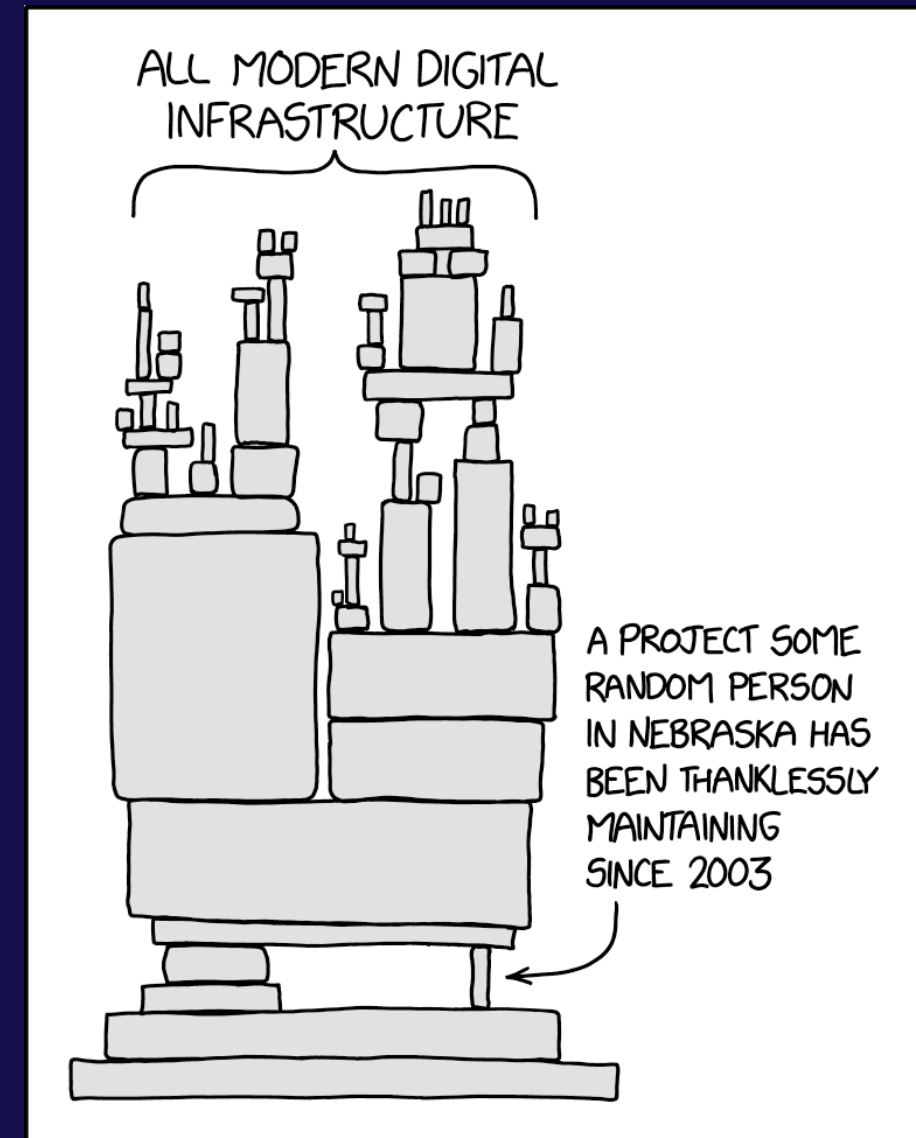


Druthers Haver
@6thgrade4ever

the most consequential figures in the tech world are half guys like steve jobs and bill gates and half some guy named ronald who maintains a unix tool called 'runk' which stands for Ronald's Universal Number Kounter and handles all math for every machine on earth

1:27 am · 03 Sep 21 · [Twitter for Android](#)

2,859 Retweets **77** Quote Tweets **16.7K** Likes



<https://xkcd.com/2347/>

Eyebrow raise or side-eye for anyone?



What is can we do about EoL
Software? (Today)



Fantasy World of Software Support

<https://foundation.app/@WanHedaNFTS/foundation/106595>



We have a plan to EOL the product when support is no longer feasible.

When a component is no longer supported, we have a plan and funding allocated to mitigate that risk.

We know and appreciate the extent that all components are supported.

We know every component of a product's software.

We know every component of a product's software.

When a component is no longer supported, we have a plan and funding allocated to mitigate that risk.

We know and appreciate the extent that all components are supported.

We have a plan to EOL the product when support is no longer feasible.

We know every component of a product's software.

This is SBOM.

SBOM = Software Bill of Materials = Ingredient list of software components

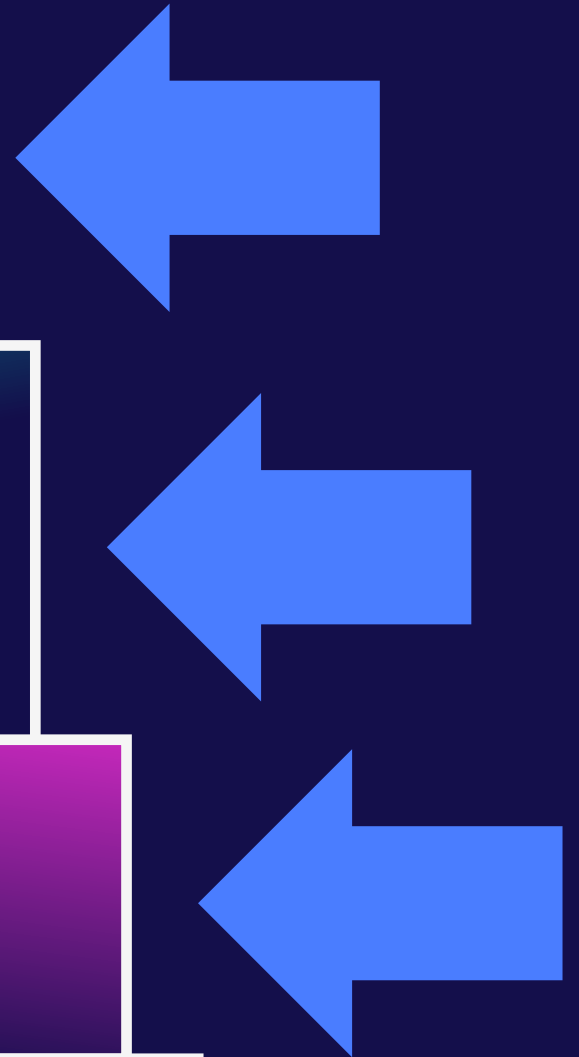
Important concept, but not something we want to dig into here.

We have a plan to EOL the product when support is no longer feasible.

When a component is no longer supported, we have a plan and funding allocated to mitigate that risk.

We know and appreciate the extent that all components are supported.

We have a plan to EOL the product when support is no longer feasible.



If there is a vulnerability, can the manufacturer fix it?

We know and appreciate the extent that all components are supported.

Who monitors for security issues in SW components?
What happens when an issue is found?
When can a fix be developed?
Where do update activities take place?
Why would we need to fix software?
How important is that component to functionality?

We know and appreciate the extent that all components are supported.

Windows OS (Clear EOL)

Support Dates

Listing	Start Date	Mainstream End Date	Extended End Date
Windows 10 IoT Enterprise LTSC 2021	Nov 16, 2021	Jan 12, 2027	Jan 13, 2032

<https://learn.microsoft.com/en-us/lifecycle/faq/windows>

Support Dates

Listing	Start Date	Retirement Date
Windows 10 Home and Pro	Jul 29, 2015	Oct 14, 2025

Releases

Version	Start Date	End Date
Version 21H2	Nov 16, 2021	Jun 13, 2023
Version 21H1	May 18, 2021	Dec 13, 2022

Open source component (No support, maybe?)

Google

open source time zone code

All

Images

Books

News

About 3,800,000,000 results (0.60 seconds)

https://github.com › graphhopper › timezone

graphhopper/timezone - GitHub

Timezone project providing a simple way to turn local time. www.graphhopper.com/open-source

https://github.com › eggert

eggert/tz: Time zone database and code

Time zone database and code. Contribute to GitHub.

Product

Solutions

Open Source

Pricing

graphhopper / timezone Public

<> Code

Issues 1

Pull requests

Actions

Projects

Security

Insights

master

3 branches

2 tags

Go to file

Code

oblonski Merge pull request #7 from afoeder/patch-1

7220c5d on May 9, 2019 90 commits

timezone-core

add copyright - fix #1

5 years ago

timezone-webapp

add copyright - fix #1

5 years ago

world-data

separate data from lib - related to #6

5 years ago

.gitignore

ini commit

6 years ago

.travis.settings.xml

mv travis stuff

5 years ago

.travis.vml

mv travis stuff

5 years ago

The Graph Hopper Timezone component we use in [Product] will not be supported starting next year, so we started rolling out an update to swap it for a different one.

When a component is no longer supported, we have a plan and funding allocated to mitigate that risk.

The project is funded through the post-market development budget.

The Graph Hopper Timezone component we use in [Product] is not supported and has critical vulnerabilities.

We are unable to mitigate those vulnerabilities.

What do we do now?

When a component is no longer supported, we have a plan and funding allocated to mitigate that risk.

This is the culmination of all the discomfort.

Why are we trying to remove therapy delivering products from their users?

We have a plan to EoL the product when support is no longer feasible.

For most products, this is not planned today, which makes it uncertain and scary for the business.

With appropriate planning, this could just be a normal part of the product lifecycle, and not an emergency or fire drill.

We have a plan to EoL the product when support is no longer feasible.

Creative solutions?

New business models:

Think like other companies - All the printers in this building don't need to be owned by Medtronic. We can pay someone for the service and never have to worry about updates or service.

Influence regulators:

If we've got the update process perfected, but are running into issues with regulatory approval, we can make a case for change.

Modularize products:

Make it easy to update individual components on a regular basis. Be able to replace the product's computer without having to swap the entire thing.

Share common platforms:

If everyone is using the same base software, one group can more easily maintain it.

What else comes to mind?



More discussion?



Thank you for coming!

Judd.Larson@Medtronic.com
Security@Medtronic.com