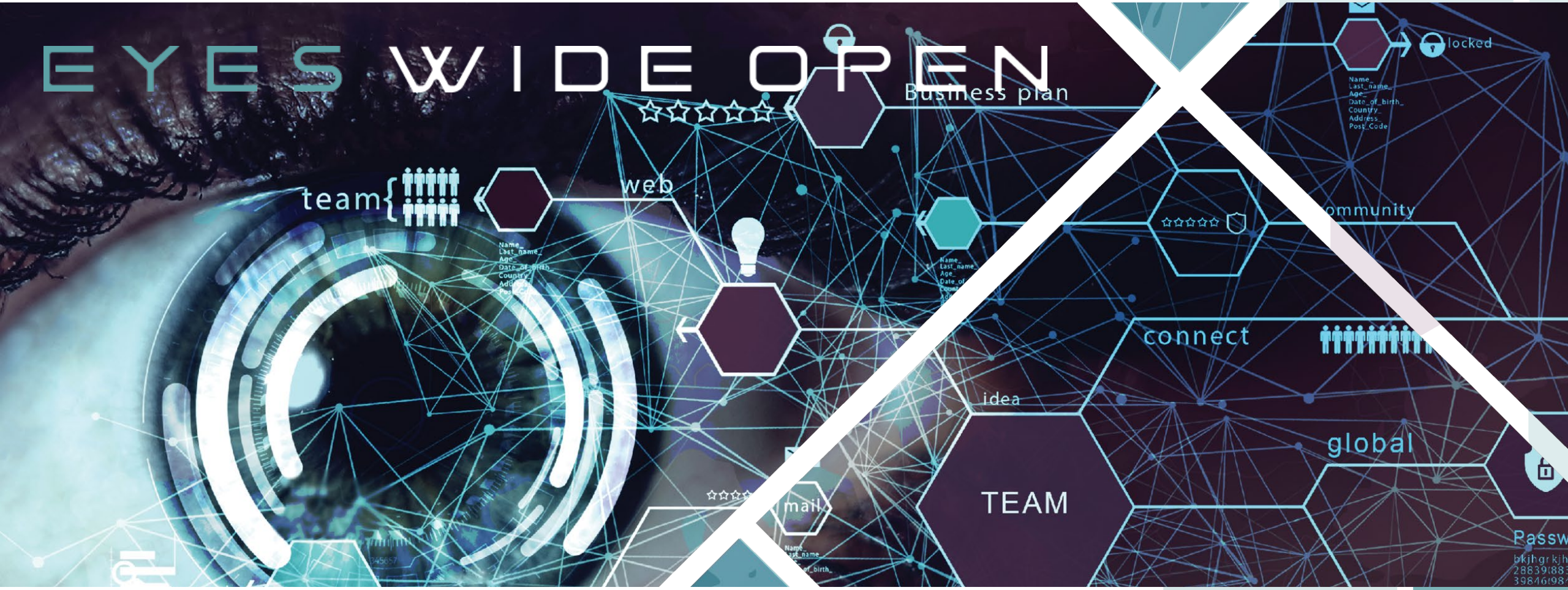
12TH ANNUAL LEADERSHIP EVENT

CYBER SECURITY SUMMIT

Security solutions through collaboration.™

TITLE SPONSOR

Island



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.

Medtronic

Engineering the extraordinary

Medical Device Software End of Life Planning

2022-10-20

Judd Larson

Medtronic

Engineering the extraordinary

EoL Group Therapy

2022-10-20

Judd Larson

Medtronic

Engineering the extraordinary

EoL Stages of Grief

Denial

Anger

Bargaining

Depression

Acceptance

2022-10-20

Judd Larson

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

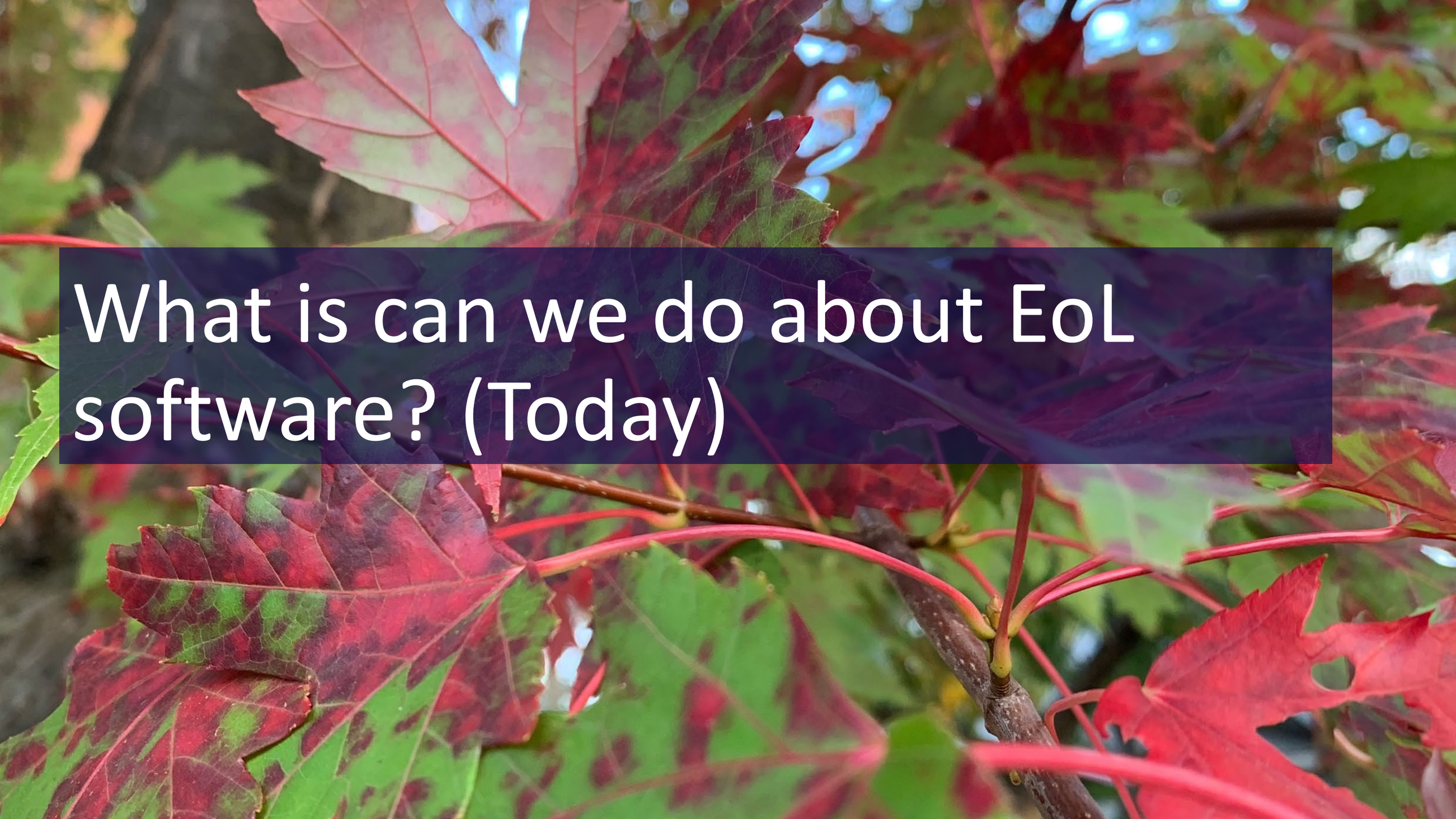
Medtronic

What products are you thinking about?

Medtronic


What is EoL

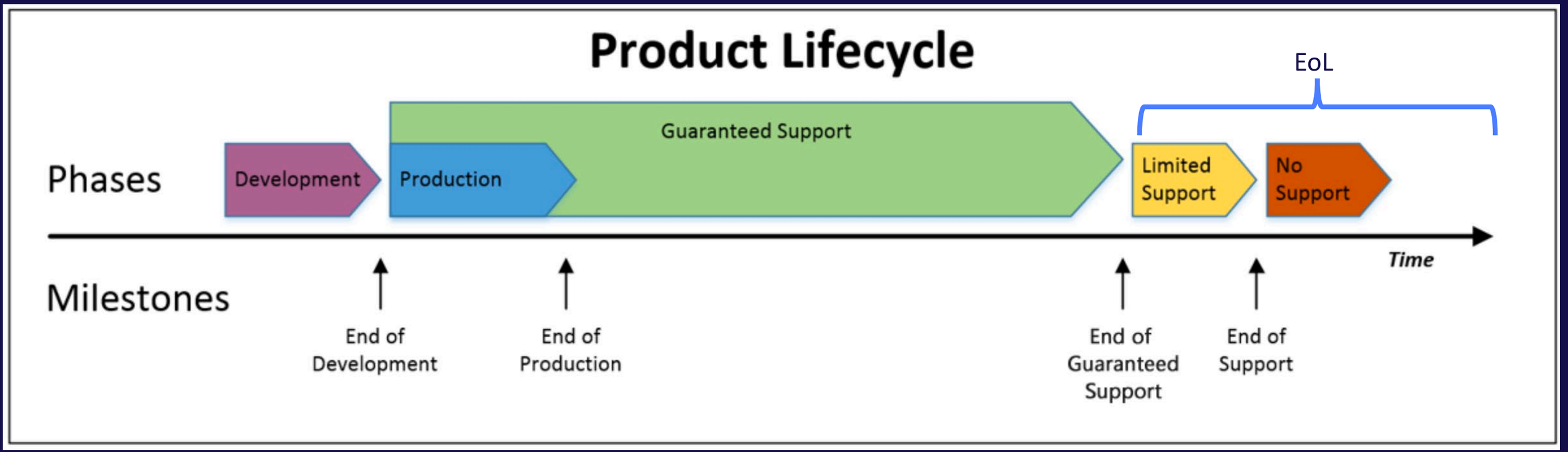

What is unsupported software?


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

What is EoL

& Why can lack of software support drive it?

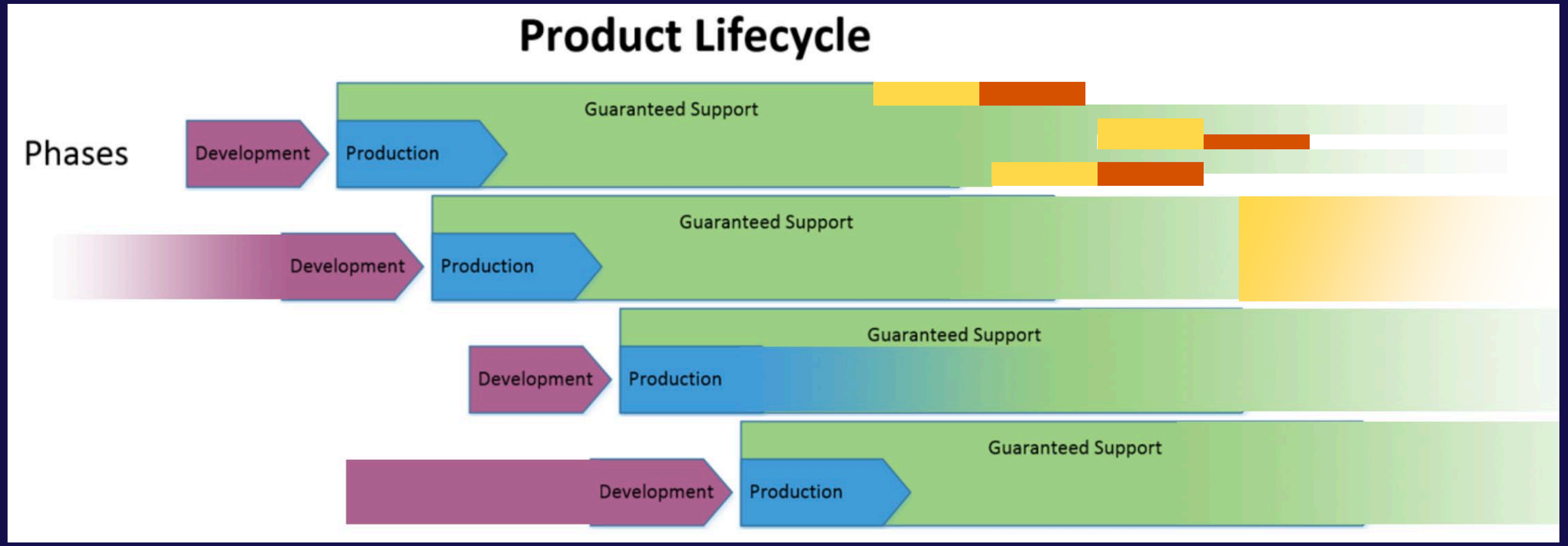
Terms



Any other terms?

Medtronic

My understanding of reality



Medtronic

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

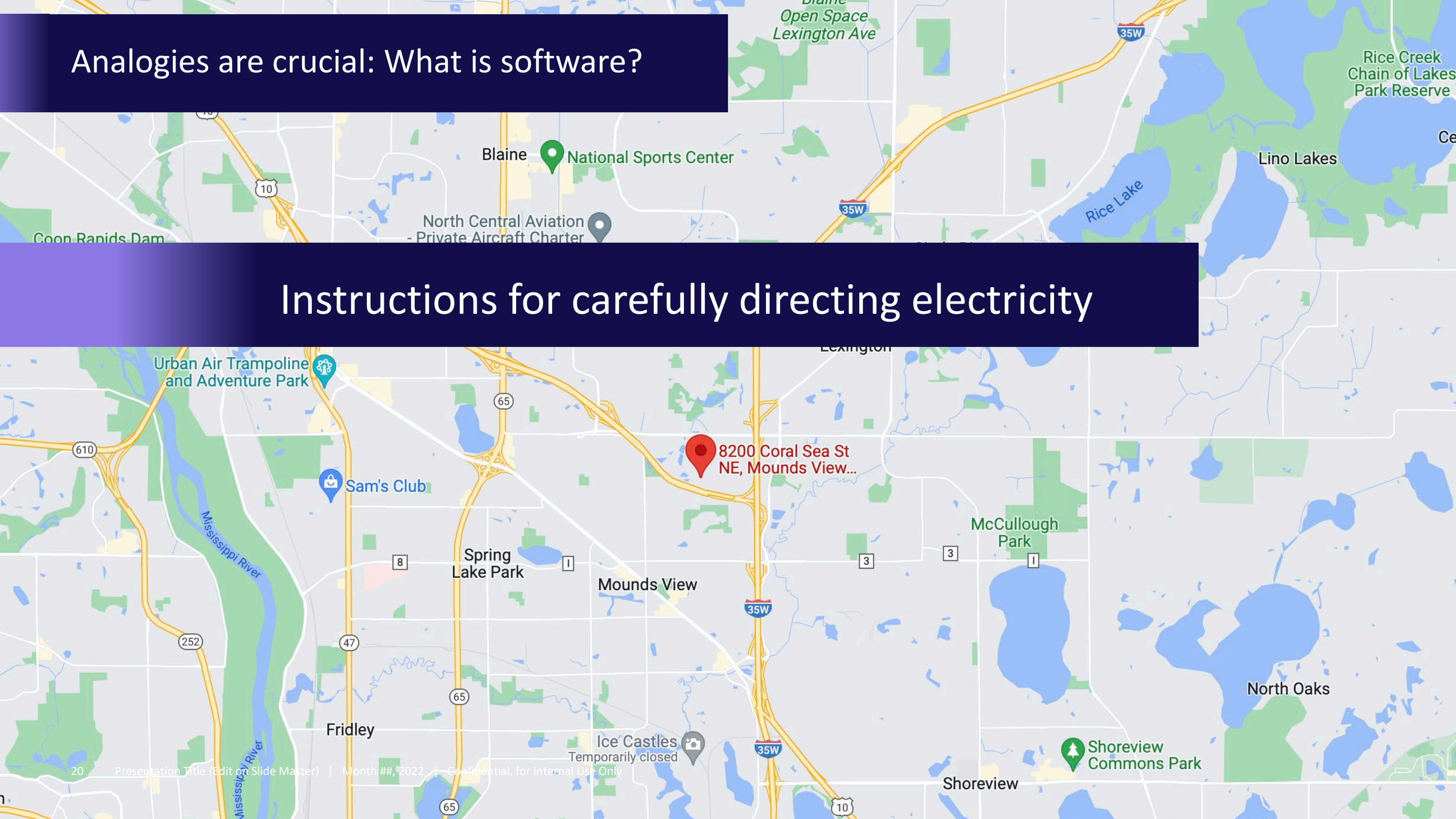
Different business functions have very different thoughts on EoL timing

Global implications of EoL vary

More?


What is unsupported software?

Analogies are crucial: What is software?

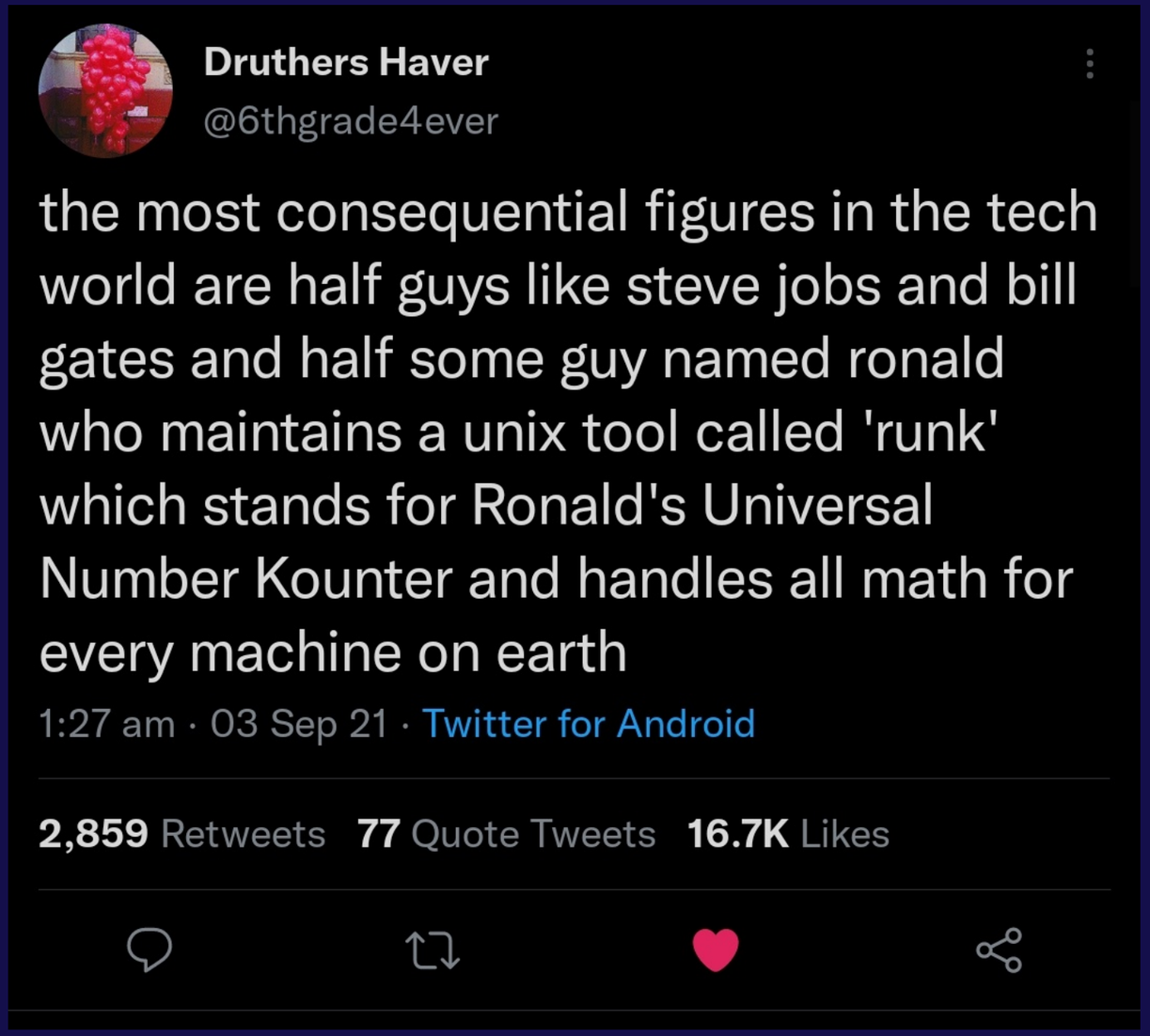


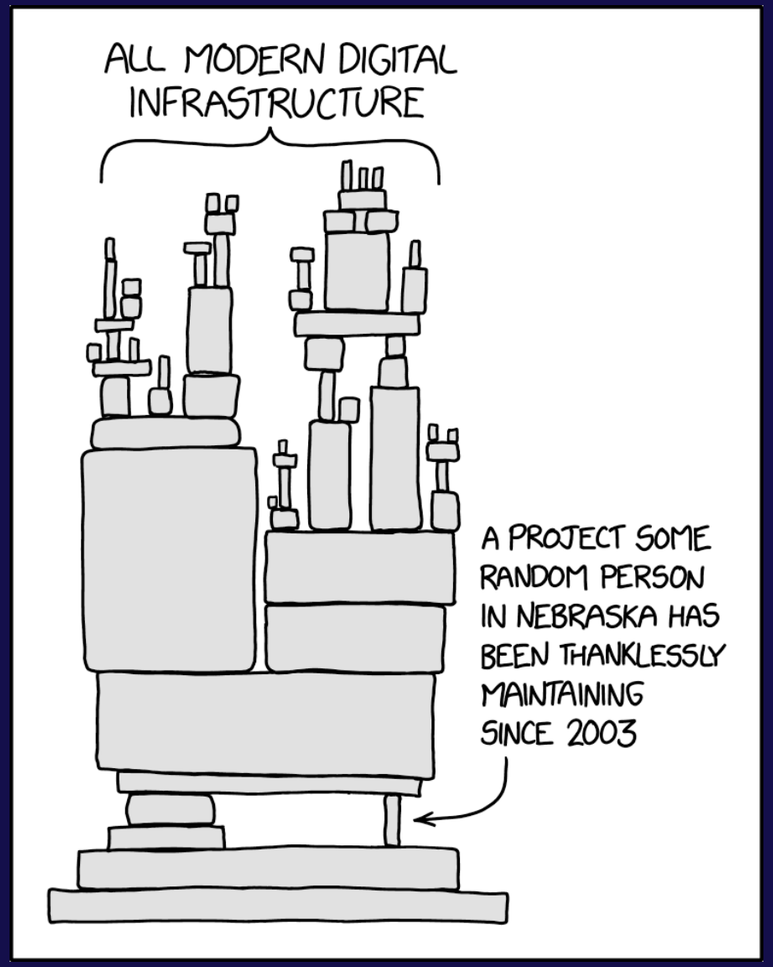
Instructions for carefully directing electricity

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

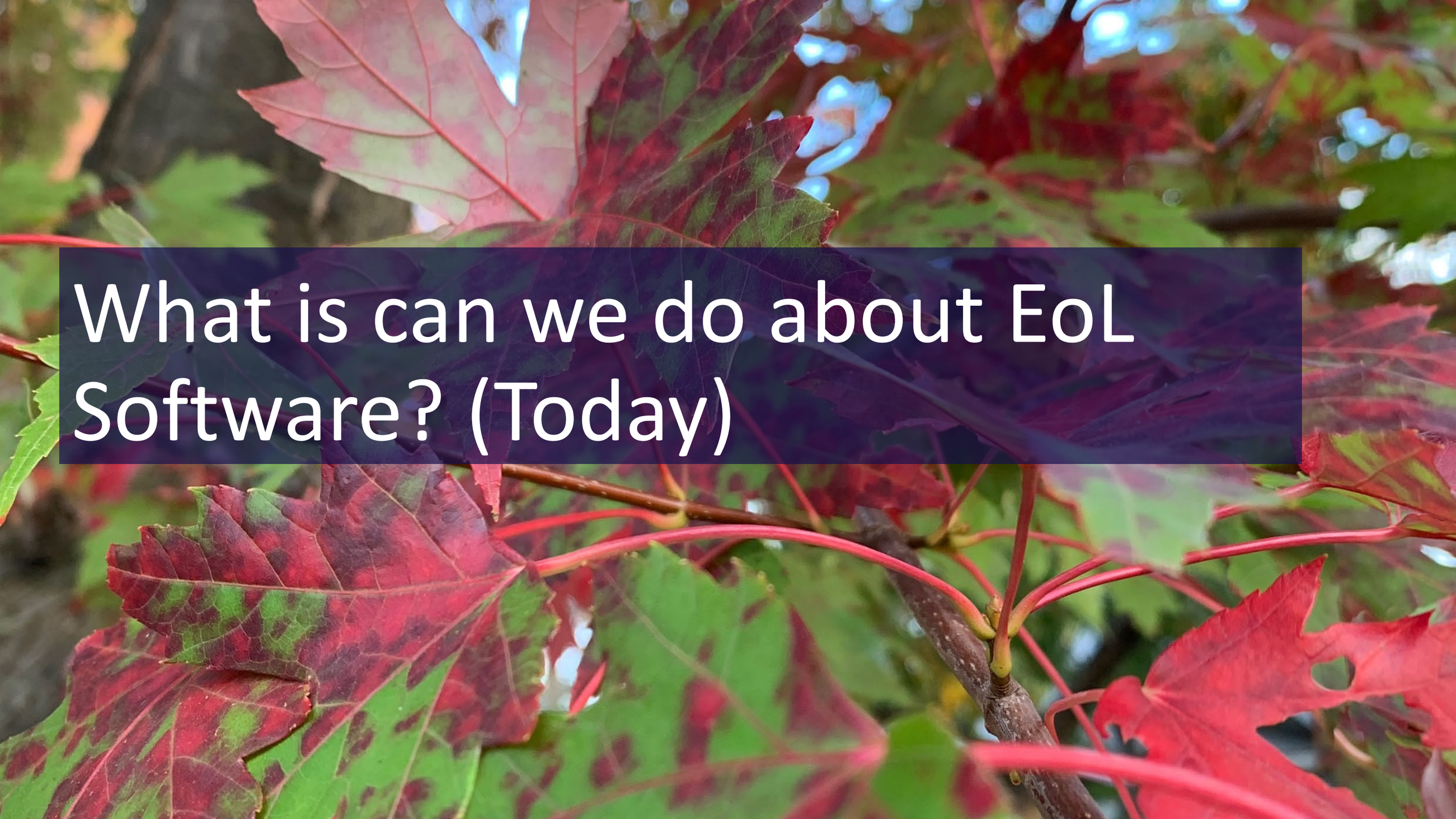




https://xkcd.com/2347/

Eyebrow raise or side-eye for anyone?

Medtronic



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.

Medtronic

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

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

Medtronic

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

Support Dates

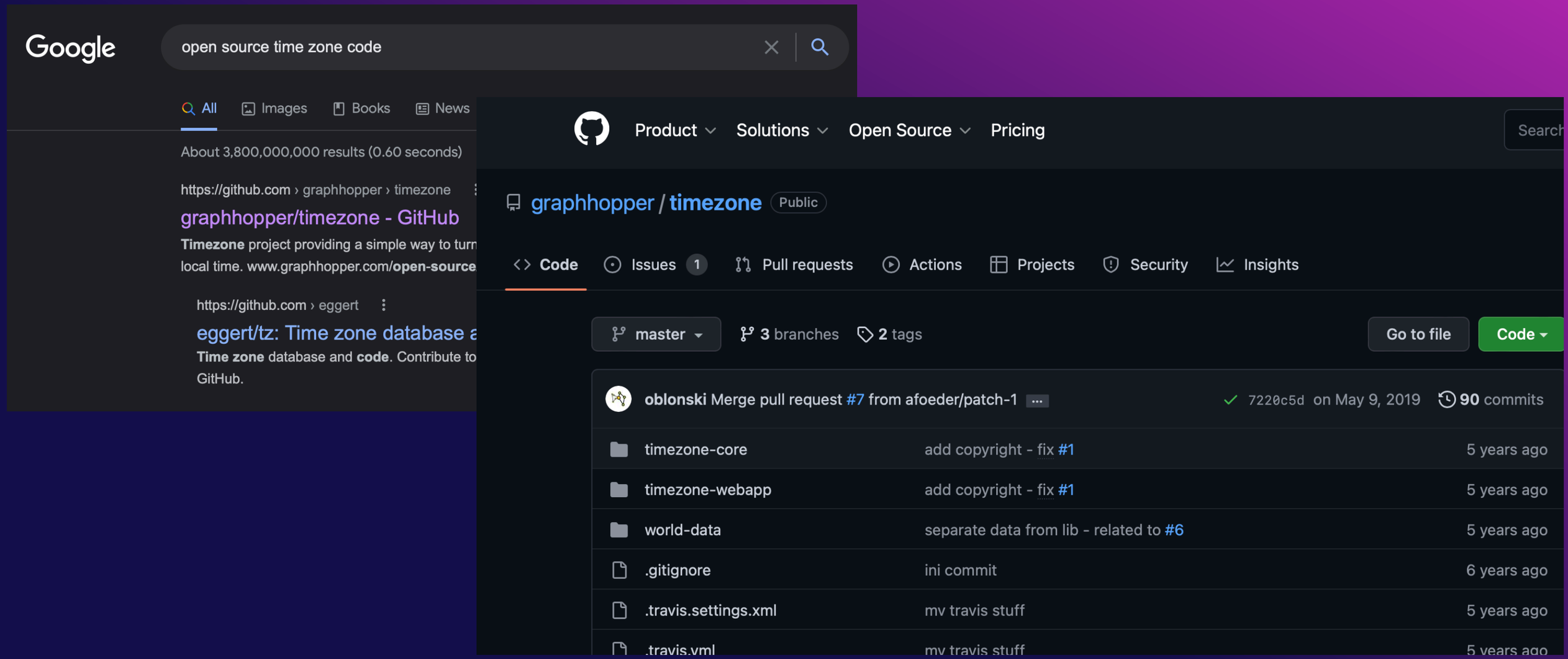
Listing	Start Date	Retirement Date
Windows 10 Home and Pro	Jul 29, 2015	Oct 14, 2025

Releases

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

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

Open source component (No support, maybe?)



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.

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

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

Medtronic

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 is 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 is 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