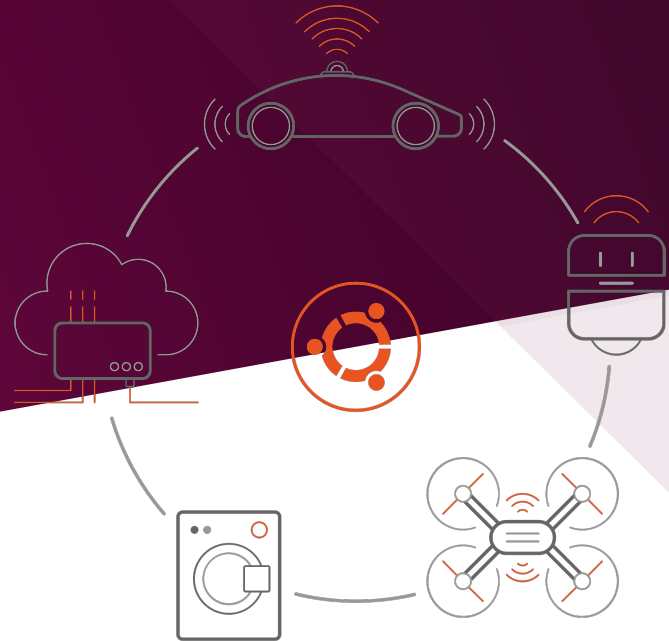# Ubuntu Core 22

The ultra-secure embedded Ubuntu -
Optimised for IoT and embedded devices

CANONICAL ubuntu

Welcome to Ubuntu Core 22 webinar

In this webinar, you will learn...

- Why?
- How? Ubuntu Core recap
- What's new on Ubuntu Core 22?
- What's coming up next?
- Success stories, shared by Advantech
- Ubuntu certified program
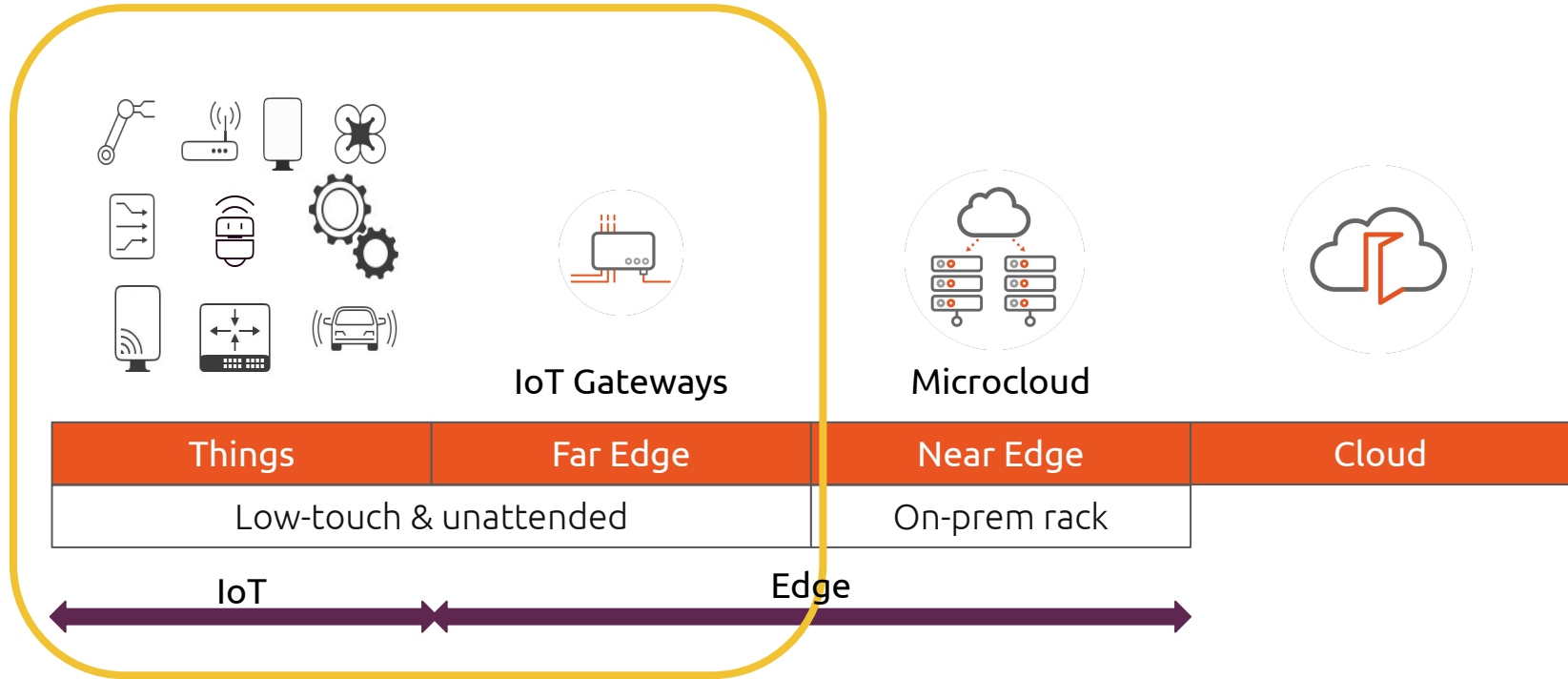- Q&A + Feedback

Taiten Peng

IoT Field Engineering

Canonical

ubuntu
Delivered by Canonical

Canonical
Ubuntu Core

What kind of devices are we speaking about?

IoT Gateways

Microcloud

Things	Far Edge	Near Edge	Cloud
Low-touch & unattended		On-prem rack	

IoT

Edge

Security matters

The internet runs on free open-source software. Who pays to fix it?

Volunteer-run projects like Log4J keep the internet running. The result is unsustainable burnout, and a national security risk when they go wrong.
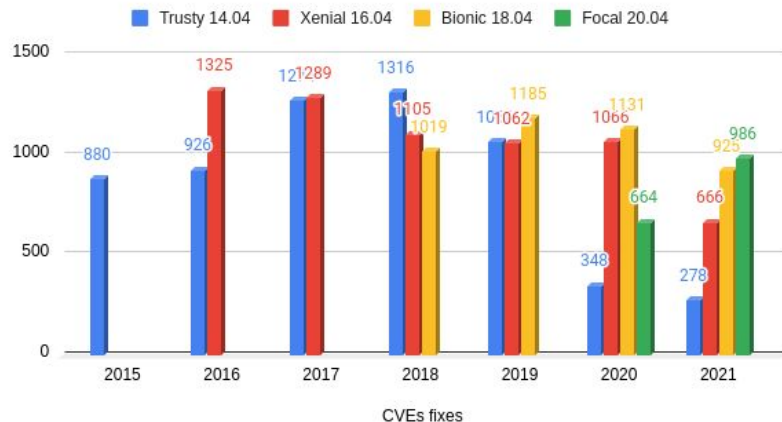
By

> *Patrick Howell O'Neill*
> *archive page*

December 17, 2021

https://www.technologyreview.com/2021/12/17/1042692/log4j-internet-open-source-hacking/

- CVE's are Common Vulnerabilities & Exposures

- Critical CVEs come once/twice a year

- Embargo CVEs come once a month or more

CVE fixes vs Ubuntu LTS

Legend: Trusty 14.04 (blue), Xenial 16.04 (red), Bionic 18.04 (yellow), Focal 20.04 (green)

Year	Trusty 14.04	Xenial 16.04	Bionic 18.04	Focal 20.04
2015	880			
2016	926	1325		
2017	1271	1289		
2018	1316	1105	1019	
2019	1057	1062	1185	
2020	348	1066	1131	664
2021	278	666	925	986

CVEs fixes

Challenges in IoT & Edge

Time To Market & Development Cost

85% of IoT initiatives not launched after a year of development

Technology Talent Shortage

45% of IoT initiatives are struggling to meet requirements

Custom & Bespoke Software

50% of custom software development projects fail

Meeting Security Requirements

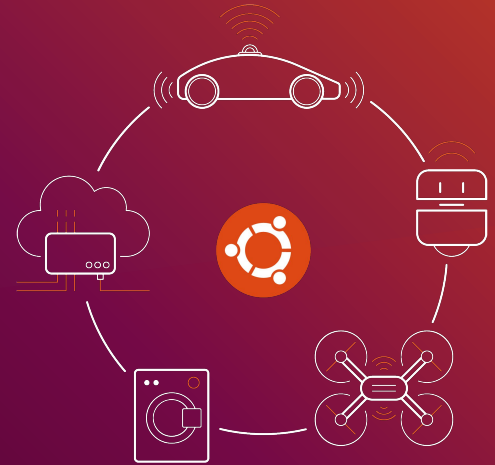77% of companies say IoT has created huge security gaps

Developers and manufacturers want to focus on their application

Trusting a reliable and secure underlying framework

For the whole (long) life of their devices on the field

What is Ubuntu Core?

Ubuntu Core

Secure IoT Embedded Linux OS for meeting the complex requirements of IoT

Designed for IoT
Optimized Size &
Modern Containerized
Architecture

Thriving Ecosystem
Include silicon,
development boards & Edge
Gateways

Reduced Time to Market
Pre-integrating building blocks
of OS, Security, OTA & apps
on popular hardware

Ultra Secure
Advanced security
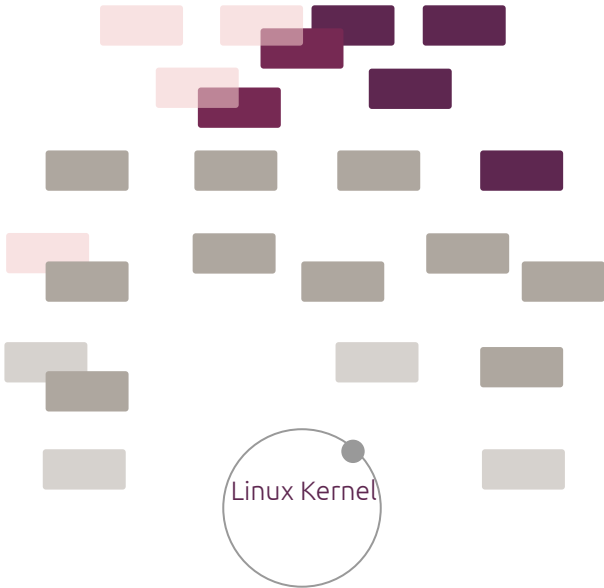features available
out of **the box**

Trusted by many global leaders for IoT & Edge use cases
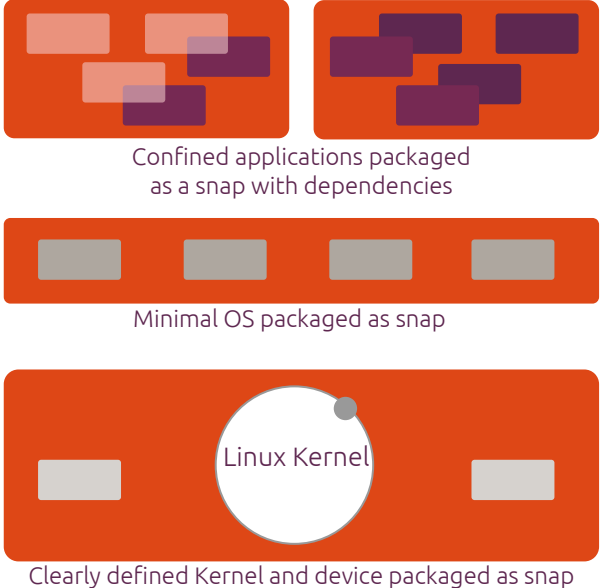
Modular, Containerized Architecture

Classic

Ubuntu Core

Confined applications packaged
as a snap with dependencies

Minimal OS packaged as snap

Linux Kernel

Clearly defined Kernel and device packaged as snap

Linux Kernel

Legend:

Application A   Application B   OS package   Shared library   Device driver

What's new on Ubuntu Core 22?

Ubuntu Core 22 Highlights

Released close to 22.04 LTS

Remodelling

System Update UC20 → UC22

Validation Sets
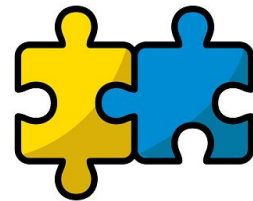
Piboot-only for RPI

MAAS Support

Real Time Beta

PREEMPT_RT kernel patches (Hosted at the Linux Foundation) are the de-facto Linux real-time implementation and are slowly being mainlined
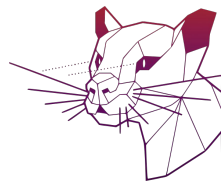

- Provides deterministic response time to service events
- System failure if missed deadline, regardless of system load
- For extreme latency-dependent use cases

Real-time Ubuntu Linux now available in beta

Released close to Ubuntu 22.04 LTS

22.04 LTS
Focal Fossa

April 2020

Core 20

Ubuntu Core 20

February 2021

22.04 LTS
Focal Fossa

April 2022

Ubuntu Core 22

Ubuntu Core 22

June 2022

2020

2021

2022

Remodelling (Device onboarding)

- Modify the list of pre-defined snaps of a device
- Change the device brand/model (ODM whitebox remodelling)
- Assign to a different IoT App Store (ODM whitebox remodelling)
- Update UC20 → UC22 in the field

Change the identity of a device ⇒ Modification of the Model Assertion

System update (UC20 → UC22)

- Upgrade the whole system from a previous version
- Extend effectively the support period of the OS
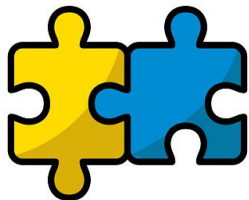- The partition layout has been preserved

Version is changed through remodelling

Validation Sets

Help a set of interdependent snaps maintain their testing and certification integrity, as well as help orchestrate their updates

- Simplify application dependency deployment and help manage devices
- Keep application compatibility and consistency during updates
- Locked-down appliances (only specific snaps)

Definition via validation-set assertions ⇒ presence, revision

… and much more

- Factory reset

- Quota groups ⇒ CPU and memory quotas

- Performance and footprint improvements

- Microk8s

Learn more:
ubuntu.com/core/docs
snapcraft.io/docs

ubuntu core documentation

Success stories sharing

Advantech - Smart Factory
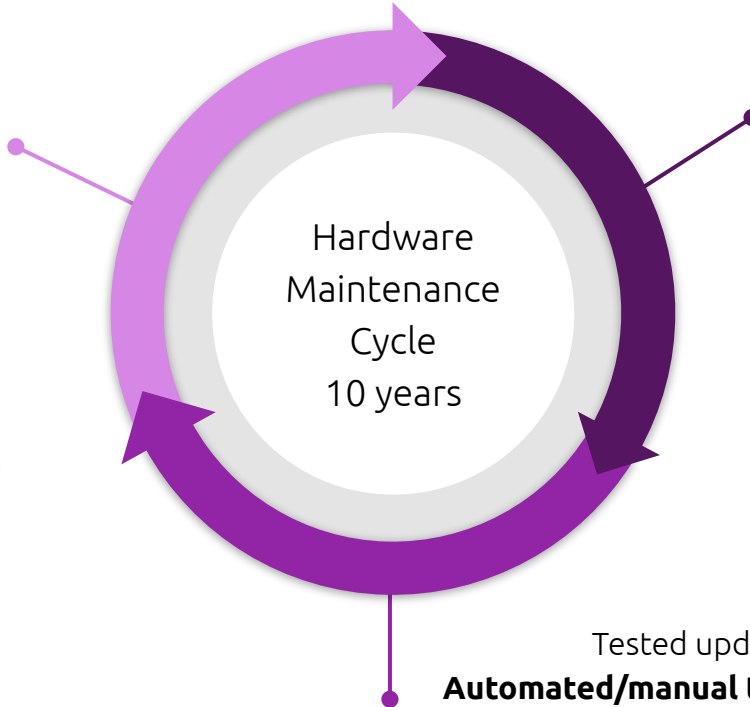
Advantech - Smart Building

IoT Certification
Ubuntu Certified Program

Certification Overview

Regression fixes
Issues from the tests are fixed then update released to user

Security updates and fixes
Latest CVE and bug fixes are integrated into Ubuntu

Hardware
Maintenance
Cycle
10 years

Tested updated image
Automated/manual tests are run against the Updated OS with the hardware

Ubuntu Certified Device

Secured

The hardware is tested for every single security update and any required fixes are made before they are released

Faster cheaper

Faster : choose certified hardware so you can focus on developing your soltuion rather than fixing hardware
Cheaper : 5 years free update from Canonical

Ultra reliable

100+ of tests perform against each h/w, s/w components for robustness before issuing certification

Well supported

We worked closely with our hardware partners for any field generated issues and bugs; so you won't get leave beyond
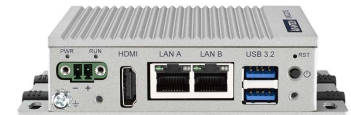
IoT Certification Partners

Find More Ubuntu Certified Devices

https://ubuntu.com/certified/devices

Thank you. Questions?