timesys

2022 CYBERSECURITY SURVEY RESULTS

FOR IOT DEVICE MANUFACTURERS

WHAT WE DID

Timesys collaborated with ecosystem and media partners like **Advantech, Lineo, Arm PSA Security, RidgeRun, CNX Software, Embedded.com,** and **LinuxGizmos** to conduct a survey of more than 100 industry professionals.

The purpose of the survey was to gather valuable insight into **where IoT device manufacturers are on their cybersecurity journey.**

WHO WERE THE INDUSTRY PROFESSIONALS?

Of the 105 individuals interviewed, **61.8%** were **software developers**, **16.4%** were **management/executives**, and **8.2%** were **cybersecurity/product security**.

Representing 90% of respondents, the top 5 industries were **IoT, industrial, networking, automotive, and medical.**

THE SURVEY RESULTS

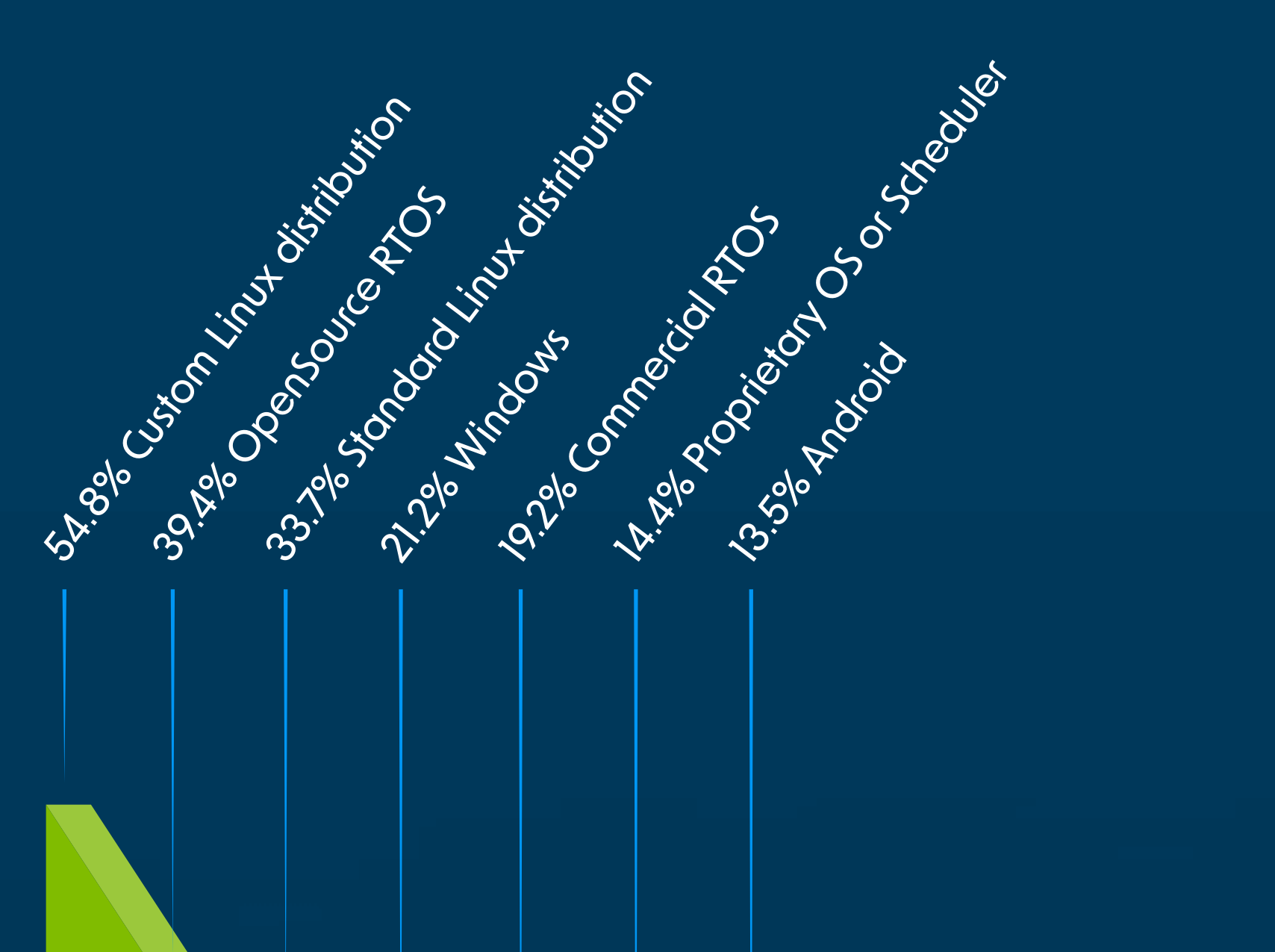
See the full breakdown and survey results here:

bit.ly/2022securitysurvey

OPERATING SYSTEM OF CHOICE

59% OF COMPANIES USE MULTIPLE TYPES OF OS

54.8% USE CUSTOM LINUX DISTRO



DRIVING FACTOR FOR SECURITY REQUIREMENT

76% CUSTOMER security requirements

VS

39% ORGANIZATIONAL cybersecurity guidelines

Customer requirements is the most important driving factor for security requirements followed by compliance, standards, and then companies with internal cybersecurity mandates.

Of IoT companies surveyed, **76% said meeting customer's security requirements or needs** was a driving factor, but **only 39%** said the same of **meeting internal organizational cybersecurity guidelines.**

SECURITY PROCESSES EMPLOYED

We asked what security processes were employed during the product life cycle and found that **the most implemented processes were incorporating OS and application security features** at 46% and **security requirement gathering and threat modeling** at 37%.

Additionally, survey respondents had either implemented or were planning to implement: **validating compliance, vulnerability management, and software updates.**

The majority were planning to implement software supply chain and incident monitoring and management.

SECURITY LAYERS

The top 10 security-by-design features that survey respondents were concerned about implementing matches the most recently published **National Institute of Standards and Technology** (NIST) guidelines.

MOST COMMON CONCERNS

71.4% SECURE COMMUNICATION (encrypted and authenticated)

60% SECURE FIRMWARE update/OTA update

58.1% ACCESS CONTROL principles of least privilege

NEARLY **60%** OF SURVEY RESPONDENTS PROVIDE "SCHEDULED/REGULAR" SECURITY UPDATES AT LEAST ONCE PER YEAR.

TOP 3 CHALLENGES

71% of executives and managers surveyed said they faced the following top 3 challenges:

1. LACK OF IN-HOUSE EXPERTISE
2. INSUFFICIENT TOOLS AND PROCESSES FOR LONG TERM MAINTENANCE
3. TIME-TO-MARKET PRESSURE TO DELIVER MORE FUNCTIONALITY OVER SECURITY

MOST LIKELY TO INVEST IN

90% of executives and managers surveyed picked the following top 3 areas for investment:

- ✓ VULNERABILITY MONITORING AND MANAGEMENT TOOL
- ✓ SECURITY AUDIT AND/OR PENETRATION TESTING
- ✓ LONG TERM OS SECURITY MAINTENANCE MANAGED SERVICE

WHAT WE LEARNED

Security usually isn't seen as a feature, but **customers expect devices to be highly secured even in the Minimum Viable Product (MVP) stage.**

On top of that, industry standards are **requiring stricter security** at each turn.

WHY AREN'T DEVICES MORE SECURE?

So why aren't Internet of Things (IoT) device manufacturers taking every measure possible to secure their devices?

Lack of expertise, **lack of resources**, and **insufficient tooling and processes** all present challenges.

HOW WE CAN HELP

Timesys bridges this gap with **efficient security solutions for the full device lifecycle.**

Learn more about how we **build, secure, and maintain open-source embedded software platforms** at:

www.timesys.com/solutions

timesys