# XIoT Cybersecurity Solutions for the Water and WasteWater Sectors

*Jennifer Lyn Walker, Director of Infrastructure Cyber Defense, WaterISAC*

*Eric Ervin, Global Cybersecurity Director for Utilities and Manufacturing, 1898 & Co*

*Ryan Bowery, Principal Solution Engineer, Claroty*

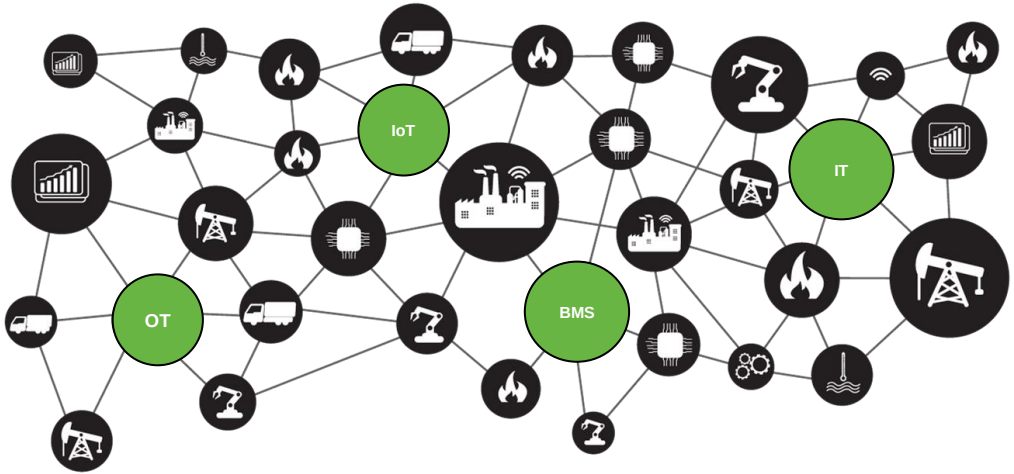
CLAROTY

# The Modern Industrial Network

**The interconnectivity that drives productivity**

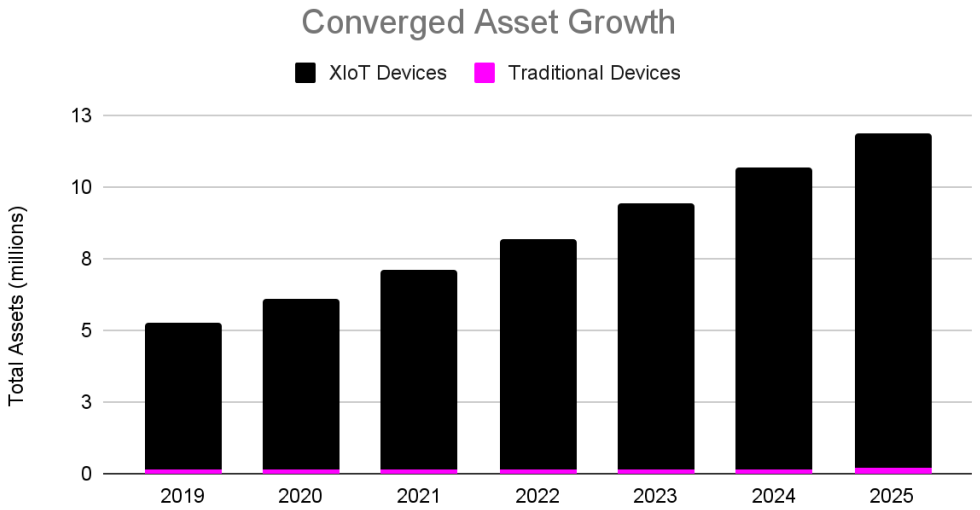
**The Extended Internet of Things (XIoT)**

*The ever-growing web of connected devices that span and support cyber-physical systems and range from both legacy and greenfield OT assets, to IT and IoT devices, to building management system equipment.*



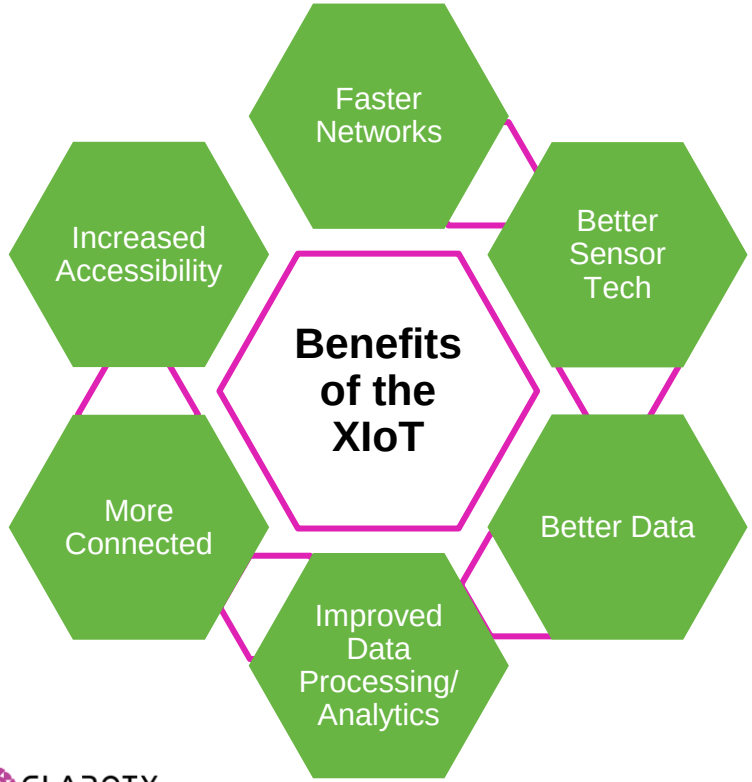
# The Growth of the XIoT

**The rapid proliferation of cyber-physical systems that cannot easily be secured**




**Sources:**
Gartner, Forecast: PCs, Worldwide, 2019-2025, 1Q21 Update
Gartner, Forecast: Servers, All Countries, 2019-2025, 1Q21 Update
Gartner, Forecast: Internet of Things, Endpoints and Communications, Worldwide, 2019-2029

# XIoT Opportunities and Challenges




**Top Challenges**

**Rapid device expansion increases exposure**

**Diversity of devices leads to decreased visibility**

**Assets spread across large geographic areas**

**Increased skills gap between IT and OT staff**

# Cybersecurity Challenges Across the Sector

## Asset Discovery

Discover all XIoT assets on an industrial network, extensive attributes about them, and their normal communication patterns

## Remote Facilities

Remote, unmanned facilities over vast geographic areas requiring remote access for maintenance and auditing purposes

## Regulatory Requirements

Evolving requirements under the America's Water Infrastructure Act (AWIA) calling for detailed risk and resilience assessments

# Meeting These Challenges

**Requirements for achieving cyber resilience in water and wastewater facilities**

## Asset Discovery

| | |
|---|---|
| **Flexibility** | Asset discovery in the way most suitable for network architecture |
| **Fluency** | Enriching the asset database with the information required to achieve cyber and operational resilience |
| **Domain Expertise** | Understanding the unique stakeholders in and requirements of Water and Wastewater facilities |

## Remote Facilities

| | |
|---|---|
| **Scalability** | Ensuring stability and data integrity across vast geographic areas |
| **Remote Access** | Enabling quick, efficient, and secure third-party remote access to reduce MTTR and associated costs |
| **Durability** | Equipment that is suitable for use in hazardous and extended exposure environments |

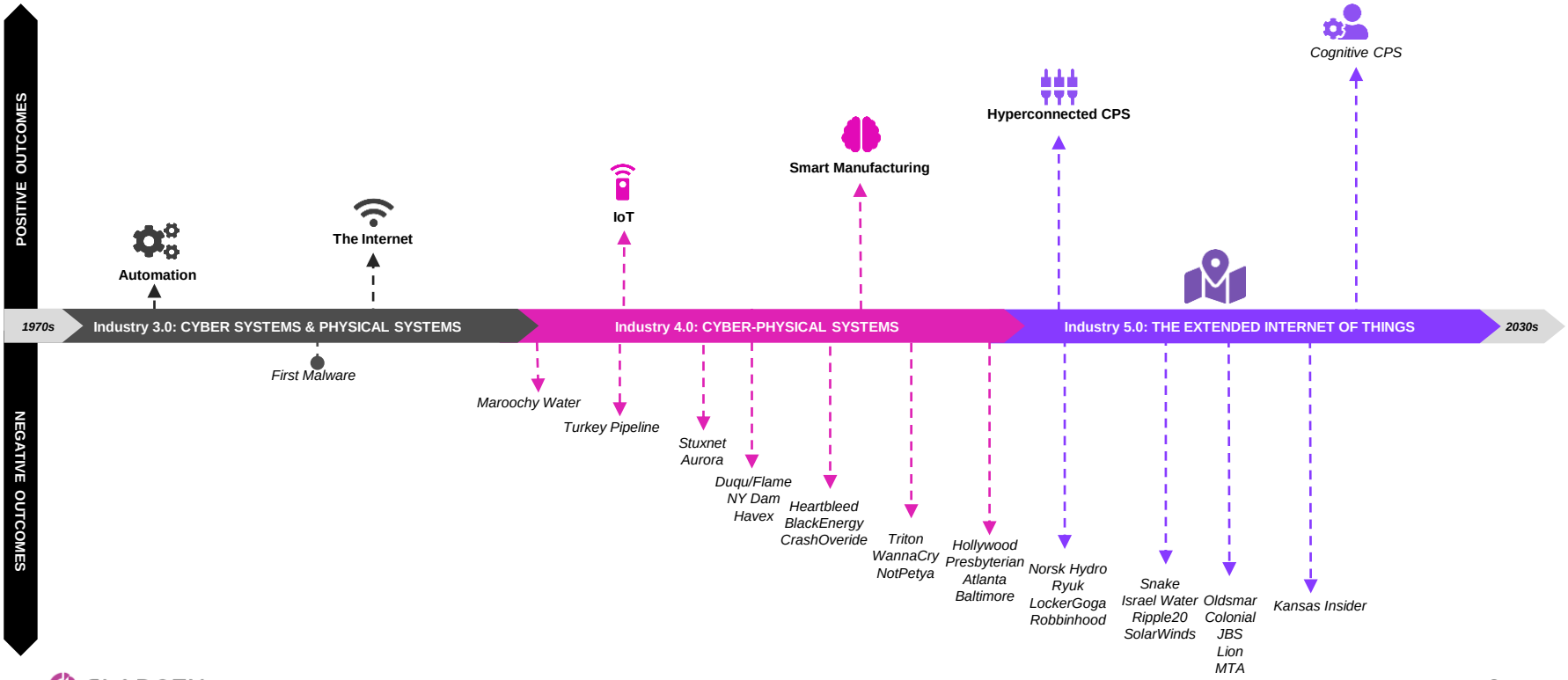
# Meeting Regulatory Challenges

**Requirements for achieving cyber resilience in water and wastewater facilities**

| | | | |
|---|---|---|---|
| **NERC CIP** | **IEC 62443** | **CIS Top 18** | **15 Cybersecurity Fundamentals for Water and Wastewater Utilities** |

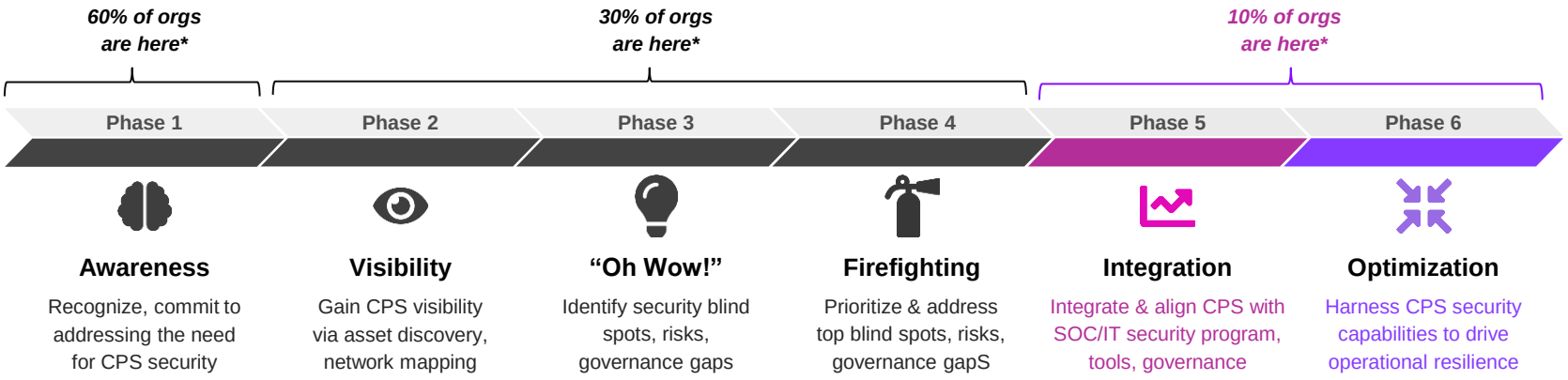
# The Rapid Proliferation of CPS

**Threats to industrial environments are increasing in scale and velocity**



# The Journey To Achieving Business Outcomes

**The CPS Security Journey: As Told by Gartner[1]**




[1]*Source: Market Guide for Operational Technology Security, Gartner, 2021*

# Desired Business Outcomes

**Achieving resilience in the age of connectivity**

## Cyber Resilience

- Enable continuous security posture management and compliance
- Establish a Zero Trust security architecture to minimize cyber risk
- Detect and mitigate threats before they can impact operations

## Operational Resilience

- Optimize asset management with a real-time inventory of XIoT assets
- Reduce outages due to known operational risk
- Enforce change management processes to ensure safety and process integrity

# Recent Funding Opportunities

- Congress may allocate as much as $200B securing water's critical infrastructure.
- Senate Bill 914: Drinking Water and Wastewater Infrastructure Act (DWWIA) of 2021: ~$35B proposed allocation with annual renewal.
- EPA funding increase of more than 21% proposed (~$11.2B), of which about 1/3 (~$3.6B) is designated for water infrastructure and security.

# THANK YOU