“Der schwarze Gürtel für OT-Security”

Introducing Claroty

Markus Bloem

24.01.2023

CLAROTY

Claroty At-A-Glance

Empowering organizations with unmatched security for all cyber-physical systems across the XIoT

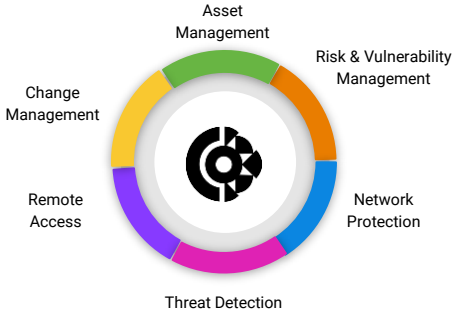
HQ: **NYC**	Founded: **2015**	Funding: **$635M (Series E)**	Customers: **600+**

DEEP DOMAIN EXPERTISE

The Extended Internet of Things (XIoT)

Industrial **Commercial** **Healthcare**

COMPREHENSIVE CAPABILITIES



GLOBAL ADOPTION

100s of Orgs, 1000s of Sites, 50+ Countries, 25+ Verticals

VALIDATION FROM LEADING INDUSTRY ANALYST FIRMS & OTHER TRUSTED THIRD-PARTIES

SC 2021 awards EUROPE WINNER

SAFETY ACT

FORRESTER WAVE LEADER 2021 Industrial Control Systems (ICS) Security Solutions

BEST IN KLAS 2021 HEALTHCARE IOT SECURITY

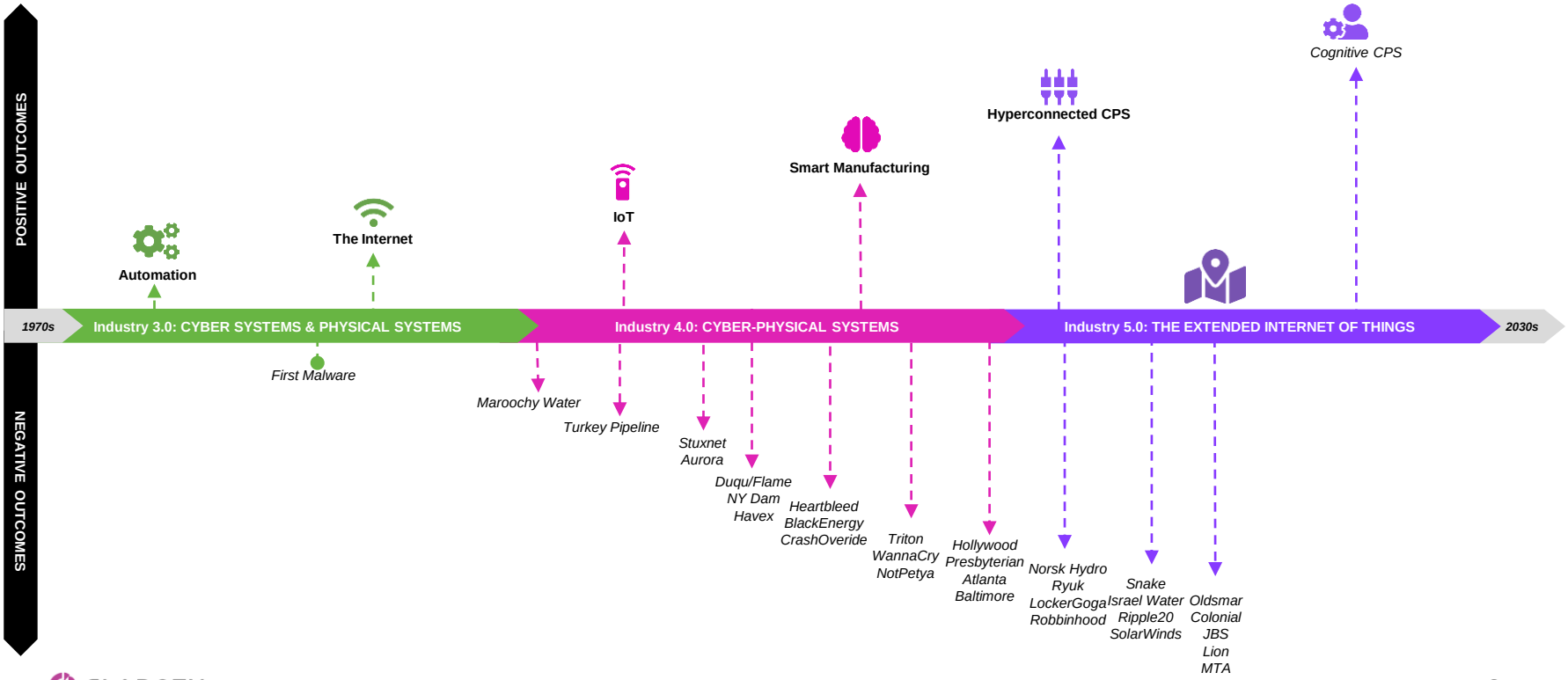
BEST IN KLAS 2022 HEALTHCARE IOT SECURITY

500 Technology Fast 500 2021 NORTH AMERICA Deloitte.

2021 CYBERSECasia READERS' CHOICE AWARDS

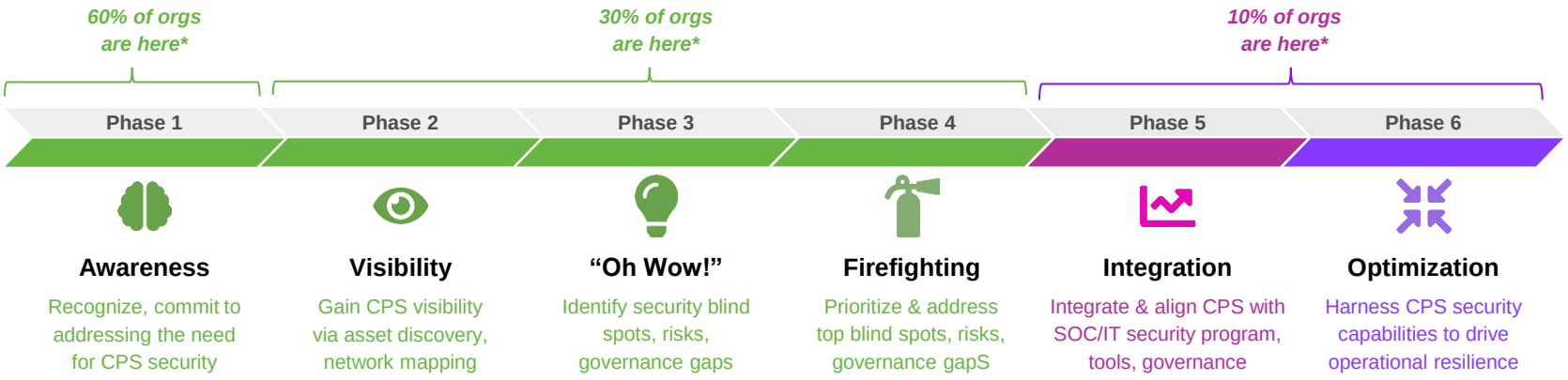
The Rapid Proliferation of CPS

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*

The CPS Security Journey: Tailored to **Your Priorities**

Three simplified, flexible onramps to achieving CPS security maturity based on what matters most to you

Control Access

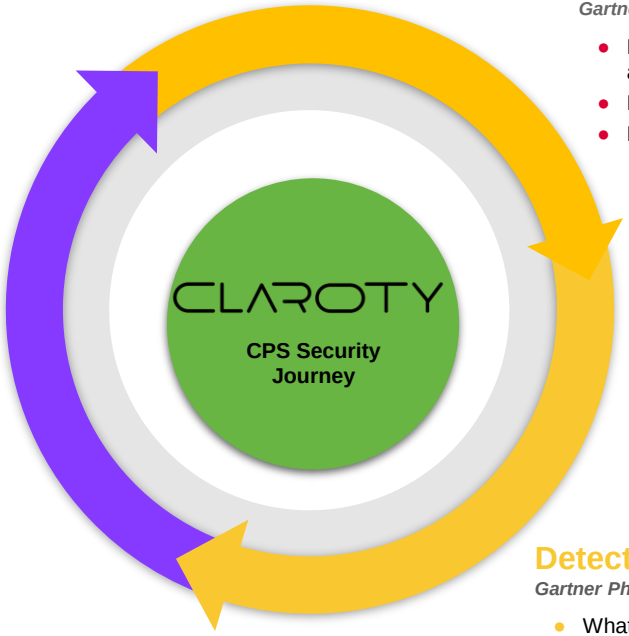
Gartner phase: 4. Firefighting

- How to provide internal & third-party personnel with remote access to your CPS based on their use cases?
- How to manage risks posed by their access?
- How to lower MTTR & reduce unplanned downtime?

Understand Your Assets

Gartner Phases: 1. Awareness, 2. Visibility, 3. "Oh Wow!"

- What assets are in your environment?
- How is your environment structured?
- What vulnerabilities & risks are present?
- How to manage those vulnerabilities & risks?



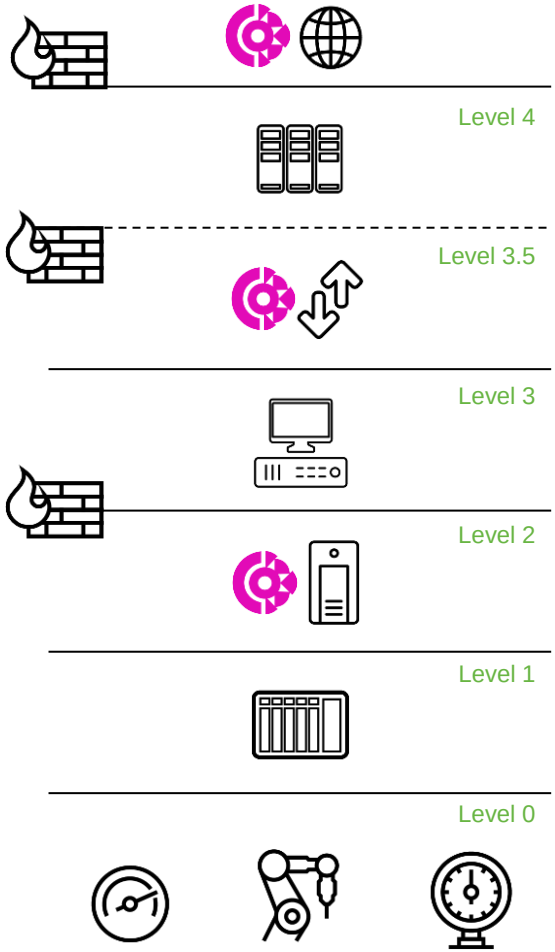
Detect & Respond to Threats

Gartner Phases: 5. Integration, 6. Optimization

- What threats are you most concerned about?
- How should your staff manage alerts?
- How can your existing tech & governance support your CPS?

Introducing Claroty Continuous Threat Detection (CTD)

XIoT Cyber Resilience Solution for your Industrial Cybersecurity Journey



Asset Discovery

Depth of Visibility Through Precision Techniques

Understanding the Network

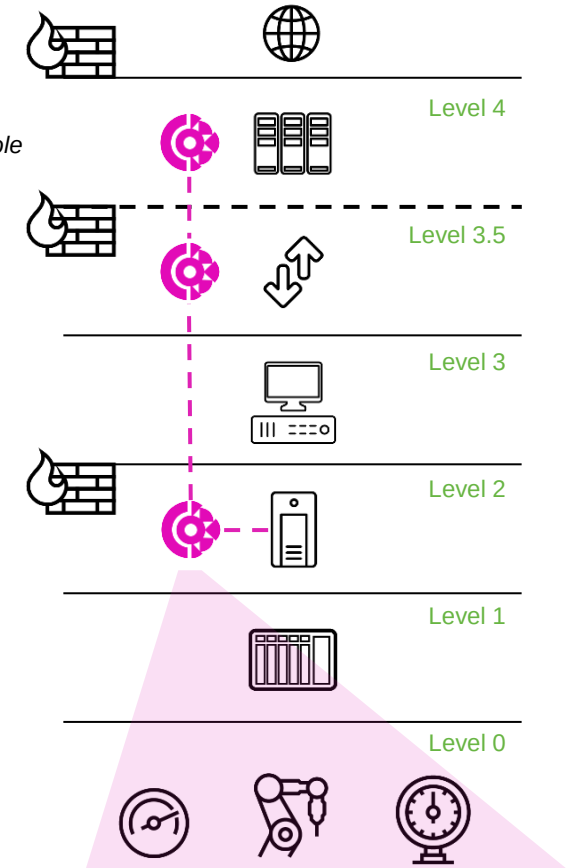
With Support for over 300 XIoT protocols

	Passive	Safe Queries	AppDB	All
Asset Enrichment	✓	✓	✓	✓
Quick Deployment	✓	✓	✓	✓
Vulnerability Insights	✓	✓	✓	✓
Scalable	✓		✓	✓
Speedy Collection		✓	✓	✓
Customizable		✓		✓

CTD Enterprise Management Console

CTD Server
- *Passive*
- *Safe Queries*
- *AppDB*

CTD Sensor
- *Passive*
- *Safe Queries*



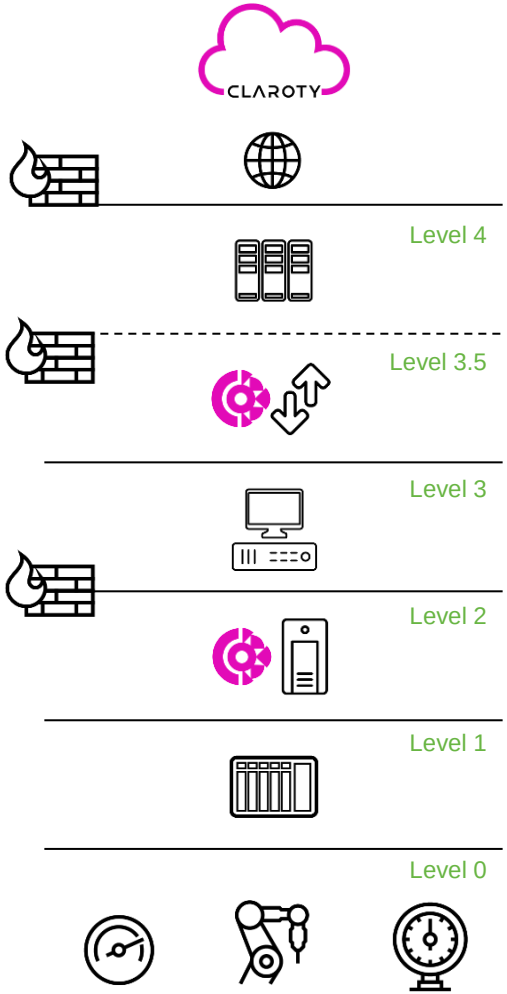
Example 3-tier deployment

CLAROTY

Claroty In Your Industrial Environment

SaaS Deployment

- Flexible, safe, and effective asset discovery methods that fit your environment
- Automated platform and security intelligence updates
- Tiered deployment with layered cloud-security controls and industry standard practices



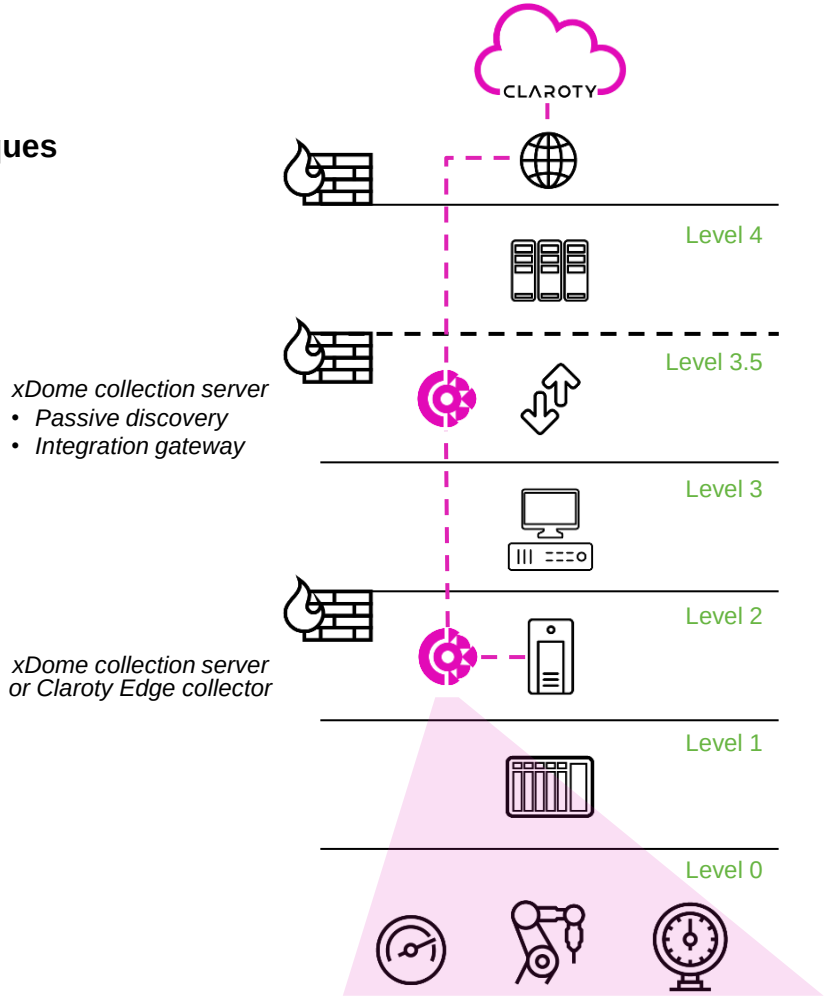
Asset Discovery

Depth of Visibility Through Precision Techniques

Understanding the Network

With Support for over 450 XIoT protocols

	Passive	Claroty Edge
Asset Enrichment	✓	✓
Quick Deployment	✓	✓
Speedy Collection	✓	✓
Scalable	✓	✓
Vulnerability Insights	✓	✓



Example 3-tier deployment

Claroty Your Way

Extending Core IT Cybersecurity Tools to the Industrial Environment

Asset Discovery & Enrichment

DHCP/DNS

Infoblox

Microsoft

BLUECAT

BT

Network Management

cisco Prime; DNA-C

aruba Airwave

solarwinds

Active Directory

vmware

Patch Management

Microsoft SCCM

Quest

MDM

vmware Workspace ONE

jamf

Intune

MOBILETRON

Network Infrastructure

cisco

aruba

juniper

Vulnerability & Risk Management

RAPID7 InsightVM; Nexpose

tenable T.IO; T.SC; Nessus

Qualys.

Network Protection

Firewalls

cisco

Check Point

paloalto

vmware NSX

FORTINET

FIREEYE

NAC

cisco ISE

FORESCOUT

aruba ClearPass

FORTINET FortiNAC

Threat Detection

Endpoint Security

CROWDSTRIKE

Microsoft ATP

vmware

SentinelOne

TANIUM

SOAR

CORTEX XSOAR

SWIMLANE

SIEM

splunk>

RSA

LogRhythm

tripwire

IBM QRadar

graylog

MICRO FOCUS

sumo logic

Asset and Change Management

Ticketing

servicenow

Cherwell SOFTWARE

Asset Management

accruent

nuvolo

servicenow

CLAROTY

CLAROTY INDUSTRIAL

DEMO

CLAROTY INDUSTRIAL

Vielen Dank