# IT/OT Security mit Crowdstrike und Claroty

*Wolfgang Schwed Crowdstrike*

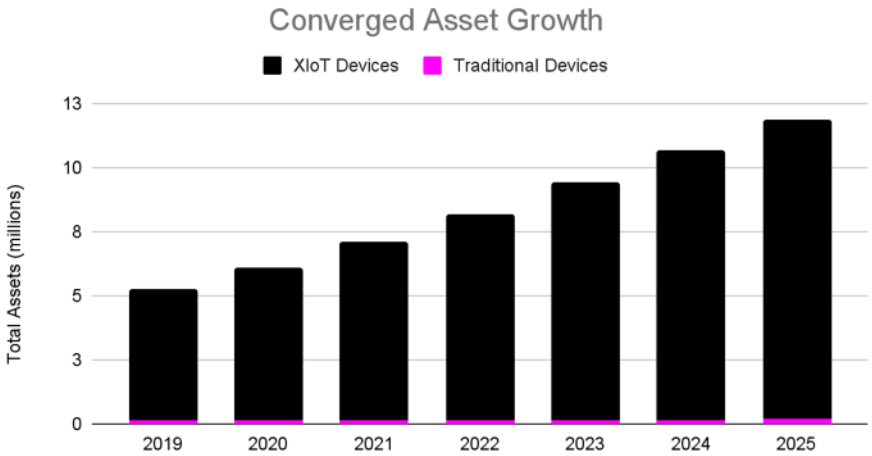
*Werner Schlatter Claroty*

CROWDSTRIKE

CLAROTY

# The Growth of the XIoT

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




## Top Challenges

**Rapid device expansion increases exposure**

**Diversity of devices leads to decreased visibility**

**Increased frequency and severity of attacks**

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

**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

## eCRIME BREAKOUT TIME

# 62'


# Adversaries Increasing in Speed and Precision

### Defenders must act quickly

To contain the threat and minimize cost and damage, defenders must respond within the breakout time

### They weaponize YOUR tools and accounts

Adversaries use valid accounts and tools to move laterally, making it nearly impossible to detect abnormal activity and a potential breach

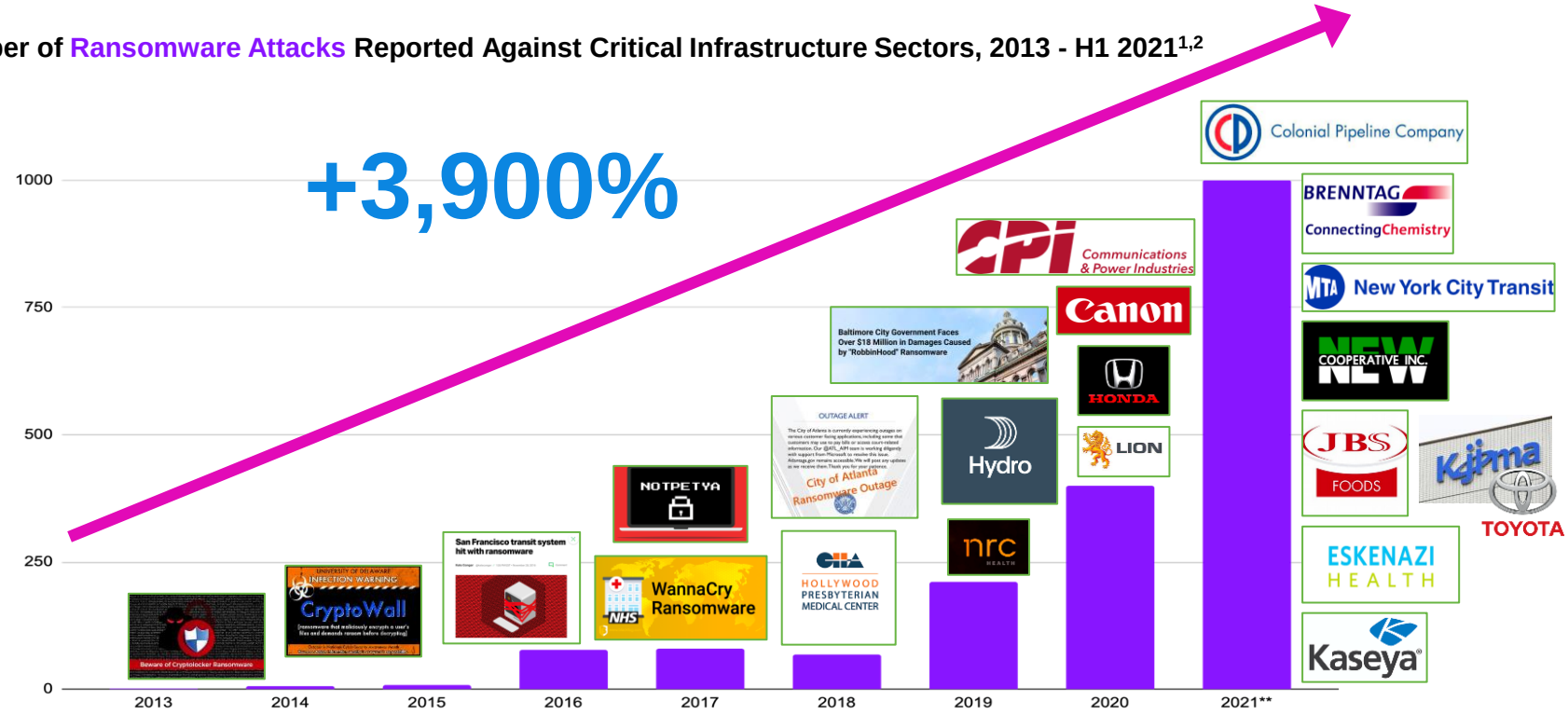
### Fastest breakout time: 2 min, 7 sec

Nearly all security teams are not equipped to respond in less than 2 minutes

# Digital Transformation Creates Digital Risk

Cyber attacks are increasing in frequency and impact on Cyber-Physical Systems (OT-IOT-IIOT)

**Number of Ransomware Attacks Reported Against Critical Infrastructure Sectors, 2013 - H1 2021[1,2]**

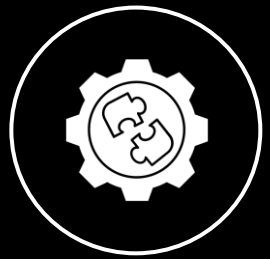



[1] Predicts 2022: Cyber-Physical Systems Security — Critical Infrastructure Focus, Gartner, 2021
[2] Ransomware Volumes Hit Record Highs as 2021 Wears On, Threatpost, 2021

# Modern IoT/OT Security Challenges

## Targeted, sophisticated attacks

Highly targeted for ransomware and espionage



## Operational complexity

Patching sometimes not possible, lack ability to be proactive

## Visibility

Unclear boundaries and lack of visibility across IT/OT gap

## Skills shortage

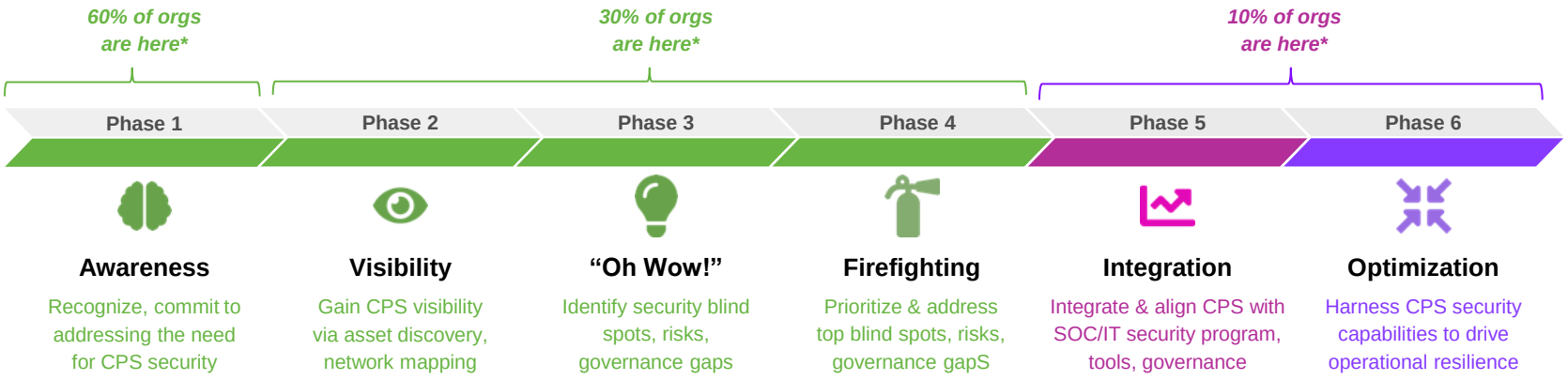
Lack of support and resources for OT/IoT integration/security



CROWDSTRIKE

# The Journey To Achieving Business Outcomes

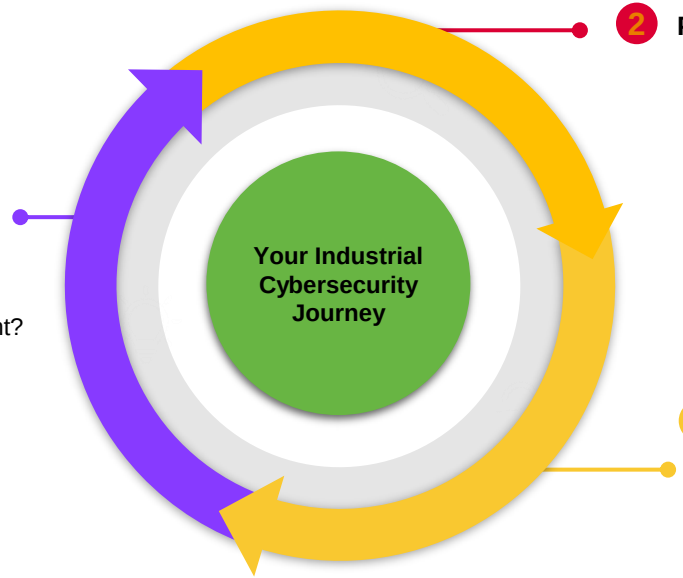
**The CPS Security Journey: As Told by Gartner[1]**




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

# Meeting Customers on their Industrial Cybersecurity Journey

## Selecting the Right Onramp Based on Enterprise Maturity and Priorities




**1 Priority: Understand Your Network**

- What assets are in your network?
- How is your network structured?
- What vulnerabilities and risks are present?
- How can you manage those risks?

Reveal | Protect

**2 Priority: Control Access**

- How can you provide internal and third-party personnel with remote access to your network?
- How should you manage the risks posed by their access?
- How should you respond to incidents related to their access?

Protect

**3 Priority: Detect Threats**

- What threats are you most concerned about?
- How should your staff manage alerts?
- How can your existing IT security tech stack support your industrial network?

Detect | Connect

# The Journey to Achieving Cyber Resilience

**Our approach tailored to your priorities**

**DISCOVER**

**MITIGATE**

**CONNECT**

**OPTIMIZE**

**ASSET DISCOVERY**

Comprehensive enterprise-wide XIoT asset visibility and communication profiling

**VULNERABILITY & RISK MANAGEMENT**

Identify vulnerabilities in the operational network and prioritize risk remediation efforts to enable continuous security posture management and compliance

**NETWORK PROTECTION**

Network segmentation through tailored recommendations and access controls to enable a Zero Trust architecture in your operational environment

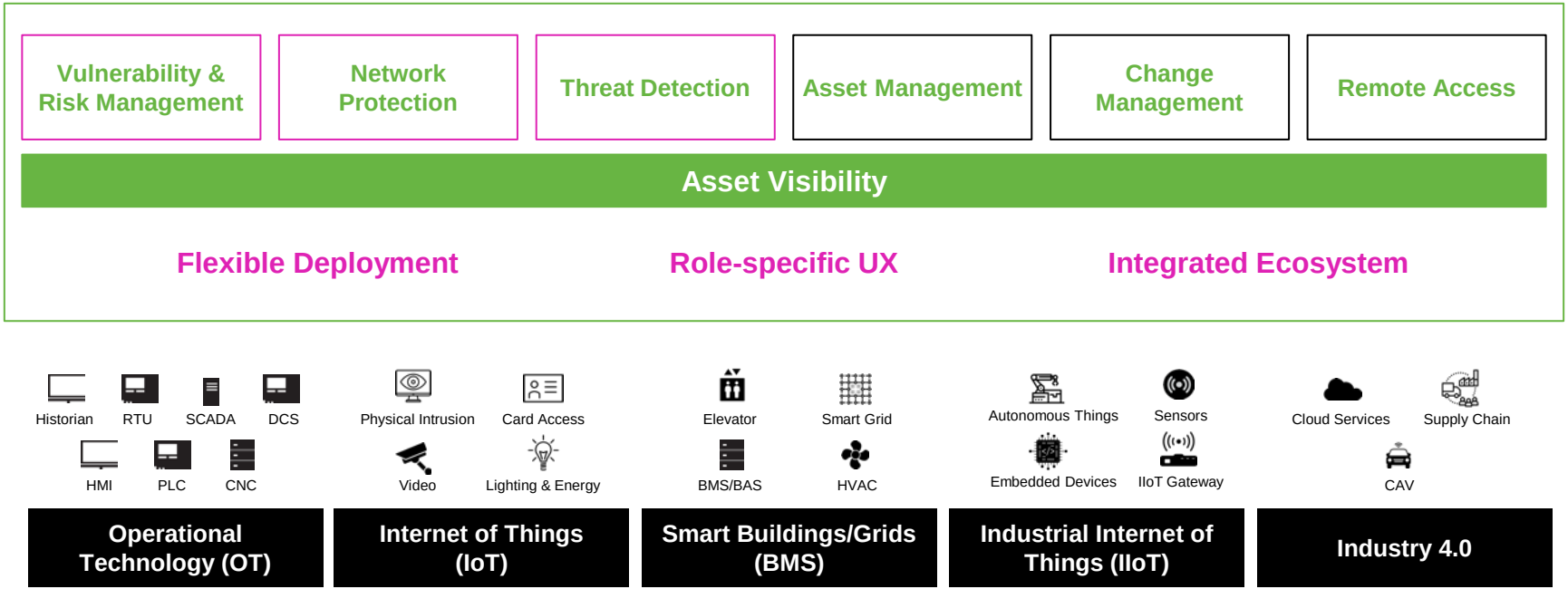
**THREAT DETECTION**

Detect threats and integrate with existing SOC solutions to mitigate cyber attacks before they can impact operations

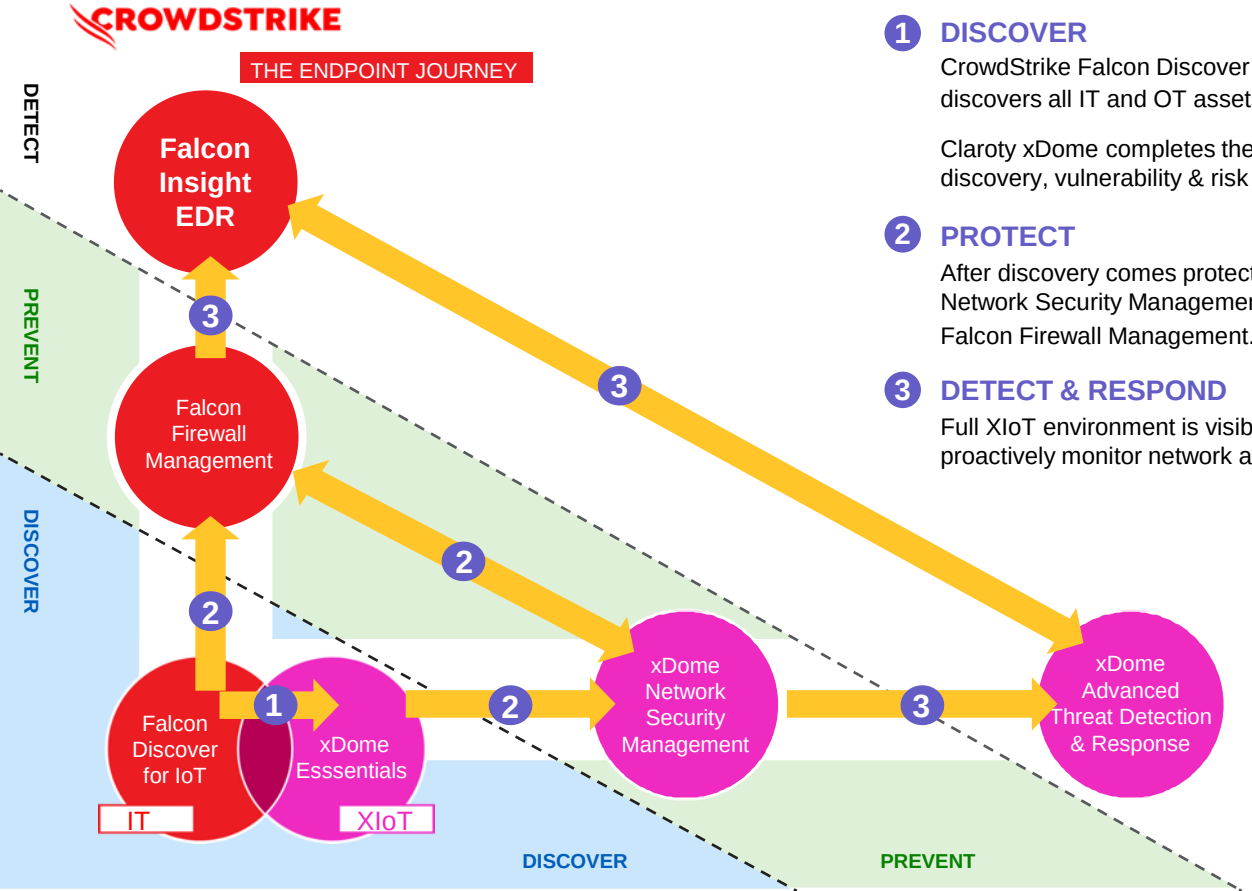
**CUSTOMER JOURNEY**

# Claroty xDome

**A modular portfolio for your cyber resilience journey**



# The CrowdStrike-Claroty Customer Journey




**1 DISCOVER**

CrowdStrike Falcon Discover for IoT, embedding Claroty Edge, discovers all IT and OT assets within the modern connected enterprise.

Claroty xDome completes the XIoT puzzle by providing enhanced XIoT asset discovery, vulnerability & risk details, and additional device-specific insights

**2 PROTECT**

After discovery comes protection. xDome makes this easy via the Network Security Management orchestration module, enforced by Falcon Firewall Management.

**3 DETECT & RESPOND**

Full XIoT environment is visible and protected, xDome and Falcon proactively monitor network and endpoints sources for potential threats.

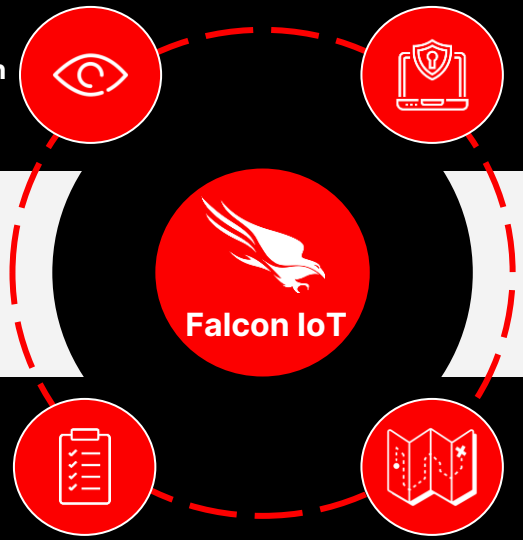
CLAROTY

THE NETWORK JOURNEY

# Crowdstrike is uniquely positioned to solve the most pressing IoT/OT security challenges

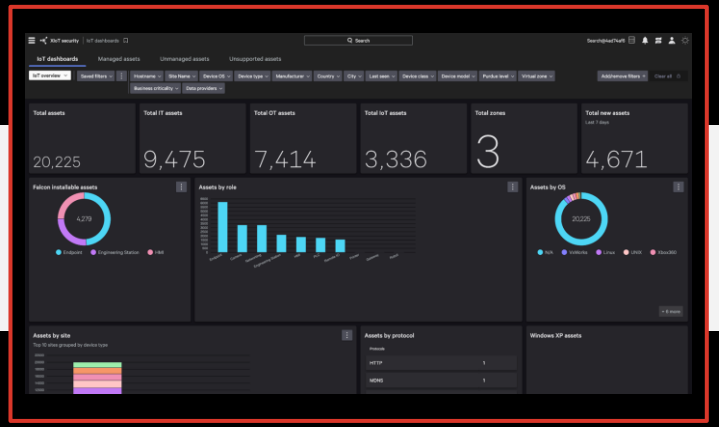
Complete visibility in *10 mins or less*

Extend industry-leading EDR/XDR to IoT/OT




ICS vendor certified

Asset relationship mapping




**Comprehensive, simplified visibility**

**Leave no endpoint unprotected**

**Accelerate OT Digital Transformation**



CROWDSTRIKE