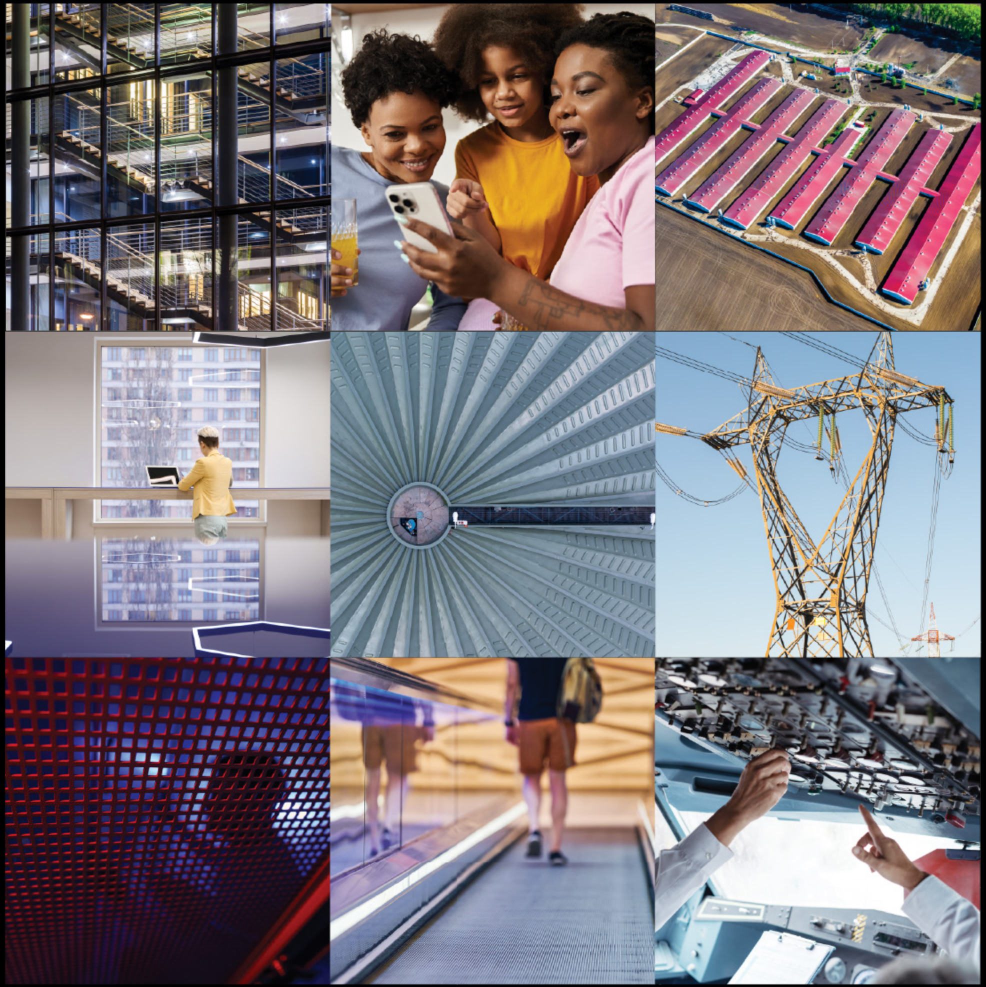
CLAROTY

2025 WORLD READINESS GUIDE

Life, uninterrupted.



Is the world prepared for Life, uninterrupted?

Cyber-physical systems security is not just about stopping threats.

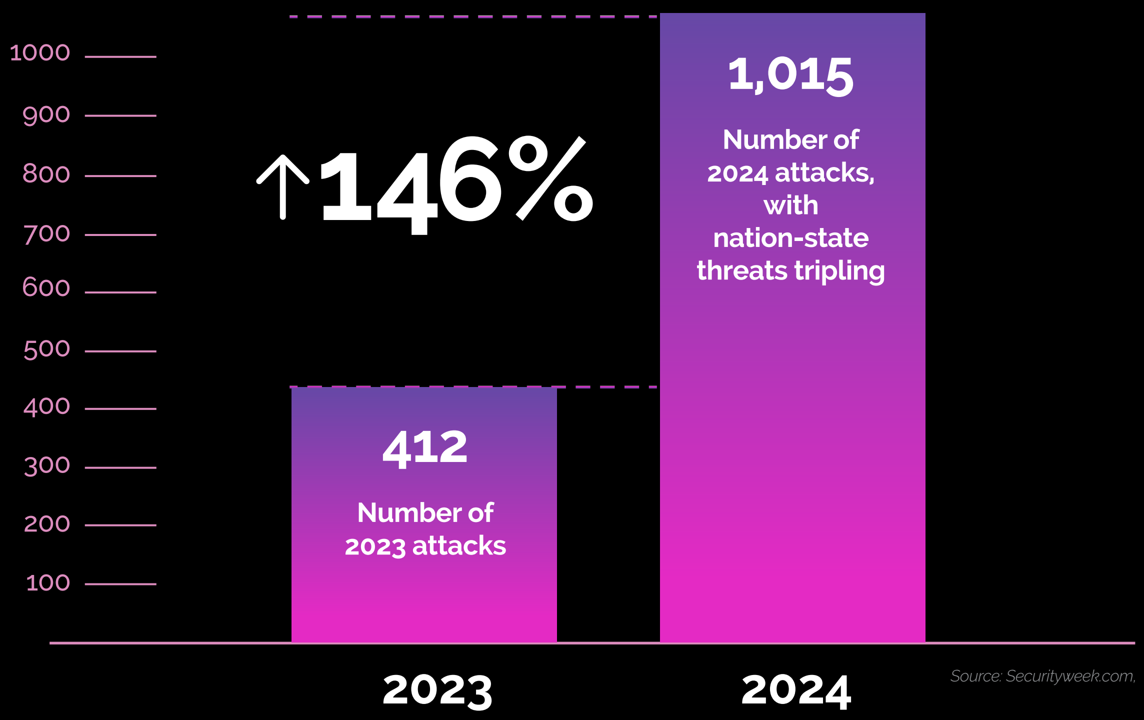
It's the foundation of modern life.

We live together in an interconnected, global ecosystem. When supply chains, hospitals, commerce, infrastructure, and governments run smoothly, economies and the people in them thrive. But when these systems are disrupted, life is interrupted.

STUDIES INDICATE

A lack of unified OT-IT teams and low investment in detection capabilities reduce efficacy and response speed, yet even as threats intensify, most organizations struggle with coordination and mature processes.

CYBER-PHYSICAL ATTACKS ON OT SYSTEMS



Source: Securityweek.com,

AND

75%

Industrial organizations that detected malicious cyber activity in their OT environments

Source: Palo Alto Networks global survey

24%

Industrial organizations that had to shut down OT operations due to cyberattacks

Source: Palo Alto Networks global survey

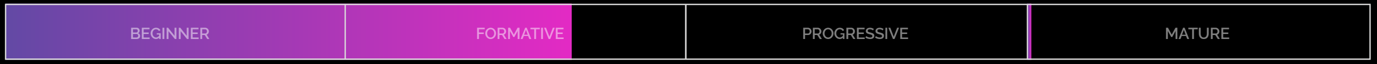
YET

Even as threats intensify, most organizations struggle with coordination and mature processes.

WORLDWIDE CYBERSECURITY READINESS

71%

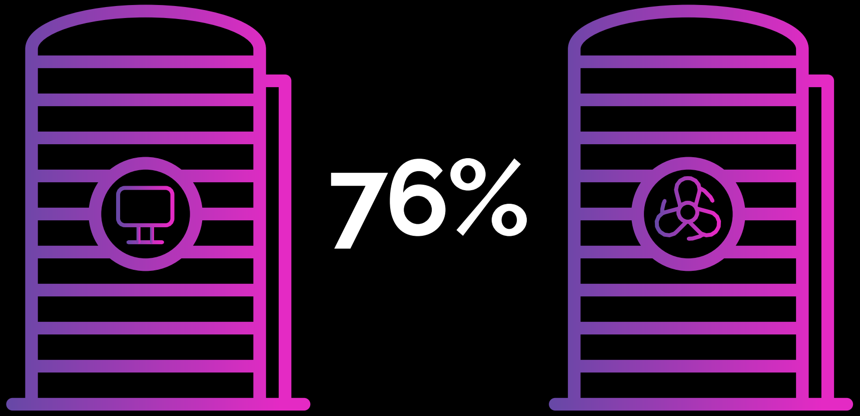
3%



Source: Wikipedia

Worldwide organizations falling into the two least-prepared cybersecurity readiness

Worldwide organizations classified as having "mature" cybersecurity readiness



76%

IT

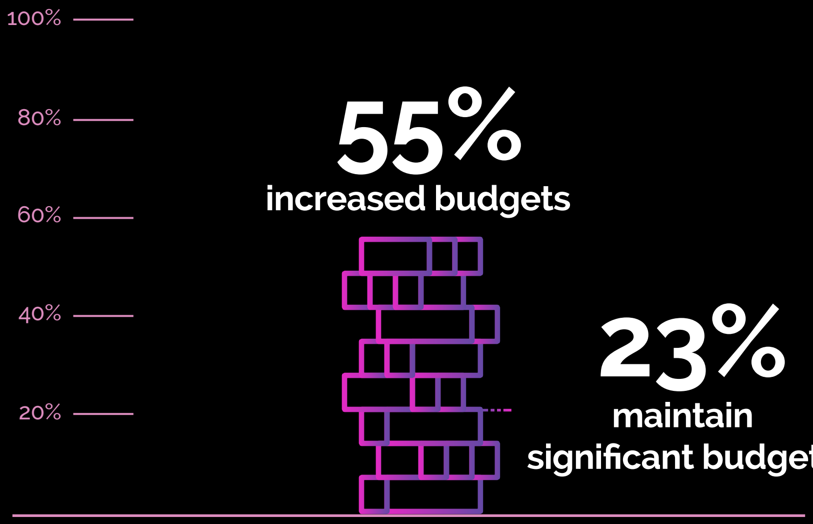
OT

Organizations that still maintain siloed IT and OT teams

Source: Cisco

AND ONLY

ORGANIZATIONAL OT SECURITY BUDGETS 2023-2025



55%
increased budgets

23%
maintain significant budgets

Source: Industrialcyber.co

Life, uninterrupted requires preparation.

Protecting mission-critical systems must be a top priority investment now and in the future as attack surfaces continue to expand. Human safety, business continuity, manufacturing uptime, and consumer trust remain at serious risk for global disruption.

STUDIES INDICATE

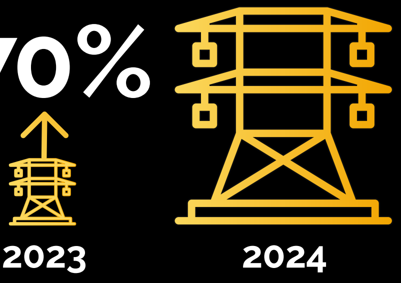
When cyber threats infiltrate physical systems, human life is at risk.

+60
per day

Rise in daily U.S. power grid exposure points, numbering almost 24,000

Source: Reuters

70%



Surge in cyber attacks against U.S. utilities with an average of 1,162 attacks up from 689

Source: Reuters

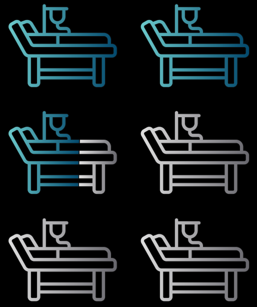
99%

Hospital networks that contain active Known Exploited Vulnerabilities (KEVs)

Source: Claroty

44%

In 2024, APAC experienced the highest percentage of healthcare attacks



Source: IBM

How to ensure Safety, uninterrupted.

Gain complete visibility into the attack surface threat actors can target in utilities infrastructure (power grids, water, and sanitation) and hospital networks as threats rapidly evolve.

This growth is not due to malicious actors, but to digital transformation and modernization (e.g., smart meters, cloud platforms, IoT sensors).

Every new connected point becomes a potential attack vector. Without full visibility and segmentation, these sectors are at increased risk of systemic disruption, especially as adversaries automate reconnaissance and make use of AI as a tool.

STUDIES INDICATE

Uptime is everything, and when interrupted, it can be catastrophic to your business.

90%

Impacted firms took hours or longer to return systems to service

Source: Gartner

$5.6M

Average cost per hour of unplanned OT downtime in manufacturing

Source: Gartner

YET STILL

75%

Industrial Building Management Systems (BMS) that contain known exploitable vulnerabilities

Source: Claroty

1 or 2 per year

Times most OT systems are patched, often months after vulnerabilities are found

Source: Claroty + Ponemon Institute

How to ensure Uptime, uninterrupted.

Establish real-time visibility and control over smart building systems like HVAC, elevators, lighting, and access controls, as they become increasingly connected through IoT platforms and remote vendor access.

These systems were not designed with cybersecurity in mind, yet they now form the backbone of operational uptime.

Without unified monitoring and segmentation across IT and OT environments, commercial facilities risk cascading disruptions from a single exploited entry point, whether via a compromised contractor credential or vulnerable automation controller.

STUDIES INDICATE

When systems halt, life comes to a standstill.

220%

Increase in global cyber-related supply chain disruptions since 2020

Source: Weforum

27%

Organizations with a documented cyber-physical business continuity plan

Source: Sans.org 2023 report

35%

Industrial plants that lack a specific cyber-incident response plan for OT

Source: Axios

+87%

Surge in ransomware incidents on industrial plants in 2024

Sources:The Fastmode

How to ensure Continuity, uninterrupted.

Unify IT and OT security, gain real-time visibility into all connected assets, and ensure that every facility and vendor has a continuity plan ready before an attack occurs.

One compromised OT asset can halt production, shipping, or critical services, so continuity depends on more than recovery; it demands prevention. As ransomware and supply chain attacks surge, causing billions in losses and weeks-long shutdowns, businesses must build resilience at the source.

STUDIES INDICATE

Once trust is lost in systems, safety, or service, it’s hard to regain.

78%

Consumers that say a security incident permanently erodes trust in a brand

Source: PWC

40%

CISOs who believe a cyber-physical breach would cause greater reputational damage than a traditional data breach

Source: Firtinet

How to ensure Trust, uninterrupted.

Sustaining trust means proactively securing physical systems, communicating readiness, and building transparency into every layer of cyber-physical defense.

Trust is the invisible backbone of every system, and when cyber-physical systems are breached, the impact isn't limited to downtime or data loss; it shakes public confidence in the safety, reliability, and intent of an organization.

As attacks become increasingly targeted and high-profile, from national infrastructure to global brands, consumers and stakeholders expect not just protection, but also proof of resilience.

]

CLAROTY

Life, uninterrupted.

With the right cyber-physical security measures, commitment, budgets and partnerships in place, human safety, business continuity, operational uptime, consumer trust – and life itself – goes uninterrupted.

Gain full visibility and real-time detection in your network

Eliminate blind spots where attacks dwell for hours, days, or longer.

Develop a rapid response plan

Learn how to shrink an attack recovery from hours to minutes, stopping cascading harm.

Take a unified approach

Secure IT+OT in one pane, ready for compliance and future threats.

Monitor proactive intelligence

Leverage Team82 insights and threat data to stay ahead of the ever-expanding attack footprint.

CLAROTY

We envision a future where the cyber and physical worlds safely connect.

Claroty, named a leader by Gartner™, protects critical infrastructure for healthcare, industrial, commercial and governmental organizations against threats coming from connected devices, keeping humans safe, businesses up and running, and nations secure.

Its Team82 Research, shared with its partners and security experts around the world, and the Nexus Cyber-physical Systems Protection Community is furthering the knowledge needed to continue the fight against bad actors threatening critical infrastructure worldwide.

Visit website

Book a Demo