CLAROTY merlin group

March 11, 2025 | Washington, DC

XCCELERATE

Advancing Cyber Innovation for Government

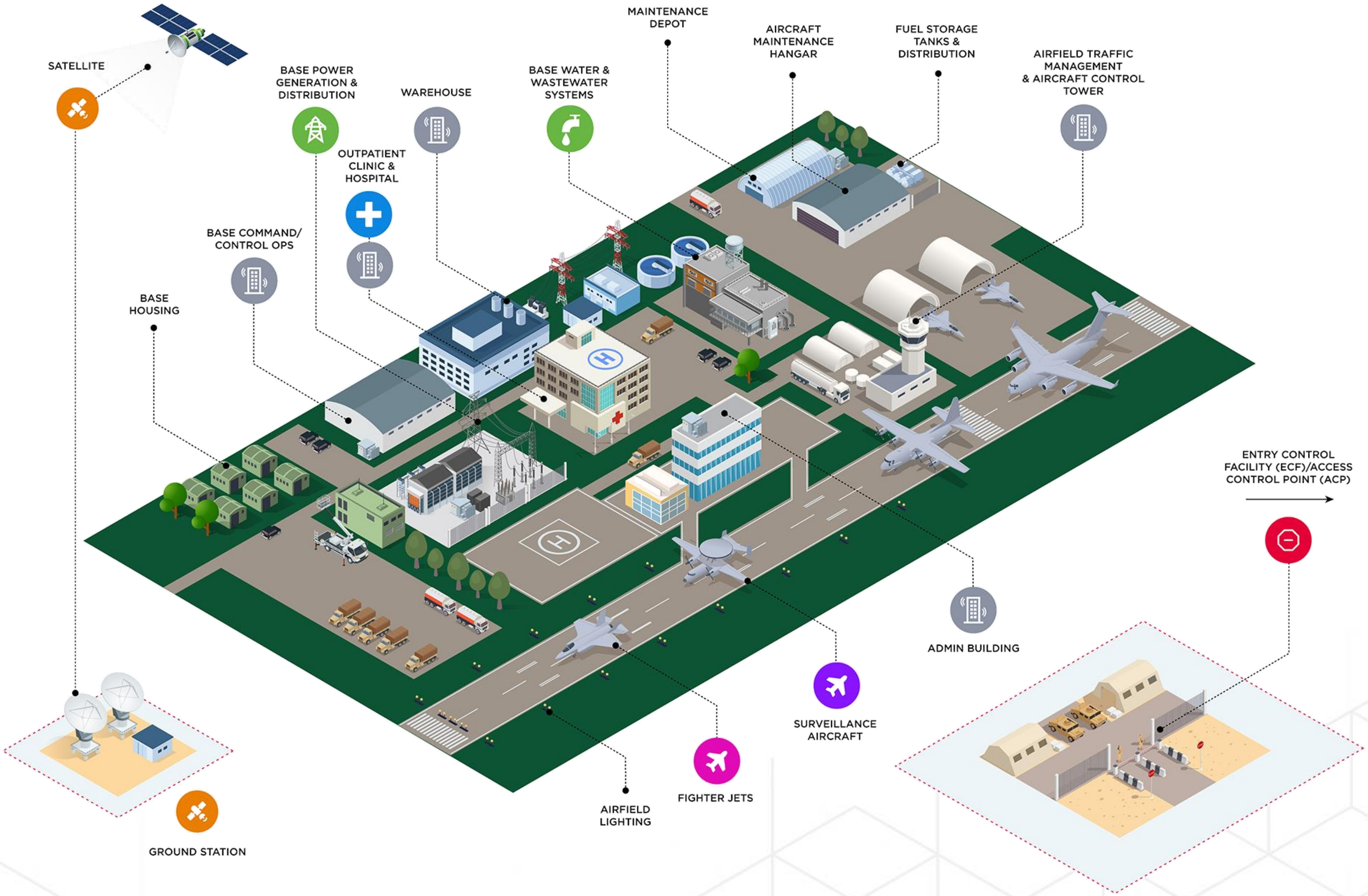
Securing OT & ICS Networks

“The OT Network Blind Spot – Risks & Vulnerabilities Are Closer Than They Appear”

What is OT Network Security & Why Should We Care?

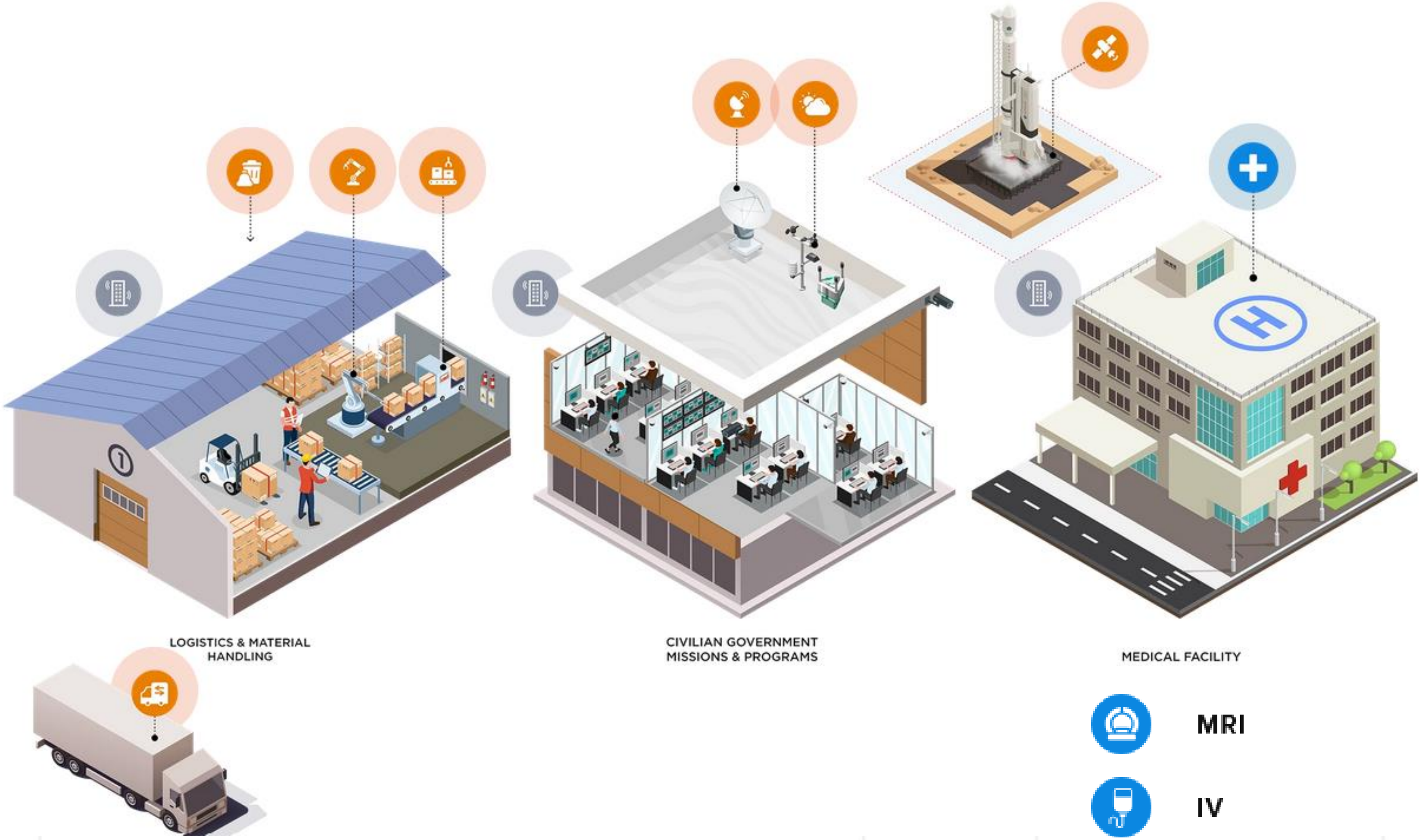
OT Networks For Military Installations

- Backup Power
- Fuel Distribution
- Fuel Storage
- Base Power Distro
- Base Power Gen
- Mission Water System
- Water Storage
- Potable Water
- Public Works
- Manufacturing
- Building Controls


SATELLITE
BASE POWER GENERATION & DISTRIBUTION
WAREHOUSE
BASE WATER & WASTEWATER SYSTEMS
MAINTENANCE DEPOT
AIRCRAFT MAINTENANCE HANGAR
FUEL STORAGE TANKS & DISTRIBUTION
AIRFIELD TRAFFIC MANAGEMENT & AIRCRAFT CONTROL TOWER
OUTPATIENT CLINIC & HOSPITAL
BASE COMMAND/ CONTROL OPS
BASE HOUSING
ENTRY CONTROL FACILITY (ECF)/ACCESS CONTROL POINT (ACP)
ADMIN BUILDING
SURVEILLANCE AIRCRAFT
FIGHTER JETS
AIRFIELD LIGHTING
GROUND STATION

Operation/Mission Systems & Services

- LOGISTICS SYSTEMS
- TRANSPORTATION SYSTEMS
- MANUFACTURING WASTE/ CLEANUP OPERATIONS
- SATELLITE COMMS
- WEATHER SYSTEMS
- SPACE SYSTEMS
- AUTOMATED MATERIAL HANDLING (AMHE)

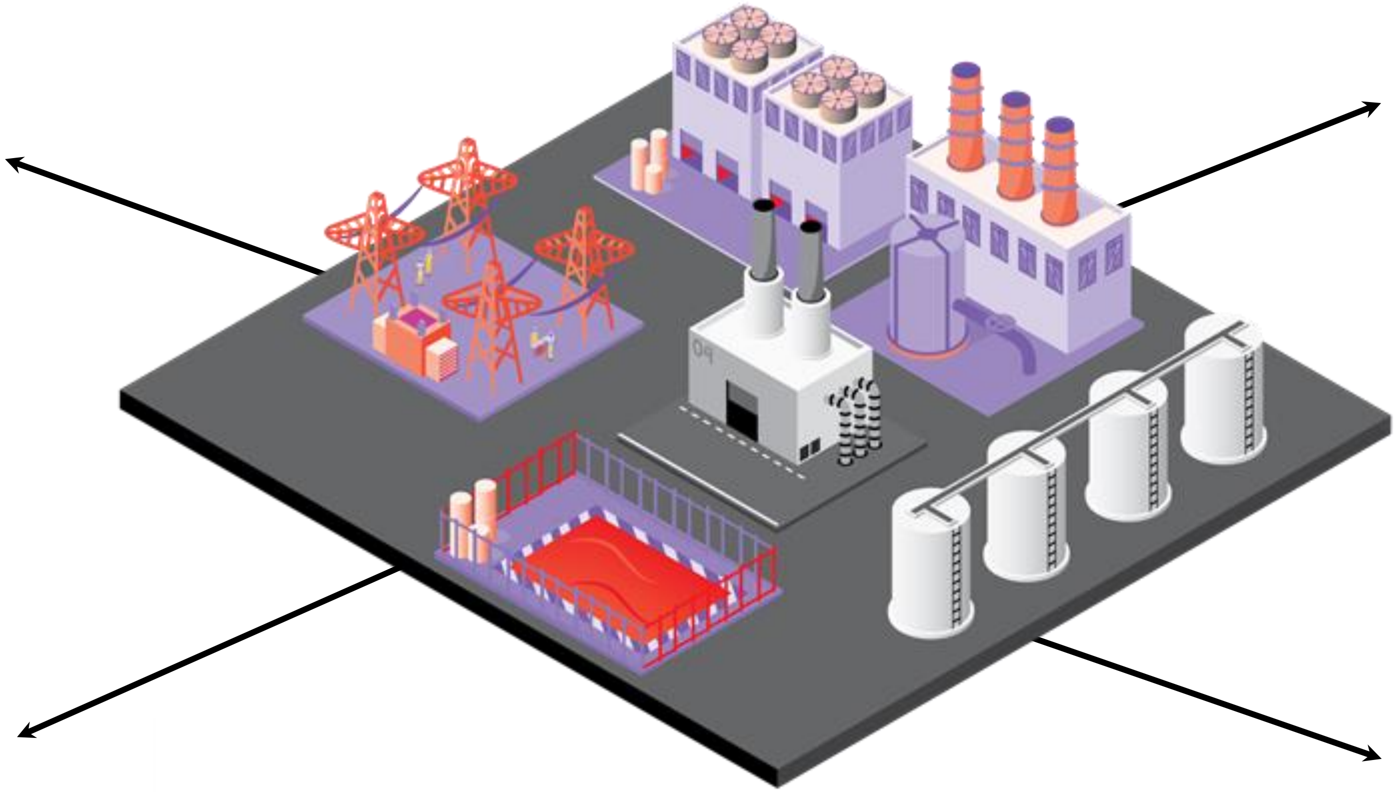

LOGISTICS & MATERIAL HANDLING
CIVILIAN GOVERNMENT MISSIONS & PROGRAMS
MEDICAL FACILITY

- MRI
- IV
- XRAY

Disruptions From OT Cyber Attacks are Increasing

67%
incurred at least $100,000 in financial impact due to a cyber attack

49%
Of CPS organizations experienced 12+ hours of downtime due to a cyber attack



45%
of organization stated at least half of their CPS are connected to the internet

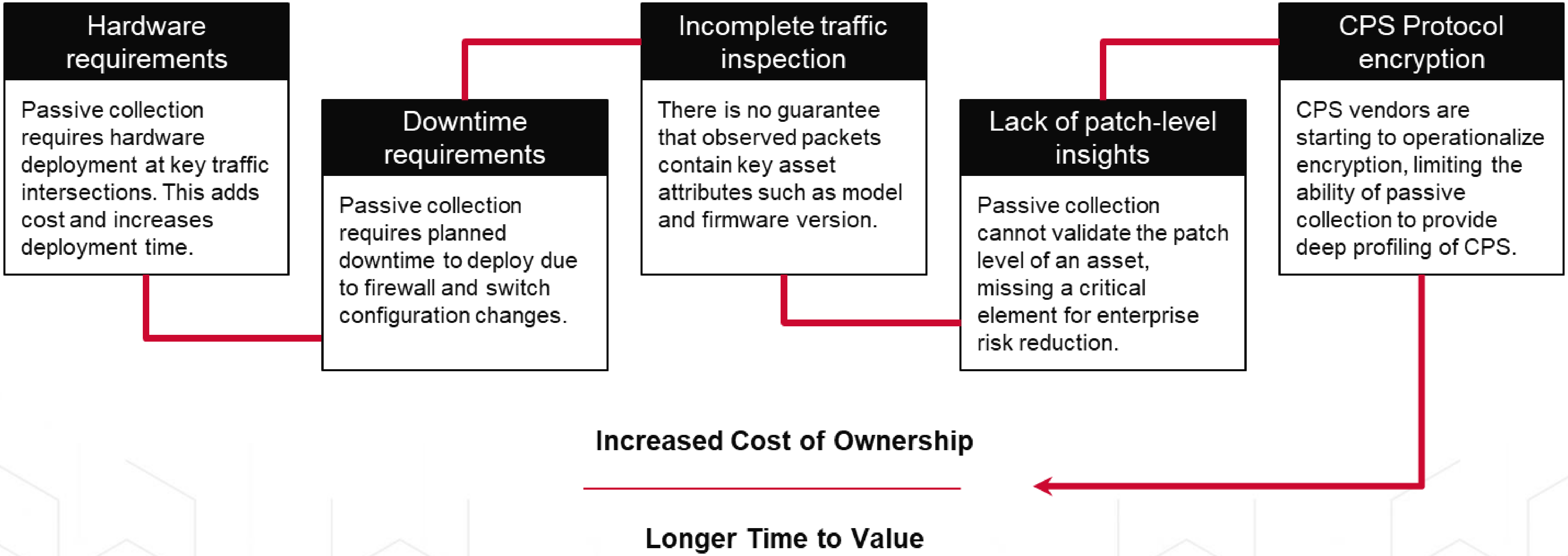
82%
Experienced at least one cyber attack that originated from third-party access

OT Asset Visibility, Risk Assessment & Threat Detection

OT Security Challenges for US Federal & DoD Agencies

- Asset Inventory Mandates
- Risk & Vulnerability Assessments
- Threat Detection & Response
- Preparing OT Networks for Zero Trust

Asset Inventory: Limitations of Passive Discovery



Hardware requirements

Passive collection requires hardware deployment at key traffic intersections. This adds cost and increases deployment time.

Downtime requirements

Passive collection requires planned downtime to deploy due to firewall and switch configuration changes.

Incomplete traffic inspection

There is no guarantee that observed packets contain key asset attributes such as model and firmware version.

Lack of patch-level insights

Passive collection cannot validate the patch level of an asset, missing a critical element for enterprise risk reduction.

CPS Protocol encryption

CPS vendors are starting to operationalize encryption, limiting the ability of passive collection to provide deep profiling of CPS.

Increased Cost of Ownership

Longer Time to Value

A New Approach to Asset Inventory: Dynamic Discovery

Safe Queries

Targeted discovery of assets in their native protocol

Claroty Edge

Speedy, host-based asset profiling through localized queries

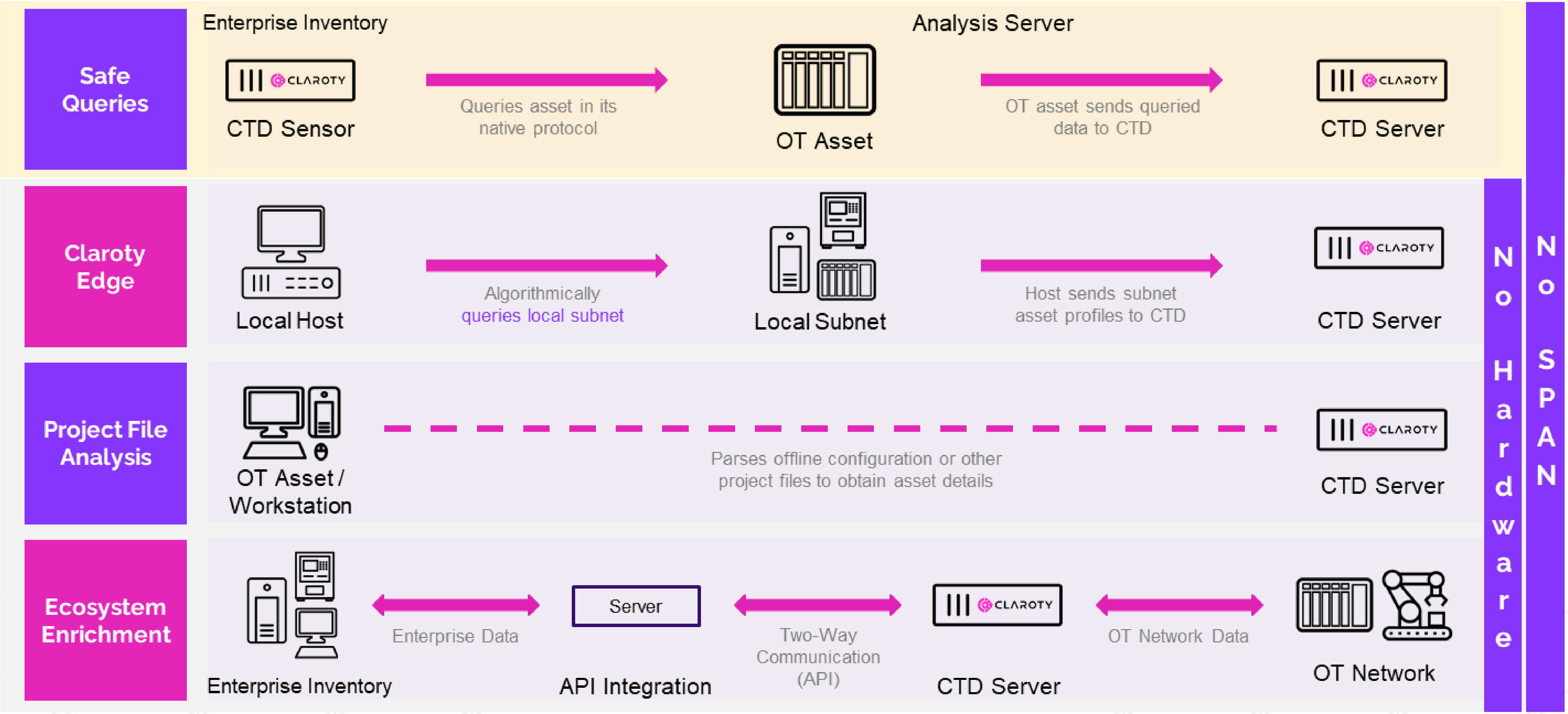
Project File Analysis

Regular ingestion of offline configuration files for asset enrichment

Integrations

Enriching visibility without hardware or configuration changes

Dynamic Discovery: How It Works



Safe Queries

Enterprise Inventory — Analysis Server

CTD Sensor → Queries asset in its native protocol → OT Asset → OT asset sends queried data to CTD → CTD Server

Claroty Edge

Local Host → Algorithmically queries local subnet → Local Subnet → Host sends subnet asset profiles to CTD → CTD Server

Project File Analysis

OT Asset / Workstation - - - Parses offline configuration or other project files to obtain asset details - - - CTD Server

Ecosystem Enrichment

Enterprise Inventory ↔ Enterprise Data ↔ Server (API Integration) ↔ Two-Way Communication (API) ↔ CTD Server ↔ OT Network Data ↔ OT Network

No Hardware

No SPAN

Complete OT Visibility: A Phased Approach

Strong OT cybersecurity **requires a foundation of in-depth visibility**

1

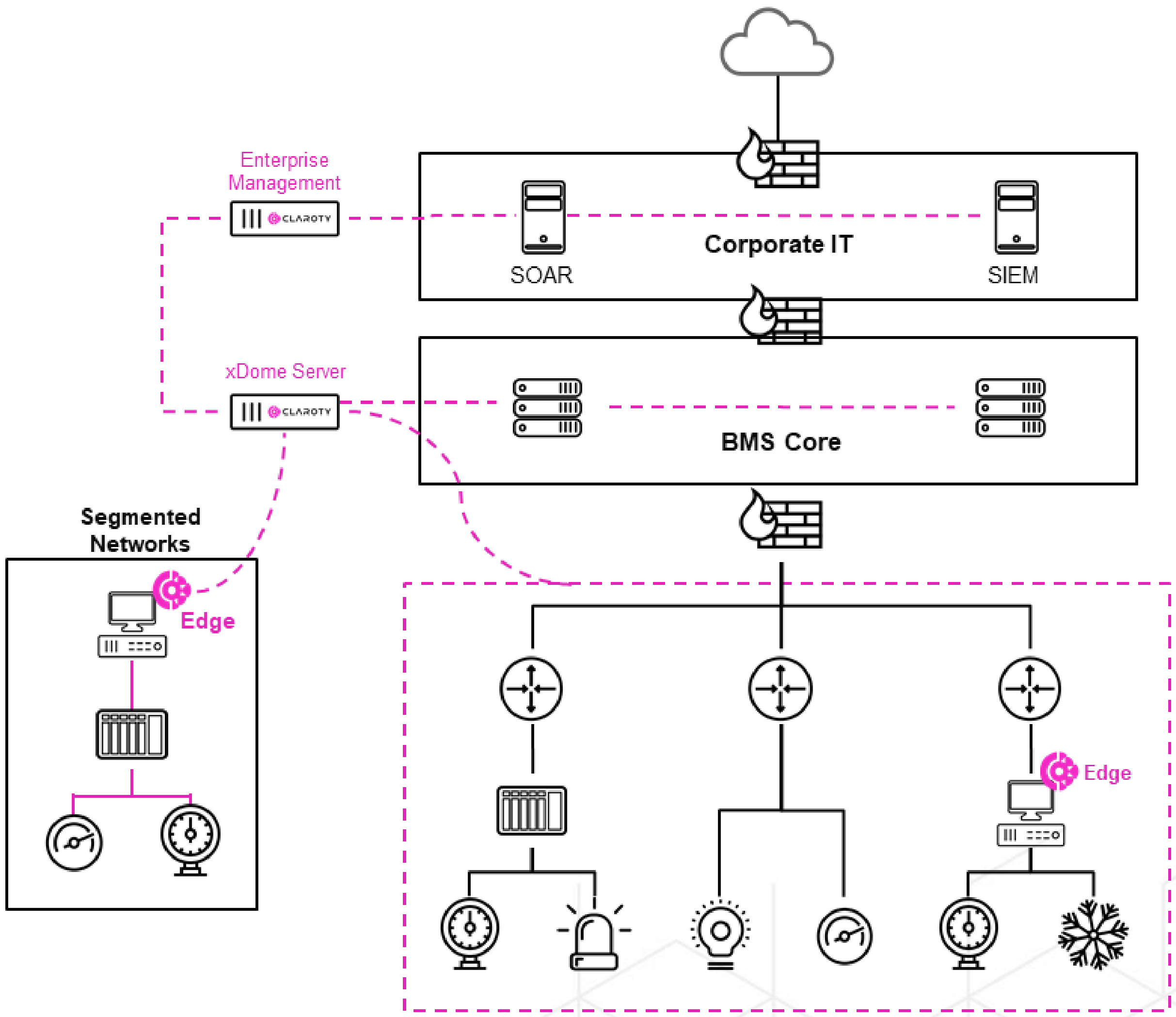
Dynamic Discovery leverages a combination of **safe queries** and **existing ecosystem data**

- ✓ Deep asset profiles
- ✓ Broad, actionable insights
- ✓ No hardware required
- ✓ Low deployment resources

2

Adding **passive collection** to enhanced additional requirements

- ✓ Continuous threat monitoring
- ✓ CPS communication profiling



CLAROTY

Secure Access for OT Networks

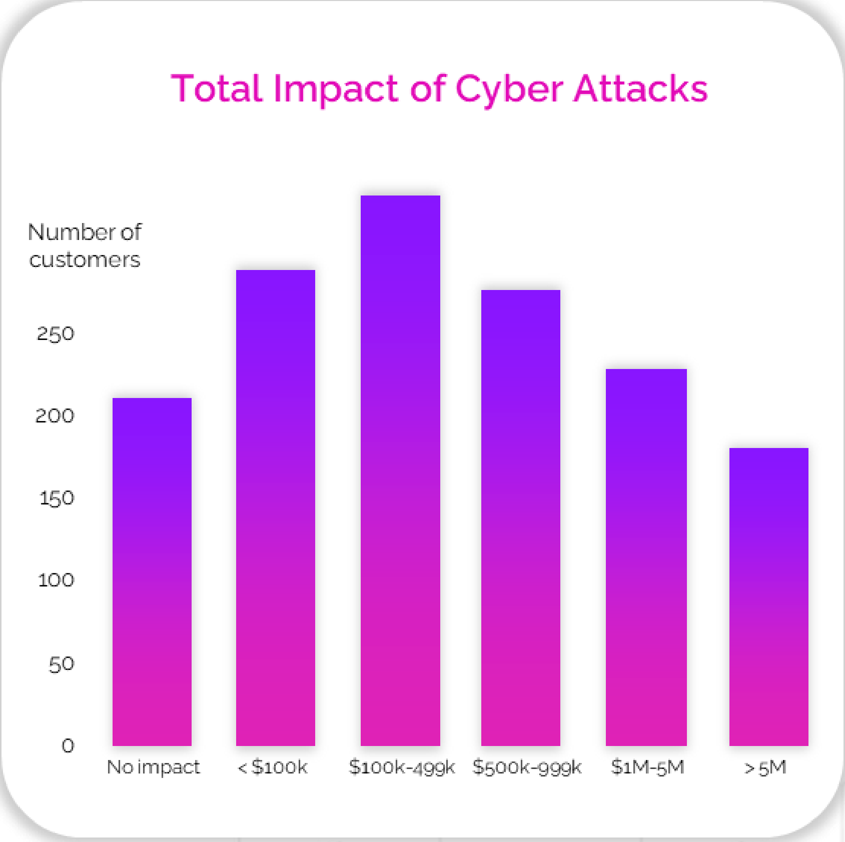
Remote Connectivity Introduces Risk For OT Networks

82% of organizations experienced **at least one cyber attack** related to 3rd party access to CPS environment

63% of organizations have only partial or **no understanding of 3rd party connections** to their CPS environments

45% of organizations experienced **5 or more attacks related to remote access**

The Global State of CPS Security 2024



Source: https://claroty.com/resources/reports/the-global-state-of-cps-security-2024-business-impact-of-disruptions

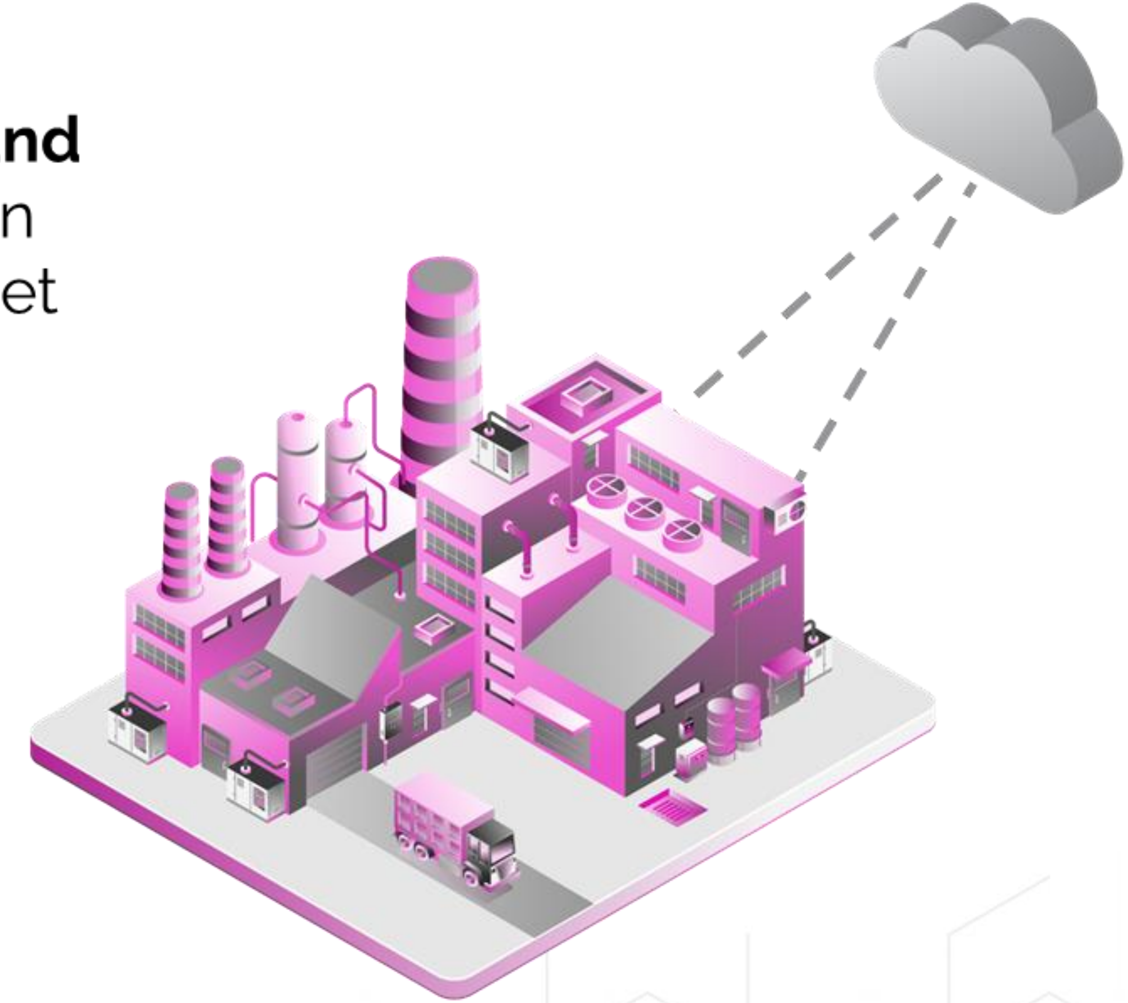
Remote Connectivity In The OT Environment

An analysis of **thousands of HMIs and EWSs** revealed that **13%** maintain an insecure connection with the internet

⬇

36%

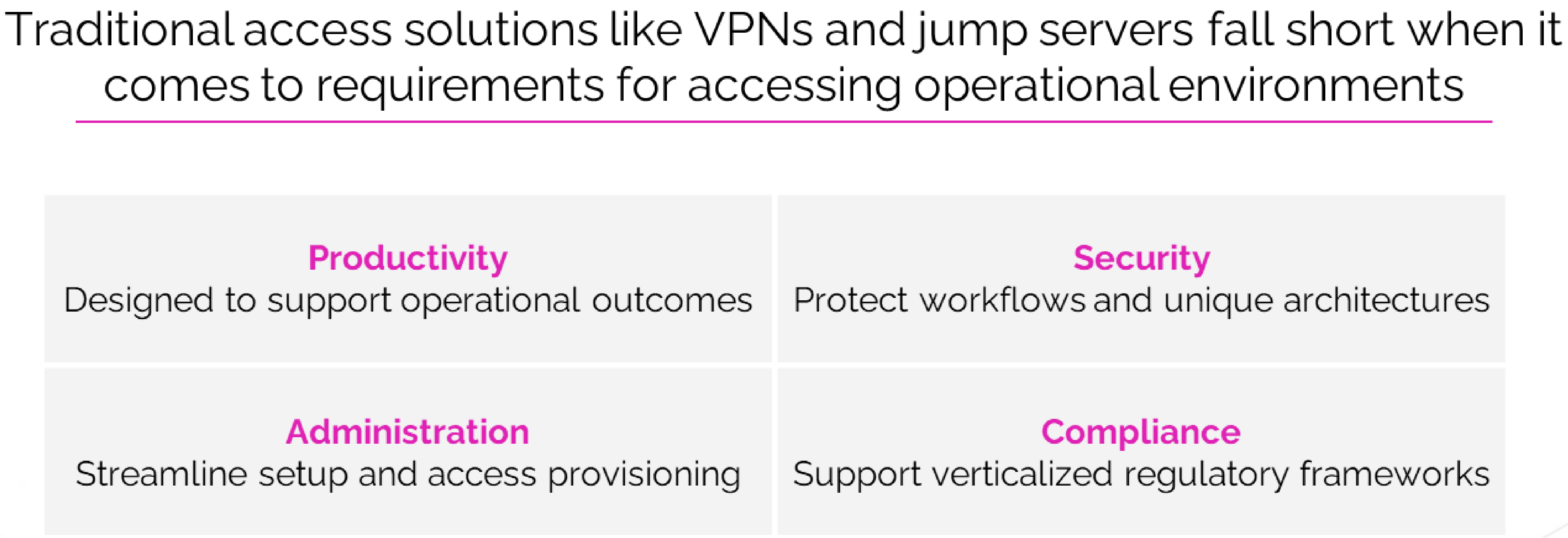
Of these have at least one exploited vulnerability



Data captured from the Claroty xDome installed base

HMI: Human Machine Interface
EWS: Engineering Workstation

OT Systems Require Tailor-Made Secure Access Solutions



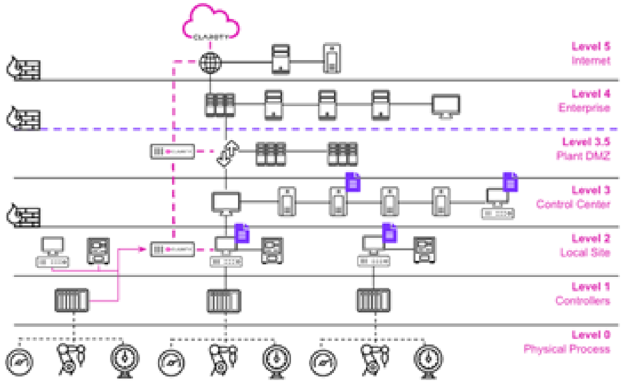
Traditional access solutions like VPNs and jump servers fall short when it comes to requirements for accessing operational environments

Productivity Designed to support operational outcomes	**Security** Protect workflows and unique architectures
Administration Streamline setup and access provisioning	**Compliance** Support verticalized regulatory frameworks

Why OT Systems Require A Specialized Approach To Secure Access

	Traditional IT solution	CPS Implications
Productivity	Lacks agentless access and struggles in high-latency environments.	Hinders operations and maintenance of assets in remote sites, creating **risk of downtime and increased MTTR**.
Security	Broad network access with limited session control, violating Zero-Trust principles.	**Increases OT asset exposure**, risks of privilege escalation, lateral movement, and operational errors.
Administration	Manual identity and access management, lacking centralized governance.	**Requires specialized CPS knowledge** for managing user lifecycles and granular RBAC.
Compliance	Fail to effectively log and report network changes in real-time.	Creates compliance gaps, **result in audit challenges** and an **increased operational risk**.

Driving OT Security Through Secure Access Controls



What is the scope of your secure access program?

What level of user access and control is required?

Which regulatory frameworks do you closely align with?

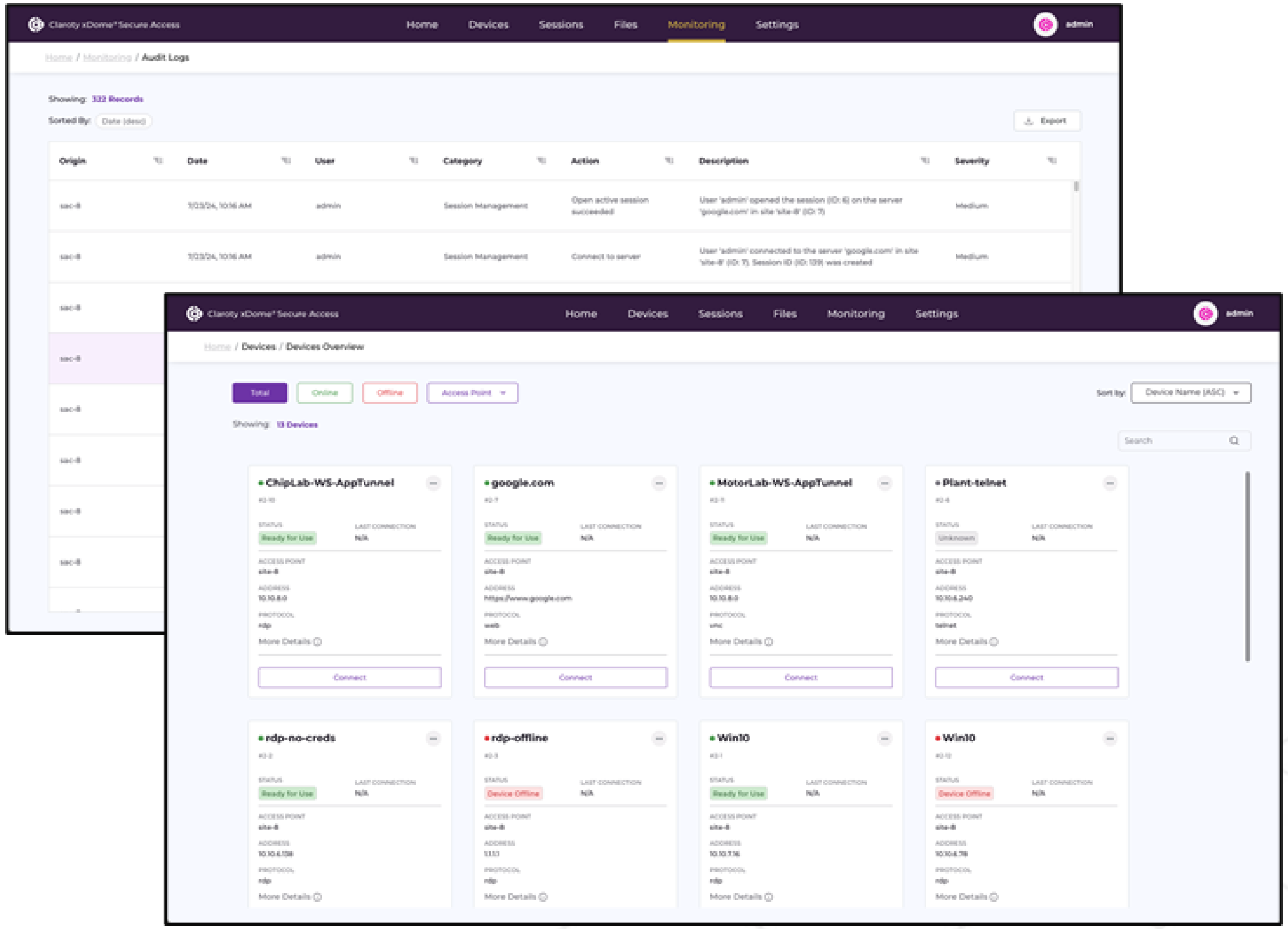
Claroty xDome Secure Access: Tailor-Made Secure Access for OT

Supporting the **operational integrity** of mission-critical assets

Seamless first and third-party access

Risk and attack surface reduction

Simple administration and governance



Home / Monitoring / Audit Logs

Showing: 332 Records

Sorted By: Date (desc)

Origin	Date	User	Category	Action	Description	Severity
sac-8	7/23/24, 10:16 AM	admin	Session Management	Open active session succeeded	User 'admin' opened the session (ID: 6) on the server 'google.com' in site 'site-8' (ID: 7)	Medium
sac-8	7/23/24, 10:16 AM	admin	Session Management	Connect to server	User 'admin' connected to the server 'google.com' in site 'site-8' (ID: 7). Session ID (ID: 139) was created	Medium
sac-8						
sac-8						
sac-8						
sac-8						
sac-8						
sac-8						

Home / Devices / Devices Overview

Showing: 13 Devices

ChipLab-WS-AppTunnel
#2-10
STATUS: Ready for Use
LAST CONNECTION: N/A
ACCESS POINT: site-8
ADDRESS: 10.10.8.0
PROTOCOL: rdp
More Details ⓘ

google.com
#2-7
STATUS: Ready for Use
LAST CONNECTION: N/A
ACCESS POINT: site-8
ADDRESS: https://www.google.com
PROTOCOL: web
More Details ⓘ

MotorLab-WS-AppTunnel
#2-11
STATUS: Ready for Use
LAST CONNECTION: N/A
ACCESS POINT: site-8
ADDRESS: 10.10.8.0
PROTOCOL: vnc
More Details ⓘ

Plant-telnet
#2-6
STATUS: Unknown
LAST CONNECTION: N/A
ACCESS POINT: site-8
ADDRESS: 10.10.6.240
PROTOCOL: telnet
More Details ⓘ

rdp-no-creds
#2-2
STATUS: Ready for Use
LAST CONNECTION: N/A
ACCESS POINT: site-8
ADDRESS: 10.10.6.138
PROTOCOL: rdp
More Details ⓘ

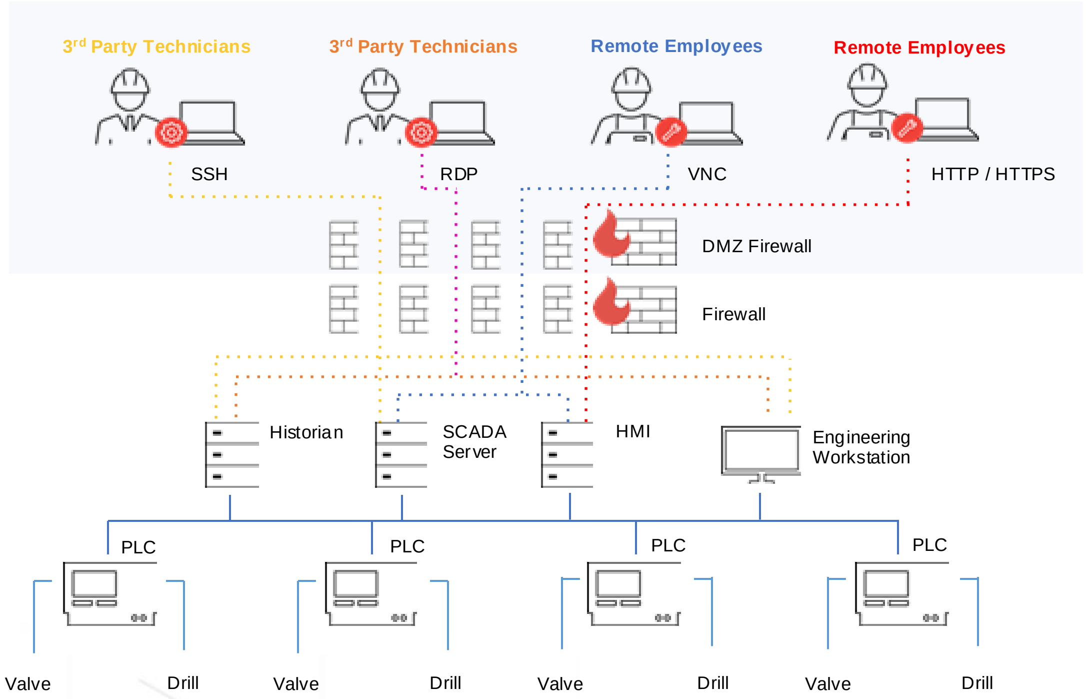
rdp-offline
#2-3
STATUS: Device Offline
LAST CONNECTION: N/A
ACCESS POINT: site-8
ADDRESS: 1.1.1.1
PROTOCOL: rdp
More Details ⓘ

Win10
#3-1
STATUS: Ready for Use
LAST CONNECTION: N/A
ACCESS POINT: site-8
ADDRESS: 10.10.7.16
PROTOCOL: rdp
More Details ⓘ

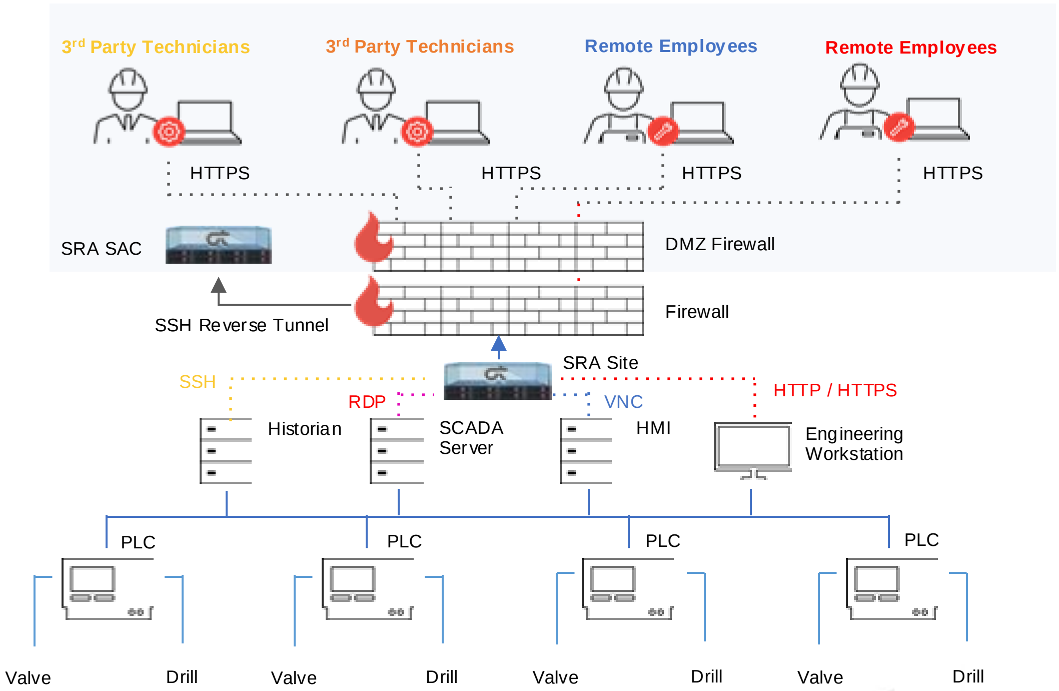
Win10
#2-12
STATUS: Device Offline
LAST CONNECTION: N/A
ACCESS POINT: site-8
ADDRESS: 10.10.6.78
PROTOCOL: rdp
More Details ⓘ

Claroty xDome Secure Access: Solution Overview

Without Secure Access

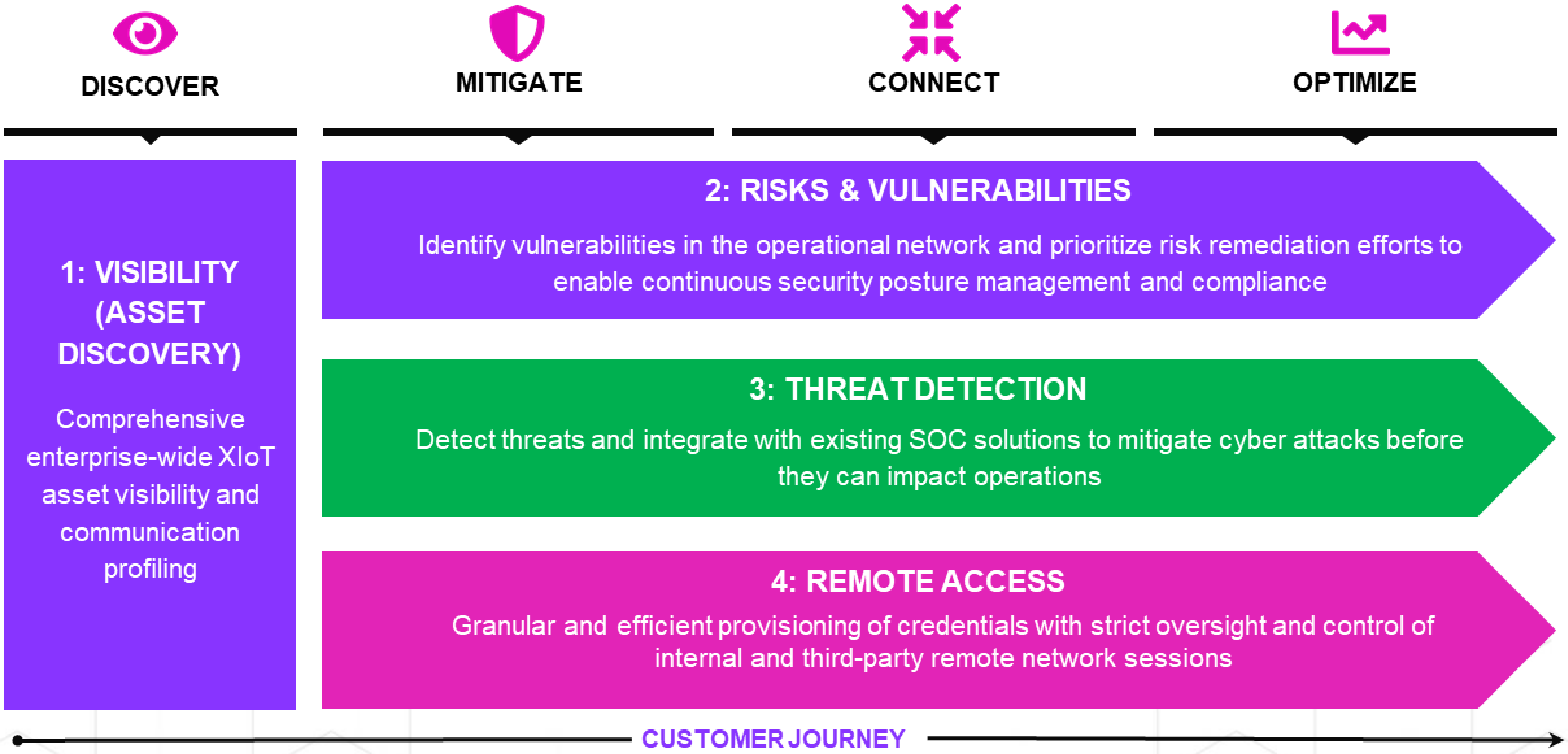


With Secure Access



Claroty Solutions For Securing OT Networks

The Journey To Achieving OT Cyber Resilience



DISCOVER

MITIGATE

CONNECT

OPTIMIZE

1: VISIBILITY (ASSET DISCOVERY)

Comprehensive enterprise-wide XIoT asset visibility and communication profiling

2: RISKS & VULNERABILITIES

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

3: THREAT DETECTION

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

4: REMOTE ACCESS

Granular and efficient provisioning of credentials with strict oversight and control of internal and third-party remote network sessions

CUSTOMER JOURNEY

Claroty Solutions for Securing OT Networks

Claroty xDome

Claroty Continuous Threat Detection (CTD)

Claroty xDome Secure Access

Exposure Management

Advanced risk and vulnerability management with prioritization guidance, risk assessment, and reporting capabilities.

Network Protection

Protect asset zones with zone mapping recommendations, policy creation, and custom communication alerting.

Threat Detection

Continuously monitor your network for known threats and anomalous activity, and investigate alerts with SOC integrations.

Secure Access

Frictionless and secure remote access for operations in industrial environments by internal and third-party users.

CPS Zone Management

Comprehensive Asset Visibility

Questions