

## SOLUTION OVERVIEW

# Claroty xDome Secure Access

Delivering Secure Access for Cyber-Physical Systems

Cyber-Physical Systems (CPS), such as those found in industrial control systems, are the core components of the highly complex and extensive world of manufacturing, healthcare, and other critical infrastructure sectors. As these systems become increasingly interconnected—simple, secure, and reliable access to operational networks has shifted from a convenience into a necessity. Accelerated by the results of adopting remote access technologies, this shift has better enabled organizations to optimize production, reduce travel costs, and manage operational issues for the wide variety of diverse stakeholders involved. Despite its benefits, increased connectivity is linked to the proliferation of cyber attacks in recent years—leading 25% of organizations to consider remote access and asset management to be the biggest gap in their CPS cybersecurity program<sup>1</sup>.



## Productivity Demands

Connect in order to drive efficiencies and improve metrics like mean-time-to-repair (MTTR)



## Increased Threat Landscape

Increased attack surface at a time when cybercrime is more accessible & deployable than ever



## Regulatory Pressures

Governments act to protect environments that underpin national security and public safety

xDome Secure Access (SA) is a flexible, purpose-built remote access solution catered to meet the specific needs of CPS environments. It operationalizes the balance between frictionless access and secure control over third-party interactions with CPS—**enhancing productivity, reducing risk and administrative complexities, and ensuring compliance** across both cloud and on-premises operations.

## Key Takeaways

- **Designed for CPS Operations:** Secure Access is built for the unique needs of both first and third-party users and the complex production environments in which they operate
- **CPS-Specific Security:** Whether deployed in the cloud or on-premise, Claroty protects against the risk of remote exploitation while preserving sure architectural best practices like the Purdue Model
- **Reduce Administrative Resources:** Alleviate the complexity of generating, provisioning, and maintaining identities with purpose-built, just-in-time credential management
- **Maintain Compliance:** Adhere to growing regulatory pressures and avoid noncompliance penalties with advanced logging and recording of access sessions.

<sup>1</sup> The Global State of Industrial Cybersecurity, 2023, Claroty, <https://claroty.com/resources/reports/the-global-state-of-industrial-cybersecurity-2023>.

## Why CPS Requires A Specialized Solution

Traditional access solutions like VPNs and jump servers have proven increasingly ineffective and inefficient for providing access to operational networks because they were not built for the unique operational constraints, security considerations, or personnel needs of their users.

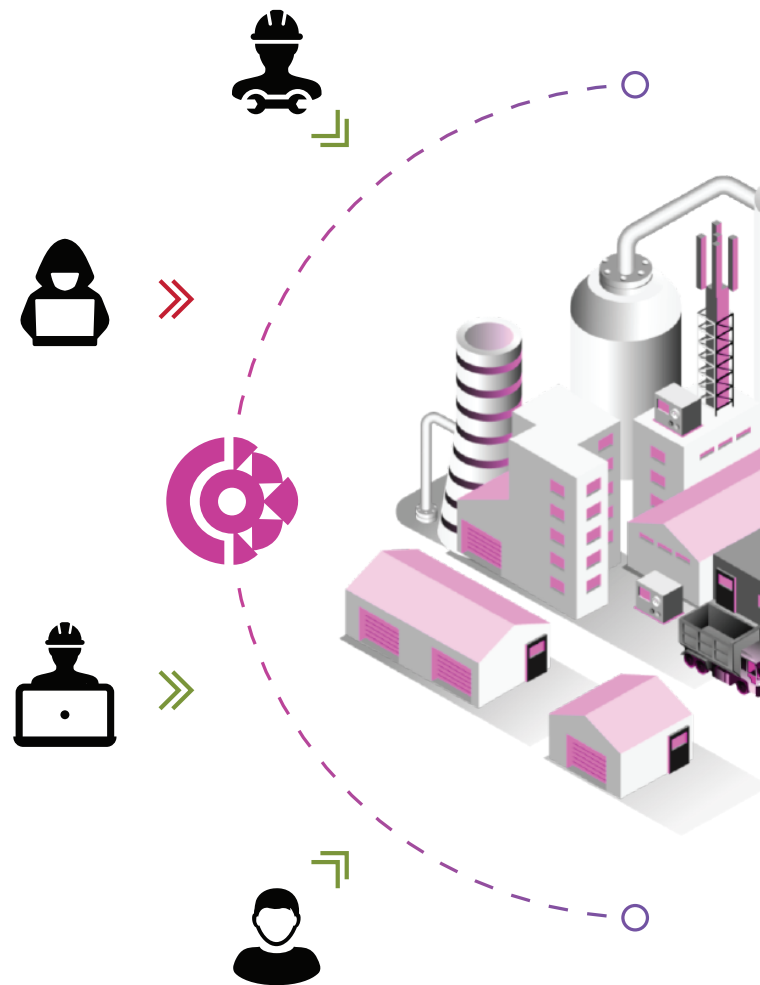
A built-for-purpose CPS secure access solution combines the ability to provide privileged access management for a variety of operational tasks and seamlessly administer identity governance across a diverse user base. These, in combination with embracing the principles of Zero-Trust, enable organizations to offer granular access controls that support operational workflows while minimizing the attack surface in business critical environments.

## Securing Operations with xDome Secure Access

xDome Secure Access was built for the operational environment—providing security, control, and easy access to business critical assets regardless of location. This solution ensures a flexible and agentless deployment within a CPS-ready architecture that supports consistent operations in high-latency environments, with capabilities involving enhanced access control with Zero-Trust policy management, real-time monitoring and recording of access sessions, and comprehensive audit logs of session actions.

### CPS-Native Capabilities Enabling Remote Operations


- Agentless remote access via RDP, SSH, HTTP/S, VNC
- Micro tunneling for OT-specific protocols
- Just-in-time access requests/provisioning
- File transfers for remote operations
- Session logging and video recording
- Live monitoring with disconnect controls
- Integrations with IdP, SIEM, ICAP solutions, and others



These capabilities enable core outcomes for manufacturing and other critical infrastructure environments


Improved Productivity	Minimize Risk	Reduced Complexity	Maintain Compliance
Reduced Travel Expense	Narrow Attack Surface	Reduced Administrative Cost	Minimize Fines & Fees
Avoid Downtime	Improved Network Integrity	Extend Value of Existing Tools	Enhanced Audit Response
Improved MTTR	Proactive Incident Response	Enhanced Scalability	Improved Security Posture
Simplify Training Cycles	Eliminate Rogue Access	Improved Security Controls	Boost Operational Integrity

Why a Cloud Solution?




**Real-Time Updates**

xDome Secure Access is updated as soon as new versions are available, removing complex update schedules and rollout measures across multi-site deployments.



**Security**

Claroty solutions employ Zero Trust principles to reduce cyber risk as well as boast certifications such as ISO/IEC 27001, SOC 2 Reporting, GDPR, and more.



**Simplicity**

Cloud solutions reduce total-cost-of-ownership by removing physical deployment barriers and the burden of monitoring the surrounding infrastructure.

*By consuming less time and resources deploying, updating, and maintaining the platform, xDome Secure Access provides a lower overall TCO as a SaaS solution*

Recognizing that no-two operational networks are identical, xDome Secure Access maintains a flexible deployment model that supports a multi-tier secure architecture in both cloud and on-premise environments. This flexibility allows Claroty to tailor our solution delivery in a way that accommodates the unique operational requirements, cost considerations, or regulatory boundaries – and to easily migrate users to a cloud environment when and if required.

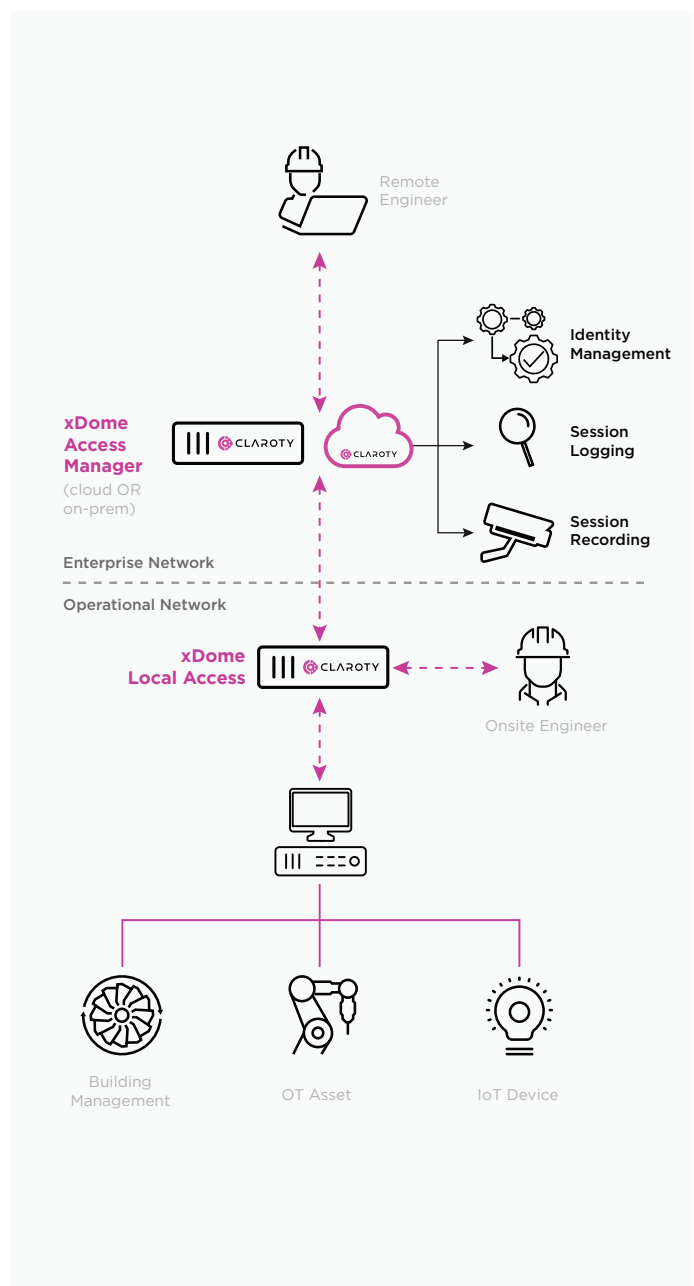
## How It Works

xDome SA works by segmenting user access into multiple stages by applying the principles of Zero Trust to access policy management across our xDome Access Manager and xDome Local Access points.

- **xDome Access Manager:** Hosted in the cloud or on-premises, Access Manager provides a single pane of glass view to the entire deployment and is the portal through which users connect to the network.
- **xDome Local Access Point:** Located in the operational network to communicate with local devices and digitally represent their interface to the user.

These two components communicate using encrypted tunnels across the operational boundary, adhering to operational cybersecurity best practices and ensuring that remote users never have direct access to the process network while supporting their access needs. Sessions are logged and can be recorded for incident response and future auditing.

xDome Secure Access enhances productivity, reduces complexity and risk, and ensures compliance with regulatory frameworks across a variety of industries. Unlike traditional remote access solutions xDome is purpose-built for the specific needs of manufacturing and other critical infrastructure environments and helps to reduce cyber risk exposure, bolster business continuity, and protect critical CPS processes.



## About Claroty

Claroty has redefined cyber-physical systems (CPS) protection with an unrivaled industry-centric platform built to secure mission-critical infrastructure. The Claroty Platform provides the deepest asset visibility and the broadest, built-for-CPS solution set in the market comprising exposure management, network protection, secure access, and threat detection – whether in the cloud with Claroty xDome or on-premise with Claroty Continuous Threat Detection (CTD). Backed by award-winning threat research and a breadth of technology alliances, The Claroty Platform enables organizations to effectively reduce CPS risk, with the fastest time-to-value and lower total cost of ownership. Claroty is deployed by hundreds of organizations at thousands of sites globally. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America. To learn more, visit [claroty.com](https://claroty.com).