# Industrial Networks Secured

## Our Mission

Claroty was conceived to secure the industrial control networks that run the world's most critical infrastructures from cyberattack.  The Claroty Platform provides extreme visibility, cyber threat detection, and secure remote access for OT/ICS networks. Claroty's unmatched management and elite research teams are building an unparalleled suite of integrated products addressing the full spectrum of cybersecurity protection, detection, and response requirements.

## Your Result

Better security, safety, and reliability for your critical OT environments.

www.claroty.com

CLAROTY
Clarity for OT Networks

# Chemical Industry Case Study

Multi-Unit
Agrochemical Plant

# Foreword

## Chemical Cyber Threat Landscape – Overview

The cyber threat landscape for OT networks is changing rapidly. The classic nation state threat actors, targeting critical infrastructure, are now joined by multiple groups that are leveraging newly disclosed attack tools (such as the ones leaked from the NSA trove by the ShadowBrokers group). New threats include both cyber criminals executing impactful ransomware campaigns as well as the rising potential for jihadists or other terrorists to leverage widely available, and very sophisticated tools and techniques to cause harm.

During the second half of 2017, adversaries using leaked tools disabled numerous OT networks. Unlike nation state threats, the recent attacks did not specifically target plants. However, the indirect or "overspill" damage from these ransomware attacks on various manufacturing plants have mounted to hundreds of millions of dollars. The bottom line is that multiple new and potentially potent threats exist that chemical plant asset owners must now monitor for and actively defend against.

Within the OT ecosystem, the chemical industry features a fundamental dependency between process control and human and environmental safety. The production of fertilizers, plastics, pesticides, and petrochemicals entails the storage and processing of toxic materials, which necessitates additional safety responsibilities on top of plant reliability and productivity requirements.

According to Eric Cosman, a recognized industry leader in cybersecurity for industrial systems and a recognized expert in chemical manufacturing controls:

> ***"Virtually all chemical plants have some sort of computer-based automated control system. If you somehow compromise [that system], bad things could happen depending on the nature of the plant – that could range from spills of material, to some sort of overpressure or venting, or, in the worst case, even some sort of explosion."***

Chemical companies worldwide are acknowledging the rising risk of a cyberattack on their industrial network, and the impact an attack can have on the safety and reliability of industrial process. For example, cybersecurity is natively integrated in the U.S. Responsible Care® Security Code. Advanced organizations are responding with specific efforts to enhance the cybersecurity posture of their industrial networks. However, securing a chemical facility network holds several unique challenges, related mostly to how these networks are designed, built, and maintained.

A typical chemical facility network consolidates several production sites into a single network, typically with no logical isolation between sites. As a result, many endpoints within these networks can serve as a stepping stone, enabling attackers to access multiple sites. Additionally, routine maintenance activities, such as firmware upgrades, security patches, and network troubleshooting are carried out independently by external contractors, often accessing these networks remotely, providing adversaries with additional attack vectors.

Unmonitored remote connections, combined with the production sites internal connectivity create additional security blind spots that often go unnoticed and unattended due to lack of a working culture between the process control and the IT networking teams, and the lack of technology providing visibility into OT network configuration and traffic. The resulting lack of coordination and visibility exposes chemical plants to an expanded attack surface area and makes plants increasingly vulnerable to attack.

This case study describes in detail the deployment process of the full Claroty Platform in an agrochemical plant. It starts with overview of the plant's physical and network structure, followed by the security concerns and threat scenarios raised by the plant's team. It then shows samples of Claroty platform security findings and explains the risk mitigation role of each product in the platform: Continuous Threat Detection, Secure Remote Access, and Enterprise Management Console.

# Plant Description

## Physical Architecture

The plant produces vast assortment of products – insecticides, plant-protection, raw chemicals for various industries, and others – which involve the processing of highly toxic materials. There are 12 production units within the site, 9 of them currently active.

Each production unit has its own local control room with two Windows machines acting as both HMI and EWS. The standard routine is that major changes (such as between batches) are performed by the central team, while minor adjustments are carried out internally using Online Edits. Each site comprises 10 - 12 controllers in an outdoor cabinet, connected to ~1000 remote I\Os.

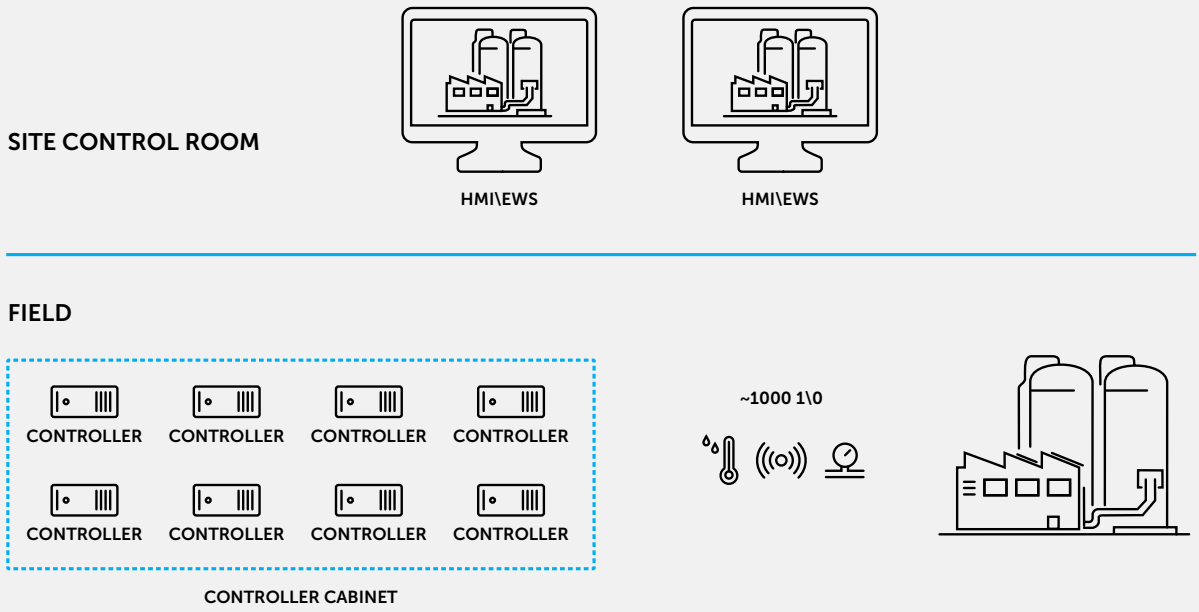



Diagram 1 – site: controllers, machines

All production units send data to a central control room for a holistic view of the entire plant's activities. There is a dedicated team manning the central control room, governing overall continuity, and configuration changes within the production sites.

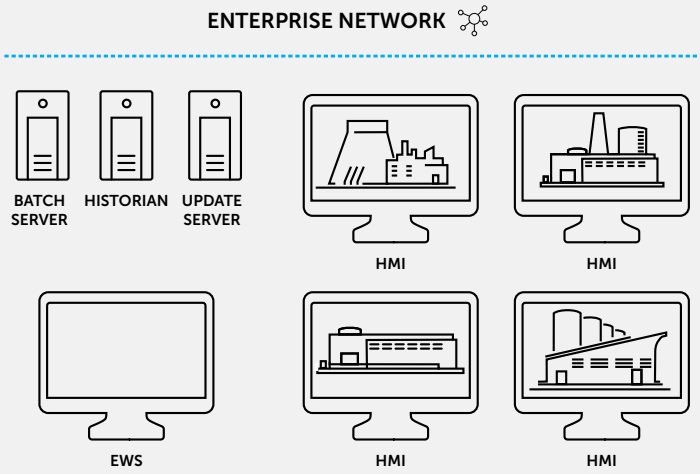



Diagram 2 – central + sites

# Network Architecture

## Process Logic VS Network Logic

The 9 production units operate independently from each other. The logical assumption would be that this separation would be reflected in the corresponding networking infrastructure. However following installation of Claroty platform, we discovered that the initial networking of the plant wasn't carried out with such reflection in mind. The various sites are not logically separated from each other and feature various connections between sites.

The reason is simple – as in many chemical plants of its kind, there is no in-house networking team. The initial building of the network was carried out by the turnkey contactor that was commissioned for this project when the plant's network was shifted to Ethernet. This contractor chose the most cost-effective networking implementation that would keep all assets connected.  Following maintenance activities throughout the years were conducted by external contractors as well. This resulted in a significant mismatch between the network topology and the production logic. While this gap does not bear any implication on the plant's productivity, it introduces multiple redundant unmonitored connections and cross-site connections which threat actors can leverage for sustained presence and lateral movement, greatly decreasing its cybersecurity resilience.

## Remote Connections

Both the central control room and the sites networks feature occasional internet connections to various third parties - automation vendors, network technicians and software providers. These connections are not monitored in the central control room, and do not abide to a central access policy.

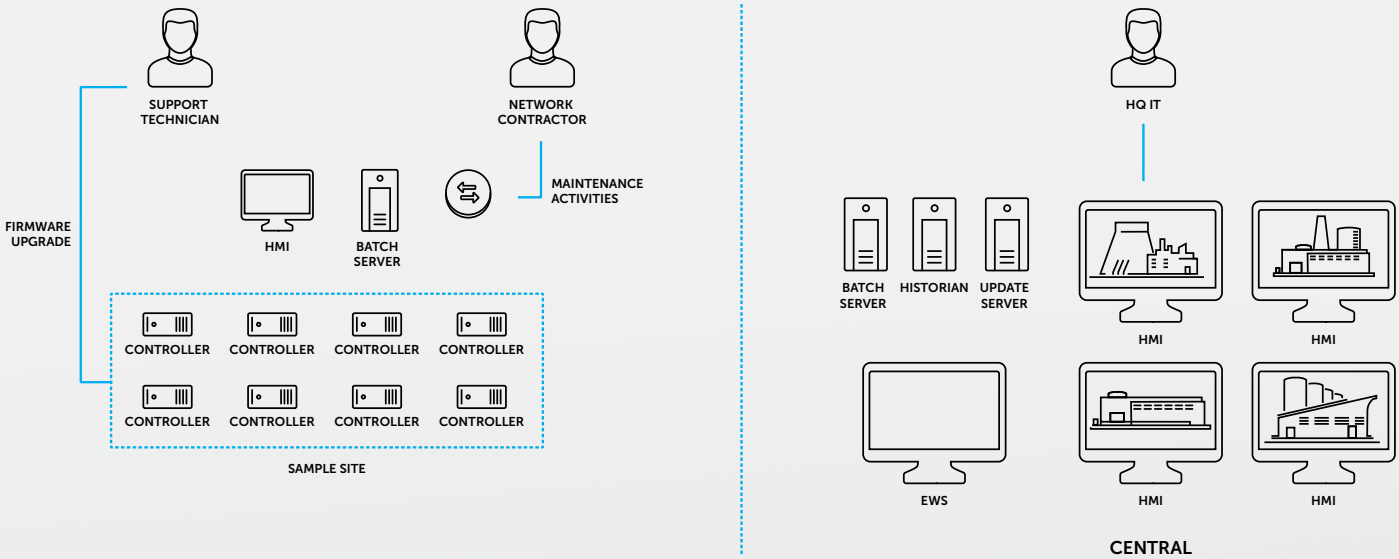



Diagram 3 – external remote connections

## State of Network Visibility

The plant's control team knows which controllers govern each process due to the local and central HMIs that fully capture all process data in real time. However, there is no equivalent visibility into the underlying networking infrastructure and to the network's actual exposure to the internet.

# Cyber Threat

The plant's security team expressed the following concerns:

### Non-targeted attack:

- **Description:** Non-OT malware shutting down or slowing performance of OT Windows machines (HMI, batch server, Historian, etc.)
- **Vector:** Internal\third party using an infected computer to perform maintenance activities.
- **Impact:**
  - **Dysfunctional HMI:** Loss of view would probably lead to initiated shutdown until HMI becomes functional again, through either malware removal or machine reimaging.
  - **Dysfunctional batch server:** Compromise of data and system integrity. Various regulations require detailed documentation of all process stages. Failing to comply with these requirements could result in disqualifying the entire batch. Here also production would be halted until the batch server is restored to operational routine. Compromise of data and system integrity.

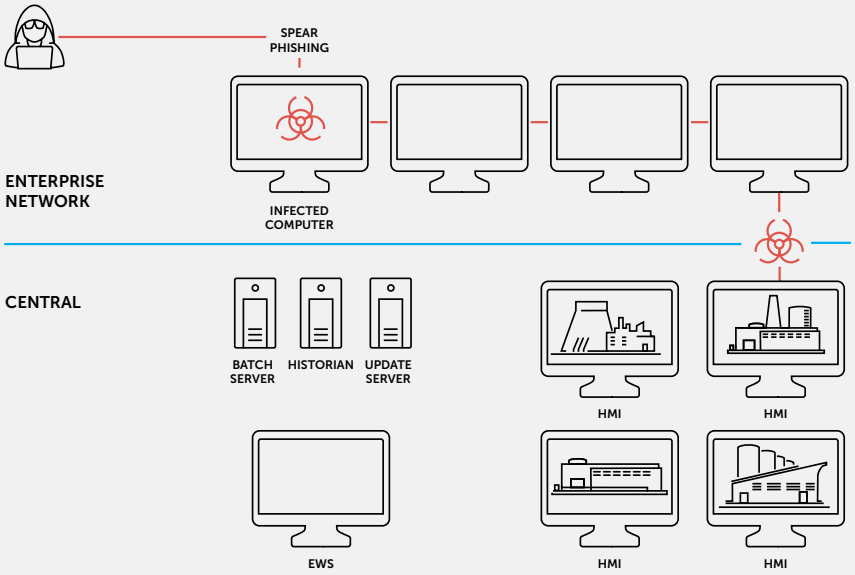



Diagram 4a – non-targeted attack

  - **Degraded performance of HMI\batch server:** A malware which consumes the HMI\batch server CPU would cause slower response and result with degradation of batch quality. Discovery of this issue would depend on the plant's quality assurance process. Failing in discovery would result in shipping lesser quality products, damaging the brand, and exposing the company to liability claims. Unlike the previous dysfunction scenarios, a more rigorous investigation would be required to isolate the problem's root cause and pinpoint the infected endpoint, eliminate the malware, and close the security gap that enabled the initial infection.

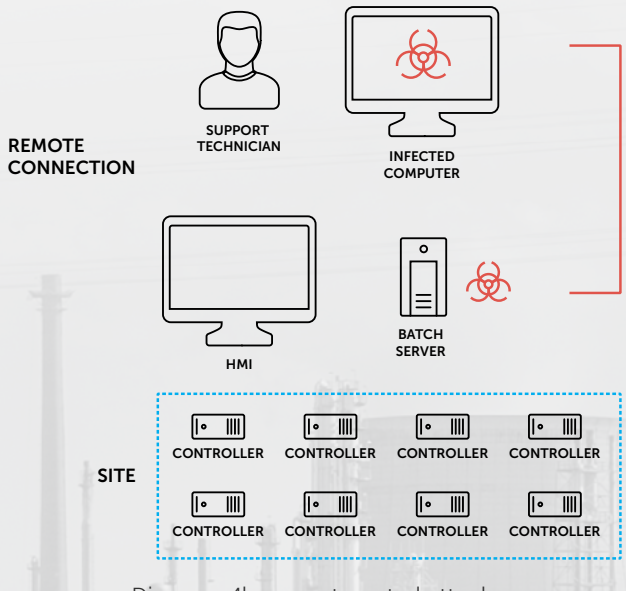



Diagram 4b – non-targeted attack

Targeted attack:

- **Description:** Purpose-built attack on the plant's OT network, leveraging its built-in security weaknesses. Threat actors would aim at causing high-profile physical damage to equipment, environment or, in extreme cases, even human lives.
- **Vector:**
  - **Physical:** The site's large size, enables attackers (insider or external) to approach the controllers in stealth and perform a logic change through a USB drive.
  - **Network:** The OT network architecture introduces various attack surfaces for both initial compromise and prolonged stay. As explained before, the standard routine in the plant is that configuration downloads are carried through the EWS in central control room, while minor parameter adjustments are owned by each site's control team which use Online Edits from a single Windows machine that contains both HMI and EWS software. An attacker that successfully compromises one of these local site machines could easily leverage its EWS software to download a rogue configuration code, changing the process values.
- **Impact:**
  - **Release of toxic materials in the plant:** Endangering of human lives. Site shutdown until all the plant is cleaned.

**Release of toxic materials to the environment**: Considerable environmental damage. Heavy costs of cleaning and restoration activities, as well as exposure to legal claims. Presumably, this is much less likely.

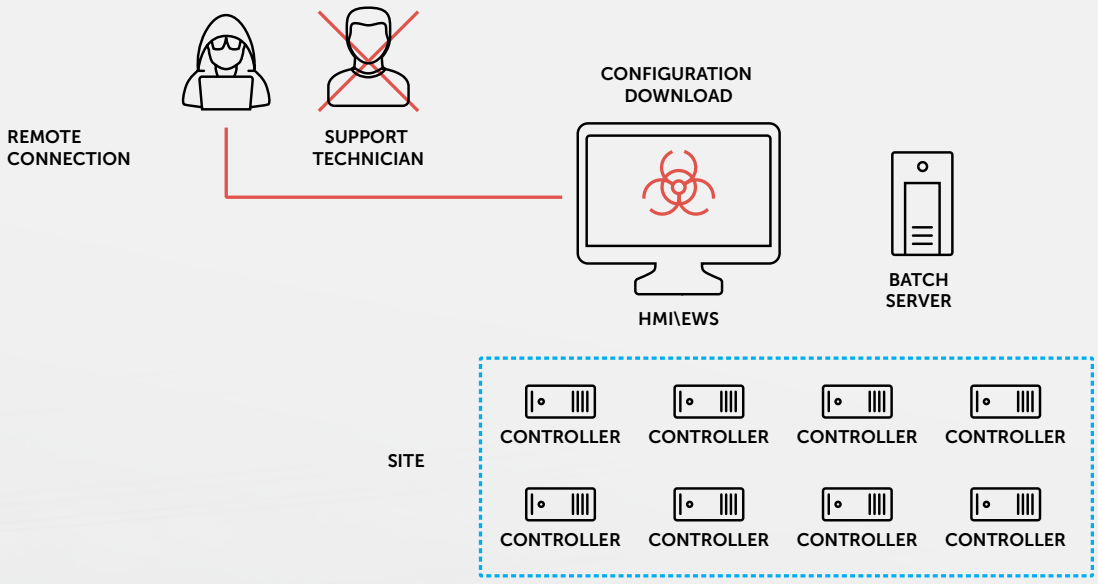



Diagram 5 – targeted attack

# Claroty Platform

## Deployment Plan

**Claroty** provides a fully integrated cybersecurity platform purpose-built for OT:

- **Continuous Threat Detection:** passive monitoring\DPI product for real-time detection of malicious presence\activity
- **Secure Remote Access:** access policy enforcement and control product to safeguard networks from the threats introduced by unmonitored third-party and employee network access
- **Enterprise Management Console:** centralized management interface that aggregates the data from Claroty products from multiple sites, and displays a unified view of their assets, activities, alerts, and access control

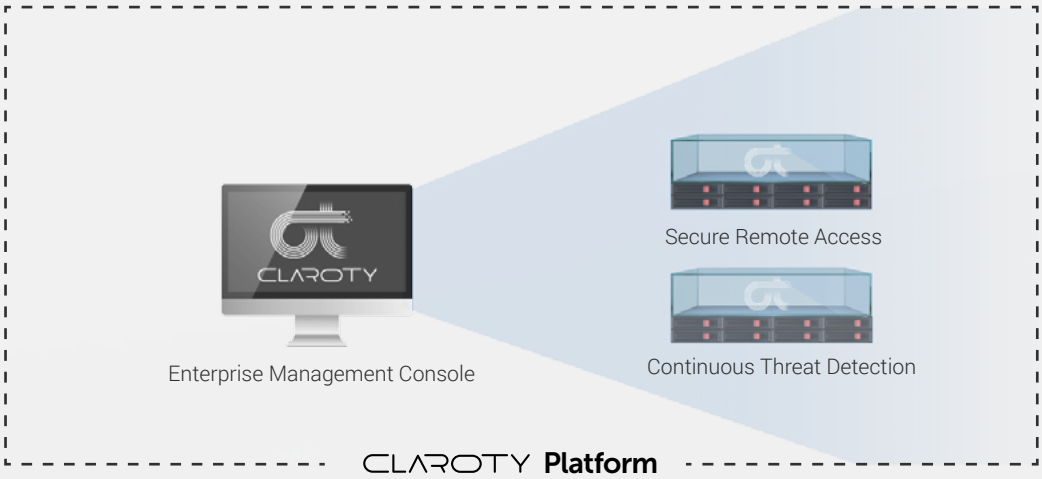



Diagram 6 - platform

The next section walks through the deployment process of each product.

## Continuous Threat Detection

Continuous Threat Detection gathers and analyzes network data – basically listening to all the communications to discover control and other assets (e.g., controller, HMI, remote I\O, engineering stations, and networking gear) and to build a detailed "baseline" model of normal network operations. Different assets generate network traffic in varying time intervals, depending on the specific function of the asset and the environment. The common timeframe required for the entire set of OT assets to generate their routine traffic is approximately 2-3 weeks.

Initially, Continuous Threat Detection is configured to run in training mode, to learn the network's standard behavior and establish a behavioral baseline. During this learning period, the Claroty team reviews the aggregated findings with the customer – sharing immediate insights about the OT ecosystem. These insights range from pure security findings, such as insecure remote connections, inadequate segmentation, or weak passwords, to various server misconfigurations that affectoperational workflow.

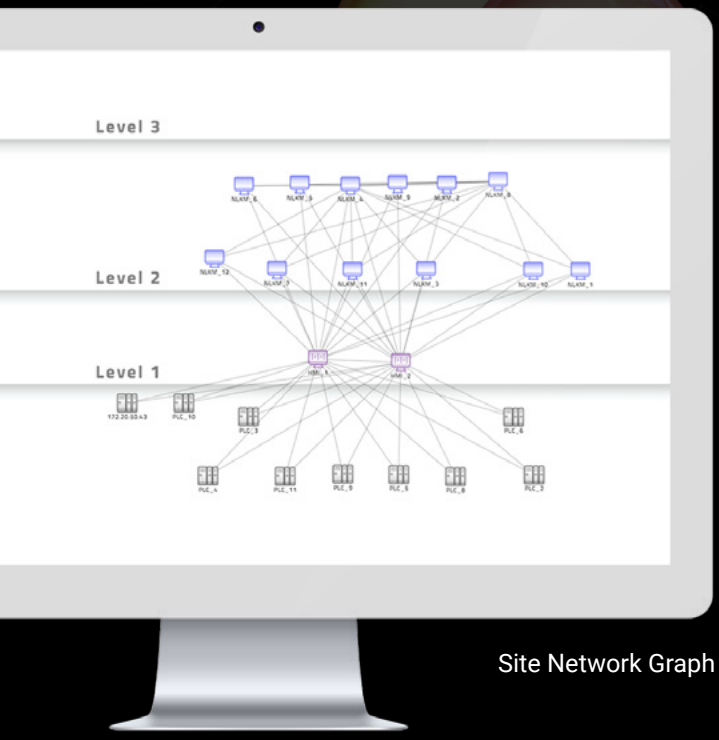
During the learning period, it is important to be aware of the possibility that the environment might be already compromised. The Claroty deployment team ensures that any malicious presence is detected, remediated, and prevented from being absorbed in the baseline.

Once training mode is complete, Continuous Threat Detection shifts to operational mode, where the system provides real-time monitoring and raises an alert upon detection of deviations from the baseline. For example, Continuous Threat Detection can generate an alert when a new device is plugged into the network (e.g., a contractor laptop), when critical changes are made (e.g., a PLC configuration download or PLC mode change), and when malicious activity is detected on the network (e.g., port scan, man-in-the-middle, unknown/anomalous traffic).

The entire OT network is now visible and monitored through a single console, enabling the customer to track changes and to rapidly detect, investigate, and respond to security incidents and potential operational issues.

**Let us now zoom in on one of the production sites and follow the deployment process, as well as related findings and insights.**

# Continuous Threat Detection - Sample Site Findings




Site Network Graph

## Sample Site Network

The network graph shows the typical network layout of a production site in the facilities, and the connections between assets in various levels (the remote I\Os are omitted here).

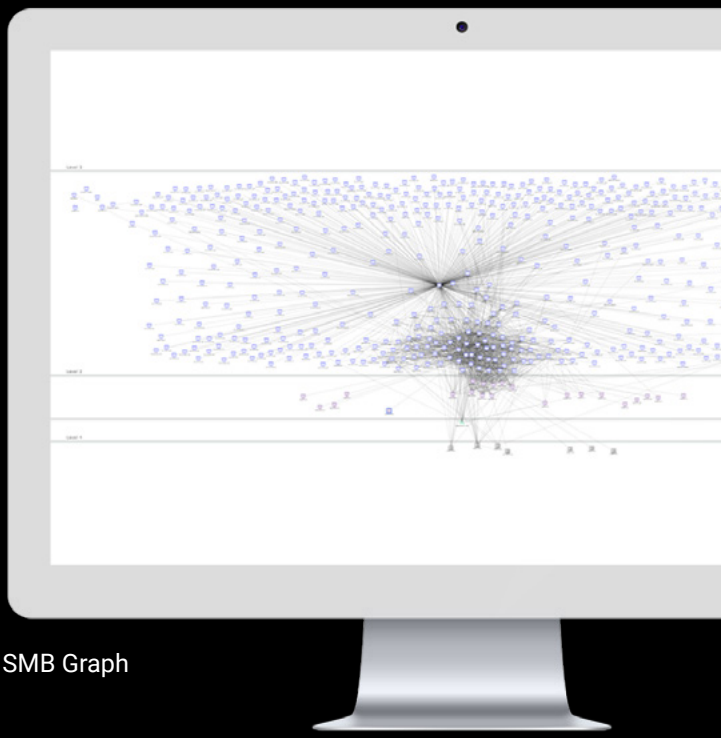

Nested Asset

## Nested Asset Communicating With DMZ

Nested assets present a security challenge that only can be addressed by knowledge of both OT and cybersecurity domains. In this case, the nested controller (Level 1 bottom) uses a network card to communicate with the HMI\EWS via the nesting controller (level 1 up). However, it apparently has an additional network card through which it communicates independently with a Windows machine in the DMZ – most probably for remote vendor maintenance activities. This is a security gap because compromise of the DMZ machine can open for the attacker a path to this controller and through it to the entire site's network.

## Open SMB Ports

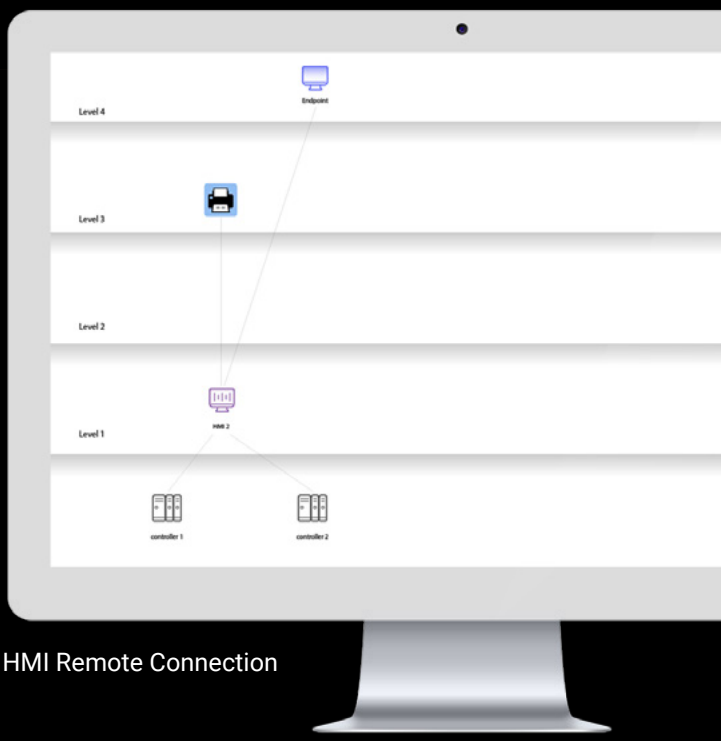
SMB is a common vector for self-propagating malware (the classic example is Conficker, but two prominent attacks in 2017 – WannaCry and NPetya – have utilized it as well). As the screenshot here shows, SMB traffic is present in nearly all nodes in the network (note that this is a screenshot of the entire facility's OT network, not only the sample site). The immediate action item is to limit SMB traffic to only the nodes that essentially need it, and monitor closely their respective traffic.



SMB Graph

## Non-Monitored Remote Connections

Immediately following the generation of the network graph (within minutes from the beginning of training mode), outbound connections of control level nodes appeared. There was no monitoring or auditing of the traffic that took place through these connections, nor would the site operators have any way of knowing if any of these connections were leveraged by threat actors to enter the network.




HMI Remote Connection

# Secure Remote Access

Claroty Secure Remote Access is software designed to minimize the risk remote users, including employees and contractors, introduce to industrial networks. The system provides a single, manageable interface through which all remote users connect and authenticate, prior to performing software upgrades, periodic maintenance, and other system support activities.

Network administrators employ the system to control which users are granted access to industrial control assets and for what purpose. The system enforces password management and access control policies, governs remote connections, and monitors and records remote access sessions:

**Proactively** – through granular user and asset policies governing which assets authorized users can see and access, when they can log into each asset, and the authentication-level required for access.
**In real time** – by using manual access permissions and "over-the-shoulder" real-time video visibility into all the user's activity – including a "red button" ability to terminate an ongoing session.
**Retroactively** – by generating activity reports filtered by user, asset or session, and providing video recordings of all remote sessions.

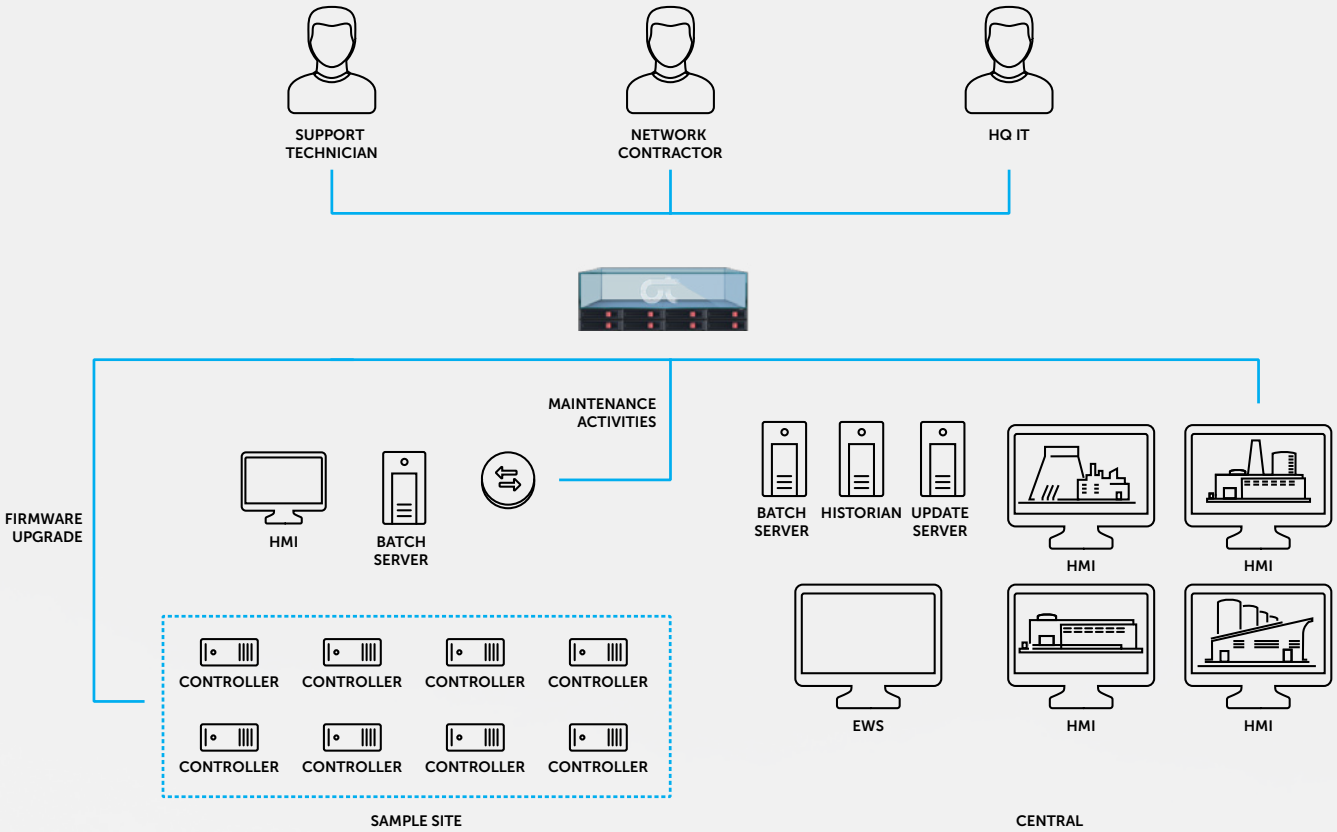
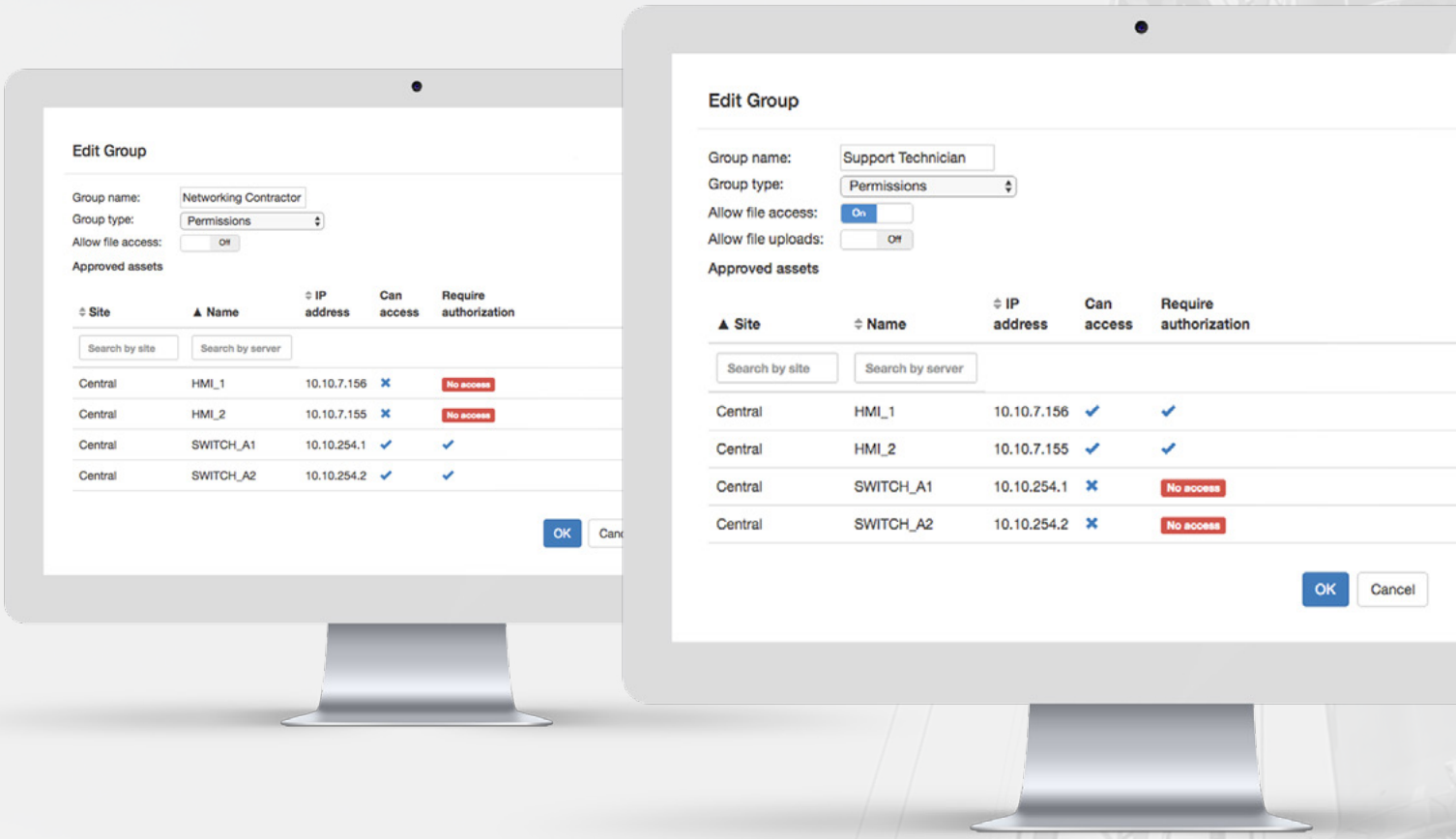


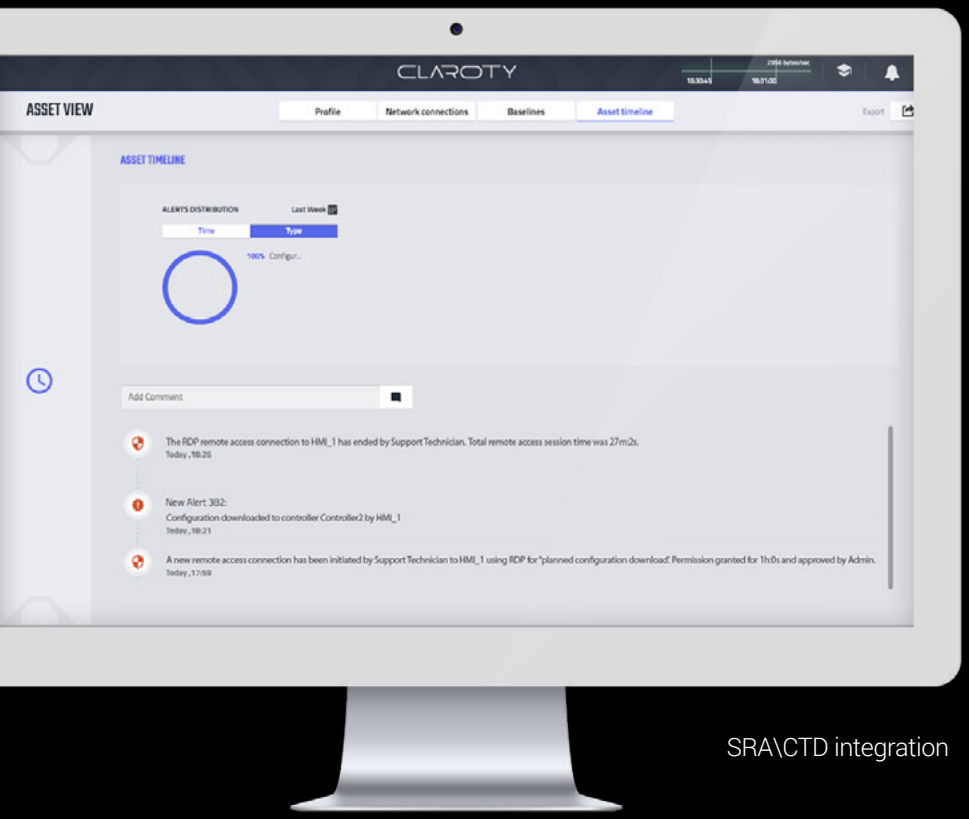

Diagram 6 - external connections after installation of Secure Remote Access

The natural deployment choice in this plant was in the central control room. The plant team has used Continuous Threat Detection connection discovery to build a list of all existing remote connections. All parties involved were notified that the existing connections were terminated – the termination was implemented with new firewall rules – and that, from now on, establishing a connection would require logging in to the Secure Remote Access console. The following screenshots show sample access policies for various remote user groups.

Networking Contractor
remote user group policy

Support Technician
remote user group policy

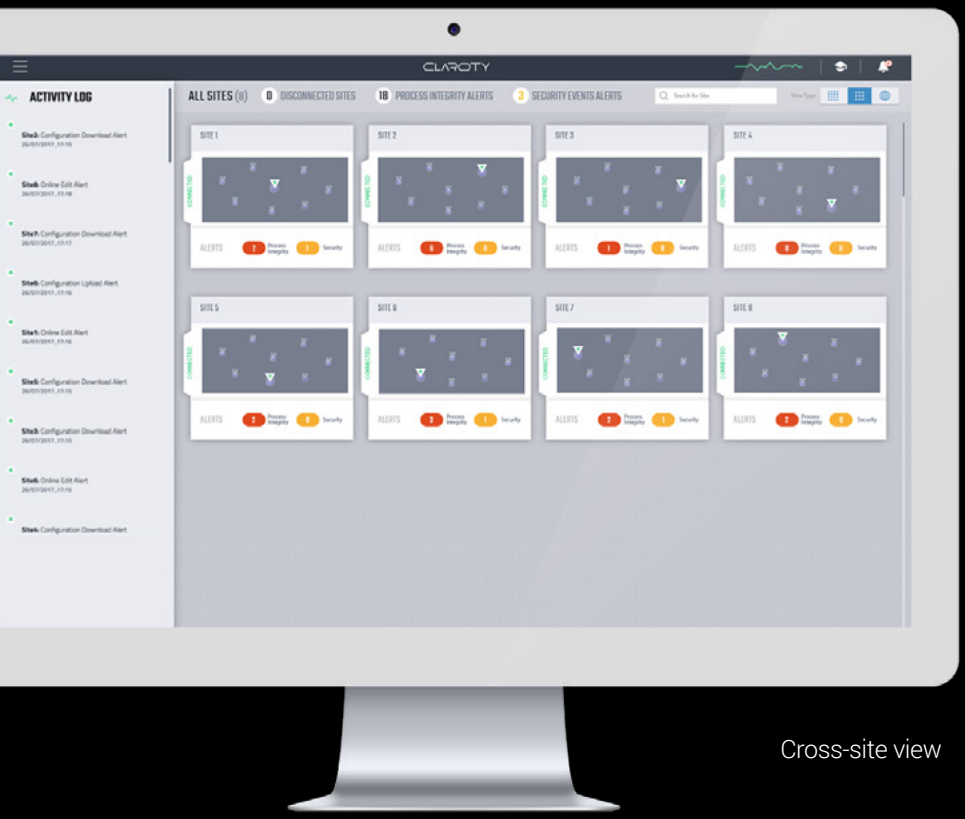





SRA\CTD integration

## SRA\CTD Integration

CTD Activity Timeline shows whenever an asset's remote session through SRA begins and ends, as well as its activity during the session. This serves as an additional in-depth security layer that enables operators to validate that the remote user's stated purpose indeed aligns with the actual activity, mitigating the threat of an attacker who has compromised a remote user's machine to access the network (see diagram 6: targeted attack)




Cross-site view

## Enterprise Management Console

Claroty Enterprise Management Console is a centralized management interface that aggregates the data from Claroty products from multiple sites, and displays a unified view of their assets, activities, alerts, and access control.

# Conclusion – The Claroty Difference

Claroty Platform has addressed the two critical cybersecurity challenges our chemical customer faced – monitoring the network's internal traffic to detect malicious presence and actions, and controlling the multitude remote access connections the plant's network encloses.

It is only through visibility and control of all assets and traffic that a true shift in security posture can occur. Claroty rises up to this challenge with a fully integrated platform that provides security insights to enhance the network's security hygiene, advanced filters for proactive threat hunting within the network, real-time anomaly detection that pinpoints any critical changes in network traffic, and a centralized control and monitoring interface for remote connections.