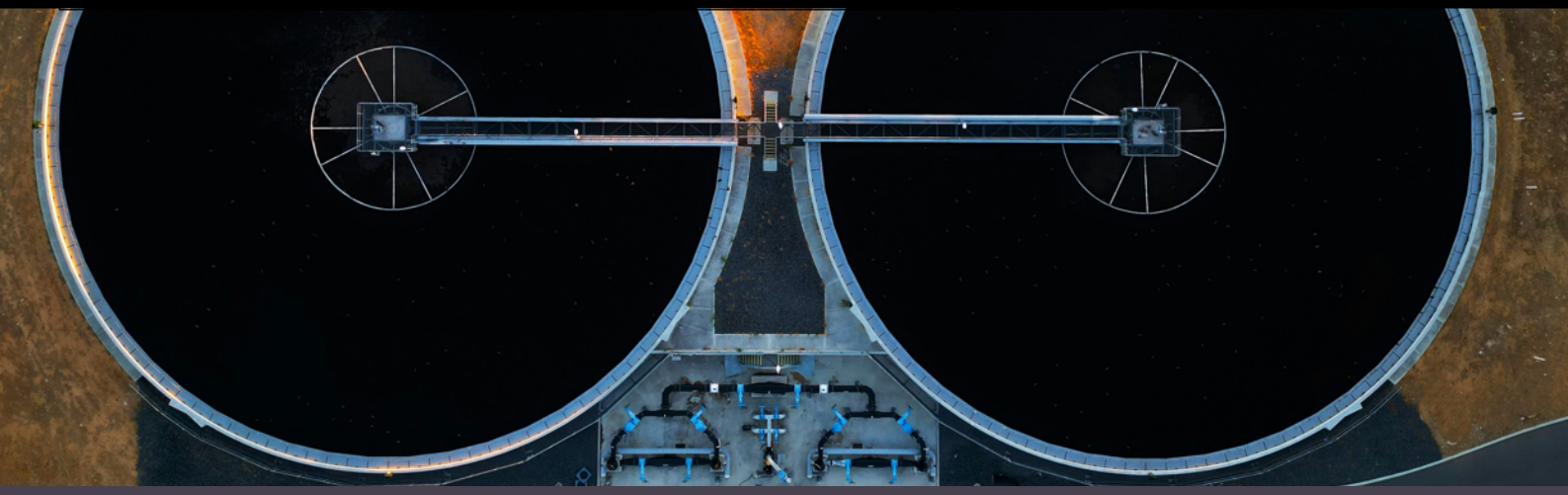
goldilock

# USE CASE 03



# Goldilock FireBreak for Water Utilities

A new line of defense for the unique and diverse, critical OT and IT areas of the water utility sector. The Goldilock FireBreak™ protects assets from the physical layer up

Goldilock FireBreak provides the ultimate physical failsafe against these threats, utilizing patented Layer 1 isolation to render critical assets, like SCADA command nodes and chemical dosing systems, completely invisible and unreachable to remote adversaries. Unlike software-only defenses that can be bypassed by zero-day exploits, FireBreak's hardware-enforced air gap definitively halts lateral movement. FireBreak actions the insight of software by integrating with the existing security stack via its RESTful API, enabling a high-confidence digital alert to trigger immediate, hardware-enforced physical isolation in milliseconds.

## Why water operators choose FireBreak

**Absolute invisibility = zero attack surface** Physically disconnecting critical systems renders them invisible and utterly unreachable to sophisticated adversaries. This definitively stops sabotage and ransomware by removing the digital target entirely.

**Future-proof security for legacy infrastructure** FireBreak integrates seamlessly with SCADA, ICS, and DCS equipment, acting as a definitive compensating control for un-patchable legacy systems without requiring costly or disruptive modernization.

**Rapid, non-disruptive deployment** Flexible API integration allows for immediate implementation without operational downtime, giving demonstrable cyber resilience and rapid incident containment.

**True Zero Trust segmentation and access** By enabling just-in-time physical access, FireBreak enforces the core tenets of Zero Trust. It eliminates IT/OT convergence risks and halts lateral movement from administrative networks to kinetic control environments.

## Key features and strategic benefits for the water sector

- **Fast-to-Deploy : Physically isolated OT segments**
  **Benefit:** Isolate critical OT systems (e.g., SCADA, PLCs, chemical dosing control) from all networks during idle periods, eliminating remote attack vectors.
  **Example:** A chemical feed control server responsible for water disinfection only establishes a physical network connection for scheduled software updates or when an authorized technician requires direct, time-bound access for maintenance. Outside these specific windows, the physical network link is entirely severed.
- **Air-gapped backups for rapid recovery**
  **Benefit:** Store system configuration files, operational data, and backup images on a physically unreachable device, safe from ransomware and deliberate remote corruption, minimizing downtime and preventing data loss.
  **Example:** In the event of a cyber incident such as a ransomware attack that compromises primary SCADA servers, operators can quickly restore the system to its pre-attack state using a known-clean backup residing on a FireBreak-protected storage element.
- **Role-based physical access control**
  **Benefit:** Access to designated OT systems is strictly controlled at the physical network connection level, granted only to authorized personnel during pre-approved and limited time windows. Hardware-level verification, such as physical keys or security tokens, can be required before a physical connection is established, and all connection and disconnection events are logged immutably.
  **Example:** A third-party maintenance contractor servicing a pump control node at a remote site is granted physical network access via FireBreak for a predefined maintenance window, with a detailed, immutable access log.
- **Segment IT from OT with impenetrable barriers**
  **Benefit:** FireBreak creates hardware-enforced physical segmentation between the more vulnerable IT environment and the critical OT domain, preventing lateral movement into systems controlling physical water processes.
  **Example:** Even if a phishing attack compromises an IT server, FireBreak prevents attackers from using that foothold to manipulate pump stations or chemical treatment systems.
- **Prevent insider and supply-chain breaches**
  **Benefit:** Eliminate persistent access risks through pre-scheduled, single-use connection windows.
  **Example:** When a SCADA vendor performs a firmware update, access is granted only for a defined duration and automatically severed once complete.
- **Regulatory compliance and incident-response readiness**
  **Benefit:** Meet NIS2, ISO 27001, and national CNI requirements for resilience, segmentation, and access control, with immutable logs supporting audit readiness.
  **Example:** During regulatory audits, water companies can present immutable FireBreak logs showing precise connection times, authorized personnel, and termination events.