



USE CASE 13



Goldilock FireBreak in Healthcare

The convergence of physical and digital infrastructure within modern healthcare facilities has created a new, critical frontier for cybersecurity. The security of clinical data, Operational Technologies (OT), and patient safety are now a leadership-level responsibility.

Goldilock's FireBreak™ offers a revolutionary, hardware-enforced cyber defense that surpasses traditional software barriers. Irrespective of software-based attacks or breach risks, by controlling network connectivity at the physical layer (Layer 1), FireBreak™ provides a specific and auditable way to physically isolate critical medical infrastructure and Electronic Health Records (EHRs). This allows healthcare institutions to regain ultimate control, surgically severing attack paths and creating a verifiable "air gap" on demand. It is an essential control for achieving true operational resilience in an era where the line between a logical breach and a physical medical crisis has disappeared.

Goldilock FireBreak™ delivers a profound return on investment by pivoting from ever-growing expenditure on reactive defense systems to a more strategic cost avoidance. In the healthcare sector, where the price of operational paralysis is measured in the hundreds of thousands per hour, and where a healthcare data leak can cost tens of millions, FireBreak serves as the definitive digital insurance policy.

By institutionalizing an engineered air gap around uncorrupted clinical backups and identity infrastructure, hospitals can bypass the exhaustive, ground-up network rebuilds that typically follow a ransomware event, instead facilitating a deterministic restoration process that limits downtime to hours rather than weeks.

Ultimately, this hardware-enforced certainty provides a quantifiable ROI by securing legacy medical devices and shielding the institution from the catastrophic financial, legal, and reputational fallout of a total clinical collapse. In a nutshell, it allows you to be certain what systems are accessible or protected and be confident any active threat level can be responded to.

The FireBreak™ Solution: Practical Use Cases for Demonstrable Resilience

Goldilock FireBreak™ provides tangible, hardware-enforced solutions to these challenges. By focusing on the physical control of connectivity, it enables practical security strategies that action the insight of your current cybersecurity software solutions.

Use Case 1: Surgical Containment of IT/OT Threats

Benefit: Isolate life-critical medical devices and Electronic Health Record (EHR) systems from a corporate IT network compromise, resolving the "Control Dilemma" by preventing a catastrophic clinical outage without requiring a full hospital shutdown.

- **Practical Deployment:** A FireBreak™ device is installed in-line at the network boundary between the hospital's administrative IT network and the segregated clinical segments managing MRI scanners, blood testers, and EHR databases. The device is integrated with the facility's Security Orchestration, Automation, and Response (SOAR) platform via its secure RESTful API.
- **Process:** Upon detection of a high-confidence ransomware incident on the IT network, such as a fast-moving Black Basta or ALPHV variant introduced via a phishing attack on an admin workstation, a pre-defined incident response playbook is automatically triggered. The SOAR platform sends an authenticated command to the FireBreak™ device, which instantly and physically severs the Layer 1 connection between the IT and clinical segments in milliseconds. The life-critical medical infrastructure continues to operate safely in an isolated "Island Mode," maintaining uninterrupted access to patient records and diagnostic equipment. This gives the SOC team the time and physical certainty needed to remediate the IT network, knowing the clinical environment is invisible and unreachable to the threat.
- **Regulatory Alignment:** This capability provides a powerful and decisive containment measure, directly supporting the HIPAA Security Rule by ensuring the confidentiality, integrity, and availability of patient data through physical air-gapping. It serves as a tangible implementation of the NIST Cybersecurity Framework 2.0, specifically fortifying the Protect and Respond functions by providing a hardware-enforced failsafe that prevents lateral movement and halts the propagation of sophisticated cyber-physical threats.

Use Case 2: Strategic Protection of Legacy Medical Infrastructure

Benefit: Radically reduce the attack surface of un-patchable, mission-critical equipment, such as diagnostic imaging controllers (MRI/CAT scans) and laboratory information systems, allowing for their continued, secure operation. By implementing physical isolation, healthcare organizations can securely "sweat" high-value legacy assets that run on outdated operating systems, extending their lifecycles without accepting a state of continuous, unmitigated risk.

- **Practical Deployment:** A vulnerable but essential medical device is moved to a dedicated, isolated network segment. A Goldilock FireBreak™ appliance is installed as the sole physical gateway for this segment, acting as a hardware-enforced "digital circuit breaker" between the legacy asset and the broader clinical network.
- **Process:** The system adopts a "disconnected-by-default" posture, meaning the default state for the segment is physically severed at the hardware layer. This "Island Mode" renders the un-patchable device completely invisible and unreachable to remote threats and prevents it from being used as a pivot point for lateral movement. On a strictly scheduled basis, controlled via a secure, out-of-band management channel, FireBreak™ can be triggered to establish a brief,

time-bound physical connection to a secure monitoring station for essential data polling or telemetry. The connection is automatically and physically severed the moment the authorized window closes.

- **Regulatory Alignment:** This strategy serves as a definitive compensating control when traditional software patching is technically or operationally impossible. By physically removing the attack path, the facility demonstrates a mature, risk-based approach to security that directly aligns with the HIPAA Security Rule regarding access control and workstation security. Furthermore, it fortifies the Protect and Respond functions of the NIST Cybersecurity Framework 2.0, providing auditors with immutable, physical evidence of proactive risk mitigation that surpasses the limitations of software-defined logical segmentation.



Disconnect to protect, on demand.

sales@goldilock.com | goldilock.com

