goldilock

Protecting your networks

Today's hyper-connected networks are vulnerable to attack from the outside-in and the inside-out. Whether by software vulnerability exploits or microscopic gaps buried in the complexity of advanced, modern configurations.

Disconnect to protect, on demand

FireBreak™

Military grade global enterprise scale
Physical connection controller
Absolute network access control to your defenses and assets

The Treats | **FireBreak** | **Your Defense** | **Your Assets**

Across defense, critical national infrastructure, public organizations and many enterprise sectors, there is a constant battle to address complex and fast scaling cyber threats. They are all characterized by software-on-software attacks, which means taking control of connections at the physical level, controlling the wire and fiber puts you back in control. Firebreaks create a hard-stop protection for your network segments and gives you absolute connection control, on demand.

sales@goldilock.com | **goldilock.com**

goldilock

Mission Context
In modern defense cyber operations, milliseconds matter. Zero Trust mandates and AI-driven threats require a decisive, automated response—not just alerts. Goldilock FireBreak™ bridges the gap between cyber detection and physical disconnection, giving the Department of the Air Force the ability to remove critical systems from the threat surface instantly via secure API integration.

A Smarter, Faster Defense
FireBreak™ connects directly into existing defense cybersecurity ecosystems through a secure RESTful API, enabling automated disconnection triggered by your SIEM, SOAR, or Zero Trust orchestration platforms. If a threat is detected, the API can execute a physical disconnect at Layer-1 within milliseconds—no human intervention required. This automation aligns with Zero Trust principles by ensuring connections exist only when validated, and it meets RMF requirements for contingency and incident response.

Invisible and Immune
Unlike traditional network security tools, FireBreak™ is invisible to adversaries because it has no IP or MAC address. It uses electromechanical relays to isolate at the physical layer, making it immune to malware or network-based attacks that could bypass software defenses.

Ready for Defense Operations
FireBreak™ supports high-speed fiber and copper connections, offers dual power and redundant API paths for resilience, and deploys without requiring changes to existing infrastructure. Whether used to air-gap mission networks on demand, contain ransomware outbreaks, protect SCADA/ICS infrastructure, or simulate cyberattack scenarios during training, it provides decisive action when it matters most.

Strategic Value for DAFITC
By making physical isolation an automated, API-controlled capability, FireBreak™ turns what was once a manual, last-resort measure into a precise, proactive tool for mission assurance. Threat detection is fast—FireBreak™ makes the response faster.

Mission Context
In modern defense cyber operations, milliseconds matter. Zero Trust mandates and AI-driven threats require a decisive, automated response—not just alerts. Goldilock FireBreak™ bridges the gap between cyber detection and physical disconnection, giving the Department of the Air Force the power to remove critical systems from the threat surface instantly via secure API integration

A Smarter, Faster Defense
FireBreak™ connects directly into existing defense cybersecurity ecosystems through a secure RESTful API, enabling automated disconnection triggered by SIEM, SOAR, or Zero Trust orchestration platforms. When a threat is detected, the API can executea physical disconnect at Layer-1 within milliseconds. This capability aligns with Zero Trust principles by ensuring connections exist onlywhen validated, while also meeting RMF requirements for contingency and incident response. Because the system operates at the physical layer, it remains immune to software-level compromise.

Technical Models and Capabilities
The FireBreak™ range offers several models tailored to different operational requirements. The FireBreak 4 provides four ports for smaller, mission-specific enclaves or high-security equipment racks, ideal for tactical deployments. The FireBreak 8 doubles capacity, supporting mid-scale operations or multiple critical systems in parallel. The flagship FireBreak 12 is built for large-scale defense environments, with twelve ports capable of isolating multiple mission networks simultaneously. All models support both copper and fiber interfaces, offer switching speeds measured in milliseconds, and use hardened electromechanical relays for true physical disconnection.
In terms of integration, every model supports dual redundant power supplies and dual API control paths, ensuring operationalresilience even in contested or degraded network environments. The devices have no IP or MAC address, rendering them invisible to adversaries, and all API traffic is encrypted and authenticated for secure orchestration.

Invisible and Immune
Unlike traditional network security tools, FireBreak™ is completely undetectable on the network. Its isolation mechanism operates outside the data plane, meaning no malware, rootkit, or remote exploit can override the disconnection process. This invisibility andimmunity make it particularly suited for defending C2 systems, classified enclaves, and operational technology such as SCADA and ICS networks.

Ready for Defense Operations
FireBreak™ can be deployed without reconfiguring existing infrastructure and is compatible with both garrison and forward-operating environments. It can air-gap mission networks on demand, contain ransomware outbreaks before they propagate, protect critical infrastructure, and even simulate cyberattack conditions for red-team training. The ability to switch from connected to completely isolated in milliseconds gives commanders and cyber operators a decisive advantage in contested information environments.

Strategic Value for DAFITC
By transforming physical isolation into an automated, API-controlled process, FireBreak™ turns what was once a manual, last-resort action into a precise, proactive cyber defense tool. It integrates seamlessly into the same automated incident response workflows already in use, ensuring that threat detection is immediately followed by decisive action.

Disconnect to protect, on demand.

sales@goldilock.com | **goldilock.com**