goldilock

USE CASE 05

Data center sector

Protecting national data centers by enhancing protection, segmentation and continuity against cyber threats and CNI.

In today's hyper-connected world, data centers form the bedrock of our digital existence, underpinning everything from ubiquitous cloud services and intricate enterprise IT ecosystems to critical government operations and sensitive financial transactions.

The threat landscape facing these vital infrastructures is becoming increasingly sophisticated and remains relentless. Organisations grapple with escalating risks, including highly evasive ransomware attacks, constant danger of social engineering, insider threats, and the lateral movement of malicious actors within complex virtualised or multi-tenant environments.

Traditional, software-centric security measures, while essential, often prove insufficient against these advanced persistent threats, leaving critical assets vulnerable when software controls are confounded, compromised, configured inadequately, or suffer delays in response.

Recognising the critical importance of this infrastructure, the US Department of Energy (DoE) and National Telecommunications and Information Administration (NTIA) are focussing on critical risks, the EU under NIS2 Directive have defined new criticality and UK Government in September 2024 designating data centres, including cloud operators utilising them, under Critical National Infrastructure (CNI). Many other countries are following suit. These initiatives underscore the indispensable role these facilities play in a modern economy and society, alongside essential services like energy, water, and transportation. This CNI status brings increased scrutiny, advancing regulation, and a heightened focus on implementing robust security measures to protect against the entire range of threats.

Adding to the complexity, the rise of Artificial Intelligence (AI) is driving a surge in demand for specialized data centres, emphasizing the need for highly robust security solutions and the absolute protection of the newest and fastest emerging compute utility.

The global data center market is projected to reach $1 trillion by 2027, fuelled by the AI expansion. This growth is accompanied by a significant increase in power consumption, with AI data centres potentially requiring 68 gigawatts of power globally by 2027, an amount equivalent to the total power capacity of a large state.

Goldilock's innovative FireBreak solution introduces a fundamental shift in data center security: the capability for physical isolation of mission-critical systems and their data in an instant, via secure remote control.

This hardware-enforced separation provides an ultimate, last line of defence, acting as a controlled physical air gap when software-based controls have been bypassed or are rendered ineffective during a cyber incident. FireBreak offers an incremental layer of cyber resilience that goes beyond logical segmentation, ensuring the absolute inaccessibility of targeted assets to malicious actors at the most fundamental level, a capability that is now essential in the context of data centres being designated as critical national assets.

Goldilock's FireBreak Physical Connection Controller delivers a revolutionary, hardware-enforced cyber defense purpose-built for the modern data center, where the stakes have never been higher. As hyperscale and AI-powered data centers become the digital backbone of the global economy, they face relentless cyber threats, unprecedented power demands, and strict regulatory scrutiny. FireBreak goes beyond traditional software barriers by physically isolating critical IT systems, server clusters, and backup infrastructure from all network connectivity, eliminating remote attack vectors entirely.

By physically disconnecting these assets from all networks and segments when not in use, during maintenance, or at times of heightened risk, FireBreak renders them invisible and inaccessible to cyber threats. This creates a totally shielded security perimeter, crucial for environments where downtime, data loss, or compromise can have catastrophic ripple effects across industries and nations. FireBreak's network-invisible control channel enforces a hardware isolation barrier that software alone cannot match. The result? A disconnected environment becomes an unassailable legal data security domain, supporting tamper-proof evidence protection and full compliance with data sovereignty mandates – delivering unmatched assurance for today's digital-first enterprises.

Designed to meet the demands of Critical National Infrastructure (CNI) resilience frameworks, including NIS2 and sector-specific regulatory mandates, Goldilock FireBreak™ offers uncompromising cyber-physical protection that aligns with Zero Trust principles. Whether protecting AI model training clusters, high-density compute racks, core network switches, or sensitive customer data repositories, FireBreak empowers data center operators to maintain operational continuity, uphold client trust, and defend against the ever-escalating cyber threat landscape.

Why cybersecurity in the data center requires a radical shift

The rapid evolution of all types of data centers, including hyperscale, colocation, enterprise, AI, and edge facilities, has dramatically expanded the attack surface, often outpacing traditional security measures. With global business, digital services, and public trust relying on secure, resilient data center operations, protecting this infrastructure requires proactive, robust security that goes beyond reactive patching. As a core pillar of Critical National Infrastructure, data centers demand only the most advanced solutions. Goldilock delivers a breakthrough in security with hardware-enforced physical isolation for servers, storage, network switches, and backups. This ensures data center assets remain invisible, inaccessible, and protected from even the most sophisticated cyber threats.

As data centers scale to meet the demands of cloud, AI, and high-density computing, uncompromising, hardware-based security is essential. Goldilock FireBreak empowers operators across all data center types to maintain uptime, client trust, and resilience in today's digital-first world.

Critical threats facing the data center sector

- **Ransomware and remote access exploits:** Data centers of all types; hyperscale, enterprise, colocation, AI, and edge, are frequent targets for ransomware and remote access attacks. Threat actors exploit remote management tools, VPNs, and exposed services to alter configurations, exfiltrate data, or shut down critical systems, resulting in costly downtime and reputational damage.
- **State-sponsored espionage and sabotage:** Nation-state actors increasingly target data centers as part of cyber warfare and espionage campaigns, aiming to disrupt essential services, steal sensitive information, or undermine national security and economic stability.
- **Insider threats (intentional or accidental):** Employees, contractors, or third-party vendors with privileged access can unintentionally introduce malware or, in some cases, deliberately cause harm. Whether for financial gain, sabotage, or under duress.
- **Supply chain attacks:** Attackers compromise software, hardware, or service providers to infiltrate data center environments, bypassing perimeter defences and embedding malware or backdoors in critical infrastructure.
- **Cloud and multi-tenant vulnerabilities:** The rise of cloud-native and multi-tenant data centers introduces risks such as privilege escalation, insecure APIs, and cross-tenant attacks, potentially exposing sensitive workloads and customer data.
- **DDoS and service disruption:** Distributed denial-of-service attacks can overwhelm data center networks, disrupt hosted services, and degrade performance, impacting both providers and their customers.
- **Physical security breaches:** Unauthorised physical access, whether by tailgating, social engineering, or compromised access controls, can lead to theft, tampering, or destruction of hardware and data.
- **Legacy infrastructure vulnerabilities:** Many data centers still rely on legacy systems and unsupported hardware that lack modern security controls, making them attractive targets for exploitation.
- **AI and high-performance computing risks:** AI-focused data centers are particularly attractive to attackers seeking to steal proprietary models, training data, or disrupt critical AI workloads that support business and government operations.
- **Regulatory pressures and public scrutiny:** With regulations like NIS2, GDPR, and country-specific CNI mandates, data centers face increasing requirements for demonstrable cyber resilience, rapid incident response, and transparent reporting – under the watchful eye of regulators and the public.

Real-world FireBreak deployment scenarios across all data center types

Colocation and multi-tenant data centers

Challenge: Preventing cross-tenant threats and meeting CNI regulations.

FireBreak solution: Deploy FireBreak between tenant environments and core infrastructure. Integrate with management portals and SIEM systems for automated, real-time isolation of compromised tenants, stopping lateral movement.

Enterprise data centers

Challenge: Protecting critical systems (domain controllers, backup servers, hypervisors) during privileged operations or incidents.

FireBreak solution: Install FireBreak between key assets and the network. Use API-driven automation to disconnect during high-risk activities or on SIEM/SOAR alerts, containing threats instantly.

Cloud and hyperscale operators

Challenge: Securing backup environments and orchestration platforms from ransomware and advanced threats.

FireBreak solution: Place FireBreak between backup infrastructure and production networks. Automate connections only during backup windows, disconnecting immediately after to protect vital data.

AI and HPC data centers

Challenge: Safeguarding proprietary AI models, GPU clusters, and sensitive training data.

FireBreak Solution: Isolate AI compute clusters and storage from external networks, connecting only during authorized windows or research sessions.

Edge and micro data centers

Challenge: Securing distributed, often unmanned, edge sites processing sensitive or real-time data.

FireBreak solution: Deploy FireBreak at remote nodes, enabling remote or automated disconnection if anomalous activity is detected.

Financial services data centers

Challenge: Ensuring compliance, auditability, and transaction integrity.

FireBreak solution: Integrate FireBreak for physical segmentation and detailed access logging, supporting regulatory audits and zero-downtime requirements.

Healthcare data centers

Challenge: Protecting health records and clinical systems from ransomware and unauthorized access.

FireBreak solution: Use FireBreak to disconnect EHR and imaging systems during off-hours or as soon as a threat is detected.

Disaster Recovery (DR) sites

Challenge: Keeping DR infrastructure uncompromised until needed for failover.

FireBreak solution: Physically isolate DR assets, activating connections only during disaster declarations or scheduled tests for clean, reliable recovery.

Government and national security data centers

Challenge: Enforcing the highest assurance for classified and mission-critical systems.

FireBreak solution: Use FireBreak for role-based, auditable physical segmentation, ensuring only authorized, logged access to sensitive systems

Why data center operators choose Goldilock FireBreak

Absolute invisibility = Zero attack surface

When critical data center systems; servers, storage, network switches, AI clusters, and backup infrastructure are physically isolated by FireBreak, they become completely inaccessible, even to the most advanced cyber adversaries. No IP address, no digital presence, no opportunity for remote attack.

Future-proof security for any infrastructure

FireBreak seamlessly integrates with all types of data center environments, from legacy hardware to modern, cloud-native, and AI-driven systems. Whether your facility is hyperscale, colocation, enterprise, edge, or a high-security government or financial site, FireBreak delivers advanced protection without costly or disruptive upgrades.

Rapid, non-disruptive deployment

FireBreak can be installed quickly and flexibly, using secure SMS commands, physical key switches, or API integration, without interrupting ongoing operations. Its system-agnostic design means you can enhance security across any data center type, regardless of existing infrastructure.

True zero trust segmentation and access

FireBreak enforces Zero Trust principles by providing hardware-enforced segmentation and just-in-time, role-based physical access to critical assets. Only connect when necessary, and only for as long as needed. Minimising risk and exposure in every scenario, from routine maintenance to privileged AI model training.

Battle-tested in demanding data center environments

FireBreak is trusted in sectors where failure is not an option; defence, finance, healthcare, and critical national infrastructure. It's proven to deliver robust resilience against ransomware, insider threats, supply chain attacks, and state-sponsored adversaries.

Peace of mind in a dynamic threat landscape

Knowing your most valuable data center assets are physically isolated and unreachable when not in use provides unmatched peace of mind. FireBreak dramatically reduces the attack surface, helping you meet compliance requirements (NIS2, ISO 27001, PCI-DSS, SOC 2, HIPAA, and more) and assuring clients and regulators of your commitment to security.

Conclusion

Goldilock FireBreak offers a transformative and essential solution for data center operators facing the growing challenge of navigating today's complex cyber threat landscape. By providing hardware-enforced physical isolation for critical servers, storage, network infrastructure, and AI clusters, FireBreak delivers unparalleled protection against disruption, sabotage, and data manipulation.

This unique approach not only renders vital systems invisible and inaccessible to remote threats but also ensures that critical national infrastructure remains secure. Trusted by NATO and adopted across high-risk sectors, FireBreak's auditable, provable security offers the ultimate assurance, making it a critical asset for any data center committed to resilience and client trust in our increasingly digital and AI-driven world.