



## USE CASE 04



### Legal sector

Protecting client confidentiality, fortifying evidence integrity and defending against cyber threats in modern law firms. The Goldilock FireBreak™ locks down data and lock out threats.

#### **The legal landscape is a prime target for cyberattacks, with law firms managing a treasure trove of highly sensitive client documents and data, privileged communications, and legally sensitive evidence.**

The consequences of a breach are severe, and not just financial penalties, reputational damage, loss of client trust, and compromised legal proceedings. The Goldilock FireBreak Physical Connection Controller is a revolutionary hardware-enforced cybersecurity solution that removes Vital Data Assets (VDA) from the attack surface entirely. By physically disconnecting these assets from all networks and segments when not in use or at heightened risk, they are rendered invisible and inaccessible to cyber threats, creating an unreachable security perimeter.

FireBreak's network-invisible control channel creates a hardware-enforced isolation barrier that software alone can't match. The result? A disconnected environment is an unassailable legal data security domain, enhancing tamper-proof evidence protection, and full compliance with data sovereignty mandates, delivering unmatched assurance for today's digital-first legal profession.

#### **The legal sector's escalating cybersecurity crisis**

Law firms are inevitably under constant attack. Sophisticated cybercriminals, nation-state actors, and even malicious insiders are relentlessly targeting legal institutions. We all know why. Because legal firms are data-rich; housing confidential corporate documents, financials, case strategies, M&A materials, and highly sensitive personal information. Traditional software-based security measures, while necessary, are proving ever vulnerable against evolving attack vectors, they simply cannot keep up with today's advanced threats.

The legal sector demands the most advanced solutions – and Goldilock provides a security solution that goes beyond digital barriers and provides a tangible, physical shield against cyber intrusion.

#### **Critical threats facing the water sector**

- **Ransomware attacks:** Crippling firm operations, extorting exorbitant ransoms for the release of indispensable client files and core case management systems.
- **Data breaches and confidentiality compromises:** Exposing sensitive client information, violating attorney-client privilege, and triggering significant legal and devastating financial repercussions.

- **Compromised evidence integrity:** Undermining the admissibility of crucial evidence in legal proceedings, potentially leading to adverse judgments and professional liability.
- **Insider threats (malicious and negligent):** Intentional data theft or accidental data leaks by employees with privileged access.
- **Evolving compliance mandates:** Navigating a labyrinth of complex and stringent data privacy regulations (e.g., GDPR, CCPA, local data sovereignty laws) that span multiple jurisdictions.
- **Business continuity and disaster recovery failures:** Inability to quickly recover from cyber incidents, leading to prolonged downtime and disruption of legal services.

## The FireBreak difference: Securing the legal sector through true physical isolation

Goldilock's FireBreak Physical Connection Controller provides a game-changing approach to legal cybersecurity by implementing true physical disconnection of critical digital assets from all networks – including the internet – when they are not actively required. This hardware-enforced isolation eliminates the attack surface, making the protected data and systems effectively invisible to cyber threats. When critical systems are offline by design, they can't be hacked.

### Key features and real-world applications for law firms

#### Client-dedicated secure digital vaults

**Benefit:** Create physically segregated, offline digital vaults for each client or high-profile case. This ensures that a breach in one area cannot compromise other sensitive client data, drastically limiting the blast radius of any potential incident.

**Example:** A firm handling a major class-action lawsuit can store all related documents and communications in a dedicated FireBreak protected vault, completely isolated from the firm's general network and other client files.

#### Evidence integrity and chain of custody

**Benefit:** Implement time-controlled, auditable access for authorized parties (e.g., opposing counsel during discovery with court approval). Maintain an immutable chain of custody with comprehensive access logs, ensuring the integrity and admissibility of digital evidence in court.

**Example:** During e-discovery, specific document sets can be made accessible to opposing counsel for a defined period through a secure, FireBreak controlled connection. All access attempts and modifications are meticulously logged, providing an unalterable audit trail.

#### Ransomware-proof, air-gapped backup and recovery

**Benefit:** Schedule regular, automated backups to FireBreak protected, physically disconnected storage. In the event of a ransomware attack, firms can rapidly restore operations from a clean, untainted backup without yielding to ransom demands.

**Example:** Daily backups of critical case files and financial records are automatically stored on a FireBreak isolated drive. If the primary network is infected with ransomware, the firm can quickly restore operations from the secure backup without any interaction with the compromised systems.

### Robust internal threat mitigation

**Benefit:** Implement scheduled or on-demand access to sensitive files based on roles and responsibilities. FireBreak prevents unauthorised employee access when it's not required, significantly reducing the risk of insider threats, both malicious and accidental. Multi-factor authentication can be enforced at the hardware level for an additional layer of security during authorised access periods.

**Example:** A paralegal working on a specific case is granted access to relevant documents only during their working hours. Outside of these hours, the data is physically inaccessible, preventing unauthorised viewing or modification.

### Granular practice area network segmentation

**Benefit:** Physically isolate network segments for different practice areas (e.g., litigation, intellectual property, M&A). This prevents lateral movement of attackers within the firm's network, containing breaches and protecting sensitive data in other departments.

**Example:** If the IP department's network were compromised, the FireBreak enforced segmentation would prevent the attackers from accessing sensitive client data within the corporate law or real estate departments.

### Global data compliance and sovereignty

**Benefit:** Meet stringent data privacy regulations like GDPR, HIPAA (for firms handling healthcare-related legal matters), and various international data sovereignty laws with greater confidence. FireBreak allows firms to maintain critical client data within their physical control and jurisdiction, minimizing risks associated with cloud storage and cross-border data transfers.

**Example:** A law firm with international clients can utilize FireBreak to ensure that client data subject to specific regional data sovereignty laws remains physically isolated and under their direct control within the relevant jurisdiction.

## Why legal firms choose Goldilock FireBreak

### True cyber isolation

When disconnected, your most critical legal data and systems are not just logically separated, they are physically unreachable, rendering them invisible to remote attackers.

### Purpose-built for legal workflows

Features like immutable audit logs, secure time-based third-party access for evidence sharing, and granular user access controls are designed with legal processes in mind.

### Seamless operational integration

Activate or revoke access through flexible methods like API integration with existing legal tech platforms, secure SMS commands, or a physical switch – minimising disruption to established workflows.

### Aligned with zero trust security models

Limits access strictly to what's needed, when it's needed, with no standing connections, no assumed trust, and no digital exposure.

### **Audit-ready for regulatory compliance**

Helps meet GDPR, data sovereignty, and industry-specific mandates, while demonstrating best-in-class security to clients and auditors alike.

### **Ultimate peace of mind**

Knowing your most sensitive client data, privileged communications, and critical evidence are protected by a virtually impenetrable, hardware-enforced barrier.

### **Conclusion**

In an era of escalating cyber threats, relying solely on software-based security is a gamble legal firms can no longer afford. Goldilock FireBreak offers a paradigm shift in legal cybersecurity, providing a robust, hardware-enforced layer of protection that goes beyond conventional defences. By physically isolating critical digital assets, Goldilock FireBreak empowers law firms to safeguard client confidentiality, ensure evidence integrity, meet complex compliance mandates, and ultimately, uphold the trust their clients place in them

**Disconnect to protect**, on demand.

[sales@goldilock.com](mailto:sales@goldilock.com) | [goldilock.com](https://goldilock.com)

