Perimetra

CASE STUDY

Industry: Legal Services

Services: Fully Managed Cybersecurity

How Hidden Ransomware Was Stopped Before It Disrupted Operations for a Regional Law Firm

When a ransomware attack struck without warning, Perimetra contained it early and gave the firm clear proof of what happened.

Executive Summary

A local law firm needed dependable protection against fast-moving cyber threats without relying on staff to spot problems first. Perimetra's managed cybersecurity service detected and stopped a ransomware attack on a Friday afternoon before the team knew it was underway, then delivered an automated report detailing the event. The firm avoided a potentially disruptive incident and gained immediate proof of service value.

Challenges

- The firm faced an active ransomware threat that could have interrupted legal work and access to critical case files.
- Internal staff had no immediate visibility into the attack as it unfolded, creating dangerous awareness gaps.
- Any successful encryption event could have delayed client service and strained confidence in daily operations.
- Leaders needed fast, credible confirmation of what happened without relying on manual investigation alone.
- As a law firm, the business had to protect sensitive information while keeping attorneys and staff productive.

Perimetra's Approach

Key Actions:

- Perimetra continuously monitored the environment and identified suspicious activity before the firm noticed signs of trouble.
- The team acted quickly to stop the ransomware event before it could escalate into a visible business disruption.
- Perimetra delivered an automated incident report that documented the event clearly for internal review and assurance.
- Protection was delivered through an ongoing managed security service rather than waiting for the client to raise a ticket.
- The response combined proactive detection with immediate containment to reduce exposure during a high-risk Friday incident.

Solutions

- Managed ransomware detection and response helped the firm address threats in real time without adding internal burden.
- Proactive security monitoring created earlier visibility into malicious activity than the client could achieve alone.
- Automated incident reporting gave leadership clear evidence of what occurred and confidence in the response taken.
- An always-on cybersecurity service reduced dependence on after-the-fact discovery and manual escalation paths.
- A prevention-focused approach protected day-to-day legal operations while supporting continuity and client trust.

The Result

- Perimetra stopped a ransomware attack before anyone at the firm knew it was happening.
- The firm avoided a potentially serious interruption to legal work, communications, and access to critical systems.
- Automated reporting showed exactly what occurred, giving stakeholders fast clarity without extra investigation.
- The incident reinforced confidence that proactive cybersecurity oversight was protecting the business in real time.
- Leadership viewed the single prevented event as enough value to justify years of ongoing service.

"Perimetra stopped a ransomware attack on a Friday afternoon before anyone on our team knew it was happening. The automated report showed exactly what occurred. That alone paid for years of service."

David M.
Managing Partner, Regional Law Firm

Stop Threats Before They Spread

See how proactive cybersecurity can catch attacks early, reduce disruption, and give your team confidence in every response.

Schedule A Consultation

Perimetra

(888) 893-6687

perimetra.security