threatER

7 Things Legal Firms Need to Know About Protective DNS

Law firms are sitting on some of the most valuable data in existence. M&A terms that move markets. Litigation strategy. Privileged client communications. Financial records protected by decades of professional obligation.

That data has a target on it. And one of the most effective, most overlooked layers of protection available to legal firms today operates at a place most attorneys have never thought about: DNS. Here is what legal firms need to understand.

1. NEARLY EVERY CYBERATTACK AGAINST YOUR FIRM STARTS WITH A DNS QUERY

Before ransomware executes, before credentials are stolen, before a phishing page loads in a browser, there is a DNS query.
DNS is the internet's address book. When anyone at your firm clicks a link, opens a browser, or connects to an external service, their device asks a DNS resolver: "What is the address for this domain?" That query happens billions of times a day on every network, which is exactly why attackers have learned to weaponize it.

Phishing links, malware download URLs, command-and-control callbacks, data exfiltration destinations: all of them require a DNS resolution to function. Protective DNS sits at that resolution point and blocks malicious queries before the connection ever completes. The attack cannot proceed if the address never resolves.

2. BLOCKING AT DNS IS EARLIER THAN ANY OTHER CONTROL YOU HAVE

Most security tools operate after something has already happened. An endpoint agent fires when a process behaves suspiciously. A SIEM generates an alert when log events match a pattern. Email filters scan a message after it arrives in the inbox.

Protective DNS operates before any of that. It intercepts the query in transit, evaluates the destination against real-time threat intelligence, and either allows or blocks the resolution before any payload reaches a device or user.

For a law firm, this timing difference is significant. A blocked DNS query means the phishing page never loads, the malware never downloads, and the attacker never establishes the foothold that leads to the ransom demand. No endpoint alert. No incident response. No breach notification to clients.

3. YOUR ETHICAL OBLIGATIONS EXTEND TO HOW YOUR NETWORK HANDLES THREATS

ABA Model Rule 1.6 requires attorneys to make reasonable efforts to prevent unauthorized access to confidential client information. As of 2026, 42 states have made technology competence an enforceable ethical standard, not an optional best practice.

Regulators and bar associations are increasingly specific about what "reasonable efforts" means in practice. Documented, auditable security controls are part of that standard.

Protective DNS is one of the most auditable controls available. Every blocked query is logged. Every threat category is documented. When a bar inquiry or client audit asks what your firm did to protect their data, a DNS enforcement layer provides a concrete, timestamped record of threats intercepted before they could cause harm.

4. LEGAL FIRMS ARE TARGETED BECAUSE OF WHAT THEY HOLD, NOT THEIR SIZE

Ransomware attacks against law firms rose 48% in 2025. Firms of 10 to 49 attorneys reported the highest incident rates, a pattern that reflects deliberate targeting of midsize firms, not random selection.

The reason is the data. A single breach at a law firm can expose confidential information from dozens of clients simultaneously. Attackers running extortion operations value that leverage enormously. Ransom demands against legal targets have ranged from $500,000 to $21 million.

Protective DNS disrupts the attack chain at its earliest stage. The phishing email that delivers initial access contains a link. That link requires a DNS resolution. If the resolution is blocked, the attacker's entry point closes before they ever get inside.

5. PROTECTIVE DNS COVERS THE THREATS YOUR EMAIL FILTER MISSES

Email security tools catch a significant volume of phishing attempts. They do not catch all of them, and they do not catch the threats that arrive through other channels: malicious links in SMS messages, compromised websites visited during research, drive-by downloads from legitimate-looking domains registered hours before the attack.

Protective DNS covers all of these because it operates at the network layer, not the email layer. It does not matter how a malicious domain reaches a user's device. If a DNS query goes out to that domain from your network, protective DNS evaluates it and blocks it if it is flagged.

For legal professionals who regularly research opposing parties, visit court filing systems, and click links from clients and opposing counsel, this breadth of coverage matters.

6. CLIENTS ARE STARTING TO ASK ABOUT IT

The 2025 Integris Law Firm Cybersecurity Report found that nearly 40% of clients would fire or seriously consider firing a firm after a data breach, and 37% would warn others about the experience.

Clients at larger organizations, particularly financial institutions, healthcare companies, and publicly traded companies, are increasingly including security questionnaires in their outside counsel retention process. DNS-layer protection is among the controls that sophisticated clients and their security teams now look for specifically.

Being able to say that your firm blocks malicious DNS traffic in real time, with logged evidence of every intercepted threat, is a concrete answer to a question that more clients are beginning to ask.

7. IT REQUIRES NO AGENTS, NO HARDWARE, AND MINIMAL CONFIGURATION

One of the practical barriers to security adoption at law firms is complexity. Tools that require endpoint agents on every device, or hardware appliances at every office, or dedicated staff to manage and tune them, simply do not get deployed.

Protective DNS does not have those barriers. It operates at the resolver level, meaning protection applies to every device on the network, including personal devices used for work, without installing anything on individual machines. Configuration is typically a DNS settings change. Coverage is immediate.

For a firm without a dedicated IT security team, that simplicity is the difference between having a meaningful protection layer and having none.

THE BOTTOM LINE FOR LEGAL FIRMS

Protective DNS is not a replacement for broader security practices. It is the layer that operates earliest in the attack chain, before threats reach users, devices, or data. For legal firms carrying ethical obligations around client confidentiality, facing targeted ransomware campaigns, and increasingly accountable to clients who scrutinize security posture, that early interception layer is one of the highest-value controls available.

threatER's EnforceDNS delivers protective DNS built for organizations where client confidentiality is not negotiable. **See how it works at threater.com**