LEGAL SERVICES THREAT INTELLIGENCE REPORT

Privilege Under Attack: Defending Your Law Firm Against Modern Cyber Threats

eSENTIRE
THREAT RESPONSE UNIT

Introduction

As the legal sector has adopted new technologies and hybrid work models, the threat surface, which is the collection of points an attacker can use to gain access into a protected IT environment, has grown broader and more complex to manage.

Law firms and legal services organizations hold unparalleled access to non-public, confidential data across all facets of the public and private sectors.

As a result, they face significant cyber threats from adversaries seeking to extort payments, steal and sell sensitive data, and retaliate for client representation as a form of political activism.

Sensing opportunity, threat actors have intensified their activities against law firms and legal services organizations. The 2022 Legal Technology Survey Report from the American Bar Association (ABA) reported that 27% of law firms had experienced a security breach — and the threat landscape has only grown more sophisticated since then.

Over the past 12 months, eSentire's Threat Response Unit (TRU) observed a **20% year-over-year increase in incidents targeting the legal sector**; out of all the threats observed, 56.3% of threats were credential- or identity-focused.

The legal sector recorded an 86% overall intrusion ratio compared to other industries — and attacks that did progress moved faster than in almost any other sector.

Today's attackers have shifted their strategy.

Rather than relying on broad malware campaigns or technical exploits, they now focus overwhelmingly on identity theft and credential compromise to exploit the trust-based, time-pressured nature of legal work itself.

In this threat intelligence report, we explore the current threat landscape impacting law firms and legal services organizations, highlight the most prevalent attack vectors observed by TRU in 2025, and offer actionable recommendations to help protect against cyberattacks, strengthen defenses, and minimize business disruption.

Why Law Firms and Legal Services Organizations Are Prime Cyber Targets

Law firms and legal services organizations have become increasingly attractive targets for cybercriminals due to the extraordinary concentration of high-value, confidential data they hold combined with a historically fragmented approach to cybersecurity.

As attackers grow more sophisticated, they see law firms not as isolated targets but as repositories of privileged intelligence spanning every industry they serve.

The scale of the problem is accelerating. In 2025, incident responses involving law firms nearly doubled compared to 2024, according to Baker & Hostetler's annual Data Security Incident Response Report.

Moreover, the average cost of a data breach for law firms reached $5.08 million in 2024 — a more than 10% year-over-year increase.

In fact, threat data compiled by eSentire's Threat Response Unit (TRU) confirms this trajectory, recording a 20% year-over-year increase in legal sector incidents in 2025 alone.

Access to Extraordinarily Valuable Data

The fundamental reason law firms are prime targets is the breadth and sensitivity of the data they hold. Unlike most organizations, which hold data relevant to their own operations, law firms serve as custodians of confidential information across dozens of industries simultaneously.

A single mid-size firm may hold:

- Trade secrets and intellectual property from technology and life sciences clients
- M&A strategies, deal terms, and pre-announcement transaction intelligence
- Personal and health information tied to litigation involving thousands of individuals
- Financial records, settlement terms, and account details
- Privileged communications that, if exposed, can compromise ongoing legal proceedings

This makes a breach at a law firm qualitatively different from most other sectors. When attackers breach a law firm, they gain intelligence that can be leveraged for financial fraud, market manipulation, competitive espionage, or extortion across every client the firm serves, not just the firm itself.

The consequences can be severe. In 2024, Orrick, Herrington & Sutcliffe paid $8 million to settle a class action lawsuit after a data breach exposed the personal information of over 600,000 individuals. Plus, when Berkeley Research Group was hit by ransomware in March 2025 during a $700 million leveraged buyout, the attack exposed M&A intelligence across hundreds of concurrent deals.

Inconsistent Cybersecurity Maturity

Despite the volume and sensitivity of data they protect, law firms consistently lag behind other industries on cybersecurity investment and preparedness.

According to the 2024 ABA Cybersecurity Tech Report, 36% of law firms reported experiencing a security incident in the past year, yet only 34% had a formal incident response plan in place.

Many law firms lack dedicated security personnel entirely, so cybersecurity responsibilities frequently fall to general IT staff who are managing dozens of other priorities.

Smaller and mid-size firms are particularly vulnerable: without dedicated IT or security resources, threats can persist undetected for weeks or months. However, larger firms are not immune; when cybersecurity is just one part of a general IT role, sophisticated intrusions can slip under the radar.

This gap between data value and security maturity makes the legal sector disproportionately attractive compared to better-defended industries. Attackers have recognized that law firms often hold data equal in value to that of their financial services or healthcare clients, but with materially weaker defenses.

Time-sensitive Deadlines Create Exploitable Pressure

Since legal work is defined by hard deadlines (i.e., court filings, deal closings, regulatory submissions, and client response windows), threat actors have become acutely aware of this operating environment and deliberately exploit it.

Ransomware is frequently deployed immediately before major deal closings or court dates, when the cost of downtime is highest and the pressure to pay is most acute.

For example, ClickFix browser attacks, which present fake error messages claiming that a document viewer or e-filing system needs immediate remediation, exploit the same psychology: the “I need to fix this now to meet my deadline” instinct. TRU’s data shows ClickFix attacks hit the legal sector at 13.39% of incidents, more than 4.6% above the cross-industry average.

Similarly, attackers time BEC campaigns and AiTM phishing operations to coincide with active transactions, when email volumes are high and professionals are processing financial instructions under time pressure.

This is not opportunistic targeting; it is a deliberate exploitation of the legal sector’s operating model.

The Trust-Based Business Model as an Attack Surface

Legal work fundamentally depends on trust and open communication. Attorneys exchange highly sensitive information daily with clients, opposing counsel, courts, regulators, and expert witnesses.

This creates conditions that are inherently favorable for phishing and impersonation attacks:

- Legal professionals expect unsolicited communications from new parties so a court notice, a document request, or an opposing counsel inquiry arriving from an unknown address is entirely normal.
- Published court filings, bar association records, case databases, and LinkedIn profiles give attackers detailed intelligence to craft highly convincing spearphishing lures that reference real cases, clients, and relationships.
- Attorney-client confidentiality creates a cultural reluctance to report or disclose incidents, which can extend attacker dwell time and delay remediation.

The result is a sector where social engineering attacks can achieve unusually high success rates.

Expanding Third-Party and Supply Chain Risk

Law firms sit at the center of complex ecosystems of clients, courts, regulators, co-counsel, expert witnesses, and technology vendors. This interconnectedness creates substantial supply chain risk.

Attackers exploit trusted relationships in two primary ways: by compromising vendors and partners that have privileged access to firm systems, and by using knowledge of existing relationships to make phishing lures more convincing.

The 2023 MOVEit file transfer breach demonstrated this risk at scale, affecting multiple law firms that used the compromised platform to exchange client data. In each case, a trusted third-party platform became the entry point into firm environments.

As legal sector technology adoption accelerates, spanning document management, eDiscovery, e-signature, and practice management platforms, the number of third-party integration points that attackers can exploit continues to grow.

Additionally, law firms are increasingly subject to client-imposed cybersecurity requirements. Larger clients and those in regulated industries now conduct formal third-party risk assessments of outside counsel and may require specific security controls or certifications as a condition of engagement.

This has transformed cybersecurity from an internal concern into a competitive and commercial one.

Regulatory Exposure That Compounds the Damage

Unlike many other sectors, a breach at a law firm can trigger regulatory obligations not just for the firm itself, but for every client whose data was held.

Law firms operating on behalf of clients in healthcare, financial services, or other regulated industries may face HIPAA, GDPR, PCI, FINRA, and SEC obligations because of a breach even though the incident occurred at the law firm, not the client.

The 2023 Covington & Burling case illustrated this dynamic starkly: the SEC subpoenaed the firm for the names of 298 publicly traded clients whose data may have been exfiltrated, establishing that law firms cannot fully shield client identity from regulators following a breach.

Meanwhile, ABA Model Rule 1.6(c) obligates attorneys to make reasonable efforts to prevent unauthorized disclosure of client information. Failure to do so can result in disciplinary action, malpractice claims, and bar complaints on top of any regulatory penalties.

Only 34% of law firms currently have a formal incident response plan in place (ABA, 2023), meaning most firms would be responding to one of the most complex regulatory environments in business without a documented playbook.

Understanding the Current Threat Landscape

For legal services organizations to effectively manage cyber risk, they must first understand both their current security posture and the specific threats they face.

Most law firms and legal services organizations lack dedicated cybersecurity programs or personnel, meaning their defenses have likely failed to keep pace with a rapidly evolving attack surface.

The IT environment within many legal sector organizations remains a complex mix of legacy and modern solutions.

Additionally, the widespread adoption of cloud-based document management, eDiscovery platforms, e-signature tools, and collaboration software like Microsoft Teams has significantly expanded the digital attack surface.

Several forces continue to reshape the technology stack within law firms:

- **Cloud migration:** Many firms are moving file sharing and document management from on-premises to cloud-based services, reducing physical footprints but introducing new access control challenges.
- **Shadow IT:** Technologies used outside of official IT oversight expand an organization's attack surface and introduce unmanaged risk.
- **Hybrid and remote work:** Remote work has become permanent for many legal professionals. VPN solutions, remote conferencing, and collaboration tools have expanded the perimeter that security teams must defend.
- **Client and partner demands:** Larger clients increasingly require formal third-party risk assessments and impose technology requirements on the firms they work with.

eSentire's Threat Response Unit analyzed incidents within the legal services industry across our global customers throughout the past year and the data reveals a decisive shift: the legal sector is no longer primarily targeted through technical exploits or broad malware campaigns.

Threat actors are now focused almost entirely on identity — stealing credentials, bypassing authentication, and impersonating trusted parties.

56%	Of threats focus on identity theft over technical exploitation
86%	Overall intrusion ratio
+20%	Year-over-year increase in legal incidents over 2025

Source: eSentire, May 2026

The Shift to Identity-Centric Attacks

The most significant finding is the dominance of identity-based attacks. **Credential theft and account compromise now account for 56.3% of all threats to the legal sector**, making legal professionals the primary attack surface, not the technology infrastructure itself.

Breaking this down further, TRU found that **45% of all incidents involved account compromise** while 11% were phishing attempts targeting user credentials directly.

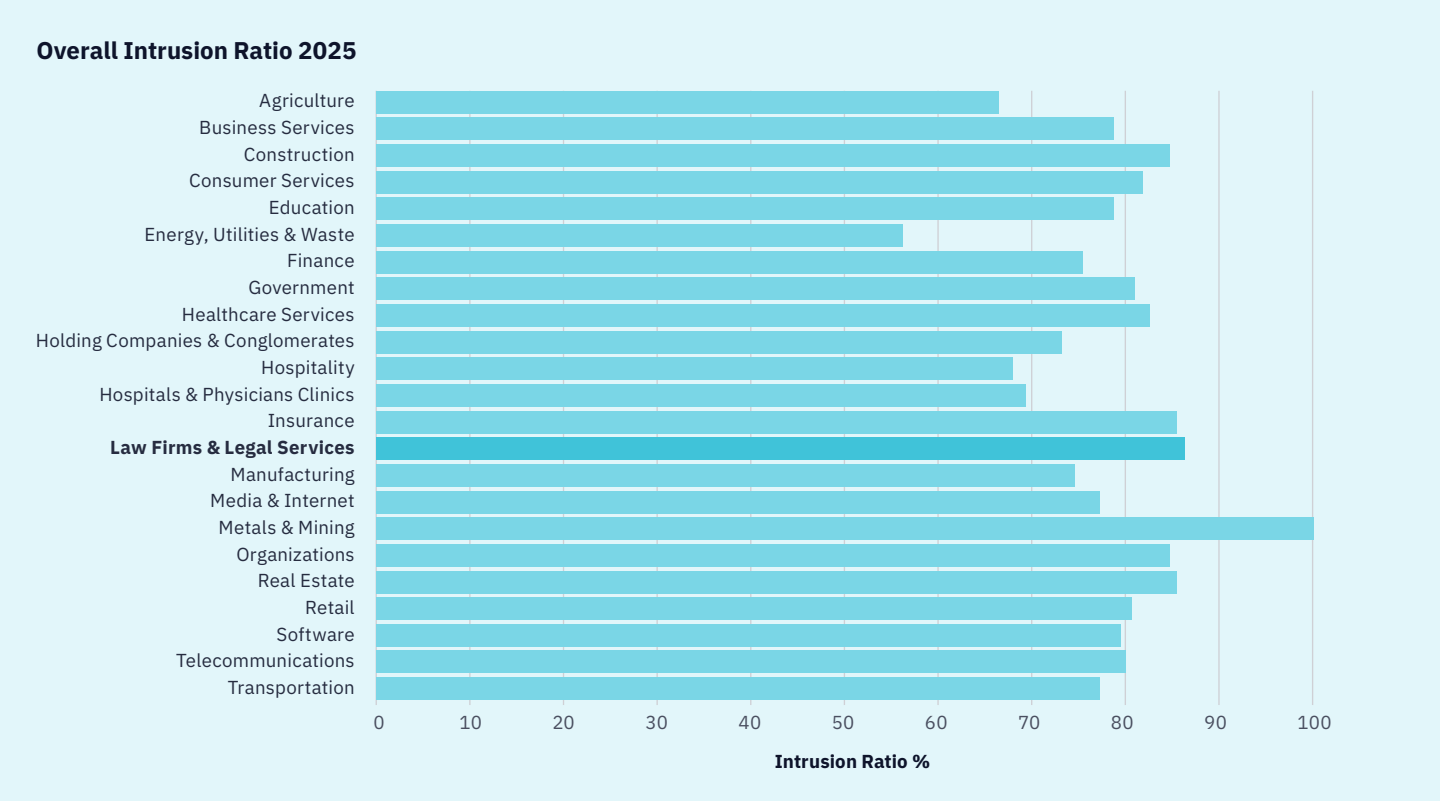
This shift reflects a deliberate strategic decision by threat actors. Legal email accounts contain privileged communications, client data, M&A intelligence, and litigation strategies.

Gaining access to a single account can yield far more value than deploying ransomware and can be monetized repeatedly without tipping off defenders.

Intrusion Ratio: Legal Sector Leads All Industries

In 2025, the legal sector recorded an 86% overall intrusion ratio, meaning that in 86% of incidents observed, the attack progressed beyond initial access into active intrusion (Figure 1).

This is significantly higher than the cross-industry average and reflects the high-value nature of legal targets.

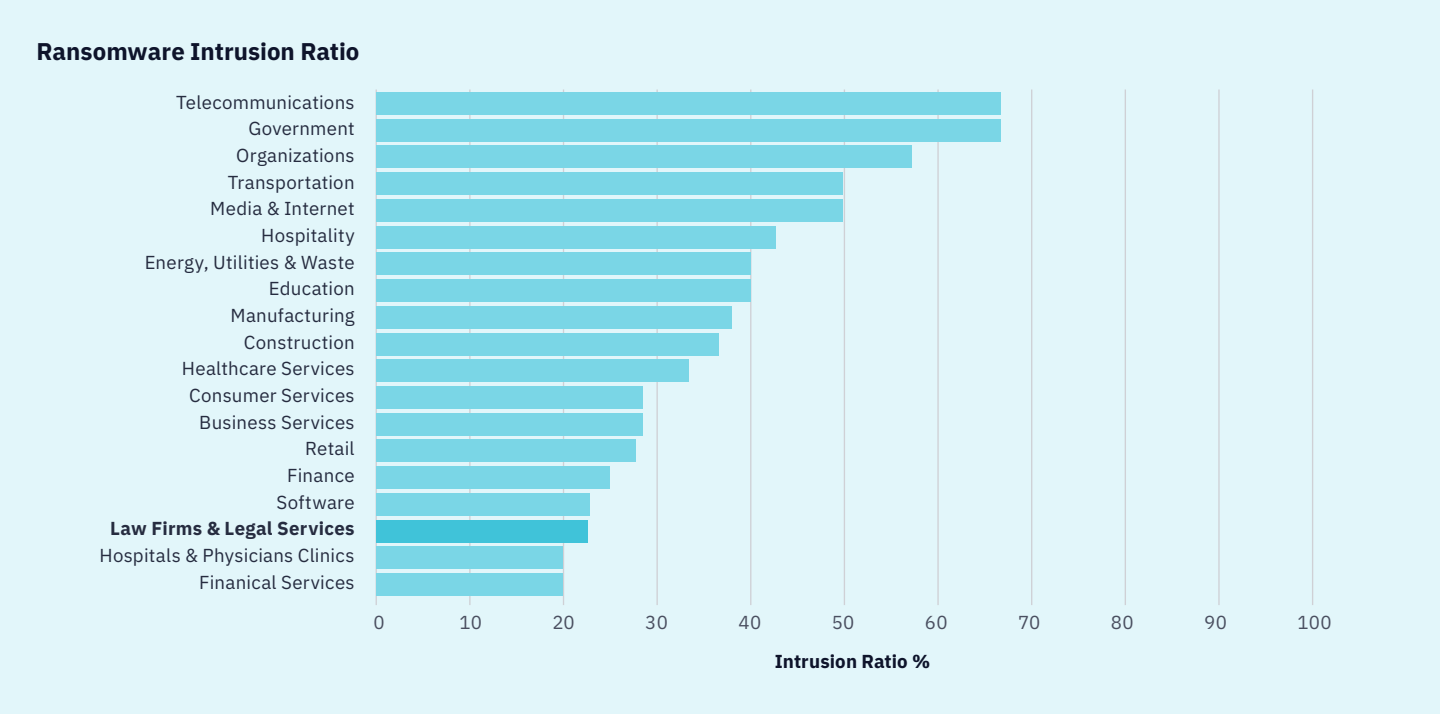


86% Intrusion Ratio for the Legal Sector

Legal Services saw an 86% overall intrusion ratio compared to other industries in 2025, placing it among the most targeted sectors globally.

When ransomware-specific intrusion ratios are examined, legal sits at approximately 23%, relatively lower than some sectors, suggesting that attackers prioritize data theft and account access over operational disruption in the legal space (Figure 2).

The true damage in the legal sector often occurs silently: credentials exfiltrated, privileged communications accessed, and client data sold or weaponized without triggering obvious alarms.



23% Ransomware Intrusion Ratio

Legal Services saw a 23% ransomware intrusion ratio compared to other industries in 2025.

Top Initial Access Vectors

The legal sector initial access data reveals a pronounced human-centric attack strategy (Figure 3).

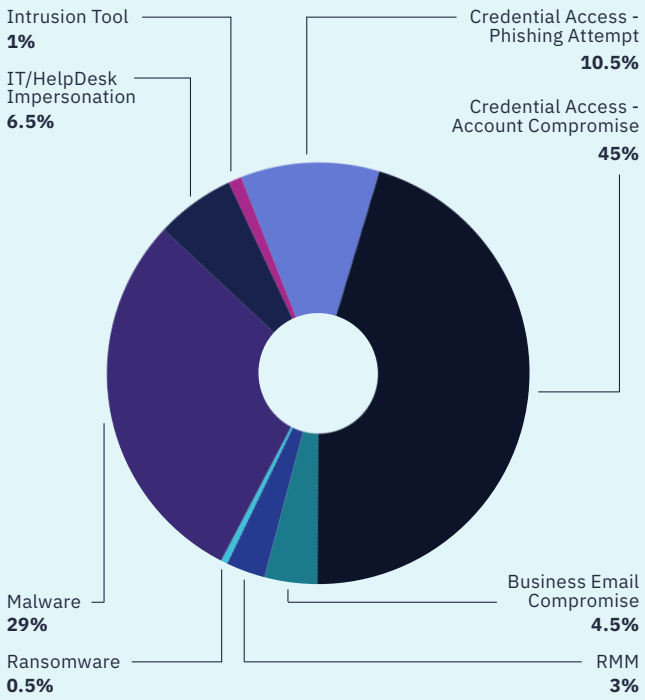
With **61.87% of incidents stemming from email and browser-based social engineering**, including AiTM phishing, ClickFix attacks, spam, and Microsoft Teams abuse, legal professionals represent both the primary target and the primary vulnerability.

AiTM Phishing: The #1 Initial Access Vector

Adversary-in-the-Middle (AiTM) attacks now account for 28.57% of all initial access events in the legal sector, making it the single most common entry point.

AiTM attacks work by proxying the authentication process: even when a user correctly enters their credentials and completes MFA, the attacker captures the resulting session cookie and gains authenticated access.

Breakdown of Initial Access Vectors



The dominance of AiTM attacks in the legal sector tells three important stories:

- **MFA is present but being systematically bypassed**. The comparatively low rate of traditional credential theft (16.96% vs. 26.01% cross-industry average) suggests MFA has been deployed across many firms, but attackers have evolved to bypass it.
- **Credential value in legal is extremely high**; threat actors are investing in sophisticated AiTM infrastructure specifically for legal targets, indicating the ROI justifies the technical complexity.
- **Email is the crown jewel**; access to legal email means access to privileged communications, client data, wire transfer instructions, and the ability to impersonate partners convincingly.

> *Tycoon2FA, a Phishing-as-a-Service platform, was responsible for 52.3% of all AiTM-related account compromises in the legal sector in 2025. This platform dramatically lowers the barrier for conducting sophisticated AiTM attacks, enabling even low-skill threat actors to systematically target legal professionals at scale.*

ClickFix: Exploiting Deadline Pressure

Browser-based ClickFix attacks, which primarily deliver the NetSupportManager RAT malware, hit the legal sector at 13.39% (vs. 8.77% industry average), the second-largest positive deviation observed.

ClickFix attacks present users with fake browser error messages or prompts claiming that a document viewer, e-filing system, or court portal requires an immediate action to function.

Legal professionals routinely encounter legitimate technical issues accessing case-critical systems, and attackers exploit the “I need to fix this now to meet my deadline” mentality that defines legal work. This means that ClickFix is a workflow exploitation vector unique to high-pressure professional environments.

Microsoft Teams: A Trusted Channel Weaponized

Microsoft Teams abuse accounts for 6.25% of initial access in the legal sector, nearly double the cross-industry average of 3.40%. This reflects the legal sector’s deep integration with collaboration platforms, accelerated by hybrid work adoption.

Attackers leverage Microsoft Teams in two primary ways: sending malicious links through what appear to be internal communications, and impersonating IT helpdesk or leadership figures through Email Bombing campaigns that precede Teams-based social engineering.

Users tend to apply lower suspicion to what feels like internal communication, creating a trusted channel that is increasingly an external attack vector.

Malware in the Legal Sector

Malware accounts for 28.8% of threats to the legal sector in 2025.

While this represents a significant volume, the composition of that malware has shifted meaningfully compared to prior years: the sector has moved away from banking trojans and broad-spectrum ransomware distributors toward a more targeted mix of RATs, infostealers, and loaders.

Remote Access Trojans (RATs) — 34.8% of Malware

RATs now represent the largest malware category in the legal sector. The NetSupportManager RAT, which relies on a legitimate remote support tool weaponized for persistent surveillance and access, accounts for 26.2% of all malware detections. This is a significant shift from prior years, when legal threats were dominated by malware distributors like GootLoader and Qakbot.

NetSupportManager is typically delivered via ClickFix lures, exploiting the same deadline-pressure dynamic described above. Once installed, it provides attackers with persistent, stealthy remote access to a compromised workstation, enabling ongoing surveillance, credential harvesting, and lateral movement.

Infostealers — 30.4% of Malware

Infostealers specialize in silently locating and copying sensitive data directly from infected machines: browser history, stored passwords, session cookies, and endpoint fingerprint telemetry. This data is typically sold on dark web marketplaces and used to enable follow-on attacks.

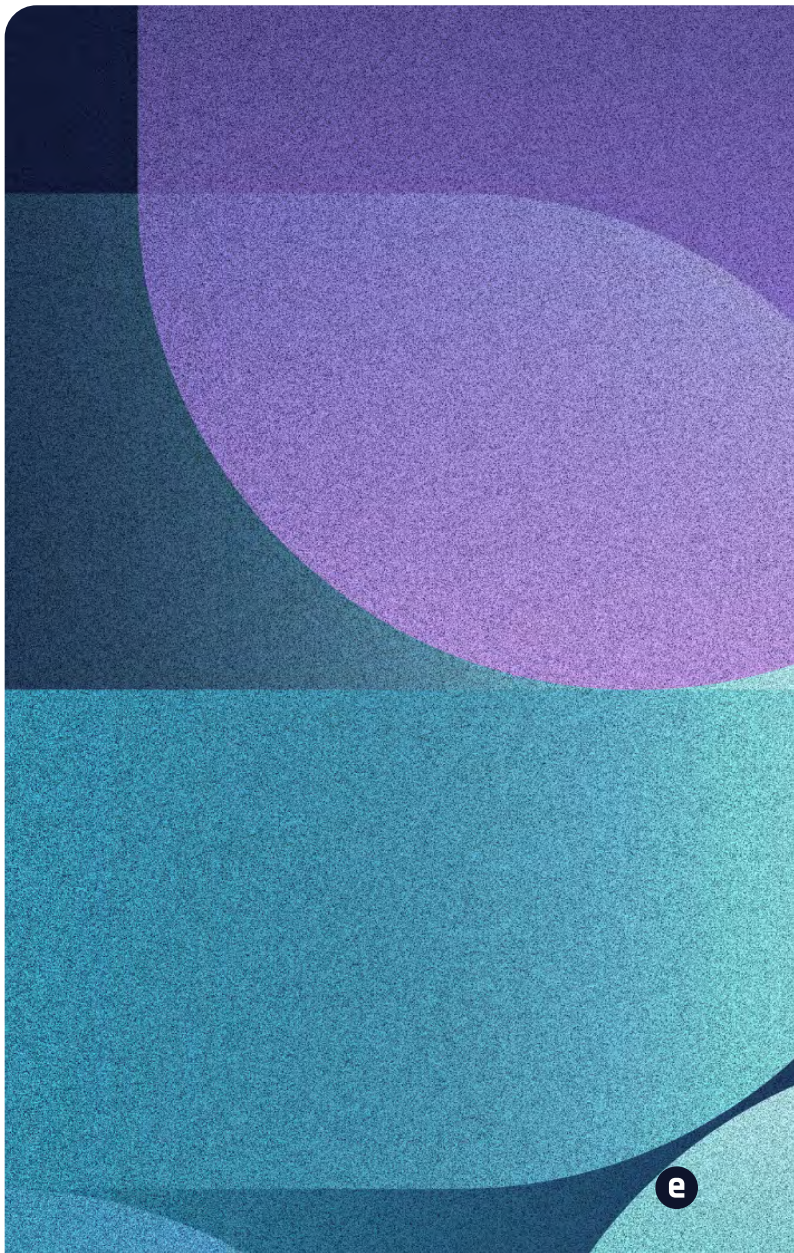
The top infostealers observed in the legal sector were Lumma Stealer (9.6%), StealC (4.8%), and Rhadamanthys (4.8%).

Infostealer activity in legal environments is particularly damaging because stolen credentials and session tokens can provide access to document management systems, client portals, and privileged email accounts long after the initial infection is remediated.

Loaders — 30.4% of Malware

Loaders deliver a small initial payload that allows the attacker to profile the target before deciding what to deploy next.

Their prevalence in the legal sector reflects a calculated, intelligence-led approach: attackers establish a foothold first, then assess the value of the target before committing to ransomware deployment, data exfiltration, or persistent access.



Recommendations to Build a Foundation of Cyber Resilience

Managing cyber risk within legal services organizations must start with building a foundation that combines employee security awareness, hardened defenses, identity protection, and properly managed third-party relationships.

All cybersecurity initiatives should be championed by senior leaders, especially partners whose names are on the masthead. While it is not their responsibility to become IT experts, senior leaders must recognize that security needs are constantly evolving and empower the IT organization with appropriate resources.

1 Prioritizing Identity and Credential Security

Given that 56.3% of threats in 2025 were credential- or identity-focused, traditional MFA alone is no longer sufficient. The rise of AiTM attacks demonstrates that session-based protections must complement authentication controls.

- Deploy phishing-resistant MFA (e.g., FIDO2/passkeys) to eliminate AiTM attack vectors.
- Implement conditional access policies that evaluate device health, location, and behavior in addition to credentials.
- Monitor VPN and identity platform logs continuously for anomalous session activity that may indicate stolen cookies or unauthorized access.
- Regularly validate that remote access controls work as designed through adversarial simulation, not just periodic audits.

2 Enhance Security Awareness

Since the most common attack vectors exploit employees directly, through AiTM phishing, ClickFix lures, and Teams impersonation, security awareness training is a first-order defense — not a compliance checkbox.

- Use industry-specific threat scenarios that reflect the actual lures targeting legal professionals — fake document requests, court portal errors, Bar Association complaints.
- Run realistic phishing simulations that include AiTM-style credential harvesting, not just traditional link-click tests.
- Specifically train users to recognize ClickFix-style browser prompts and “IT helpdesk” impersonation approaches via Teams.
- Establish a culture of transparent reporting where employees are encouraged to flag suspicious activity without fear. Quick reporting allows rapid containment before lateral movement occurs.
- Enforce email authentication protocols (DMARC, DKIM, SPF) to reduce spoofing and thread-hijacking attacks.
- Meet CLE accreditation requirements for legal professionals where applicable.

3 Managing Trusted Relationships

Trusted relationships with clients, partners, and technology vendors become attack vectors when they lack adequate security controls. The legal sector's supply chain risk is compounded by the publication of legal documents, court filings, and professional relationships that give attackers actionable intelligence.

To address third-party risk, we recommend the three Ps framework:

- **Prevention:** Implement company-wide policies that incorporate security requirements before onboarding third parties.
- **Policies:** Apply a formalized, multi-step due diligence process for vendor evaluation, with senior management support.
- **Promises:** Establish contractual obligations and consequences for third-party data breaches, and revise risk policies when incidents occur.

4 Adopt a Defense-in-Depth Strategy with Closed-Loop Intelligence

Ensure security controls layer across endpoints, email, network, cloud, and identity with intelligence flowing continuously between offensive and defensive operations.

- Implement zero-trust architecture to verify and limit user access to only the data required at any given time.
- Deploy a **24/7 multi-signal Managed Detection and Response (MDR) solution** to detect and isolate threats before lateral spread.
- Ensure detection models are continuously improved by exposure findings and offensive validation results — not tuned once during onboarding and left static.
- Log VPN and domain controller activity to track intruder movements and identify initial access events.
- Establish backup systems and test restoration/recovery procedures regularly — paying particular attention to domain controllers.

5 Preempt Attackers Before They Strike — Managed CTEM and Offensive Validation

A managed **Continuous Threat Exposure Management (CTEM) program** gives you a program. For law firms, where a single compromised credential can cascade into a full-scale breach across client data, CTEM is no longer optional.

- Continuously probe your environment from an attacker's perspective — mapping your full attack surface, validating which exposures are actually exploitable in your live environment, and confirming that remediations hold.
- Prioritize exposures based on adversarial reachability and business criticality, not CVSS scores alone.
- Use offensive validation findings to tune your detection models — closing the loop between exposure management and real-time defense.
- Use continuous adversarial simulation (breach and attack simulation) to confirm that patched vulnerabilities are actually closed in your environment.

6 Prepare for Ransomware and Incident Response

Have a formal incident response plan that covers ransomware, account compromise, and hands-on intrusion scenarios — including procedures for data recovery, client notification, regulatory reporting, and public communication. Only 34% of law firms currently have one.

- Test backup systems regularly. Backups should be encrypted, network-segmented, and recovery-tested — not just assumed to work.
- Engage a **Digital Forensics and Incident Response (DFIR) provider** on retainer before you need them. Pre-arranged IR support dramatically reduces response time and limits breach scope.
- Ensure your incident response plan accounts for the multi-regulatory complexity legal firms face: a single breach may trigger HIPAA, GDPR, FINRA, and state-level notification obligations simultaneously.

How eSentire Protects Law Firms and Legal Services Organizations

eSentire is a global leader in AI-powered Controlled Autonomy SecOps, with more than 2,000 customers across over 35 industries in 80 countries and growing. Founded in 2001, the company protects the world's most targeted organizations and critical infrastructure from known and unknown cyber threats.

eSentire's Controlled Autonomy SecOps operating model pairs agentic AI operatives via the Atlas AI Platform with engineered human-judgment controls backed by its 24/7 SOC to deliver expert-depth security outcomes at machine speed, without ceding accountability to opaque automation.

Our 24/7 Cyber Analysts and Elite Threat Hunters have stopped nation-state actors targeting high-profile client data, identified new social engineering threats in the legal sector, and successfully prevented ransomware gangs from shutting down operations for our legal clients.

eSentire protects over 14,000 attorneys across the ALM 100 and ALM 200 — from small firms with as few as 15 attorneys to the largest firms with over 1,400 attorneys. We are proud partners of the International Legal Technology Association (ILTA) and the Association of Legal Administrators (ALA), and we actively share threat intelligence with the Legal Services Information Sharing and Analytics Organization (LS-ISAO).

Key Industry Challenges	How eSentire Managed Detection and Response Helps
Access to Confidential Information	Our 24/7 SOC Analysts and Elite Threat Hunters actively hunt for threats across your entire environment — ingesting signal from any vendor stack. We detect intrusions and contain attacks before client data can be exfiltrated. Every containment action is explainable and reversible.
Operational Disruption and Cost of Downtime	Atlas investigates and contains threats autonomously within customer-defined authority envelopes — stopping intrusions before malware can propagate across your firm's environment, with every action policy-bounded.
Supply Chain & Third-Party Risk	Atlas maps your full attack surface, including third-party integrations and vendor connections, to conduct adversarial validation to identify exploitable paths before attackers do.
Preventing Ransomware and Identity-based Attacks	We monitor your attack surface 24/7 with multi-signal coverage across endpoint, network, log, cloud, and identity data sources — providing deep investigation and kill-switch response capabilities against credential-based and ransomware threats. Atlas continuously monitors for anomalous session activity, credential misuse, and AiTM-specific behavioral indicators — detecting identity-based intrusions that bypass traditional MFA controls at machine speed.
Regulatory and Compliance Requirements	Our 24/7 SOC leverages proven runbooks mapped to PCI, HIPAA, GDPR, CCPA, and state-level regulations. Every autonomous Atlas action produces a human-readable audit trail — the explainability and policy-bounded authority documentation that regulators, boards, and cyber insurers now require.
Meeting Bar Requirements	We offer CLE-accredited user awareness training and risk management assessments tailored to the legal profession.

Protect What's Next

We're here to help! Submit your information and an eSentire representative will be in touch to help you build a more resilient security operation today.

LET'S TALK SECURITY →

eSentire

eSentire is a leader in Controlled Autonomy SecOps, protecting 2,000+ organizations across 35+ industries around the world. Founded in 2001, the company's Controlled Autonomy SecOps operating model pairs agentic AI operatives with engineered human-judgment controls, delivering expert-depth security outcomes at machine speed without ceding accountability to opaque automation. Powered by the unified agentic AI Atlas Platform, eSentire's Atlas AI + 24/7 expert human SOC coverage delivers offensive capabilities that preempt exposures before attackers do, detect, and respond to stop threats in real time. For more information, visit **www.esentire.com** and follow **@eSentire**.