SOLUTION BRIEF:

Securing the Legal Sector

Law firms have unparalleled access to valuable information across all facets of the public and private sectors. For decades, criminals have demonstrated how to attack law firms with proven methods that lead to massive ransomware outages, public exposure and crippling reputational damage. Typically, they use publicly available court records and settlement documents to create lures that ensnare legal professionals. Financial account information, mergers and acquisitions records, investment strategies, and healthcare records are all well established and profitable material to be circulated by criminals in the dark markets.

Milestone breaches at two prominent Wall Street law firms showcased the potential to steal non-public information for the purposes of insider trading.[1] The firms involved represented global banks and Fortune 500 companies in everything from lawsuits to multibillion-dollar merger negotiations. A year later, the well defended firm, DLA Piper, was crippled in the NotPetya ransomware attacks that also shut down major shipping firms and the national healthcare system in the United Kingdom. Since then, law firms have been exploited over unwanted exposure surrounding their high net-wealth clients and celebrities[2] and targeted for exploitation by compromising their file-sharing systems.

The motivations behind these cyber attacks include:

- Profit from stolen information
- Use law firms to reach their client data
- Publicly disrupt operations for purposes of extortion
- Retaliation for representation of politically ionized clients

Legal firms need cybersecurity expertise to proactively detect, disrupt and remediate cyber threats before they become business impacting. It is important to align with a cybersecurity partner that understands the intricacies of your business operation. At eSentire we are not only the Authority in Managed Detection and Response services, but we have successfully demonstrated the ability to protect law firms from ransomware gangs and state-sponsored actors.

We help legal firms:

1. Monitor their environments 24/7
2. Disrupt known and unknown threats
3. Stop breaches before they impact business operations
4. Avoid regulatory violations
5. Mitigate Supply Chain Risk
6. Meet Bar Requirements

Trusted Partnership and Expertise

eSentire provides Managed Risk, Managed Detection and Response and Digital Forensic and Incident Response services. Our 24/7 Cyber Analysts and Elite Threat Hunters have stopped nation states targeting law firms, identified new threats against the legal vector and discovered new attack methods. Our experts have successfully prevented ransomware gangs from shutting down operations or creating damaging public incidents for our legal customers.

eSentire is proud to protect over 14,000 attorneys in the ALM 100 and ALM 200. We work with firms of varying sizes 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 work closely with American Bar Association (ABA), Law Society, contribute to the Harvard Law School programs, and regularly offer CLE accredited courses. Our security experts are often featured in legal industry publications, and we actively share threat intelligence with the Legal Services Information Sharing and Analytics Organization (LS-ISAO).

Preventing Operational Disruption

eSentire Managed Detection and Response (MDR) services hunt threats and suspicious activity to investigate in minutes and contain these attacks before they become business disrupting for you and your clients. In numerous cases, the eSentire 24/7 Cyber Analysts have discovered instances of ransomware gangs in law firm environments and prevented them from establishing a hold. Sample support included:

- Using endpoint technologies to prevent the disabling of defenses
- Detection of malicious administrative activity through remote access tools using proprietary machine learning algorithms
- Blocked active attempts to deploy credential collection tools, malware payloaders and even multiple ransomware attacks

Avoiding regulatory violations

In addition to securing the legal sector, eSentire MDR protects over 6.5 trillion dollars in assets across highly regulated industries including investment, banking, insurance and healthcare providers. Our Security Operations Centers leverage hardened run books that include plays to manage issues and reporting for PII, PCI, HIPAA, GDPR, CCPA and even state-level regulations including the New York Department of Finance Cybersecurity Rules and Regulations (NYCRR 500). We identify and prioritize these critical assets based on regulatory requirements, and can provide forensic reporting in the case of regulatory notification.

Mitigating supply chain risk

Many breaches are often traced back to vendors. We recognize that your clients retained your firm, consider vendors an extension of your business, and therefore vendors are your responsibility to secure. We identify core services, such as document management, time tracking, file share and document signing, and prioritize these services for monitoring. Our MDR services have repeatedly caught and stopped vendor compromises before the vendor reported the vulnerability. Our Managed Risk Services provide complete security assessments, risk assessments and offer recommendations on security strategy to improve security maturity and reduce cyber risks.

Meeting Bar Requirements

Working closely with hundreds of law firms and thousands of lawyers, we understand what it takes to protect your firm and ensure that you meet competence and confidentiality requirements. Our services evolve with your practice needs as we secure changes in technology including supporting cloud adoption and making remote work secure and scalable. In addition to our Managed Detection and Response services, eSentire offers CLE-accredited user awareness training, and risk management assessments to review cloud-services, vendor risk, and virtual law firm best practices.

About Managed Detection and Response (MDR)

At eSentire, our comprehensive approach to MDR helps organizations test, mature, measure and protect their environments from a multitude of risk factors. Our MDR services rapidly identify and contain threats that bypass traditional security controls. Ingesting signals from your on-premises, cloud and hybrid environments, we combine endpoint, network, log, vulnerability and cloud data to identify known and elusive threats. Averaging 15 minutes from threat identification to containment, we ensure attackers don't have the time to achieve their objectives.

Key Challenges	How eSentire MDR Services Help
Access to Confidential Information	Our 24/7 Security Operations teams actively hunt for threats across your environment. We detect intrusions and contain attacks before they can exfiltrate data.
Operational Disruption	We detect malicious administrative activity through remote access tools and stop intrusions before they can deploy malware throughout your environment
Meeting Bar Requirements	eSentire offers CLE-accredited user awareness training and risk management assessments
Avoiding Regulatory Violations	Our SOC leverages proven run books which include plays to manage issues and reporting for PII, PCI, HIPAA, GDPR, CCPA as well as state level rules

eSentire is capable of supporting your firm with end-to-end comprehensive cybersecurity services. Our expertise includes:

Managed Risk Services

Strategic services including Vulnerability Management, Managed Phishing and Security Awareness Training to identify gaps, build defensive strategies, operationalize risk mitigation and continuously advance your security program.

Managed Detection and Response Services

We deliver complete and robust Response. By combining cutting-edge machine learning XDR, human security expertise and security operations leadership, we hunt and disrupt known & unknown threats before they impact your business.

Digital Forensics and Incident Response Services

Battle-tested Incident Commander level expertise driving incident response, remediation, recovery, and root cause analysis. Emergency Preparedness and Emergency Response services as well as industry-leading 4-hour Threat Suppression SLA with eSentire IR Retainer available.

Why Law Firms Partner with eSentire

- Decades of experience protecting law firms from ransomware and nationstate attacks
- Vested partnerships with ILTA, ALA, ABA and LS-ISAO
- Comprehensive service offering to drive the firm's security strategy and provide 24/7 support
- CLE-accredited training and risk assessments
- We understand the intricacies of the legal industry and can help you protect your business and clients

> Excellent customer service, comprehensive set of monitoring services. Innovation and improvements to existing services and continued innovation for increasing visibility.
>
> - Christopher Meinders
> *Security Manager, Baker Botts LLC*

[1] *https://www.wsj.com/articles/hackers-breach-cravath-swaine-other-big-law-firms-1459293504*
[2] *https://variety.com/2020/digital/news/entertainment-law-firm-hacked-data-breach-lady-gaga-madonna-bruce-springsteen-1234602737/*

If you're experiencing a security incident or breach contact us **1-866-579-2200**

eSENTIRE

eSentire, Inc., is The Authority in **Managed Detection and Response** Services, protecting the critical data and applications of 1000+ organizations in 70+ countries from known and unknown cyber threats. Founded in 2001, the company's mission is to hunt, investigate and stop cyber threats before they become business disrupting events. Combining cutting-edge machine learning XDR technology, human expertise, and proven security operations leadership, eSentire mitigates business risk, and enables security at scale. The Team eSentire difference means enterprises are protected by the best in the business with a named Cyber Risk Advisor, 24/7 access to SOC Cyber Analysts and Elite Threat Hunters, and industry-leading threat intelligence research from eSentire's Threat Response Unit (TRU). eSentire provides Managed Risk, Managed Detection and Response and Digital Forensic and Incident Response services. For more information, **visit www.esentire.com** and follow **@eSentire**.