SOLUTION BRIEF:

Focus on Cybersecurity: Legal

Law firms are uniquely situated within the overall cybersecurity landscape. They exist at the center of a complicated web of relationships that include major industries, governments and individuals in positions of power. For a lawyer, dealing with sensitive information is routine regardless of the type of law they are practicing. This dynamic guarantees that law firms will continue to be one of the top industry verticals targeted by threat actors.

Despite being a prime target, the legal industry has been slow to catch up to the ever-evolving threat landscape. The American Bar Association's 2019 Cybersecurity Report produced some troubling results. One in four respondents (26 percent) reported that their firm had experienced a breach within the previous year. Over half of the respondents (53 percent) from firms with over 100 attorneys claimed they were unaware if their firm had ever experienced a breach. However, the number of firms who reported having a formal cybersecurity incident response plan dropped six points from the previous year to 65 percent[1].

Juxtapose these numbers with what we know about the confidence of hackers and the concerns are amplified. Seventy-seven percent of hackers claim they are either rarely, or never detected in an environment. Sixty-two percent say they rarely or never run into an environment they can't penetrate. Additionally, hackers don't hold a high opinion of their opponents, with 74 percent believing that security teams don't know what to look for when trying to secure their networks from attacks[2].

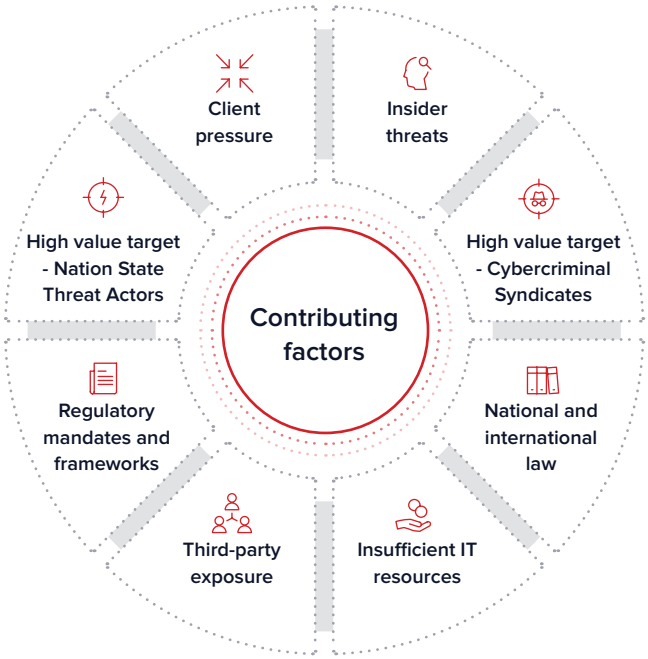
Data Breach Observations

2020 Verizon Data Breach Investigations Report

Threat Sources
- External **75%**
- Internal **22%**
- Partner **3%**
- Multiple **1%**

Threat Actor Motives
- Financial **93%**
- Espionage **8%**
- Ideology **1%**

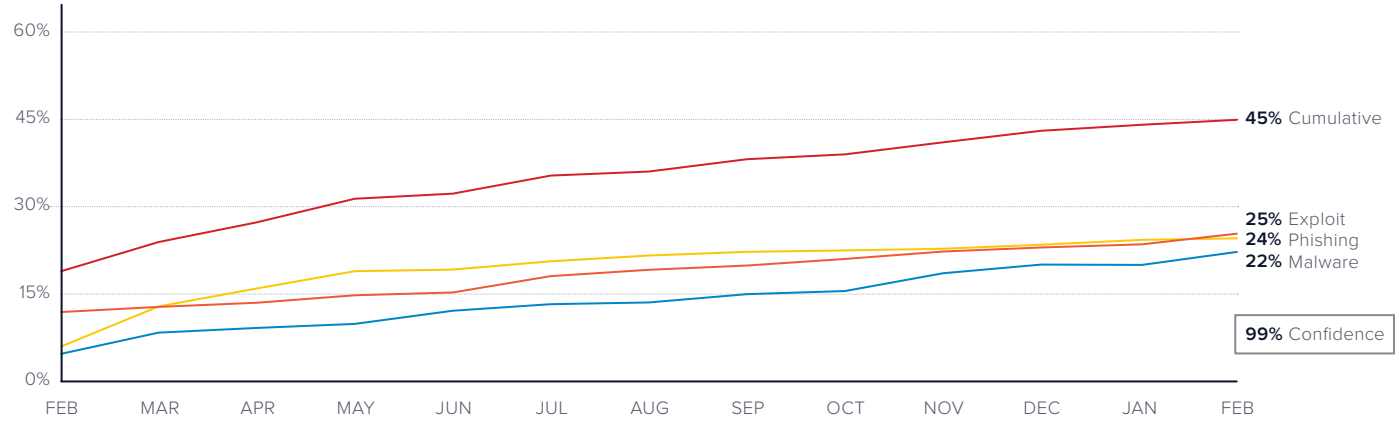
Types of Data Compromised
- Personal **75%**
- Credentials **45%**
- Other **32%**
- Internal **27%**



[1] *2019 ABA Cybersecurity Report*
[2] *2018 Nuix The Black Report*

eSentire: Observing Risks Within the Legal Industry for Two Decades

Figure 1: Observed probability of one or more security events due to a bypass of existing security controls per location.



We understand the unique cybersecurity challenges faced within the legal industry. Many of our oldest and most engaged clients are law firms, with the legal industry playing a vital role in eSentire's growth as the leader in Managed Detection and Response (MDR). Our experience and expertise in the industry results in many valuable insights from our Security Operations Center (SOC). As of May 2020, our legal clients are facing a 45 percent cumulative probability of a security event in the next 12 months (Figure 1).

Notice the difference between the terms "breach" and "event." A breach entails disruption to business and typically involves the cost factors of detection/escalation, post data breach response, notification to stakeholders and lost business according to the Cost of a Data Breach report by the Ponemon Institute. The chronology of these cost factors matters ... if a threat is swiftly and effectively addressed at the detection and escalation point, the subsequent cost factors are drastically reduced, if not eliminated completely. This is the essence of the eSentire MDR value proposition: we shrink threat actor dwell time, turning what would have been a breach into a routine security event. As mentioned earlier in reference to the ABA report, one in four law firms suffered through some form of business disruption (Figure 2). This, however, is not the case for eSentire's legal clients, who will face a malware, phishing, or exploit incident without disruption.

Figure 2: Data breach consequences for law firms

37% incident response fees	35% downtime/loss of billable hours	$178 per record lost
20% cost of replacing hardware or software	15% destruction or loss of files	$4.62M average cost of a data breach *(cost factors include notification, detection and escalation, post breach response, and lost business)*

ABA 2019 Cybersecurity Tech Report

Cloud Migration

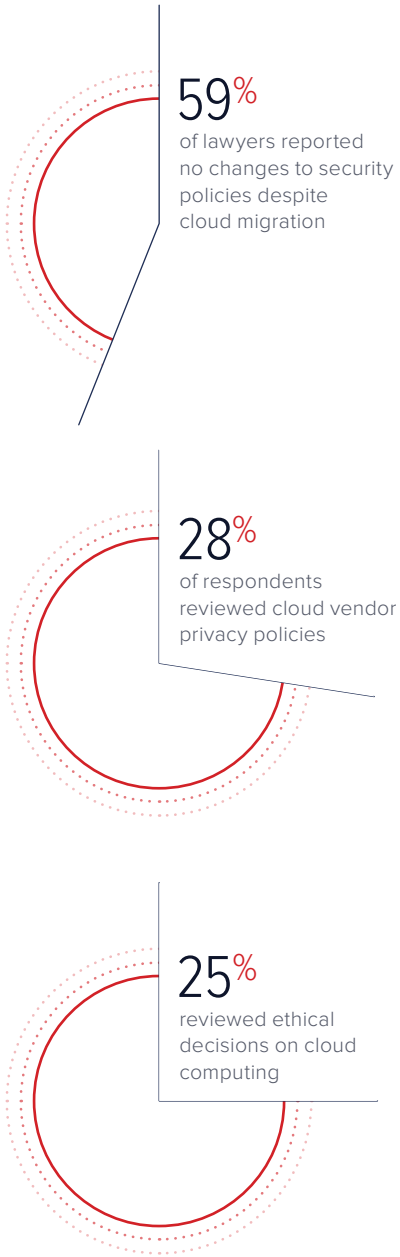
The use of cloud applications by lawyers grew to 58 percent in 2019[3]. Following the trend set in the ABA's Cybersecurity Report, it's clear that the industry has much work to do to catch up to cloud security best practices after looking at the results of their 2019 Cloud Computing Report (Figure 3).

> "Cybersecurity may be reaching a crisis point in lawyers' use of cloud services"
>
> – 2019 ABA Cloud Computing Report

On one hand, it's surprising that an industry that trades in fine print is so ill prepared from a policy standpoint. Then again, this lack of preparedness is in line with overall industry trends as the number of records exposed to poor policies and misconfigurations of cloud services rose 80 percent year-over-year from 2018-2019[4]. Threat actors no longer have to dig trenches or scale fortress walls to access your sensitive data. Today, they're walking through the front door that was left open by your IT team.

eSentire has recognized this trend and made cloud MDR a top priority. The detection and remediation of critical misconfigurations and other cloud-specific risks, in addition to the streamlining of best practices and policies, are available to legal customers within our esCLOUD solutions.

Figure 3

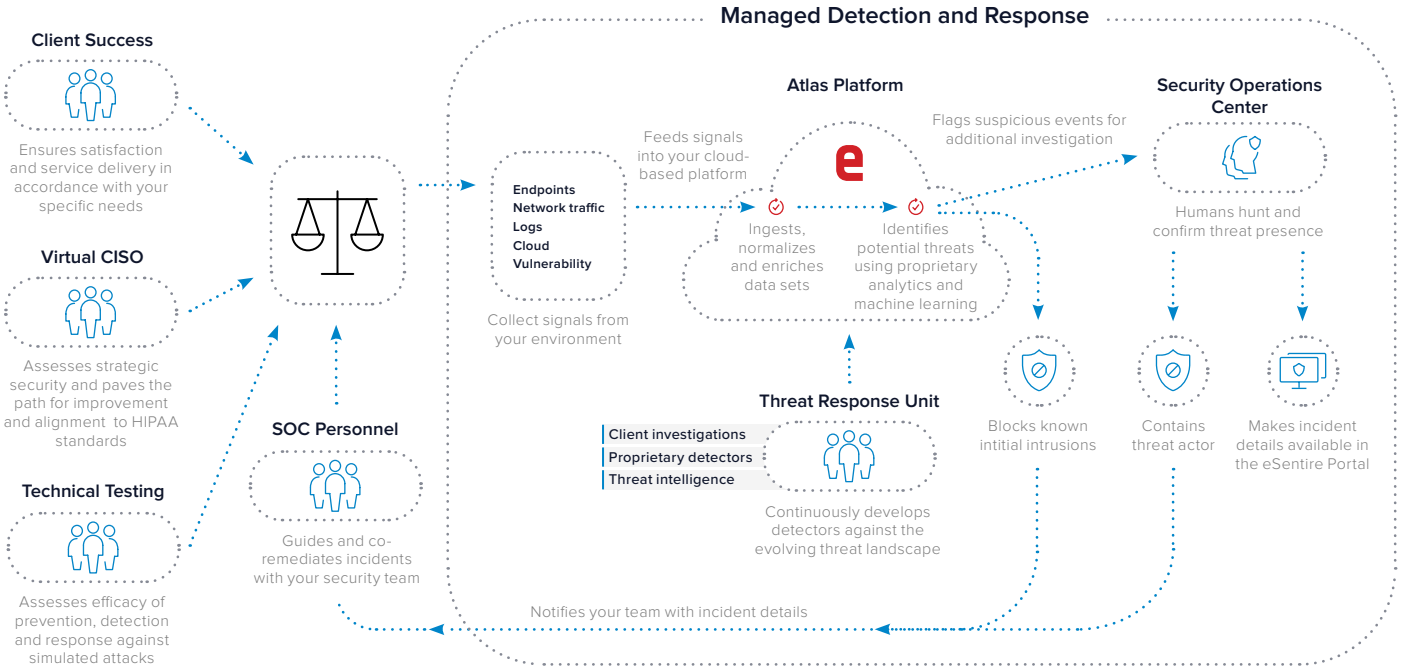


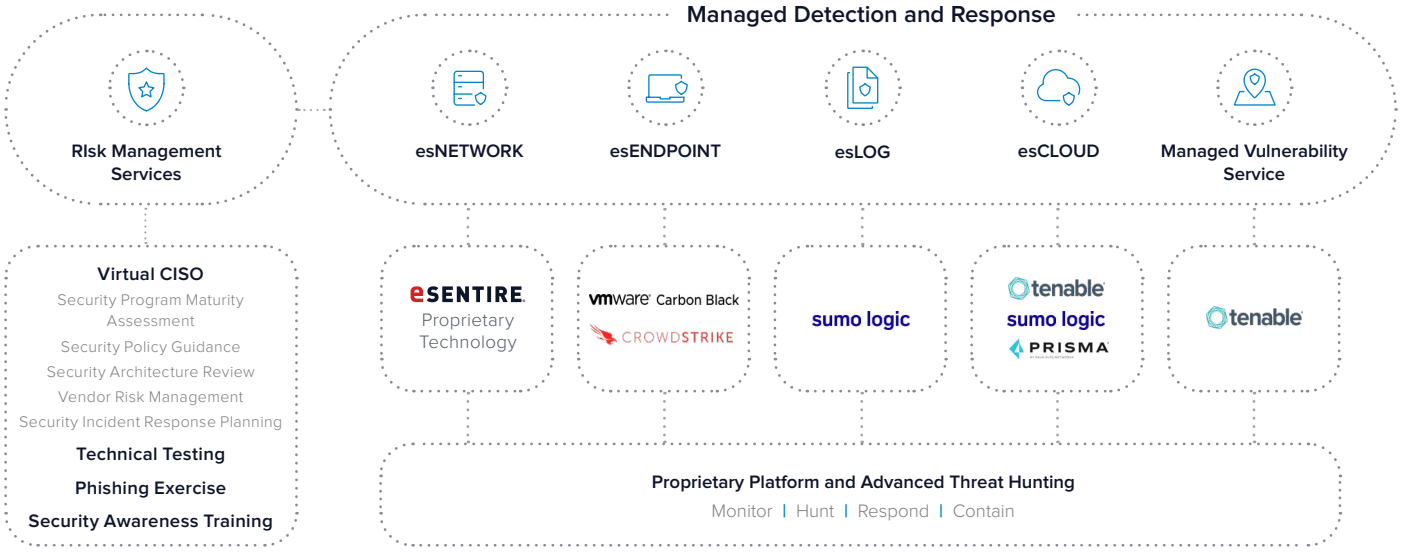
[3] *2019 ABA Cloud Computing Report*
[4] *2020 DivvyCloud Cloud Misconfigurations Report*

A Comprehensive Approach to Law Firm Protection

All law firms are a target. This isn't fear, uncertainty or doubt hyperbole, it's a statement of fact. Threat actors don't care about the size of your firm or the type of law you practice. When hit with an attack, the difference between business protection and business disruption comes down to the speed at which your firm can identify and contain threats.

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 20 minutes from identification to containment, we ensure attackers don't have the time to achieve their objectives. Our Managed Risk Programs test your existing defenses against simulated attacks, assess and measure your security posture and pave a path for resiliency that aligns to regulatory frameworks. All services are supported by a dedicated team of threat intelligence specialists focused on delivering protection in accordance with your organization's unique requirements and business objectives.





eSentire Service Alignment to Top Legal Incident Causes

	eSentire Managed Detection and Response	eSentire Managed Risk Programs

Commodity threats
• Novice threat actors (script kiddies)
• Malware
• Known
	• esNETWORK
	• esENDPOINT - Prevent
	• esLOG
	• esCLOUD
	• Managed Vulnerability Service
		• Virtual CISO
		  • Security Program Maturity Assessment
		  • Security Policy Guidance
		  • Security Architecture Review
		  • Security Incident Response Planning
		• Technical Testing

Advanced threat actors
• Cybercriminal syndicates
• Nation state
	• esNETWORK
	• esENDPOINT - Detect and Respond
	• esLOG
	• esCLOUD
	• Managed Vulnerability Service
		• Virtual CISO
		  • Security Program Maturity Assessment
		  • Security Policy Guidance
		  • Security Architecture Review
		  • Security Incident Response Planning
		• Technical Testing

Malicious insider threats	• esENDPOINT
	• esLOG
	• esCLOUD
		• Virtual CISO
		  • Security Program Maturity Assessment
		  • Security Policy Guidance
		  • Security Architecture Review
		  • Security Incident Response Planning
		  • Vendor Risk Management
		• Technical Testing

Benign/careless insider threats • Phishing • Social engineering • Misconfiguration	• esENDPOINT • esLOG • esNETWORK • esCLOUD	• Security Awareness Training • Phishing Exercise • Technical Testing

Third-party/vendor risk	• esNETWORK
	• esENDPOINT
	• esLOG
	• esCLOUD
	• Managed Vulnerability Service
		• Virtual CISO
		  • Security Program Maturity Assessment
		  • Vendor Risk Management
		• Technical Testing

Experience the eSentire Difference

Organizations worldwide trust eSentire as their first line of defense against an overwhelming threat landscape. Our 97 percent client retention rate is a testament to delivering on our core mission: a client's network can never be compromised. The specialized teams who deliver and support our services are consistently developing new defense methods that ensure your organization is protected against the latest threats.

	eSentire MDR	Pseudo MDR
24x7 always on monitoring	✓	Limited
Full spectrum visibility (PCAP, Endpoint, Log, Vulnerability, Cloud)	✓	Limited
Detection utilising signatures and IOCs	✓	✓
Detection of unknown attacks leveraging patterns and behavioural analytics	✓	Limited
Continuous elite threat hunting	✓	✗
Alerting of suspicious behaviour	✓	Limited
Alerts	✓	✓
Confirmation of true positive	✓	Limited
Remediation recommendations	✓	✓
Tactical threat containment on client's behalf	✓	Limited
24x7 investigation and SOC support	✓	✗ Need IR Retainer
Incident response plan	✓	✗ Need IR Retainer
Remediation verification	✓	✗ Need IR Retainer

EXPERIENCE AND EXPERTISE

60+
LEGAL CLIENTS

97%
CLIENT RETENTION

99%
SATISFACTION IN ONGOING OPERATIONS

30,000+
LEGAL INDUSTRY USERS PROTECTED

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

> "We have peace of mind knowing someone is watching our back during after-business hours with speed to alert, block and remediate threats."
>
> **Gary Smith,** IT Manager, *Torys LLP*

Ready to get started? We're here to help.

Reach out schedule a meeting to learn more about MDR

eSentire

eSentire, Inc., the global leader in **Managed Detection and Response (MDR)**, keeps organizations safe from constantly evolving cyberattacks that technology alone cannot prevent. Its 24x7 Security Operations Center (SOC), staffed by elite security analysts, hunts, investigates and responds in real-time to known and unknown threats before they become business disrupting events. Protecting more than $6 trillion AUM, eSentire absorbs the complexity of cybersecurity, delivering enterprise-grade protection and the ability to comply with growing regulatory requirements. For more information, **visit www.esentire.com** and follow **@eSentire**.