eSENTIRE

CHECKLIST

Legal Cybersecurity Checklist

We understand what it takes to protect your firm and ensure that you meet all cybersecurity and data privacy regulations. Our services evolve with your practice as changes in technology are ever-evolving, including supporting cloud adoption and making remote work secure and scalable.

From trade secrets to client information, you have an ethical and legal obligation to protect your firm's privileged data. Cyber-attackers who struggle to breach an organization's network more commonly see their outside counsel as an easy target.

Unfortunately, cybersecurity is an inherently difficult problem in the legal industry. Recent breaches have put third-party due diligence in the spotlight and as a result, legal firms are being held to the various regulatory obligations of their clients (e.g. HIPAA, GDPR,PCI, FINRA and SEC). And, cybersecurity isn't always top of mind, as firms naturally focus their investment on client defense, rather than cyber protection.

The evolution in new technology and cybersecurity regulations has led to the ability to select from multi-vendors in the MDR space. However, not all MDR services are equal. eSentire MDR protects over 6.5 trillion dollars in assets in highly regulated industries - like legal. 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.

To help legal firms meet client requirements, we've developed a checklist based on the six pillars laid out in The American Bar Association (ABA) Cybersecurity Handbook.

38%
of breach victims reported loss of billable hours as a consequence[1]

62%
of firms over 500 lawyers provided with cybersecurity requirements by their clients[2]

57%
YoY increase in number of legal firms that have experienced a breach[1]

3.86M
average cost of a breach[3]

[1]ABA Tech Report 2017
[2]ABA Journal March 2017
[3]2018 Cost of Data Breach Study, Phonemon

We can help you meet ABA requirements

eSentire has mapped out Managed Risk, MDR and Incident Response services for adherence to requirements.

PART 1: Cybersecurity Governance		eSentire Managed Risk Service	eSentire MDR
1.0	Cybersecurity Governance	✓	
1.A	Chief Information Security Officer or Equivalent	✓	
1.B	Cybersecurity Governance Committee (CGC)	✓	
1.C	Documented Cybersecurity Roles/Responsibilities	✓	
1.D	Documented Cybersecurity Risk Profile	✓	
1.E	Documented Cybersecurity Program	✓	
1.F	Documented Business Continuity Plan (BCP)	✓	
1.G	Documented Incident Response (IR) Plan	✓	
2.0	Classify/Inventory Information Assets	✓	
2.A	Identify Attorney-Client Data	✓	
2.B	Identify Personal Data/Identifiable Info (PD/PII)	✓	
2.C	Identify Sensitive Financial Data	✓	
2.D	Identify Transaction Records	✓	
2.E	Identify Tax Records	✓	
3.0	Map Regulatory Requirements	✓	
3.A	Map of Federal Regulations (HIPAA/GLBA) to Info Assets	✓	
3.B	Map of Jurisdictions in Which Firm/Clients Operate	✓	
3.C	Map of Federal Statutes (Appendix A)	✓	
3.D	Map of State Statutes (Appendix B)	✓	
4.0	Cyber Liability Insurance		
4.A	Documented Policy and Carrier		
4.B	First Party Loss Coverage		
4.C	Third Party Loss/Professional Liability		

PART 2: Risk Assessment		eSentire Managed Risk Service	eSentire MDR
1.0	Conduct a Risk Profile	✓	
1.A	Identify Cyber Attack Targets (Assets)	✓	
1.B	Identify Likely Cyber Attack Vectors	✓	
1.C	Identify Internal Threat Actors		✓
1.D	Identify External Threat Actors		✓
1.E	Evaluate Potential Resulting Damages	✓	

PART 2: Risk Assessment (Cont'd)		eSentire Managed Risk Service	eSentire MDR
2.0	Periodic Cybersecurity Vulnerability Assessment	✓	
2.A	Assessment Details (Who/Date)	✓	
2.B	Describe High to Critical Risks	✓	
2.C	Penetration Testing Details (Results/Date)	✓	
3.0	Periodic Physical Vulnerability Assessment		
3.A	Assessment Details (Who/Date)		
3.B	Describe High to Critical Risks		
4.0	Test Environment for New Software/Applications	✓	
4.A	Test/Dev for New Software	✓	
4.B	Test/Dev for Web Application	✓	

PART 3: Protection of Network and Data		eSentire Managed Risk Service	eSentire MDR
1.0	Risk Management Models (NIST/ISO) and Strategy	✓	
2.0	Network and Security Assets	✓	
2.A	Inventory Physical Devices and Systems	✓	
2.B	Inventory Software Platforms And Applications	✓	
2.C	First Party Loss/Professional Liability	✓	
2.D	First Party Loss Coverage	✓	
2.E	Third Party Loss/Professional Liability	✓	
3.0	Network and Information Protection Policies/Procedures	✓	
3.A	Physical Access Controls	✓	
3.B	Network Access Controls	✓	
3.C	Restricted Access/Least Privilege Access Controls	✓	
3.D	Test/Dev Environment for New Software/Apps	✓	
3.E	Controlled Baseline System Configurations	✓	
3.F	Controlled System Maintenance (Patching)	✓	✓
3.G	Controlled Removal/Disposal of Assets	✓	
3.H	Policies and Controls for Mobile/Removable Devices	✓	
3.I	Documented Policies/Controls for Data Disposal	✓	
3.J	Testing of Back-Up Systems	✓	
3.K	Periodic Compliance Audits	✓	
4.0	Data Encryption	✓	
4.A	Encrypted Data and Files	✓	

PART 3: Protection of Network and Data (Con'd)		eSentire Managed Risk Service	eSentire MDR
5.0	Remote Banking and Fund Transfers	✓	
1.A	Inventory of Financial Services Vendors	✓	
1.B	Inventory of Financial Services Vendors	✓	
1.C	Client Request and Account Validation	✓	
1.D	Policies and Procedures to Protect Financial Info	✓	
1.E	Policies to Redress Client Losses	✓	
6.0	Mobile Device Management	✓	
2.A	Strong Password Protection on Devices	✓	
2.B	Jailbroken Devices Blocked from Network	✓	
2.C	Ability to Perform a Remote Wipe	✓	

PART 4: Detection of Unauthorized Activity and Response		eSentire Incident Response	eSentire MDR
1.0	Detection of Unauthorized Activity		✓
1.A	Continuous Monitoring to Detect Cybersecurity Event		✓
1.B	Aggregation/Correlation of Logs from Multiple Sources		✓
1.C	Systems to Detect Malicious Code		✓
1.D	Network Forensics Logging		✓
1.E	Host Based Detections		✓
1.F	Host Based Forensics		✓
2.0	Incident Response	✓	✓
2.A	Documented Incident Response Protocol	✓	✓
2.B	Documented Team of First Responders	✓	✓
2.C	Documented Breach Reporting Decision Tree	✓	✓
2.D	Procedures to Determine the Scope of a Breach	✓	✓
2.E	Procedures to Remediate Breach	✓	✓
2.F	Periodic Fire Drills to Test IR Protocols and Teams	✓	✓
3.0	Threat Intelligence and Prevention		✓
2.A	Subscription to Threat Intelligence Feeds		✓
2.B	System to Whitelist and Blacklist URLs		✓

PART 5: User Testing		eSentire Managed Risk Service	eSentire MDR
1.0	User Training	✓	
1.A	Documented User Training Program	✓	
1.B	Regular Testing of Cybersecurity Awareness	✓	
1.C	Periodic Friending Attacks to Test Awareness	✓	

PART 6: Risks Associated with Vendors and Third Parties		eSentire Managed Risk Service	eSentire MDR
1.0	Cybersecurity Risk Assessment	✓	
1.A	Physical Access Controls	✓	
1.B	Network Access Controls	✓	✓
1.C	Restricted Access/Least Privilege Access Controls	✓	✓
1.D	Test/Dev Environment for New Software/Apps	✓	
1.E	Controlled Baseline System Configurations	✓	
1.F	Controlled System Maintenance (Patching)	✓	
1.G	Controlled Removal/Disposal of Assets	✓	
1.H	Policies and Controls for Mobile/Removable Devices	✓	
1.I	Documented Policies/Controls for Data Disposal	✓	
1.J	Testing of Back-Up Systems	✓	
1.K	Periodic Compliance Audits	✓	
2.0	Contract Elements Covering Cybersecurity	✓	
3.0	Segregation/Limitations to Third Party Network Access	✓	✓
4.0	Third Party Remote Maintenance Policies and Procedures	✓	
5.0	Incident Response Protocols	✓	
5.A	Documented Incident Response Protocol	✓	
5.B	Documented Team of First Responders	✓	
5.C	Documented Breach Reporting Decision Tree	✓	
5.D	Procedures to Determine the Scope of a Breach	✓	
5.E	Procedures to Remediate Breach	✓	
5.F	Periodic Fire Drills to Test IR Protocols and Teams	✓	
6.0	SSAE SOC II Security Audit and Report		

We defend against the threats facing law firms

With limited resources, it's difficult to know if you're prepared for the next big breach.

At eSentire, we work with clients ranging from small practices to the AM Law 200. Regardless of resources or a formalized security team, we work to find the right solution to ensure risk is mitigated to the firm and its clients. From managing, detecting and responding to threats in real-time to building measurable programs and policies, our goal remains the same: protect the firm and its clients from threats that traditional security technologies miss.

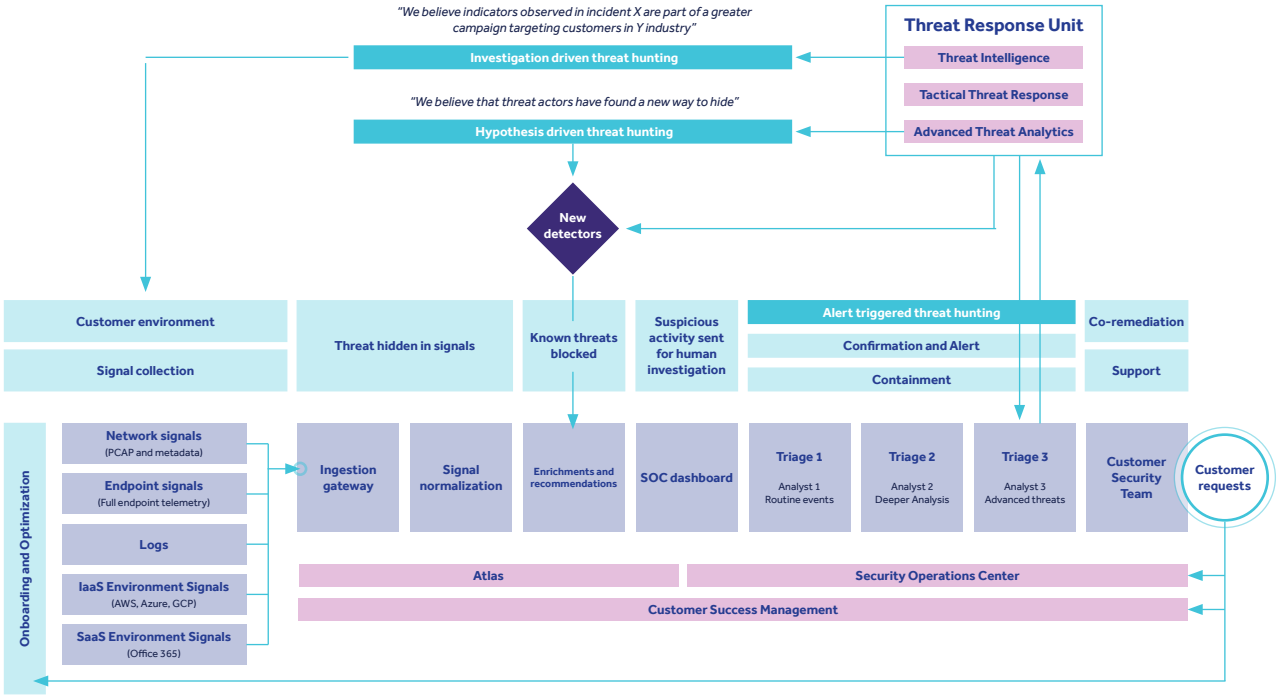
Leveraging the collective knowledge of our Threat Response Unit, security operations center, and industry-leading cybersecurity advisors, we're committed to delivering enterprise-grade protection and expert guidance on compliance to help you:

- Manage, detect and respond to threats in real-time
- Build measurable programs and policies
- Meet and exceed third-party compliance requirements
- Identify, manage and mitigate risk from vulnerabilities
- Design effective security architecture and controls

We detect the threats that other technologies miss.

The eSentire Solution

eSentire Managed Detection and Response™ (MDR) keeps organizations safe from constantly evolving cyber-attacks that technology alone cannot prevent. Our 24x7 Security Operations Center (SOC), is staffed by Elite Threat Hunters and Cyber Analysts who hunt, investigate and respond in real-time to known and unknown threats before they become business disrupting events.



eSentire Managed Detection and Response

We understand that alert fatigue is a real challenge. We support your cybersecurity program with a combination of cutting-edge machine learning XDR technology, human security expertise, and security operations leadership to mitigate your business risk, enable security at scale and drive your cybersecurity program forward.

eSentire MDR features include:

- ✔ 24x7 Always-on Monitoring
- ✔ 24x7 Live SOC Cyber Analyst Support
- ✔ 24x7 Threat Hunting
- ✔ 24x7 Threat Disruption and Containment Support
- ✔ Mean Time to Contain: 15 minutes
- ✔ Machine Learning XDR Cloud Platform
- ✔ Multi-signal Coverage and Visibility
- ✔ Automated Detections with Signatures, IOCs and IPs
- ✔ Security Network Effects
- ✔ Detections mapped to MITRE ATT&CK Framework
- ✔ 5 Machine Learning patents for threat detection and data transfer
- ✔ Detection of unknown attacks using behavioral analytics
- ✔ Rapid human-led investigations
- ✔ Threat containment and remediation
- ✔ Detailed escalations with analysis and security recommendations
- ✔ eSentire Insight Portal access and real-time visualizations
- ✔ Threat Advisories, Threat Research and Thought Leadership
- ✔ Operational Reporting and Peer Coverage Comparisons
- ✔ Named Cyber Risk Advisor
- ✔ Business Reviews and Strategic Continuous Improvement planning

Why Multi-Signal Matters

It's important to remember that MDR providers can only detect and respond to what they can see. We recommend a multi-signal approach to enlighten visibility, enhance investigation capabilities and improve containment options. The critical decisions you must address are:

- What is the scope of our attack surface now and in the future?
- What level of coverage do we require across each layer of the attack surface?
- Do we have the resources to monitor, detect and contain attackers for areas that would otherwise be uncovered by an MDR provider?

eSentire multi-signal MDR includes network, endpoint, log, cloud, vulnerability scans and behavioral sources.

Network: Protects from brute force attacks, active intrusions, unauthorized scanning and additional suspicious activity with real-time detection and response. Leverages behavioral based anomaly detection and attack pattern analysis to identify and neutralize threats traditional technologies miss. Captures summary meta data and full network packages.

Endpoint: Protects your assets from ransomware, trojans, spyware, root kits and more by combining elite threat hunting with next-generation anti-virus & endpoint detection and response capabilities to eliminate blind spots traditional prevention misses. Captures full endpoint telemetry.

Log: Ingests and stores logs across AWS, O365, DevOps and more. Aggregates meaningful and actionable intelligence from your network assets, endpoints, applications and cloud services providing critical threat visibility and detection while satisfying regulatory requirements.

Cloud: Comprehensive cloud security that identifies risks, monitors cloud platforms and stops attacks across software applications (SaaS) and cloud infrastructure (IaaS). Infrastructure as a Service available to protect AWS, Azure and GCP environments to prevent threat actors from capitalizing on misconfigurations and vulnerable environments.

Managed Vulnerability Service: MVS continuously identifies vulnerabilities across your on-premises and cloud environment with integrated eSentire experts that act as extension of your team providing analysis and remediation guidance. We schedule and execute scans, manage the platform and refine your risk profile while prioritizing and actioning remediation plans.

Behavioral Sources: Identifies malicious insider activity across unavoidable attack stages leveraging proprietary machine learning processes and elite threat hunters that contain attackers before they can disrupt business operations. Collects Netflow, Proxy and DNS Data.

eSentire MDR for Network

Real-time network threat detection and response

- **Unknown threat detection**
  Advanced anomaly detection and behavioral analytics alert and assist eSentire SOC analysts in investigating, detecting and responding to never-before-seen attacks.
- **Known-threat prevention**
  Real-time blocking of signature-based threats, including phishing, malware and botnets using thousands of rules in 40+ threat categories.
- **Full packet capture**
  Always-on full traffic capture including SSL decryption to support best-in-class forensic investigations.
- **Threat hunting**
  Dedicated threat hunters investigate unusual network signals identified by eSentire's analytics engine to ensure no threat is missed.
- **Tactical threat containment**
  Integrated mitigation capabilities that can be configured to automatically or manually "kill" TCP in real-time on your behalf.
- **Embedded incident response**
  Integrated responders perform forensic investigation, eliminate false positives and co-remediate threats with no incident retainers and no extra fees.
- **Custom rules and policies**
  Highly customizable rules and policies that adapt to your business, including executable whitelists, geo-IP and blocking access to specific sites.
- **Global threat intelligence**
  Up-to-the-minute threat protection from multiple world-renowned threat intelligence feeds.

eSentire Managed Log

Purpose-built log management for MDR

- **Log management for increased visibility, correlation and investigation**
  Collects, aggregates and monitors data across on-premises, cloud, hybrid and multi-cloud platforms like AWS, Microsoft Azure and Google Cloud.
- **Embedded threat hunting and forensic investigation**
  Embedded threat hunting and forensic investigation of aggregated log data accelerate precision and speed that facilitates rapid response and threat containment.
- **Big data and machine learning integration**
  Utilizes big data, machine learning and predictive analytics to make sense of expected and unexpected behavior across your environment with pattern, anomaly and outlier detection.
- **Real-time search and visualizations**
  Preconfigured and customizable searches and dashboards with KPIs.
- **Co-management**
  Uses a co-managed model with access to run your own advanced search queries, generate alerts, manage profiles, run reports, and investigate events alongside our SOC analysts.
- **Time to value**
  esLOG+ is a pure SaaS offering that features simple-to-deploy collectors with rich filtering capabilities that can be up and running within minutes.
- **Simplified compliance management and reporting**
  Ensures compliance mandates are met with centralized logging, continuous monitoring, and automated retention policies with various out of the box, and custom security reports that meet regulatory requirements such as HIPAA, PCI, SEC, GDPR and more.

eSentire MDR for Endpoint

Next-gen endpoint threat detection and response

- **Captures and monitors all activity**
  Continuously monitors, records, centralizes and retains activity for every endpoint in your organization.
- **Detects and scopes cyber-attacks in seconds**
  Detects unknown attacks leveraging attack patterns and behavioral analytics, not simplistic signatures or IOCs.
- **Hunts threats in real-time**
  Allows eSentire SOC analysts to hunt for known and unknown threats using advanced threat intelligence and behavioral analytics.
- **Prevents attacks from spreading**
  Locks down and isolates compromised endpoints to prevent the lateral spread of attacks.
- **Managed by 24x7 security operations centers**
  Detects, isolates and responds to threat attacks in real-time.
- **Broad, lightweight device and system support**
  Secures Mac, Linux and Windows devices for local and remote users with no performance impact to the endpoints.

Managed Risk Services

Proactively identify gaps in your security strategy and harden your defenses.
Our Managed Risk Services include:

- **Virtual CISO**
- **Penetration Testing**
- **Risk Assessments**
- **Red Team Exercises**
- **Phishing and Security Awareness Training**
- **Managed Vulnerability Service**

Managed Vulnerability Service

Find vulnerabilities before they disrupt your business with regular scanning cadences, business risk, prioritization and dedicated expertise driving continuous improvement.

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**.