Full threat visibility.
Rapid response.

eSentire
Managed Detection
and Response

SERVICES GUIDE
No matter the size, every organization is a target for cybercriminals.

But organizations that lack the cybersecurity muscle of large enterprises are among the easiest prey for cyber attackers. Using a range of methods—from simple social engineering attempts to sophisticated malware and ransomware attacks—cybercriminals can compromise a network and cause significant financial and reputational damage with alarming ease.

Traditional technologies such as firewalls, anti-virus and log management (SIEM) are a good first line of defense, but they cannot adequately protect against today’s cyber threats.

Prevention is futile unless it is tied into a detection and response capability.

— Sid Deshpande, Principal Research Analyst at Gartner

eSentire Managed Detection and Response keeps organizations safe from cyber attacks that traditional security technologies miss. Our 24x7x365 Security Operations Center (SOC), staffed by elite security analysts, hunts, investigates and responds on your behalf to known and unknown threats in real-time before they become business-disrupting events.

With a 97 percent customer retention rate, our core value has remained the same: a customer’s network can never be compromised.

We absorb the complexity of cybersecurity, delivering enterprise-grade protection against advanced threats and the ability to comply with growing regulatory requirements.

This guide provides an overview of eSentire’s comprehensive portfolio of services, detailing why our unique combination of tools, proprietary technology and expertise makes eSentire the vendor of choice to safeguard your business.
A comprehensive approach to cybersecurity

RISK ADVISORY AND MANAGED PREVENTION
- On-premises and cloud-based collectors
  - NETWORK ASSETS
  - APPLICATIONS
  - ENDPOINTS
  - ACTIVE DIRECTORY
  - IDENTITY AND ACCESS MANAGEMENT
  - CLOUD (Azure, AWS, Google Compute Platform, O365 and many more)
  - CLIENT IT/SECURITY TEAM

CLIENT

MANAGED DETECTION AND RESPONSE
- Fully managed
  - eSNETWORK
    - Inspection of network data full packet capture
  - eSENDPOINT
    - Inspection and recording of all endpoint telemetry
  - eSLOG+
    - Platform
- Co-managed

THREAT INTELLIGENCE
- Fully managed
  - Data enrichment and cross correlation of logs, PCAP and full endpoint telemetry
    - BEHAVIORAL ANALYTICS
    - MACHINE LEARNING
    - BIG DATA ANALYTICS

MANAGED DETECTION AND RESPONSE PLATFORM
- eSNETWORK
  - Inspection of network data full packet capture
- eSSENDPOINT
  - Inspection and recording of all endpoint telemetry
- eSLOG+
  - Platform

SECURITY OPERATIONS CENTER
- eSNETWORK
  - Alerts
  - Containment
  - Bi-directional communication
- eSENDPOINT
  - Co-managed remediation
- eSLOG+
  - Forensic investigation
  - Confirmation of true positive
  - Tactical threat containment
  - Co-managed remediation

SUSPICIOUS EVENTS
ANOMALIES
POTENTIAL THREATS

IDENTITY AND ACCESS MANAGEMENT
- CLIENT IT/SECURITY TEAM
See everything. Miss nothing.

Your clients, partners and regulators demand uncompromised data protection. With limited security resources and threats that are outpacing security solutions, your organization is left at risk.

At eSentire, we operate on the philosophy that every signal is potentially malicious and requires investigation until determined that it’s not. Combining purpose-built technology and human-driven hunting and analysis, eSentire Managed Detection and Response™ rapidly identifies, contains and responds to threats that evade traditional security measures. Solving for limited security resources and threats that are outpacing security solutions, eSentire mitigates the risk of a breach so you can protect your clients and partners while meeting—and exceeding—compliance mandates.

With eSentire, it’s all in. You know what you’re getting. You don’t have to worry about spending more money later on if you want additional services added. With our former provider you did, and it’s the same with the other security companies I was looking at as well.

— Investment Firm, $4.6B in Manageable Assets

Features

See everything
24x7x365 monitoring with full spectrum visibility across on-premises, cloud and hybrid IT environments.

Miss nothing
Human threat hunting with machine learning-assisted detection uncovers known and never-before-seen attacks.

Act before impact
Embedded incident response accelerates precision and speed, facilitating rapid tactical threat containment.

Harden against future attacks
Root cause investigation and remediation guidance defines corrective actions to harden security postures against evolving threats.

Full spectrum visibility

Whether on-premises, in the cloud, or somewhere in between, eSentire esNETWORK, esENDPOINT, esLOG+ and our 24x7x365 threat hunters work together to stay ahead of evolving threats.

esNETWORK
esENDPOINT
esLOG+
eSentire esNETWORK™

Real-time network threat detection and response

esNETWORK captures and analyzes all network traffic to support real-time detection and response to both known and unknown cyber threats. esNETWORK’s threat intelligence, black-listing and IPS/IDS functionality detect and block known threats. Its advanced behavior-based anomaly detection alerts and assists eSentire SOC analysts with hunting down, investigating and containing attacks that have bypassed all other security controls.

- **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.

---

## MANAGED DETECTION AND RESPONSE

<table>
<thead>
<tr>
<th>Others</th>
<th>eSentire MDR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always-on continuous monitoring</td>
<td>✔</td>
</tr>
<tr>
<td>Real-time inspection of every packet utilizing full packet capture</td>
<td>Limited</td>
</tr>
<tr>
<td>Detection utilizing signatures and IOCs</td>
<td>☐</td>
</tr>
<tr>
<td>Detection of unknown leveraging patterns and behavioral analytics</td>
<td>Limited</td>
</tr>
<tr>
<td>Active threat hunting</td>
<td>Limited</td>
</tr>
<tr>
<td>Full forensic analysis to confirm threat and eliminate false positives</td>
<td>Requires an IR retainer</td>
</tr>
<tr>
<td>Alerting of suspicious behavior</td>
<td>Limited</td>
</tr>
<tr>
<td>Alerting of confirmed threats</td>
<td>✔</td>
</tr>
<tr>
<td>Tactical threat containment on client’s behalf via TCP disruption</td>
<td>✗</td>
</tr>
<tr>
<td>Remediation recommendations</td>
<td>✗</td>
</tr>
<tr>
<td>Full support until incident is remediated and threat actor is eliminated</td>
<td>Requires an IR retainer</td>
</tr>
</tbody>
</table>
eSentire esENDPOINT™

Next-gen endpoint threat detection and response

esENDPOINT powered by Carbon Black™ eliminates blind spots, providing continuous next-gen endpoint detection and response capabilities that assist eSentire SOC analysts in hunting, investigating and containing attacks.

- **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.

<table>
<thead>
<tr>
<th></th>
<th>Others</th>
<th>eSentire MDR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continuous monitoring, recording and centralizing activity</td>
<td>Limited</td>
<td>✔</td>
</tr>
<tr>
<td>Detection utilizing signatures and IOCs</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Detection of unknown leveraging patterns and behavioral analytics</td>
<td>Limited</td>
<td>✔</td>
</tr>
<tr>
<td>Active threat hunting</td>
<td>Limited</td>
<td>✔</td>
</tr>
<tr>
<td>Full forensic analysis to confirm threat and eliminate false positives</td>
<td>Requires an IR retainer</td>
<td></td>
</tr>
<tr>
<td>Alerting of suspicious behavior</td>
<td>Limited</td>
<td>✔</td>
</tr>
<tr>
<td>Alerting of confirmed threats</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Tactical threat containment on client’s behalf via host isolation to stop lateral spread</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Remediation recommendations</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Full support until incident is remediated and threat actor is eliminated</td>
<td>Requires an IR retainer</td>
<td></td>
</tr>
</tbody>
</table>
esLOG+™

Critical visibility accelerating detection across modern hybrid IT environments

esLOG+ is a co-managed SIEM solution designed to extract meaningful and actionable intelligence from on-premises and cloud assets that accelerates targeted threat hunting and rapid response empowering our SOC analysts to stop attackers before they can become business disrupting.

- **Cross-platform monitoring and visibility**
  Collects, aggregates and monitors data across on-premises, cloud, multi-cloud, and hybrid platforms like AWS, Microsoft Azure and the Google Cloud Platform.

- **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.

---

**Managed Detection and Response**

<table>
<thead>
<tr>
<th>Others</th>
<th>eSentire MDR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring</td>
<td></td>
</tr>
<tr>
<td>24x7 monitoring</td>
<td>☑</td>
</tr>
<tr>
<td>Incident investigation and management</td>
<td></td>
</tr>
<tr>
<td>Threat hunting</td>
<td>☑</td>
</tr>
<tr>
<td>Forensics and investigation</td>
<td>☑</td>
</tr>
<tr>
<td>Correlation with full endpoint telemetry*</td>
<td>☑</td>
</tr>
<tr>
<td>Correlation with PCAP data from the network*</td>
<td>☑</td>
</tr>
<tr>
<td>False positive elimination</td>
<td>☑</td>
</tr>
<tr>
<td>Alerts</td>
<td>☑</td>
</tr>
<tr>
<td>Tactical threat containment: host*</td>
<td>☑</td>
</tr>
<tr>
<td>Tactical threat containment: network*</td>
<td>☑</td>
</tr>
<tr>
<td>Response plan</td>
<td>☑</td>
</tr>
<tr>
<td>Remediation guidance</td>
<td>☑</td>
</tr>
<tr>
<td>Reporting</td>
<td></td>
</tr>
<tr>
<td>Daily log review for PCI</td>
<td>☑</td>
</tr>
<tr>
<td>Monthly reporting (system generated)</td>
<td>☑</td>
</tr>
<tr>
<td>Creation/maintenance of standard reports</td>
<td>☑</td>
</tr>
<tr>
<td>Creation/maintenance of customized reports</td>
<td>☑</td>
</tr>
<tr>
<td>Compliance report creation/updates</td>
<td>☑</td>
</tr>
<tr>
<td>Report validation and review</td>
<td>☑</td>
</tr>
</tbody>
</table>

*Requires esNETWORK and/or esENDPOINT
eSentire Risk Advisory and Managed Prevention

eSentire Risk Advisory and Managed Prevention continuously identifies blind spots, builds a strategy around risk and operationalizes capabilities to predict and prevent known threats. Complimentary to our Risk Advisory and Managed Prevention suite of services, eSentire Managed Detection and Response (MDR) hunts and responds to the unknown. As a result, your security function is able to measure success over time and becomes adaptable to business performance drivers and the evolving threat landscape without increased risk or gaps in compliance mandates.
eSentire Risk Advisory

Trusted expertise, customized for your organization.

Part of our service portfolio, eSentire Risk Advisory provides security expertise only time in the trenches can forge, delivering valuable insights and strategic direction to all levels of your business, from the IT department to the boardroom. With Risk Advisory Services, you have instant access to dedicated experts who work with you to build and mature your cybersecurity program, conduct security testing to ensure efficacy of your technical controls, and perform advanced Risk Assessments.

vCISO

eSentire’s vCISO portfolio provides dedicated security experts to assess risks, develop cybersecurity roadmaps to address known gaps and build a comprehensive program that meets your industry and business requirements, today and tomorrow.

- **Security Program Maturity Assessment**
  Security Program Maturity Assessment (SPMA) is the foundation for the vCISO program, providing in-depth assessment of the client’s information technology environment maturity.

- **Security Incident Response Planning**
  Security Incident Response Planning (SIRP) develops a focused and pragmatic plan that identifies key steps to take when a security event happens.

- **Penetration Test (Wireless, Web App, Mobile)**
  Simulates actions of an attacker. Using the latest tactics, techniques and procedures, penetration tester attempts to infiltrate and exploit systems and gain access to data. Exercise results in identification of systematic weaknesses with areas of remediation ranked by criticality.

- **Vulnerability Assessment**
  A point-in-time exercise utilizing a scanning tool that deliberately probes a network or system to discover weaknesses. Results analyzed by security experts and prioritized by severity with remediation guidance.

- **Security Policy Review and Guidance**
  A fully realized Information Security Program that provides specific best practices for policies and procedures based on the eSentire Security Framework and NIST Cybersecurity Framework.

- **Security Architecture Review**
  Reviews technologies currently in use by your organization and provides detailed security controls and audit assessment criteria to secure the system.

- **Risk Assessment**
  Identifies risk across four key areas: organizational, programmatic (security), human and technical. Leveraging intelligence from our MDR platform, we identify and organization’s risk measured via assessments against industry standard frameworks, technical testing, phishing and malicious network activity monitoring.

- **Vulnerability Assessment**
  A point-in-time exercise utilizing a scanning tool that deliberately probes a network or system to discover weaknesses. Results analyzed by security experts and prioritized by severity with remediation guidance.

- **Security Architecture Review**
  Reviews technologies currently in use by your organization and provides detailed security controls and audit assessment criteria to secure the system.

- **Red Team**
  Combines various techniques to evade detection and prevention capabilities, including OSINT, phishing and other physical and network attack tactics. Results in assessment of prevention, detection and response capabilities. Identifies areas of greatest risk and remediation recommendations.
Managed Endpoint Defense

Next-gen prevention. Continuous threat adaptation.

Managed Endpoint Defense, powered by Carbon Black™ Defense and eSentire security experts, delivers next-generation endpoint threat prevention with continuous adaptation and hardening against your evolving threat landscape.

- **Market-leading next-generation antivirus solution**
  Full visibility into what is happening on your endpoints with advanced detection capabilities powered by CB Defense.

- **Rapid deployment**
  Dedicated eSentire experts work with you to speed deployment and tailor initial policies contextual to your unique security requirements.

- **Continuous adaptation and hardening**
  Ongoing, consultative tuning and refinement of rules and policies that results in a continuous hardened state of endpoint defense.

- **Threat intelligence integration**
  Global threat intelligence integration with eSentire Managed Detection and Response that catches threats traditional technologies miss.

- **Automated blocking**
  Stops advanced and file-less attacks with automated blocking to prevent business disruption.

- **Integrated behavioral and cloud-based reputation**
  Identifies deceptive threats and stops suspicious behavior.

- **Attack prevention**
  Locks down and isolates compromised endpoints to prevent lateral spread.

<table>
<thead>
<tr>
<th></th>
<th>DIY</th>
<th>Managed Endpoint Defense</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial agent deployment</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Initial configuration (rules and policies)</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>24x7 monitoring</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Malware, exploit and ransomware prevention</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Configurable tool, tactics and procedure blocking</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Merge and manage the signal set into a standard configuration</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Refinements and updates to account for client’s specific environment</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Basics forensics post incident</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>DIY quarantine and isolation</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Alerting of suspicious behavior</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Alerting of confirmed threats</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>False positive reduction</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>False positive elimination</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Co-managed remediation</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Host reimaging</td>
<td>☑</td>
<td>☑</td>
</tr>
</tbody>
</table>
eSentire esRECON™

Integrated MDR vulnerability scanning

esRECON is a fully managed vulnerability management service that scans your entire infrastructure—servers, databases, endpoints and web applications—to discover security vulnerabilities that can be exploited by threat actors. eSentire experts deliver actionable insight, guidance and prioritization of remediation and patching efforts to keep your organization safe.

- **World-class vulnerability scanning**
  Coverage for over 80,000+ vulnerability checks including web applications, databases, Unix, Windows and Mac to provide the industry’s most comprehensive, continuous vulnerability detection.

- **Managed by cybersecurity experts**
  Fully monitored, maintained and delivered as a service by our cybersecurity experts who provide vulnerability triage, remediation advice and consultation specific to your business.

- **Continuous visibility**
  Provides a constant view into your vulnerability posture that provides guidance for network/system configuration and controls.

- **Advanced reporting**
  Ensures actionable insights that fit your remediation processes including various reports for external and internal critical findings are sent following each scan.

- **Expert assistance**
  Scheduled reviews with eSentire experts for additional actionable insight into your security posture.

- **In-depth results**
  Credentialed scans allow for in-depth checks that use Server Message Block (SMB) and Windows Management Instrumentation (WMI) to review the specific patches that are installed on each device.

- **External critical vulnerability notifications**
  The esRECON team will reach out if a critical vulnerability is detected on your external network to ensure that patching can take place as soon as possible.

<table>
<thead>
<tr>
<th></th>
<th>DIY</th>
<th>Typical Provider</th>
<th>esRECON</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sourcing, set up and maintenance of product completed for you</td>
<td>☑️</td>
<td>Costs extra</td>
<td>☑️</td>
</tr>
<tr>
<td>Product and per seat licensing renewals</td>
<td>Not included</td>
<td>Included</td>
<td>Included</td>
</tr>
<tr>
<td>Advertising, interviewing and hiring knowledgeable staff to manage scanning</td>
<td>Required</td>
<td>Not required</td>
<td>Not required</td>
</tr>
<tr>
<td>Ad-hoc scans for remediation and new threat detection</td>
<td>☑️</td>
<td>Costs extra</td>
<td>☑️</td>
</tr>
<tr>
<td>Comprehensive reporting for all audiences</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
</tr>
<tr>
<td>Threat intelligence team to research new vulnerabilities and recommend remediation and mitigation options</td>
<td>☑️</td>
<td>Costs extra</td>
<td>☑️</td>
</tr>
<tr>
<td>Professional managed risk analysis and prioritization advice</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
</tr>
<tr>
<td>Monthly review calls with knowledgeable information security consultants</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
</tr>
<tr>
<td>Proactive notification of external critical vulnerabilities included</td>
<td>☑️</td>
<td>Costs extra</td>
<td>☑️</td>
</tr>
<tr>
<td>Immediate delivery of comprehensive scan reports</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
</tr>
</tbody>
</table>
Adoption of the term ‘MDR’ by MSSPs should be met with healthy skepticism by buyers, as Gartner has observed increasing use of the term in the last 12 months. In some situations, the use of the term is legitimately warranted. In other cases, there is little evidence that a service is really aligned to the characteristics defined in this note.

— Gartner, June 2018

The eSentire Difference

Our core value is simple: A customer’s network can never be compromised.

A solution for every need

- **SECURITY:** Ransomware Protection | Unknown Cyber Threat Protection | Insider Threat Detection | 24x7 Security Monitoring

- **INDUSTRY:** Financial Services | Hedge Funds | Legal | Healthcare | Manufacturing | Transportation | Energy

- **COMPLIANCE:** ABA | FCA | FINRA | GDPR | HIPAA | NERC | NERCRR | OEB | OSFI | SEC | SIFMA | SRA

Adoption of the term ‘MDR’ by MSSPs should be met with healthy skepticism by buyers, as Gartner has observed increasing use of the term in the last 12 months. In some situations, the use of the term is legitimately warranted. In other cases, there is little evidence that a service is really aligned to the characteristics defined in this note.

— Gartner, June 2018

See what you’re missing

eSentire Managed Detection and Response keeps organizations safe from cyberattacks that traditional security technologies miss.

Contact us to discuss your cybersecurity and compliance needs, or learn more at [www.eSentire.com](http://www.eSentire.com).
eSentire is the largest pure-play Managed Detection and Response (MDR) service provider, keeping organizations safe from constantly evolving cyber-attacks 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 $5.7 trillion AUM in the financial sector alone, 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.