Full threat visibility.
Rapid response.

eSentire Managed Detection and Response

SERVICES GUIDE

eSENTIRE

Cybersecurity starts here

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

Organizations that lack the cybersecurity muscle of large enterprises are among the easiest prey for cyberattackers. 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 are a good first line of defense, but they cannot adequately protect against today's threats.

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

– Sid Deshpande, Principal Research Analyst at Gartner

Gartner

Gartner Press Release, Gartner Says Detection and Response is Top Security Priority for Organizations in 2017, March 14, 2017. http://www.gartner.com/newsroom/id/3638017

We can help

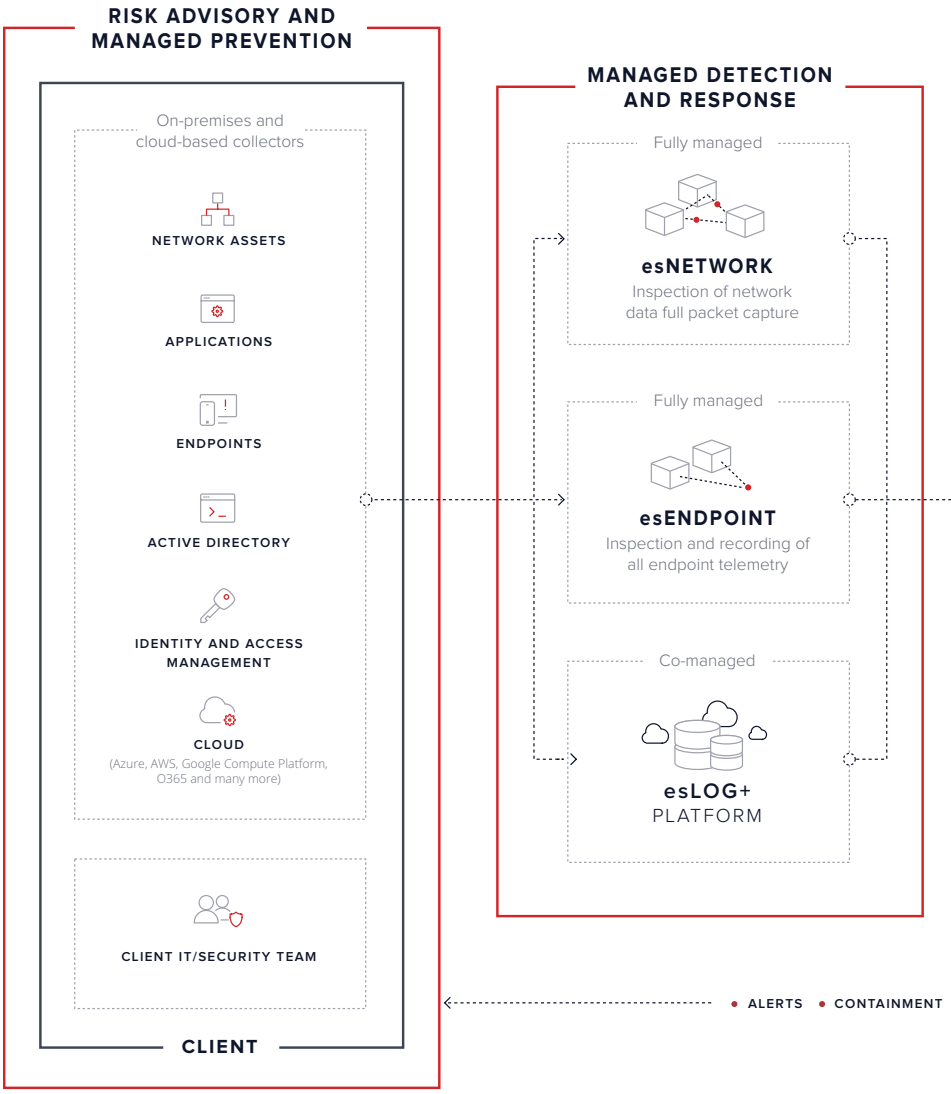
eSentire Managed Detection and Response (MDR) keeps organizations safe from cyberattacks that traditional security technologies miss. Our 24x7x365 Security Operations Center (SOC), staffed by elite security analysts, hunts, investigates and responds on your behalf to known and unknown threats in real-time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



THREAT INTELLIGENCE

MANAGED DETECTION AND RESPONSE PLATFORM

Data enrichment and cross correlation of logs, packet capture (PCAP) and full endpoint telemetry

- BEHAVIOURAL ANALYTICS
- MACHINE LEARNING
- BIG DATA ANALYTICS

SUSPICIOUS EVENTS

ANOMALIES

POTENTIAL THREATS

SECURITY OPERATIONS CENTER

- FORENSIC INVESTIGATION
- CONFIRMATION OF TRUE POSITIVE
- TACTICAL THREAT CONTAINMENT
- CO-MANAGED REMEDIATION

- BI-DIRECTIONAL COMMUNICATION

eSentire Managed Detection and Response™

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 is not. Combining purpose-built technology and human-driven hunting and analysis, eSentire Managed Detection and Response™ (MDR) 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 mangeable assets

Features

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

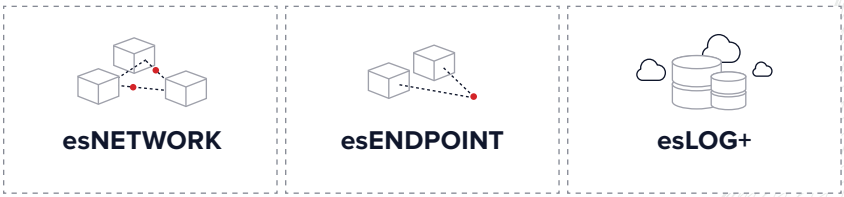
Miss nothing
Human threat hunting with machine learning-assisted detection uncovers known and never-before-seen attacks.

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.



MANAGED DETECTION AND RESPONSE

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 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

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

MANAGED DETECTION AND RESPONSE

eSentire esENDPOINT™

Next-generation endpoint threat detection and response.

esENDPOINT powered by Carbon Black™ eliminates blind spots, providing continuous next-generation 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 cyberattacks 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

	Others	eSentire MDR
Continuous monitoring, recording and centralizing activity	Limited	✓
Detection utilizing signatures and IOCs	✓	✓
Detection of unknown leveraging patterns and behavioral analytics	Limited	✓
Active threat hunting	Limited	✓
Full forensic analysis to confirm threat and eliminate false positives	Requires an IR retainer	✓
Alerting of suspicious behavior	Limited	✓
Alerting of confirmed threats	✓	✓
Tactical threat containment on client's behalf via host isolation to stop lateral spread	✗	✓
Remediation recommendations	✓	✓
Full support until incident is remediated and threat actor is eliminated	Requires an IR retainer	✓

eSentire 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 disrupt your business.

- **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 precise and 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 Software as a Service (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

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

**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

IDENTIFY

Test your defenses.
Illuminate blind spots.
Determine risk.

BUILD

Establish your baseline.
Build a strategy.
Define your plan.

MEASURE

Reevaluate defenses.
Assess progress.
Refine your approach.

PROTECT

Prevent what you can.
Detect what you can't.
Respond swiftly.

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 Virtual CISO (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 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 National Institute of Standards and Technology (NIST) Cybersecurity Framework.

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.

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

Technical Testing

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 priority.

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.

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

Security Architecture Review
Tests end users through customized simulated phishing engagements. Users that present potential risks via exploitation of the human element are identified and remediation guidance is provided to implement into security awareness programs.

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 PREVENTION

Managed Endpoint Defense

Next-generation prevention. Continuous threat adaptation.

Managed Endpoint Defense, powered by CB 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 MDR that catches threats traditional technologies miss
- **Automated blocking**
  Stops advanced and fileless 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

	DIY		Managed Endpoint Defense	
	CB Defense Standalone	Client Responsibility / Action Required	eSentire	Client Responsibility / Action Required
Initial agent deployment		✓		✓
Initial configuration (rules and policies)		✓	✓	
24x7 monitoring		✓	✓	✓
Malware, exploit and ransomware prevention	✓		✓	
Configurable tool, tactics and procedure blocking	✓		✓	
Merge and manage the signal set into a standard configuration		✓	✓	
Refinements and updates to account for client's specific environment		✓	✓	✓
Basics forensics post incident		✓	✓	
DIY quarentine and isolation		✓		✓
Alerting of suspicious behavior		✓	✓	✓
Alerting of confirmed threats		✓	✓	✓
False positive reduction	✓		✓	
False positive elimination		✓	✓	✓
Co-managed remediation		✓	✓	✓
Host reimaging		✓		✓

MANAGED PREVENTION

eSentire Managed Vulnerability Service

Comprehensive vulnerability management. Rapid risk reduction.

eSentire Managed Vulnerability Scanning identifies asset vulnerabilities with unsurpassed accuracy across traditional and dynamic IT assets. Our cybersecurity experts act as an integrated extension of your team providing analysis, guidance and prioritization of risk contextual to your business.

- **Comprehensive visibility**

  Industry-leading IT asset coverage with scanning available for more than 109,000 vulnerabilities

- **Elastic license model**

  Assets-based licensing built for dynamic and quickly changing environments that consumes a single license unit per asset, even if the asset has multiple IP addresses

- **Dynamic asset tracking**

  Group and classify assets in a single pane of glass with attributes beyond IP addresses to more accurately identify and prioritize new and existing vulnerabilities

- **Business contextual risk prioritization**

  eSentire dedicated Managed Vulnerability Service experts provide risk prioritization and guidance specific to your unique business context

- **Executive and technical reporting**

  Custom executive and detailed summary reporting available for technical and non-technical audiences

- **Regulatory requirement reporting**

  Pre-built compliance reporting and dashboards for multiple security frameworks including PCI, NIST, ISO and CIS

- **Continuous optimization and focused guidance**

  eSentire dedicated Managed Vulnerability Service experts become a genuine extension of your team providing end-to-end management that optimizes the vulnerability management lifecycle including remediation guidance, verification, scan quality assurance and weekly communication on newly discovered vulnerabilities

- **Co-managed flexibility**

  Full system access and flexibility to run your own customized scans and reporting alongside eSentire's dedicated Managed Vulnerability Service experts

- **Web application scanning (Add On)**

  Safely and accurately scan your web application portfolio without the worry of performance latency or disrupting your development team

- **PCI approved scanning vendor solution (add on)**

  Streamline and comply with quarterly scanning requirements required by PCI 11.2.2

	DIY	Typical Service Provider	eSentire
Recruiting, retaining and dedicating knowledgeable IT security staff to manage and analyze scans	Required	Not Required	Not Required
Comprehensive pre-built and customized reporting for various audiences (executive, technical, regulatory)	✗	✓	✓
Sourcing, set-up, platform maintenance	✓	✓	✓
Ad hoc scanning	✓	Extra Cost	✓
Ongoing vulnerability prioritization contextual to evolving business risk profile	✗	Extra Cost	✓
Scan accuracy verification and continuous optimization accounting for changing IT environment	✗	Extra Cost	✓
Ongoing threat intelligence communications on emerging vulnerabilities	✗	Extra Cost	✓

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 | NYCRR | 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

Gartner

	Others	eSentire MDR
24x7 always-on monitoring	✓	✓
Detection using signatures and IoCs	✓	✓
Alerts	✓	✓
Remediation guidance	✓	✓
Detection of unknown leveraging patterns, behavioral analytics, machine learning and artificial intelligence	Limited	✓
Human threat hunting	Limited	✓
False positive reduction	Limited	✓
Response plan for particular incident	Limited	✓
Endpoint tactical threat containment performed on client's behalf	Varies	✓
Endpoint visibility (Full telemetry)	Varies	✓
Log visibility (on-premises and cloud)	Varies	✓
Network visibility utilizing full PCAP	Varies	✓
Ability to correlate endpoint, network (PCAP) and log data into investigations	✗	✓
Alerting of suspicious behavior	✗	✓
Network tactical threat containment performed on client's behalf	✗	✓
Remediation verification	✗	✓

See what you are 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**.

eSentire

eSentire, 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 $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.**