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.

But organizations that lack the cybersecurity muscle of the largest 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. If you want to get serious about cybersecurity, you must combine prevention efforts with detection and response.

> 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™ keeps organizations safe from constantly evolving cyber attacks that technology alone cannot prevent. Our 24x7x365 Security Operations Center (SOC), staffed by elite security analysts, hunts, investigates and responds to known and unknown threats in real-time before they become business-disrupting events.

eSentire is the world's largest pure-play Managed Detection and Response (MDR) service provider. We've pioneered the space and have been protecting organizations from cyber attacks for the last 17 years. With a 97 percent customer retention rate and rave reviews across every industry, **our core value is simple: a customer's network can never be compromised.**

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

This guide provides an overview of eSentire Managed Detection and Response services, detailing why our unique combination of tools, proprietary technology and expertise makes eSentire the MDR provider of choice.

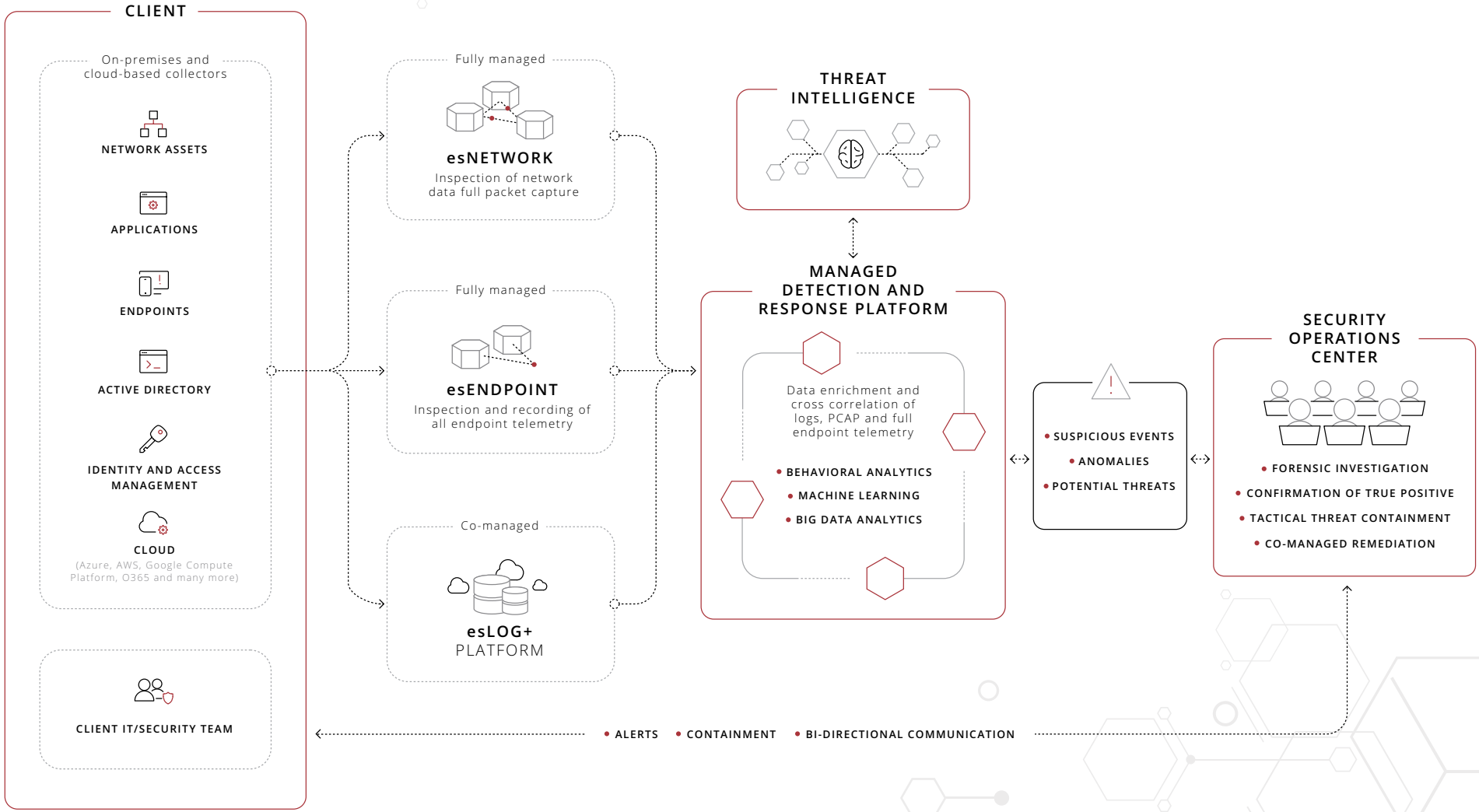
SC 2017 awards Winner

500™ Technology Fast 500 2017 NORTH AMERICA Deloitte.

50™ Technology Fast 50 2017 CANADA Deloitte.

A Better Approach to Cybersecurity

eSentire Managed Detection and Response produces full-spectrum visibility accelerating targeted threat hunting and response across today's modern hybrid IT environments.

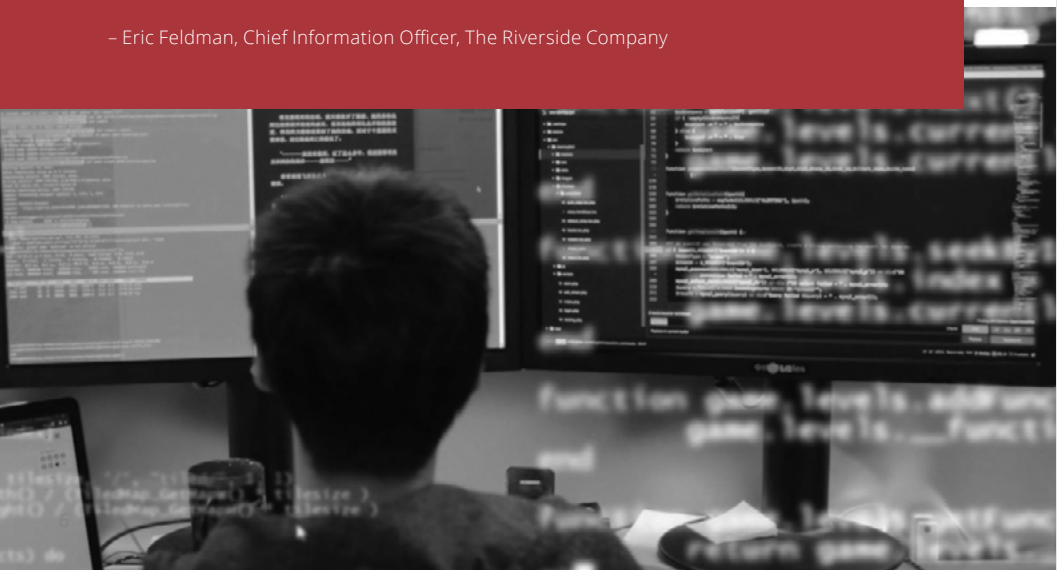


eSentire esNETWORK™

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.

> The combination of tools, technology and eSentire's Security Operations Center means that we have eyes and ears on our network at all times. We consider eSentire as an extension of our team.
>
> – Eric Feldman, Chief Information Officer, The Riverside Company



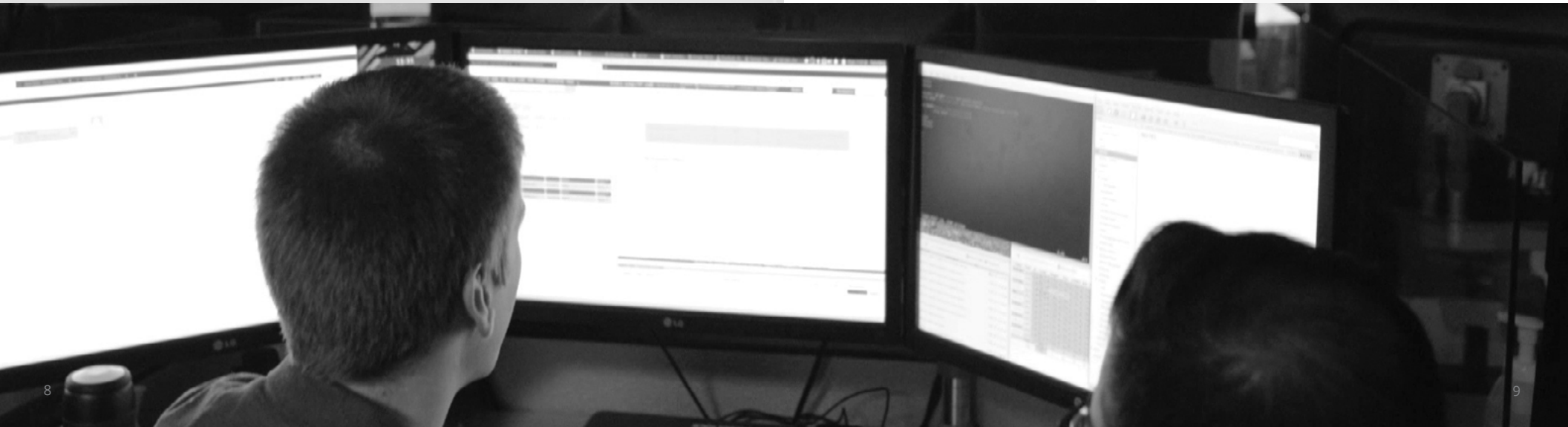
- **Unknown Threat Detection**
  Advanced anomaly detection and behavioral analytics alert and assist eSentire SOC analysts in investigating, detecting and responding to never-before-seen attacks.
- **Known-threat Prevention**
  Real-time blocking of signature-based threats, including phishing, malware 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.
- **Custom Rules & 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.
- **Targeted Retrospection**
  Allows eSentire SOC analysts to "travel back in time" to assess if a newly-discovered breach had any damaging impact on the network in the past (with eSentire TRAP™ Add-On Module).

eSentire esENDPOINT™

Next-gen endpoint threat detection and response

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

- **Captures & Monitors all Activity**
  Continuously monitors, records, centralizes and retains activity for every endpoint in your organization.
- **Detects & 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 with always-on 24x7 service.
- **Broad, Lightweight Device & System Support**
  Secures Mac, Linux and Windows devices for local and remote users with no performance impact to the endpoints.



eSentire esLOG+™

Critical visibility accelerating detection across modern hybrid IT environments

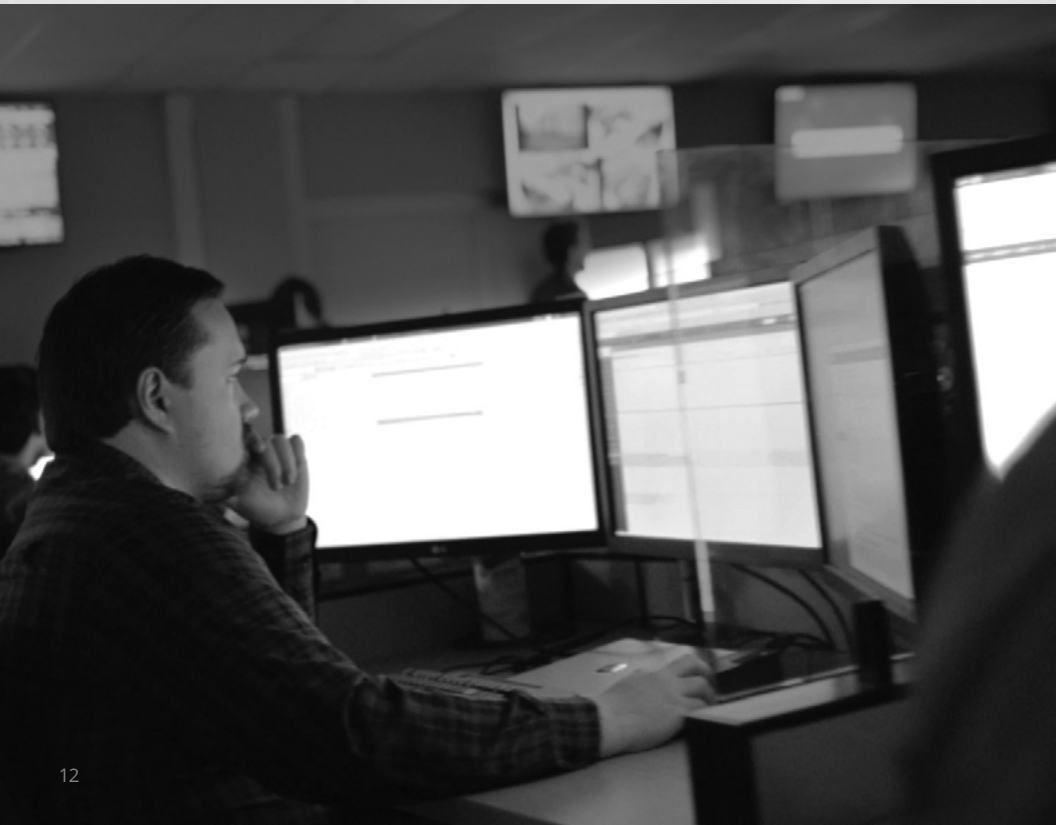
esLOG+ is a co-managed SIEM solution designed to extract meaningful and actionable intelligence from on premises and cloud assets that accelerates targeted threat hunting and rapid response empowering our SOC analysts to stop attackers before they can become business disrupting.

- **Cross-Platform Monitoring and Visibility**
  Collects, aggregates and monitors data across on-premises, cloud, multi-cloud, and hybrid platforms like AWS, Microsoft Azure, Apache, and the Google Cloud Platform providing our 24x7x365 Security Operations Center analysts with critical visibility to threats across your entire threat landscape.
- **Embedded Threat Hunting and Forensic Investigation**
  Includes embedded threat hunting and forensic investigation of aggregated log data to accelerate precision and speed that facilitates rapid response and threat containment.
- **Big Data Analytics**
  Leverages the power of big data and advanced analytics to end-user behavior, to detect anomalies (deviations from the established baseline) and to flag exceptions to identify real and potential threats.
- **Machine Learning Integration**
  Utilizes 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, giving our SOC analysts and your security team visibility into abnormal behaviors illuminating what matters most.
- **Log Retention**
  Retains all raw log data giving SOC analysts the ability to correlate information with data from esENDPOINT and esNETWORK to conduct thorough forensic investigations, drill down into details and assist with root cause analysis on any security incident.
- **False Positive Elimination**
  Increases the velocity and accuracy of threat detection so our SOC analysts can determine what is noise vs. true security events to ensure your team is only alerted to verified threats.
- **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. It offers access to all the latest capabilities without the need for time-consuming, expensive deployment and upgrades.
- **Simplified Compliance Management 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 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 cyber-attackers. 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. This validates or can pinpoint areas of improvement in your Patch Management Program.
- **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.

eSentire Advisory Services

Trusted expertise, customized for your organization

eSentire Advisory Services 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 Advisory Services, you have instant access to dedicated experts who work with you to build and mature your cybersecurity program, conduct regular assessments to ensure efficacy of your technical controls, and perform advanced Risk Assessments.

Virtual CISO

With eSentire Advisory Services, you work with 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.

- **Dedicated Security Strategist**
  A dedicated security strategist who acts as your personal virtual CISO or works with your existing CISO to provide and deliver valuable insights and strategic direction.
- **Health Check**
  A quarterly review with your team to review current status and updates to any plans and/or roadmaps.
- **Executive Briefing**
  Annual reports and presentations with detailed updates on progress towards defined cybersecurity goals and regulatory requirements.
- **Security Program Maturity Assessment (SPMA)**
  An in-depth cybersecurity maturity assessment and gap analysis based on the NIST Cybersecurity Framework.
- **Security Policy Guidance (SPG)**
  Guidance on maturing your IT and cybersecurity policies and procedures to ensure all regulatory requirements and best practices are met.
- **Security Incident Response Plan (SIRP)**
  A pragmatic plan outlining the key steps to take during an event, with annual planning exercises and mock drill testing to assess readiness.
- **Security Architecture Review (SAR)**
  An assessment of technical and audit controls that should be implemented to protect your business-critical systems.

Vulnerability Management

eSentire Advisory Services delivers an array of tactical assessments from penetration testing, vulnerability scans and phishing campaigns to more strategic Risk Assessments that provide a deep analysis of activities inside your network, based on real-time SOC analysis provided as part of our core esNETWORK services.

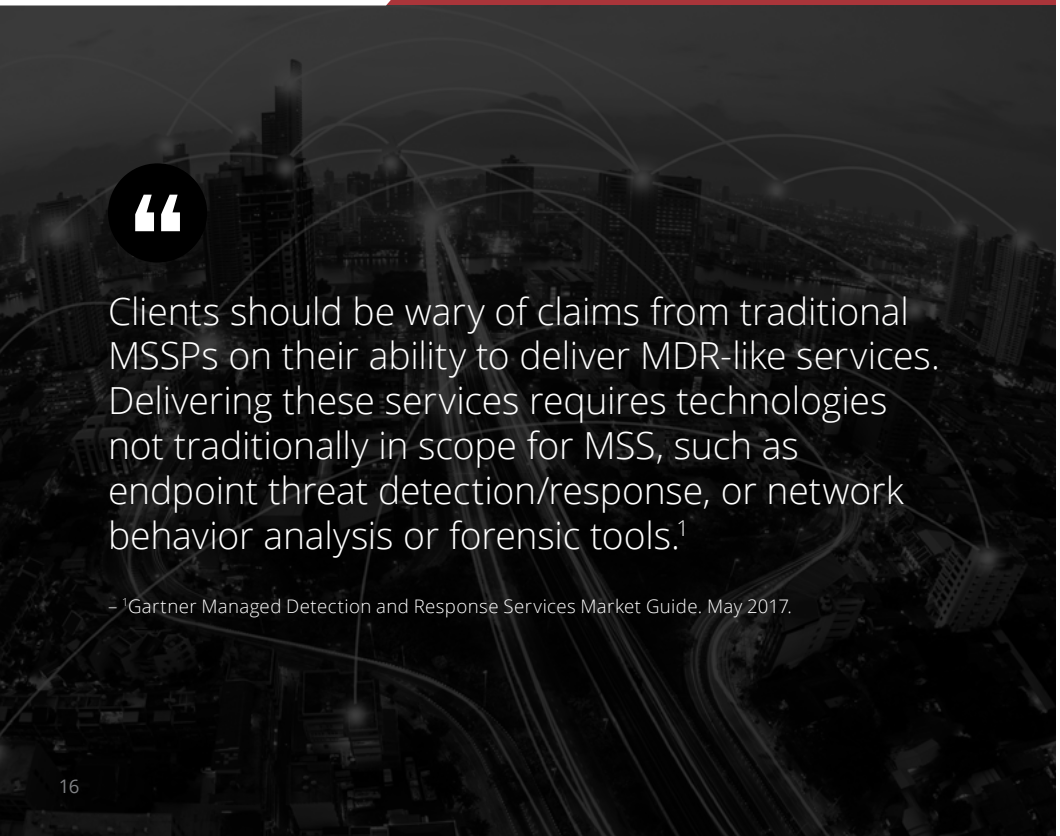
- **Penetration Testing & Vulnerability Assessments**
  Tailored assessments based on your business and regulatory requirements, with guidance on how to reduce the potential exploit window and avoid regulatory fines.
- **Risk Assessments**
  An assessment to identify unknown, active exploits within the network and determine your susceptibility to targeted phishing campaigns.
- **Phishing Campaigns**
  Simulated phishing attacks based on custom themes to help you identify the measurable cyber risk presented by your employees.

The eSentire Difference

We have developed and honed our advanced tradecraft over the last 17 years to provide Managed Detection and Response like no other. Many security service providers are jumping on the MDR bandwagon, taking shortcuts and changing their branding in an attempt to hide their shortcomings. But, there are no shortcuts to MDR. It takes years to perfect.

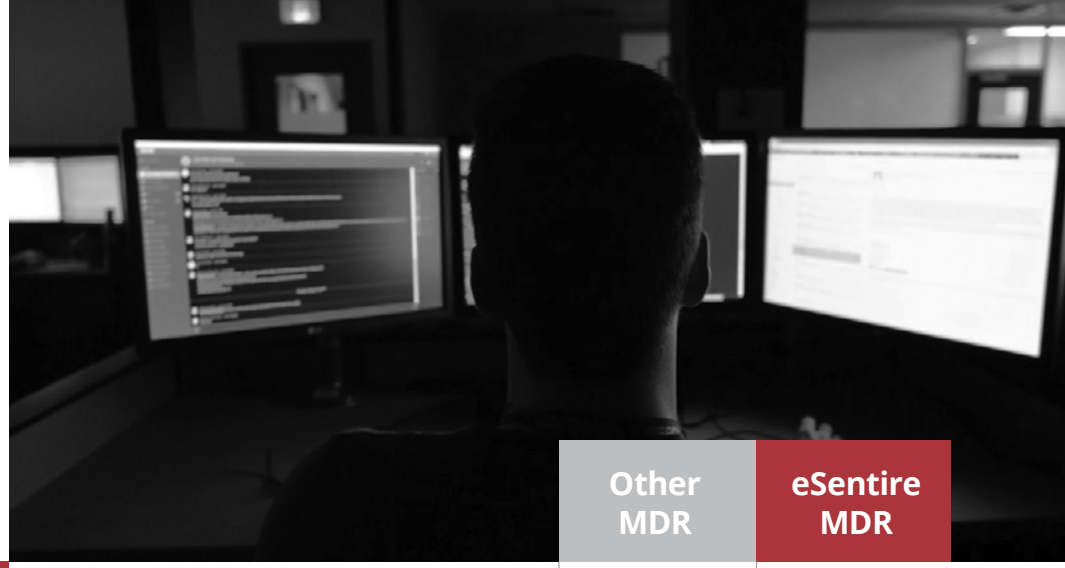
Our core value is simple:

A customer's network can never be compromised.



"Clients should be wary of claims from traditional MSSPs on their ability to deliver MDR-like services. Delivering these services requires technologies not traditionally in scope for MSS, such as endpoint threat detection/response, or network behavior analysis or forensic tools.[1]

– [1]Gartner Managed Detection and Response Services Market Guide. May 2017.



	Other MDR	eSentire MDR
24x7 always-on monitoring	(Limited)	✓
Real-time inspection of every network packet utilizing full packet capture	(Limited)	✓
Detection utilizing signatures and IOCs	✓	✓
Detection of unknown attacks leveraging patterns and behavioral analytics	(Limited)	✓
Continuous human-driven threat hunting	✗	✓
Alerting of suspicious behavior	(Limited)	✓
Alerts	✓	✓
Confirmation of true positive	(Limited)	✓
Remediation recommendations	✓	✓
Tactical threat containment on client's behalf	(Limited)	✓
24X7 forensic investigation and SOC support	✗ (Need IR Retainer)	✓
Evidence collection, dissection, processing and analysis	✗ (Need IR Retainer)	✓
Response plan for particular incident	✗ (Need IR Retainer)	✓
Remediation verification	✗ (Need IR Retainer)	✓

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

See What You're Missing

eSentire Managed Detection and Response keeps organizations safe from cyber-attacks that traditional security technologies can miss.

Contact us to discuss your cybersecurity and compliance needs, or learn more at **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 $6 trillion in corporate assets, 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.