DATA SHEET:

On-Demand Incident Response Service

4-hour threat suppression SLA, delivered remotely, anywhere in the world

Industry Leading 4-Hour Threat Suppression

We get you back to normal business operations in a matter of hours, delivering a guaranteed 4-hour threat suppression promise, anywhere in the world.

We strategically deploy our proprietary eSentire Atlas XDR Investigator agent to devices across your network. Therefore, within minutes of your call, our team will have immediate access and forensic capabilities to actively work to suppress the threat.

Elite Global Expertise

We provide you with priority access on-demand to our team of elite incident responders who are highly accredited with diverse cybersecurity backgrounds and decades of experience.

Many of our incident responders have held technical leadership positions across the Federal Government (Special Forces, FBI, DEA, CIA) and within Fortune 500 companies.

Proprietary Best In-Class DFIR Technology

Our industry-leading digital forensics and investigative tools allow us to provide immediate time to value - collecting forensics artifacts regardless of your organization's size or location - to get you back to normal business operations within hours vs days.

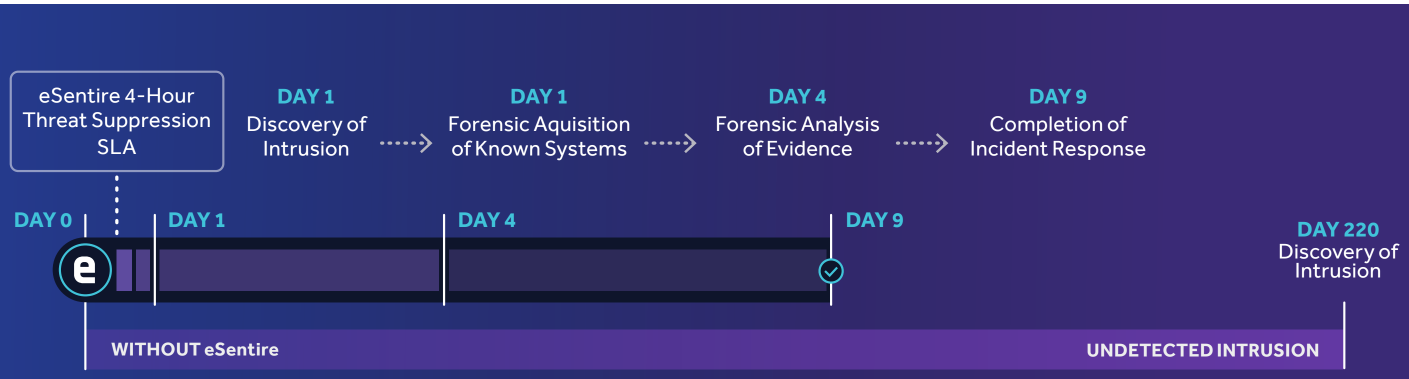
Our service is powered by eSentire Atlas XDR Investigator, our proprietary technology, which enables our team to perform end-to-end investigations remotely.

Full Support Through the Investigative Lifecycle

We provide full support throughout the investigative process including the filing of cyber insurance claims, compliance & litigation evidence preservation, transitioning findings to law enforcement, supporting legal proceedings, expert witness testimony and strengthening security gaps through the implementation of lessons learned.

When disaster strikes you need an incident response partner that can react with industry-leading speed and efficacy. Having immediate access to expert on-demand incident response services brings rapid control and stability to your organization when a breach occurs. It can be the difference between a catastrophic day and just another day at the office because how fast your organization can contain and recover from a security incident is critical to limiting business disruption, reducing costs, and salvaging reputational damage.

eSentire's On-Demand 24/7 Incident Response service provides you peace of mind with the fastest threat suppression in the industry. Through a combination of best-in-class digital forensics technology and elite responders, we can suppress a cybersecurity incident, anywhere in the world, within 4 hours. Our eSentire Atlas XDR Investigator agents are deployed once our partnership begins, resulting in time to value that is unmatched industry-wide.



eSentire 4-Hour Threat Suppression SLA

DAY 1 Discovery of Intrusion ⋯→ DAY 1 Forensic Aquisition of Known Systems ⋯→ DAY 4 Forensic Analysis of Evidence ⋯→ DAY 9 Completion of Incident Response

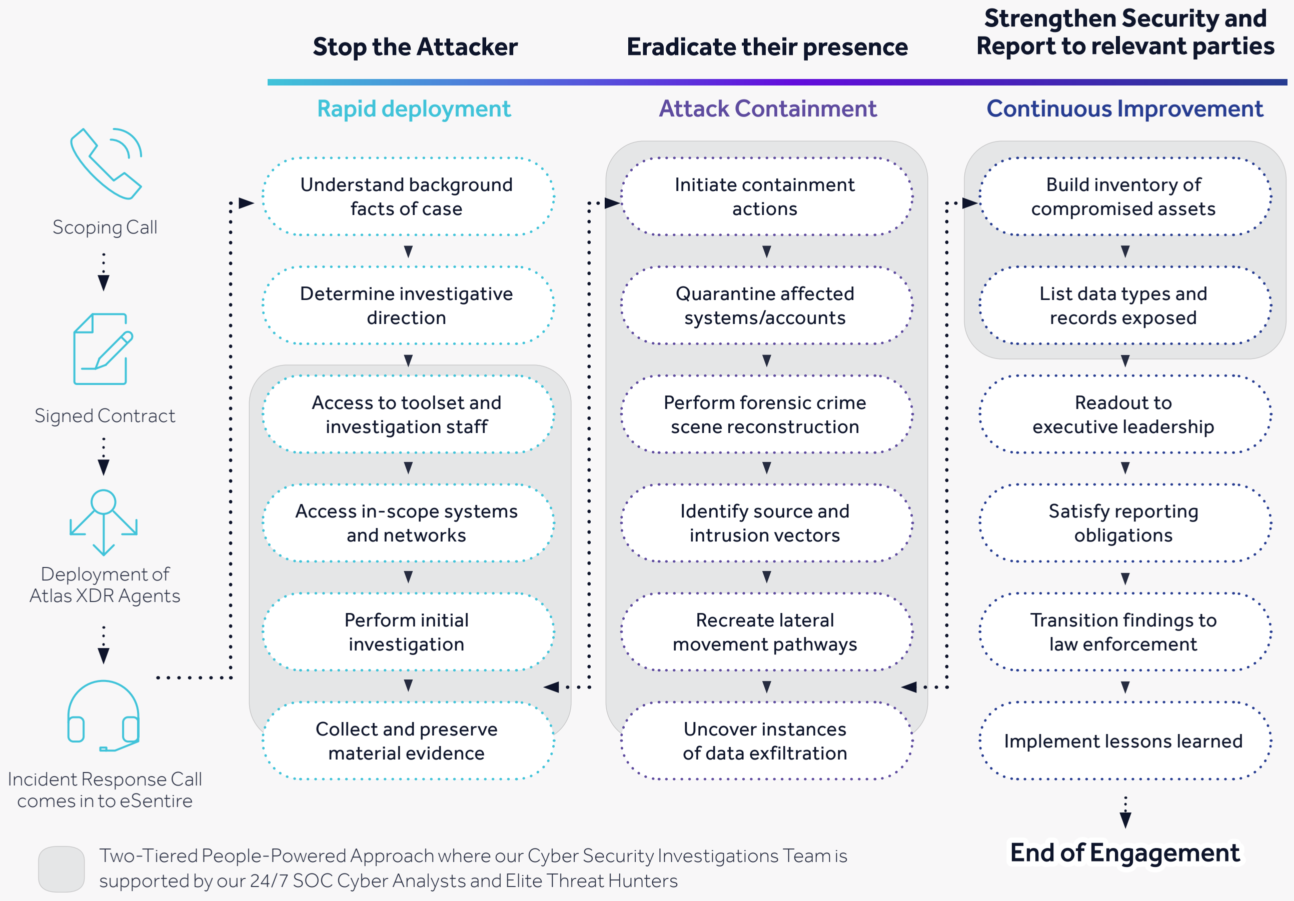
eSentire's Digital Forensics Technology Advantage

Our service is powered by our proprietary eSentire Atlas XDR Investigator agent. This digital forensics tool enables our team to perform end-to-end investigations remotely. No other company is in possession of technology that will help you triage and contain a data security breach faster. Within hours of deployment, you will know every impacted system on your network and be completing containment and remediation steps. Competing service providers and technology companies will take months to arrive at the same point of resolution.

Want to know if your breach is attributable to an external actor or an internal operator with legitimate credentials? The eSentire approach is unique in driving your results quickly so we can rapidly answer that question. If you want to take action in court, respond to a regulator, or pursue any number of other activities associated with a data breach, you will need forensically-assured data. Collecting that data is often prohibitively expensive, unless you're using eSentire Digital Forensics & Incident Response capabilities.

eSentire brings unique capabilities with its proprietary XDR and endpoint technology, with unparalleled real-time visibility across all deployed assets. Unlike legacy "dead drive" forensic tools, our platform enables cybersecurity investigators to immediately and remotely commence identifying the exact nature of a security event, determining to what extent systems have been affected, and accelerating incident response. eSentire's platform mitigates impact by substantially reducing the mean time to identify (MTTI) and mean time to contain (MTTC) cyber threats to minutes from days or even weeks.

How it works



Scoping Call

Signed Contract

Deployment of Atlas XDR Agents

Incident Response Call comes in to eSentire

Stop the Attacker

Rapid deployment

- Understand background facts of case
- Determine investigative direction
- Access to toolset and investigation staff
- Access in-scope systems and networks
- Perform initial investigation
- Collect and preserve material evidence

Eradicate their presence

Attack Containment

- Initiate containment actions
- Quarantine affected systems/accounts
- Perform forensic crime scene reconstruction
- Identify source and intrusion vectors
- Recreate lateral movement pathways
- Uncover instances of data exfiltration

Strengthen Security and Report to relevant parties

Continuous Improvement

- Build inventory of compromised assets
- List data types and records exposed
- Readout to executive leadership
- Satisfy reporting obligations
- Transition findings to law enforcement
- Implement lessons learned

End of Engagement

□ Two-Tiered People-Powered Approach where our Cyber Security Investigations Team is supported by our 24/7 SOC Cyber Analysts and Elite Threat Hunters

Features

4-Hour Remote SLA with Retainer

Quickly mobilizes investigative toolset and expert responders providing critical visibility and support across your affected networks and assets.

Rapid Deployment

Quickly mobilizes responders and investigative toolsets, putting critical visibility on your affected network and assets.

On-Site Incident Responders

Within 24 hours, anywhere in the world, we can deploy boots on the ground for on-site incident response management.

End-to-End Incident Management

Cyber Security Investigations team and supporting technologies cover the full incident response lifecycle.

Elite Tool Sets

To illuminate where attackers are present. Supports root cause analysis.

Critical Visibility

Deployment of commercially available and open-source tools, including eSentire's network, endpoint, and log technology, as needed, to collect endpoint telemetry, full network packets, netflow and log data from on-premises and cloud environments to provide multiple vantage points for analysis.

Malware Analysis

We will detect and analyze malicious files and URLs for suspicious activities to gather a deep analysis and generate comprehensive & detailed reports.

Managed Containment

Locks down and isolates threat actors preventing further spread and business impact.

Digital Forensic Analysis

Reconstructs the incident determining root cause, affected systems and attacker pathways.

Asset Handling

Secure and robust processes for asset handling and chain of custody support.

Eradication Support

Identifies exploited vulnerabilities, supports remediation of affected assets.

Confirmation

Ensures the network is secure and monitors for attacker response and persistence measures.

Compliance Satisfaction

Meets regulatory requirements with centralized collection, retention and reporting.

Litigation Support

Expert and fact witness testimony, if needed, is available.

Evidence Preservation

Gathers and stores incident details that meet legal, insurance and regulatory requirements.

Robust Reporting

Detailed finding and impacts of the cyber investigation chronicle taken with lessons learned at the executive and technical level.

The eSentire Cyber Security Investigations Team

With the eSentire Cyber Security Investigations (CSI) team, you gain access to highly credentialed responders, comprised of computer forensic practitioners with decades of experience serving government intelligence agencies, federal & city law enforcements, the United States Military and Fortune 500 companies. Our team of responders have extensive incident response experience and multiple industry certifications:

- Certified Information Systems Security Professional (CISSP)
- Licensed Private Investigator (LPI)
- Certified Hacker Forensics Investigator (C|HFI)
- Certified Computer Forensics Examiner (CCFE)
- Certified Forensics Consultant (CFC)
- GIAC Certified Incident Handler (GCIH)

eSentire CSI partners with our global SOC Cyber Analysts and Elite Threat Hunters, extending your Incident Response support and expertise across hundreds of team members with decades of experience in threat detection, remediation and recovery. Our team has deep knowledge of how targeted attacks break through, and the Tactics, Techniques, and Procedures (TTPs) adversaries use to achieve their objectives. eSentire IR procedures aren't built on rigid frameworks. Instead, we rely on flexible solutioning and hands-on incident response experience.

Delivers Results

- Attacks are quickly contained and incidents are resolved
- Recovery is supported eliminating the chance for recurrence
- Root cause analysis and threat eradication
- Systems clear for return to standard business operations

+

Power of 24/7 SOC Team

- Access to hundreds of team members
- 24/7 SOC Cyber Analysts and Elite Threat Hunters
- Expertise detecting, disrupting and responding to threats

+

Flexible Delivery Model

- Can be engaged on Retainer for Incident Response and Emergency Preparedness
- Available to address Emergency Incident Response

The Difference Between MDR and Incident Response

eSentire is proud to be recognized globally as the Authority in Managed Detection and Response. We prioritize our capability to respond and own the R in MDR. Team eSentire is proud to deliver MDR^3 - Response. Remediation. Results.

Our capability in Response is built from:

- Full threat visibility with multi-signal ingestion across network, endpoint, log and cloud sources
- Detection capabilities mapped to MITRE ATT&CK framework
- Automated detections and orchestrated blocks through our Atlas XDR Cloud Platform
- Proactive Security Network Effects amplifying detection and response capabilities across our entire global customer base
- Human intuition and threat hunting expertise for deeper investigation and analysis
- Threat isolation, containment and remediation

When your preventative tools are bypassed, have confidence that Team eSentire is there to detect, disrupt, and contain the threat. So where does MDR end and where does Incident Response begin?

eSentire Managed Detection and Response (MDR)

Based on multi-signal ingest capability we disrupt and contain attacks before they become business impacting events. We provide recommendations on remediation, or can complete remediation.

On-Demand Incident Response Retainer

4-hour threat suppression delivered remotely by our Cyber Security Investigations team who are armed with best-in-class tools to identify the root cause of an existing security incident and determine the extent to which data & assets were compromised. This helps ensure you can get back to normal business operations and we will support you through recovery & provide assistance to satisfy your stakeholder and compliance obligations. The results of our digital forensics investigations can bear scrutiny in a court of law.

By converging eSentire MDR and IR, you are able to:

- Simplify the call for help so you know who to turn to in a moment of crisis (when every second counts and emotions are running high).
- Streamline workflows, which allows us to leap off the starting blocks to deliver faster time-to-execution and time-to-value.
- Alleviate the burden from your IT team by allowing us to take on the heavy lifting of response, investigation, remediation, and reporting obligations.
- Blend leading-edge technology with responsive and dynamic service delivery.
- Achieve an unmatched understanding of a rapidly changing situation by leveraging detection and situational awareness (e.g., from endpoint, network, and log visibility) in combination with analysis and dead disk forensics.

We're here to help!

Submit your information and an eSentire representative will be in touch to discuss how our On-Demand 24/7 Incident Response Service can ensure you quickly bring control & stability to the situation, if a breach should occur.

Contact Us

eSentire also has Emergency Incident Response Support Available. If you are experiencing a security incident or have been breached, contact us ☎ 1-866-579-2200

eSENTIRE

eSentire is the Authority in Managed Detection and Response, protecting the critical data and applications of 1200+ organizations in 75+ countries, representing 35 industries 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, 24/7 Threat Hunting, 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 & 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 Incident Response services. For more information, visit **www.esentire.com** and follow **@eSentire**.