



eSentire Managed Detection and Response™ Service

Proven Cybersecurity for Small to Midsized Enterprise

eSentire Managed Detection and Response (MDR) keeps midsized organizations safe from constantly evolving cyber attacks that traditional security defenses simply cannot detect. It's smarter because it goes far beyond just intrusion prevention (IDS/IPS) and Security Information and Event Management (SIEM) by leveraging full packet capture, signature-based threat intel, behavioral and reputational-based analytics, and attack pattern algorithms to detect both known and unknown cyber threats. It's more effective because our 24x7 Security Operations Center (SOC) analysts leverage always-on full packet capture and powerful forensic tools to hunt, fully investigate, and respond to real attacks before they do harm to your network. So you can stay focused on your business rather than managing cybersecurity.

ELITE

24x7 white-glove service from world-class security analysts.

Comprehensive

The bad guys have nowhere to hide. We leave no digital stone unturned.

AGILE

Say good-bye to thousands of useless alerts and hello to a good night's sleep.

We Manage the Complexity of Cybersecurity

Defending against ever evolving cyber threats takes considerable financial investment, and access to a very limited and highly competitive pool of security experts. With eSentire, you have instant access to elite security analysts that become an extension of your team. We become your trusted advisor on a wide range of security topics, and wouldn't have it any other way.

Re-defined Security

We invented Managed Detection and Response and over the last 15 years, we have continued to raise the bar for security as a service. We recognized that relying on traditional cybersecurity defenses could not prevent attacks. Hackers move quicker than signatures and threat intelligence can respond. We hunt down dangerous, new threats by investigating unusual activity—the threats that pure technology solutions and traditional SIEM-based approaches cannot.

You Can Sleep Because We Don't

Our hunt teams are constantly vigilant, investigating new threats in real-time. They don't just alert on threats, they investigate and respond on your behalf.

Our approach to Micro-Incident Response ensures new and fast moving attacks are dealt with before they become business disrupting.

- World Class 24x7X365 Global SOC
- Advanced Cybersecurity Forensic Investigation Tools
- Embedded Micro-incident Response
- Real-time Signature-based Detection and Prevention
- Unknown Threat Detection via Attack Pattern and Behavior-based Analytics
- Real-time and Historical Vulnerability Detection and Support
- Robust Threat Intel
- Rapid Forensic Investigation and Threat Response
- Virtual CISO - Cybersecurity Regulatory Compliance
- Cybersecurity Training, Testing and Attack Readiness



Smart Cloud-Based Threat Sensors with Always-on Full Packet Capture

Powered by 200+ Industry, Government and Proprietary Threat Intelligence Feeds

Attack Pattern, Parsing Algorithms and Behavior-based Threat Detection

Log Correlation and Advanced Forensic Analysis

Powered by the RIGHT Threat Intel and Technologies for Midsized Organizations

We believe that everyone should have access to threat intelligence to fight the war on cybercrime. So, we created CYMON™ the world's largest open threat intel sharing community, and made it accessible to anyone. Our arsenal of cyber technology to hunt for sophisticated attacks goes far beyond the largely signature-based traditional threat intelligence approaches of the past; it better protects midsized enterprise from the newer, more sophisticated attacks targeting midsized organizations, 24x7.

Protection against known and unknown cyber threats including malicious software, botnets, phishing, data exfiltration, APTs, etc.

Zero network latency and a world-class 24x7 global SOC that monitors, hunts, investigates, and remediates threats so you don't have to.

Unified service that can be deployed as standalone or with your existing architecture to enhance cybersecurity protection.

Advanced protection for midsized enterprise who don't have the in-house resources or staff to manage cybersecurity.

Designed to help keep you compliant with evolving cybersecurity regulatory compliance across industries.