eSENTIRE | autodata

DATA SHEET

Switch to eSentire. Choose Proven. Get More with eSentire MDR.

Partner with the industry-leading, all-in-one Managed Detection and Response (MDR) solution to help you consolidate and save, while bolstering your security. Our proven track record, customised approach, rapid 14-day onboarding, and cost-effective MDR solution sets us apart.

Switch to the Proven Choice: The Authority in Managed Detection and Response

Are you struggling with subpar services that leave you exposed and feeling like your provider should be doing more to enhance your security posture? It's time to take control of your cybersecurity strategy and switch to eSentire, where your protection is our top priority. eSentire offers unparalleled benefits to help you prioritise your security investments and prevent business disruption:

- **Consolidate & Save** – Save up to 40% annually when you bundle 2 or more eSentire security services across endpoint, network, log, and cloud protection
- **Get Real ACTION** – We don't just provide alerts. You get 24/7 threat response & remediation including host isolation, hash blocking, account suspension, retroactive email purges, system reboots and more
- **All-In-One Solution** – Get Unlimited Threat Hunting & Unlimited Incident Handling as part of our foundational MDR service (no hidden add-ons required)
- **Multi-Signal Coverage & Over 300 Technology Integrations** – Full support for your existing tech investments
- **Augment Staff & Expertise with Personalised Protection** – eSentire's Cyber Resilience Team of SOC Analysts, Elite Threat Hunters, Threat Response Unit (TRU), and Cyber Risk Advisors act as an extension of your team from Day 1 to show An Attack On You Is An Attack On Us
- **Ultimate Flexibility** – You can Bring Your Own License (BYOL) or partner with eSentire for a fully managed solution
- **Ease of Onboarding** – Fully deployed MDR service in 14 days on average
- **Proactive Security Improvement** – We add 200 IOCs/IPs per day to our XDR platform based on positive global SOC investigations to enhance your defenses. 2023:

200K+
Global threat sweeps

1,100+
Hypothesis-based hunts

500+
Novel detections and runbooks to improve security

Not all MDR is Created Equal. Expect Complete Response.

When it comes to response, it's how we do it that makes all the difference. To build a more resilient security operation, you need an MDR provider who has your back from Day 1.

Response Speed

Our eSentire XDR platform instantly detects and blocks millions of threats per day. We add 200+ IPs & IOCs per day to our block list based on positive SOC investigations. When human intuition is required, we are on guard 24/7 to protect you with a Mean Time to Contain of only 15 minutes.

Response Expertise

We take threat response seriously by containing and remediating cyber threats on your behalf, so your business continues to run smoothly. Plus, most of our customers have less than 2 in-house resources to support their security operations so eSentire becomes a trusted extension of their team.

Response Coverage

Be confident your defenses are always one step ahead. Our global SOCs are home to the industry's only 24/7 threat hunters and with eSentire's unique multi-signal intelligence, you can remain confident that your defenses are always one step ahead.

MDR for Your Complete Attack Surface

As part of our Multi-Signal MDR service we ingest signal sources that drive data correlation, cyber threat analysis and kill switch response capabilities. When combined we deliver full attack surface visibility, deep investigation, threat detection, and complete response.

Signals	Our Technology Partners	Detection	Investigation	Response
Network	eSentire	✓	✓	✓
Endpoint	eSentire, SentinelOne, CrowdStrike, Microsoft	✓	✓	✓
Email	Microsoft	✓	✓	✓
Cloud	aws, Google Cloud, Microsoft, Lacework, sumo logic, tenable	✓	✓	✓
Log	sumo logic, Microsoft	✓	✓	✓
Identity	Microsoft, CrowdStrike	✓	✓	✓
Vulnerability Scans	tenable	✓	✓	

Seamless Integration and Threat Investigation Across Your Existing Tech Stack

eSentire MDR integrates seamlessly with the existing tools and SaaS platforms in your environment to enable continuous monitoring across your hybrid footprint, ingestion of high-fidelity data sources, and 24/7 protection from sophisticated known and unknown cyber threats with proactive threat hunts. We continuously expand our multi-signal ingestion capabilities by adding new detections and runbooks for SaaS platforms and enterprise applications. When suspicious activity is detected, we stitch together context-free telemetry to identify similar attacker tactics in your environment.

Our 24/7 SOC Cyber Analysts respond on your behalf to counter threat actor TTPs by leveraging common security infrastructure and tools (including, but not limited to):

- EDR/EPP tools
- Network security technology
- Email security platforms
- VPN providers
- Web gateway solutions

As a result, you can adopt a cost-effective approach to ensure robust coverage across your entire environment without compromising your existing investments with runbooks and integrations available for:

Cloud Infrastructure

Google Cloud · Azure · aws

Cloud Applications

Google Workspace · Azure

Cloud Platforms and Security Infrastructure

CROWDSTRIKE · Microsoft · vmware Carbon Black · SentinelOne · eSENTIRE · Barracuda · CloudGuard SaaS · citrix · cisco · Dropbox · DUO · f5 · FORTINET · mimecast · okta · paloalto NETWORKS · salesforce · proofpoint · slack · Gmail · TREND MICRO · SOPHOS · zscaler