Integrity360
your security in mind

Light the way: A CyberFire guide to smarter MDR strategy

Choosing the right MDR partner has never been more important — or more difficult. As the threat landscape continues to evolve and attackers grow bolder, organisations are increasingly frustrated by providers that:

- Deliver too much noise and not enough clarity
- Overcomplicate pricing with hidden costs
- Fail to scale or adapt as needs grow
- Under-deliver on response and remediation

Many companies sign up for MDR services expecting partnership – but instead experience platform fatigue, alert overload, and spiralling costs. Sound familiar?

This is where **CyberFire MDR** comes in. It was designed to be the antidote to all those issues. Avoiding the noise to deliver real outcomes.

MDR buyers often voice these common **frustrations:**

- **Difficult-to-use platforms** that make reporting and navigation inefficient
- **Poor support follow-through** and lack of communication on tickets
- **Slow, inconsistent remediation processes** that leave teams in limbo

CyberFire MDR responds directly to these concerns:

- **Streamlined portal and reporting** make navigation effortless
- **Dedicated Customer Success Reps** ensure accountability and clear communication
- **Guided triage and remediation** ensure you're never left chasing answers

© Integrity360

Common MDR frustrations vs. CyberFire MDR

The challenge	The solution
Alerts are often received without clear resolution paths.	Every alert includes analyst-led triage and easy-to-follow remediation steps — even for non-specialist engineers.
Feels like some alerts are just passed through from vendor tools without validation.	We filter out noise and non-actionable alerts — you get only high-fidelity, verified threats.
Lacks integration with key tools like privileged access management.	CyberFire supports broad technology integrations and evolves to match your tech stack.
The service doesn't feel embedded or aligned with internal workflows.	You get a dedicated CSR and support from six global SOCs — ensuring tight alignment and partnership.
Poor responsiveness and support from the MDR provider.	Your named CSR supports only 5–6 clients, ensuring fast, knowledgeable, and consistent support.
Limited visibility into backend data without extra fees.	Transparent access with self-service reporting and zero hidden charges.
Logs are sometimes missing or incomplete, and analyst feedback lacks depth.	All logs are accessible. Every case includes root cause, full context, and clear recommendations.
Support cases often stall or close without full resolution.	We commit to full-case lifecycle accountability — every investigation sees a clear end.
Clunky interface and concern over hidden or rising costs.	Streamlined UI and a transparent pricing model — no unexpected increases.
Onboarding is passive, documentation-heavy, and setup is often incomplete.	Hands-on, project-managed onboarding ensures you're operational quickly and completely.
Reporting and dashboard features are underwhelming.	Our Enhanced Reporting module delivers custom reports and long-term storage for compliance to your environment.
Navigation is unintuitive, and ad hoc reporting is difficult.	Our portal is built for clarity — run reports, explore data, and manage your environment easily.
Too many alerts during setup; remediation guidance is weak.	We provide guided triage, meaningful escalation, and expert remediation tailored to your environment.

© Integrity360

Expected outcomes with CyberFire MDR

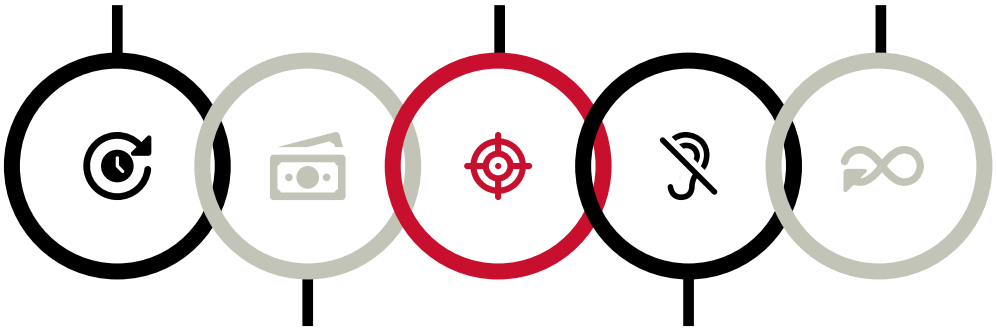
- **Peace of mind:** High-fidelity alerts mean you only hear about what matters
- **Cost control:** Transparent pricing without baked-in increases or surprise hardware needs
- **True resilience:** Built-in IR hours and post-breach detection, ready from day one
- **Compliance-ready:** Enhanced reporting that fits your audit needs
- **Always evolving:** Continuous service improvements to match your growing business
- **Trusted support:** Local expertise, proactive partnership, and customer-first service

What makes us stand apart?

Turnkey deployment
Rapid integration into any security environment in 4 weeks or less

High-fidelity threat detection
Advanced detection engineering and innovative detection rules exclusive to CyberFire MDR

Continuous security improvement
Ongoing improvements in threat detection coverage and overall security posture



Ending expensive/ unpredictable SIEM costs
Simple endpoint-based pricing

Minimal noise, maximum clarity
Prioritised, high-quality alerts only with **Full Incident Response support**

> “CyberFire doesn’t treat us like just another account. Their people genuinely want to understand our challenges and help solve them. That culture fit was one of the biggest wins for us. With our previous provider, it felt like we were always reacting. With CyberFire, we feel ahead.”

- Group IT Governance, Risk and Compliance Manager, Retail Finance Organisation

© Integrity360

What you need from MDR and how CyberFire delivers

What you need	Why it matters	Our approach
True visibility	Many services claim it. Few deliver it.	Noise-free, real-time insights backed by expert-led analysis and triage.
Actionable response	Alerts alone don't solve problems.	Analyst-guided remediation with clear steps—even for non-specialist teams.
Simplified experience	Clunky portals and hard-to-find data waste time and delay response.	Intuitive portal for live incidents, historical alerts, and on-demand reporting.
Clear, predictable pricing	Surprise uplifts and hidden charges hurt trust and budgeting confidence.	Transparent endpoint-based pricing. No forced hardware. No annual increases baked in.
Integrated approach	Detection gaps appear when MDR tools don't connect with your stack.	CyberFire supports wide integration with your platforms — flexible, extensible, and future-ready.
Responsive support	MDR should feel like a partnership, not just a platform.	Named customer success representative, low client ratio, proactive and personal service experience.
Rapid onboarding	Documentation-only setups cause delays and confusion.	Hands-on, project-managed onboarding tailored to your infrastructure.
Less noise, more signal	Too many providers still pass on every low-value alert.	We suppress duplicates, eliminate false positives, and only escalate high-fidelity threats.
Real-time access	Slow or gated data access hampers investigations.	24/7 portal access to logs, case history, alerts, and on-demand reports — no hidden data fees.
Built-in improvement	MDR shouldn't be static — it should evolve with your business.	Ongoing detection enhancements and posture improvements with tracked Defence Threats and CSIs.

Find out more www.integrity360.com

CyberFire MDR is trusted by organisations across finance, retail, healthcare, and more — including deployments of over 60,000 endpoints. Unlike noisy or bloated offerings, our mature service is designed for those who value precision, partnership, and performance.
To learn more get in touch with our experts.

© Integrity360