TRINITY CYBER

Managed Detection & Response (MDR): Broken Economics, Broken Promises

Achieve better security and business outcomes by rebalancing investment to active network defense.

White Paper

DECEMBER 2025

info@trinitycyber.com

Table of Contents

TRINITY CYBER

Executive Summary

The problem: MDR's broken economics

Managed Detection and Response (MDR) promised to solve cybersecurity's talent crisis by outsourcing threat monitoring and Security Operations Center (SOC) services to expert providers. But the MDR industry faces a fundamental structural dilemma: as client volumes grow, the flood of security alerts also grows, and hoped-for efficiencies have not materialized. Each alert requires expert triage and analysis. Gartner's October 2025 *Market Guide for Managed Detection and Response* reiterates that MDR is a human-intensive service. The result is an industry struggling with unsustainable economics and deteriorating service quality.

The structural challenges facing the MDR industry are stark:

- Only 28% of executives report complete satisfaction with their MDR providers, according to a Gatepoint Research survey reported by Cybermaxx.
- A Q3 2024 analysis, by investment bank Houlihan Lokey, notes that MDR scaling has been "elusive."
- SecureWorks, until recently a publicly traded MSSP/MDR, has since been taken private after losses.
- KPMG reports that organizations remain "uncertain about whether their MSPs are actually doing what they say."
- The European Union's cybersecurity agency (ENISA) June 2025 *MSS Market Analysis* documents systemic issues with cost, integration, and service visibility across managed security providers.

The alert trap

The core operational challenge is unsolved: MDR providers struggle to manage alert volume at scale. Further, false positives and endemic and most MDRs lack resources required for constant tuning of security tooling. As organizations expand their digital footprint, the number of alerts — each requiring expert triage — increases commensurately while the supply of qualified analysts, and the dollars to pay them, remains constrained. This creates a vicious cycle where providers must choose between profitability and service quality. Current evidence suggests many are failing at both.

The MDR market is built upon a suspect foundation: *the reactionary detection and response model*. Gartner has said that conventional detection and response, the technology stack that underlies MDR services, is fundamentally inadequate for modern, AI-accelerated, threats. According to a 2025 VulnCheck report, over 32% of exploited vulnerabilities were attacked on or before disclosure. When almost one-third of exploits happen before patches exist, reactive security, by definition, starts from behind.

In response to the limitations of the reactive detection and response model, a new approach, preemptive cybersecurity, is emerging. Preemptive cybersecurity is proactive and aims to deny, deceive, and disrupt attackers *before* they can establish a foothold within your environment. Gartner forecasts that, in response to current limitations with detection and response, and the growth of AI-enabled threats, preemptive cybersecurity will account for 50% of IT security spending by 2030, up from less than 5% today.

The path forward

As the MDR industry's current approach cannot scale, a new approach, active network defense, is required. Trinity Cyber's Full Content Inspection (FCI) technology is at the leading edge of the fundamental shift that Gartner envisions. FCI denies, deceives, and disrupts adversaries. By design, it is alertless and preemptive, addressing the major pain points of the detection and response model. By neutralizing threats inline before they reach the network — rather than detecting and responding to them after an intrusion — FCI provides active network defense and eliminates dependency upon MDR services. FCI does this by inspecting full session content (protocols, code, files) with contextual awareness that precisely identifies adversary tactics, techniques, and procedures (TTPs).

By producing a superior, more enduring form of detection and the first of its kind active network control, Trinity Cyber can reduce or eliminate reliance upon MDR services. As FCI is centrally operated, and tuned to actual adversary techniques, not an ephemeral target set, and operating at carrier scale (currently inspecting over 1.5 trillion content objects per day, and growing), FCI lowers security costs in many organizations by more than 50%, while materially improving security outcomes.

TRINITY CYBER

MDR's Breakdown

The promise vs. the reality

MDR services entered the market with a compelling value proposition: outsource your Security Operations Center (SOC) to experts who could monitor threats 24/7/365, allowing resource-constrained organizations to access enterprise-grade security without building expensive internal capabilities. **But MDR providers inherited the same Detection & Response model that created the problem in the first place.** The alert fatigue crisis never stopped, it was simply (and without sufficient economies of scale) outsourced to MDRs.

A customer satisfaction problem

As noted in the Executive Summary above, customer complaints regarding MDR are consistent across regions and industries:

- Detections incapable of rapidly addressing evolving threats
- Second and third order consequences from alert fatigue overwhelming internal teams, despite outsourcing
- Manual client engagement requirements often undermine promised efficiencies
- Unaddressed false positives impact enterprise productivity and end-user's satisfaction.

A structural problem: Detection & Response does not scale

The MDR industry's intrinsic challenge is architectural. MDR services are built on a detect-and-respond model that, amid the proliferation of AI-driven threats, Gartner has explicitly called insufficient. The implications are overwhelming:

- Skilled SOC analyst staffing is costly, and 35% of MDR providers cite skills shortages as their top challenge
- Pricing pressures frequently force cost-cutting that degrades service quality
- MDR labor offshoring arbitrage creates communication and quality gaps

- MDR providers serve customers with heavily fragmented vendor tooling, limiting standardization

- Current detection and response tooling drives unsustainable alert volumes that cannot be cost-effectively triaged. The economics of the MDR business do not support tuning to limit false positives.

The industry has created a treadmill effect, where end-customers continuously invest in inadequate detection tools that rely upon indicators of compromise (IoCs) detections (like static file hashes and IP addresses) while a) threats evolve faster than IoCs can be updated and b) MDRs cannot keep up with the alert volume. It's a losing game with no exit strategy for MDRs — except to raise more venture capital.

With new AI-driven threats, security tooling must evolve

While some tools claim that they also focus, like Trinity Cyber, upon TTP detections, upon close inspection these tools typically rely on shallow analytics and heuristics to surmise adversary patterns and sequences. This leads to unacceptably high false positive rates that either impede business operations or lead to tooling being "detuned" – lowering efficacy – to also lower false positives. In contrast, FCI has the visibility, speed, and context to actively and directly meets adversaries where they operate in live traffic.

Consider further the advances in AI-driven threats and the end of conventional detection and response is closer than many in the industry realize. As the editor of Cyber Defense Magazine explained this year in *The Black Unicorn Report*, "The arms race between attackers and defenders is now automated. Adversarial AI is evolving to launch adaptive, autonomous attacks — and defenders must counter with self-learning systems capable of predicting and neutralizing threats in real time."

Without looking at session level content, security tooling that depends upon IoCs, simple pattern matching, and shallow analytics cannot keep up. Already, many legacy vendors are rushing to train AI to make their broken processes faster, but in the end, they will waste a lot of capital and fail to solve the problem. In contrast, Trinity Cyber develops AI models to combat AI threats – and our models are focused upon enhancing an already foundationally robust approach.

Instead of overdependence upon MDR, a security approach that is identity-centric, deploys FCI, and prudently keeps EDR as a last line of defense will be, in many organizations, the optimal mix. Adding active, adaptive, and scalable FCI

prevention is a reliable way to mitigate against AI-generated threats in the rapidly evolving threat landscape.

Following the money

The MDR industry isn't simply unprofitable — it may be structurally incapable of profitability at scale. Investment banks have noticed what customers feel. Investment Bank Houlihan Lokey's Q3 *2024 Cybersecurity Market Update*, an analysis for institutional investors, states plainly: "MDR at Scale with a Strong Financial Profile Has Been Elusive." Houlihan Lokey's analysis identifies approximately 600 MDR providers in the market — the vast majority being subscale, understaffed, and unprofitable.

Consider also Secureworks. Prior to its acquisition in 2025, it was one of the few publicly-traded pure-play MDR/XDR operators. Their results show GAAP net losses of $86 million in FY2024, and continued losses into 2025 — despite disciplined operations. If a well-established provider with Dell's legacy backing struggles to reach profitability, what does that say about the 590+ private competitors burning venture capital?

A further challenge for MDR providers is that they are caught between rising costs and downward pricing pressure as end customers demand flat-rate predictable pricing. The venture model is temporarily papering-over this challenge with a recipe that consists of: 1) raise capital, 2) acquire customers at unsustainable prices, 3) grow top-line revenue, 4) raise more capital to support the existing installed base and for growth. The music will inevitably stop when profit must materialize — and the evidence, from both investment banking analysis and public financial disclosures, suggests profitability will be hard to reach, as the detect-and-respond model intrinsically requires an unscalable level of human labor.

Implications

Many MDRs may not survive a market correction. When venture capital dries up, or profitability pressures mount, what happens? Neither service degradation, vendor consolidation, or outright failure would benefit your security posture.

More importantly, the industry's extreme over-rotation towards the Detection & Response approach sets organizations up for failure — even if their MDR partner does survive.

The Future is Preemptive, not Reactive

The shift

In 2025, Gartner published research challenging reliance upon conventional Detection & Response strategies. Their conclusion is unequivocal:

> *DR-based cybersecurity will no longer be enough to keep assets safe from AI-enabled attackers. Organizations will need to deploy additional countermeasures that act preemptively and independently of humans to neutralize potential attackers before they strike.*

Gartner's forecast signals a seismic shift: by 2030, preemptive cybersecurity solutions will account for 50% of IT security spending — up from less than 5% today. The implication is clear: the market is abandoning traditional detection and response solutions in favor of preemptive cybersecurity. It is unclear how, or if, MDR providers will adapt to this evolution.

Why Detection & Response is failing

Gartner states: “Traditional reactive 'detect and respond' strategies are no longer adequate.” We think the reasons are mathematical and irrefutable:

1. **Patching can’t keep up:** VulnCheck's State of Exploitation Report for 1H-2025 documents that **32.1% of Known Exploited Vulnerabilities were exploited on or before disclosure** — meaning almost one-third of attacks now happen before patches even exist. If your primary control is “detect fast and respond faster,” you're already late for a third of the problem.

2. **Threat volume explosion:** 400,000 new malware variants are detected daily.

3. **AI-driven exploits:** Attackers use generative AI to automate reconnaissance, phishing, and exploit creation — often reducing time-to-exploit from hours to minutes.

4. **CVE Growth:** Predicted 1 million documented vulnerabilities by 2030 (up ~300% from 277,000 in 2025)

MDR services, reliant upon conventional alert-heavy and false-positive heavy tooling, cannot close these gaps. MDRs can only react to inevitable breaches. That’s not real protection — it's damage control.

TRINITY CYBER

Gartner's solution framework calls for preemptive technologies that **Deny** adversaries access through automated exposure management; **deceive** with advanced deception technologies, and **disrupt** attacker operations

This is precisely what Trinity Cyber's Full Content Inspection (FCI) threat defense engine delivers — and what MDR fundamentally cannot.

Concept	Trinity Cyber View/Method
PREEMPTIVE CYBERSECURITY	The "detection and response" approach is fundamentally flawed, because of challenges including alert fatigue, false positives, and cost. Endpoint Detection & Response (EDR), however, should be maintained as a last line of defense. Preemptive cybersecurity is necessary because of the proliferation of AI-enabled threats; Trinity Cyber uses its AI models to protect against this new class of threats.
DENY	Trinity Cyber FCI surgically neutralizes threats in real time in payloads, before they reach a customer's network or endpoints. Instead of operating as a clunky, efficiency-thwarting blocker, it is a smart, low-latency (sub millisecond) threat sanitization that does not disrupting user sessions or business operations.
DECEIVE	Trinity Cyber can not only strip threats out of live traffic, it also modifies responses inline: i.e., intercepting an adversary command and control (C2) server instruction and modifying it so that malware uninstalls, unbeknownst to the attacker. This provides the additional benefit of gaslighting attackers: they cannot tell why their efforts are in vain and are left wondering if a server's patched, their exploit's buggy, etc. Trinity Cyber deception is enhanced by its architecture: traceroutes pass without registering a hop (an attacker can't "see" Trinity Cyber).
DISRUPT	By directly targeting tactics and techniques instead of IoCs, Trinity Cyber takes advantage of the common pattern of attackers using similar software packages to conduct their operations. Trinity Cyber's "1:infinity" detection approach enables a single FCI detection to prevent many different attacks from the same family. FCI also "shields the shield," detecting and removing threats focused on NGFW vulnerabilities. Further, the Trinity Cyber architecture denies the attackers from getting the critical reconnaissance data they need to map and bypass defenses.
ALERTS & LOGS	Because FCI proactively stops threats, it is an alertless technology. The Trinity Cyber portal details all actions taken, and provides full visibility and PCAP files – think of them as "DVR for networks" -- in case an event merits investigation, or your team wants to know more. As well, integration is available for SIEM event ingestion.

Trinity Cyber Full Content Inspection: Preemptive Cybersecurity Realized

The Architectural Revolution

Trinity Cyber Full Content Inspection (FCI) engine operates inline, between adversaries and your network, performing real-time analysis and threat neutralization that makes most of MDR's Detect & Respond approach obsolete.

How FCI Works

Inline and in real-time, (with less that one millisecond of latency, so imperceptible to your end-users) FCI:

1. **Intercepts:** The network traffic you designate enters Trinity Cyber's private security plane, isolated from the internet for added security, with included SSL inspection;

2. **Inspects:** FCI fully parses and contextually analyzes content (including protocols, files, and more) in full networks sessions — leveraging 3,400+ data fields

3. **Neutralizes:** Malicious content is surgically removed from legitimate traffic

4. **Releases:** Clean traffic continues to its destination in real-time.

Unlike MDR services that detect threats after infiltration, FCI prevents them from ever entering your environment. FCI is available with all Trinity Cyber's offerings, including ZTNA and Cloud Firewall. Organizations implementing FCI have reduced security spending by more than 50% while dramatically improving their security posture.

The threat defense advantage: beyond detection theater

Trinity Cyber's FCI operates on adversarial behaviors and tactics, techniques, and procedures (TTPs) — not easily-evaded Indicators of Compromise (IOCs), like IP addresses or file hashes that AI-powered attackers change instantly.

FCI Successfully Detects and Neutralizes:

- Every CVE on CISA's Known Exploited Vulnerability list

- Zero-day exploits (demonstrated with Log4j, deployed countermeasure 4 hours after disclosure)
- Ransomware before encryption or exfiltration occurs
- Phishing, privilege escalation, steganography, command injection
- Authentication bypass and credential theft
- Advanced Persistent Threats (APTs)

Performance at Scale: Every day, FCI inspects over 1.5 trillion content objects, mitigating threat events across hundreds of billions of sessions within petabytes of data — all imperceptible to end users, with less than 1 millisecond of processing latency and virtually no false positives (more than 99.99% accuracy). Industry-leading NGFWs, IPS, and SWGs operating alongside FCI often miss these threats entirely.

Further, because FCI cleans instead of blocks, critical workflows and business processes are maintained.

What Trinity Cyber can replace

Legacy VPN, and ZTNA solutions
Conventional cloud delivered security (SSE, DNS layer security, cloud internet security gateways)
Threat Licenses in Next-Generation Firewalls (NGFWs)
Secure Web Gateways (SWGs)
Intrusion Prevention Systems (IPS)
Network Detection & Response (NDR) for ingress + egress use cases
Browser Isolation and Sandboxing
SSL Decryption Tools
And critically, over-reliance upon MDR services

Trinity Cyber delivers a fully-managed service for better outcomes.

TRINITY CYBER

Conclusion: The Future is Now

The MDR industry's foundation, built upon a failed detection and response model, is brittle. In 2025, Gartner has explicitly called out the limitations of convention Detection & Response and pointed to preemptive cybersecurity capabilities as the way forward. The MDR business model is unsustainable, propped up by venture capital, and serving customers with declining rates of satisfaction. Objectively speaking, MDR is frequently not a viable long-term strategy for defending critical assets.

Every organization faces three options:

1. **Status Quo:** Continue paying for MDR services that satisfy only 28% of executives, built on a conventional detection and response approach that Gartner says is failing, delivered by vendors with questionable paths to profitability.

2. **Incremental "Improvement":** Switch MDR vendors, add more detection tools, hire more analysts. Rearrange the deck chairs.

3. **Evolution:** At your own pace, implement Trinity Cyber's capabilities with Full Content Inspection to eliminate threats before they reach your network and endpoint, with the potential to reduce security spending by 50%+ while aligning with Gartner's recommendations for preemptive security that are the only viable path forward to combat the new generation of AI-generated threats.

Experience active network defense for yourself

Trinity Cyber invented FCI to win the fight against adversaries — not to simply detect their presence after they've infiltrated. It's time to stop subsidizing an industry that can't begin protecting you until a threat actor is already in your environment, and start implementing proven preemptive security that actually works. FCI operates at scale, deployed from SMB banks and credit unions and retailers to one of the three largest enterprise networks in the world.

Ready to learn more? Contact us today to see FCI in action.