TRINITY CYBER

Better Together: Trinity Cyber FCI with Endpoint Detection & Response (EDR)

Solution Brief

NOVEMBER 2025

240.654.1451
info@trinitycyber.com

 | 16701 Melford Blvd #300, Bowie, MD 20715

TRINITY CYBER

Executive summary

Security as we've known it is not keeping up. The *detect & respond* security stack — no matter how advanced — activates after malicious activity lands on your endpoints and network. That lag, across intrusion, detection, and response phases, escalates risk, noise, and cost.

Recognizing the limits of the *detect & respond* model, Gartner projects that preemptive security, the category that Trinity Cyber pioneered, will account for 50% of IT security spending by 2030. Preemptive security focuses up denying, deceiving, and disrupting adversaries. Employing each of these three elements, Trinity Cyber's Full Content Inspection (FCI) engine, used across the Trinity Cyber platform, is an inline capability that neutralizes attacks in real time — maintaining business processes — before the threat reaches your network and endpoints.

As a preemptive security technology, Trinity Cyber FCI is used by leading enterprises, including one of the three largest enterprise networks in the world. FCI both strengthens security posture and radically reduces alert volume. By reducing alert pressure, FCI helps enable internal, managed SOC, and Managed Detection and Response (MDR) teams to avoid alert fatigue and burnout.

Layered threat defense is a best practice. Accordingly, Trinity Cyber recommends that organization also deploy Endpoint Detection and Response (EDR) as a last line of defense. Organizations should deploy Trinity Cyber's FCI in front of their EDR to sanitize web content, file attachments, and more in real time. With this approach, Trinity Cyber FCI reduces risk, shrinking the attack surface that endpoints see. The result is fewer incidents, less disruption to critical business operations, happier end users, and a lower total cost of defense.

Interoperability with EDR Platforms

Trinity Cyber's inline FCI capability interoperates seamlessly with the EDR you choose, because FCI does not compete for endpoint control, drivers, or detections. It sanitizes content before endpoints process it, and shares rich logging context with the tools you already use, like Splunk.

Trinity Cyber FCI works with all leading EDR solutions, including those from:

- Microsoft
- Crowdstrike
- SentinelOne
- Palo Alto Networks
- Broadcom (Carbon Black)
- Huntress
- Trellix

Detection & Response Challenges

Business, communications, and transactions must continue — including when your personnel are collaborating with compromised customers, suppliers, and partners. The traditional *detection & response* security model:

- **Misses critical threats**, raising risk of ransomware, customer data compromise, and loss of intellectual property

- **Impedes productivity** by blocking or alerting vs. sanitizing in real time business-critical content
- **Frustrates users** with delays (e.g., sandboxing)
- **Overwhelms admins** with alerts and investigations.

Clearly, security grounded primarily in detection and response is not working. The market's move toward preemptive controls is a direct response to these gaps. While there are many use cases where *detection & response* tools like Network Detection and Response (NDR) can be retired for ingress – egress monitoring by Trinity Cyber FCI, we recommend maintaining Endpoint Detection & Response (EDR) for defense in depth.

How FCI is a Complementary Defense

IT and security teams need uptime with strong, real-time defenses that keep pace with business. Trinity Cyber delivers that by sanitizing threats in-line—before reaching the endpoint.

- **Full Content Inspection (FCI)** decrypts traffic (including SSL/TLS where policy allows), parses protocol, computer language, and file content, and surgically removes malware and exploit components from the objects themselves—not just blocking, but fixing content so users can continue working safely.
- **Superior threat protection.** Context-aware semantic intelligence inspects the exact layers where adversaries operate—protocol, script, and file content—to neutralize payloads and exploit chains before execution.
- **Near-zero false positives.** Security you can actually run at full strength: <0.01% false positives with full admin visibility into every action FCI takes. Today, the system protects 3M+ users.
- **Real-time operation, invisible to users.** Inline processing adds <1 ms latency, keeping people productive.
- **Proven scale.** Infrastructure that reliably inspects **1.5 trillion content objects per day**.
- **Zero-day defense.** By analyzing and modifying content rather than chasing signatures or IoCs, FCI **stops novel malware variants** from the first sighting.

Defense in depth is recommended: Trinity Cyber FCI prevents; EDR detects and responds if anything malicious still gets through. Together, they form a better security posture and user experience. Think about the different roles of FCI and EDR in a kill chain:

1. **Ingress:** FCI sits in front of endpoints—via agent ZTNA or tunnel—to sanitize attachments, links, and web content. Malicious macros, weaponized documents, embedded scripts, and exploit kits are removed in real time.
2. **Execution prevention:** Because the adversary's content is altered pre-execution, the endpoint rarely sees a runnable payload. **Your EDR is now focused on true edge cases,**

reducing noise.

3. **Lateral movement & persistence:** Beyond Trinity Cyber ZTNA lateral movement control, if anything anomalous executes, EDR remains a last line of defense — monitoring processes, memory, and persistence with host isolation and remediation.

4. **Egress protection & exfiltration:** FCI inspects outbound flows as well, disrupting common C2 patterns and neutralizing exfiltration tooling embedded in content (archives, scripts, HTML smuggling), reducing what EDR needs to chase after the fact.

Operational Advantages for IT and Security Teams

- **Fewer incidents to investigate.** By removing payloads pre-delivery, the SOC/MDR sees fewer EDR alerts and fewer false positives.
- **Shorter MTTR with better context.** FCI logs contain **content-level detail** (what was removed, where in the file or protocol), giving analysts high-value context for correlation with EDR telemetry.
- **No user or business disruption.** Unlike detonation/sandboxing, FCI does not hold content or block; it **sanitizes and lets business continue**.
- **Lower total cost of ownership.** In some environments, customers can reduce or eliminate their MDR investment. With stronger threat defense, less alert fatigue, fewer reimages, fewer help-desk tickets, and reduced spend sprawling security tooling, FCI and EDR make sense.

Business outcomes you can quantify

- **Incident reduction:** Fewer malware and ransomware footholds from email and web.
- **User satisfaction:** Real-time processing that adds **<1 ms latency**—no sandbox delays, fewer blocks, continued access to cleaned content.
- **SOC efficiency:** Material reduction in alert volume for the EDR team; clearer correlations with rich content-layer forensics.
- **Lower TCO:** Less time spent reimaging, investigating, and tuning noisy detections; reduced infrastructure for detonation/sandboxing.
- **Executive confidence:** A strategy aligned to where the market is heading—**preemptive controls first**, with EDR as a resilient backstop.

Conclusion

The industry is shifting from *detect & respond* to preemptive security — and for good reason. Trinity Cyber's Full Content Inspection delivers preemptive protection today, complementing EDR by drastically shrinking the threats that reach the endpoint.

