opentext™

EXECUTIVE BRIEF

EDR stops at detection. Threat response starts with DFIR.

Moving beyond detection to investigation, response, and resilience

According to Cybersecurity Insiders, 83 percent of organizations reported at least one insider-related incident in the past year.

In the world of cybersecurity, most organizations begin with prevention. Endpoint detection and response (EDR) solutions are now standard tools for security teams, promising to detect threats, trigger alerts, and help keep attackers at bay. For a long time, that was enough. But threat actors have evolved, and with them, the limitations of EDR have become clear.

Modern attackers are stealthy and sophisticated. They execute attacks designed to bypass traditional detection methods, slipping past EDR solutions without raising alarms. When a breach does occur, EDR might provide a signal, but it can't always answer the bigger questions: How did they get in? What did they access? What data was exfiltrated? Where did they go next?

That's where digital forensics and incident response (DFIR) comes in. DFIR gives organizations the ability to investigate incidents with forensic depth, respond decisively, and ensure regulatory compliance. Rather than being just a technical function, it's a strategic capability that transforms how security teams understand and react to threats.

The case for DFIR

While EDR tells you *something* happened, DFIR tells you *everything* that happened. It reconstructs attack timelines, identifies compromised endpoints, collects and preserves digital evidence, and enables real-time response. It doesn't just help you recover but also helps you understand, contain, and prevent recurrence.

Digital forensics and incident response is not just about identifying a threat, it's about understanding it. It's about being able to confidently say, "Here's what happened, here's how it happened, and here's how we'll make sure it doesn't happen again." This level of insight is what turns cybersecurity from a reactive function into a proactive business enabler.

For highly regulated industries, this visibility is essential. Regulatory frameworks like GDPR, HIPAA, and the SEC's cyber disclosure rules require accurate incident timelines, defensible evidence handling, and timely reporting. DFIR supports these needs with forensic-grade documentation and chain-of-custody controls.

And compliance is just the beginning. The legal exposure that follows a breach, such as class action lawsuits, data privacy fines, and reputational damage, can be mitigated when companies have strong forensic capabilities. Regulators, insurers, and customers all want to see that an organization can investigate and respond with precision.

DFIR also plays a critical role in managing insider threats. According to Cybersecurity Insiders, 83 percent of organizations reported at least one insider-related incident in the past year.[1] Many of these attacks don't trigger alerts in traditional EDR or SIEM systems because they involve authorized users abusing their access. DFIR solutions allow organizations to track user behavior, examine file access patterns, analyze registry changes, and even investigate messaging platforms and chat logs. This gives security teams the tools they need to confirm suspicions, act, and prevent future abuse.

What to look for in a DFIR solution that complements your EDR?

A modern digital forensics and incident response solution is purpose-built for SOC teams that need to seamlessly move from investigation to containment. It combines deep forensic analysis with rapid incident response in a single, scalable platform. Key capabilities include:

- **Live endpoint isolation and remediation:** Analysts can remotely disconnect compromised machines, delete malicious files, terminate rogue processes, and edit registry entries in real time.
- **Artifact-based workflows:** The solution collects only the most relevant forensic artifacts instead of imaging full disks, reducing investigation time, and accelerating evidence analysis.
- **YARA and IoC scanning:** Customizable rules enable proactive detection of threats across enterprise endpoints before an alert is triggered.
- **Seamless integration:** Open APIs allow orchestration with SIEM, SOAR, and other components of the security stack.
- **Enterprise scalability:** Designed to manage hundreds of thousands to millions of endpoints simultaneously.
- **Zero trust alignment:** Supports secure remote collections, off-VPN acquisitions, and tamper-proof evidence handling.
- **Multi-user collaboration:** Facilitates real-time case sharing, simultaneous investigations, and centralized case management across global teams.

A well-architected DFIR solution enables a seamless pivot from insight to action, minimizing dwell time, reducing risk, and eliminating manual hand-offs.

[1] Cybersecurity Insiders, *2024 Insider Threat Report*

Resources

For more information on how OpenText can help you strengthen your EDR with DFIR capabilities, contact us at OpenText DFIR ›

The executive business case: DFIR as a profit protection engine

For senior leaders, DFIR is more than a security control. It is a balance-sheet safeguard. Independent studies (IBM Cost of a Data Breach 2024) place the average global breach at $4.88 million, with US incidents climbing beyond $9 million. Breaches that linger undetected for more than 200 days cost nearly 30 percent more than those contained quickly. DFIR platforms shorten investigation and containment windows from weeks to hours, directly reducing the most expensive phase of a cyberattack: operational downtime, regulatory fines, legal exposure, and brand erosion.

A robust DFIR capability also improves cyber insurance economics. Underwriters increasingly reward enterprises that can demonstrate forensic readiness with lower premiums, higher coverage limits, and faster claims processing.

The investment case extends to human capital efficiency. Automating evidence collection and case management reduces analyst hours per incident and lowers overtime costs, while preserving scarce talent for higher-value threat-hunting and risk-reduction work.

When executives view DFIR through a financial lens, the payback is compelling:

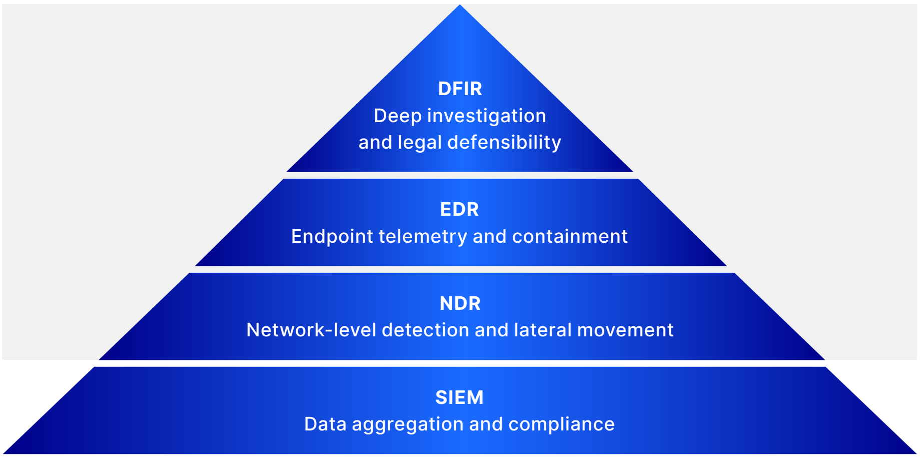
- Cost avoidance
- Cyber insurance premium optimization
- Regulatory risk mitigation

In short, DFIR converts cybersecurity from a pure cost center into a risk-adjusted ROI engine. Organizations that fund forensic readiness aren't just buying technology—they are buying predictability: predictable breach costs, predictable recovery timelines, and predictable compliance outcomes that protect revenue and shareholder value.

Conclusion: Respond with confidence

In today's cyberthreat landscape, knowing that something happened isn't enough. You need to know what happened, how it happened, and how to ensure it doesn't happen again. EDR is the starting point, but DFIR is the follow-through.

OpenText™ Endpoint Forensics & Response is just the solution to deliver the needed DFIR follow-through. It empowers your team to move from alerts to action, from chaos to clarity, and from breach to business as usual. Because in cybersecurity, precision isn't just power. It's protection.


DFIR
Deep investigation and legal defensibility
EDR
Endpoint telemetry and containment
NDR
Network-level detection and lateral movement
SIEM
Data aggregation and compliance