OpenText Endpoint Forensics & Response

Collect evidence, isolate threats, and remediate fast, because in cyber defense, DFIR precision makes all the difference

Benefits

- Scales to >1 million endpoints for broader visibility
- Artifact-driven workflows for less noise and faster response
- Endpoint isolation to contain threats and minimize disruption
- Remediation to remotely quarantine active threats

When organizations experience a breach, they often struggle to answer critical questions, such as what happened, how it happened, what data was accessed, whether the threat is still active, and whether they are legally liable. Traditional security tools either lack deep forensic visibility, slowing down response with manual workflows, or fail to maintain defensibility during investigations. The result is extended dwell time, poor root cause analysis, regulatory risk, and delayed recovery.

OpenText™ Endpoint Forensics and Response helps security teams optimize cybersecurity digital forensics and incident response by enabling them to uncover the truth faster and take immediate, decisive action, all within a single, scalable platform.

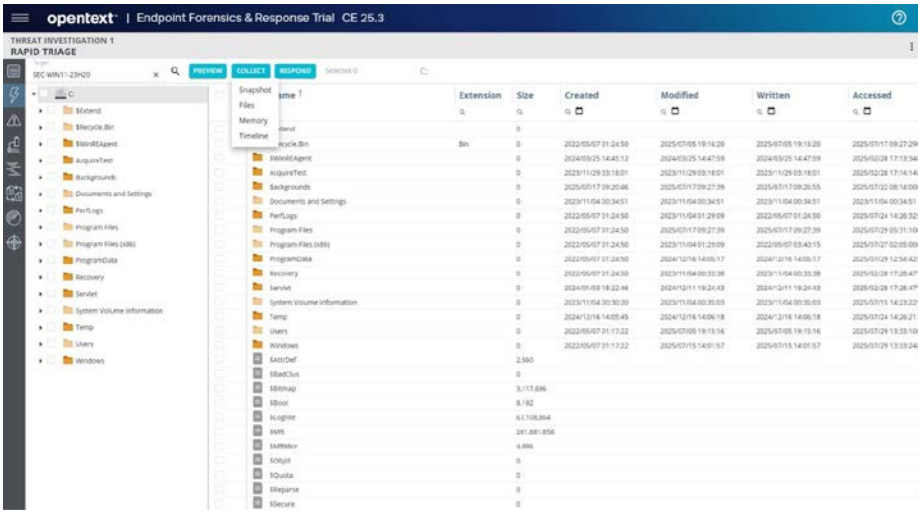
By integrating deep digital forensic capabilities with near real-time incident response functions such as endpoint isolation, file/process remediation, registry cleanup, and IoC scanning, OpenText Endpoint Forensics and Response delivers a seamlessly integrated solution that reduces dwell time, prevents lateral movement, and accelerates threat resolution.

Security professionals no longer need to pivot between tools or lose precious context. With OpenText Endpoint Forensics and Response, they can investigate and respond within the same interface, boosting productivity, minimizing disruption, and strengthening enterprise-wide cyber resilience.

Scalability: Unlike DFIR solutions that struggle with performance degradation or are designed for case-by-case use, OpenText Endpoint Forensics & Response is engineered to handle collections across more than one million endpoints simultaneously. This makes it ideal for global enterprises with distributed, hybrid environments, ensuring fast, reliable investigations without bottlenecks, even during large-scale incidents.

The OpenText Cyber Resilience Program (CRP) helps customers effectively reduce risk, preserve trust, and minimize disruption. From prevention, detection, and response to recovery, investigation, and compliance, we help organizations build cyber resilience.

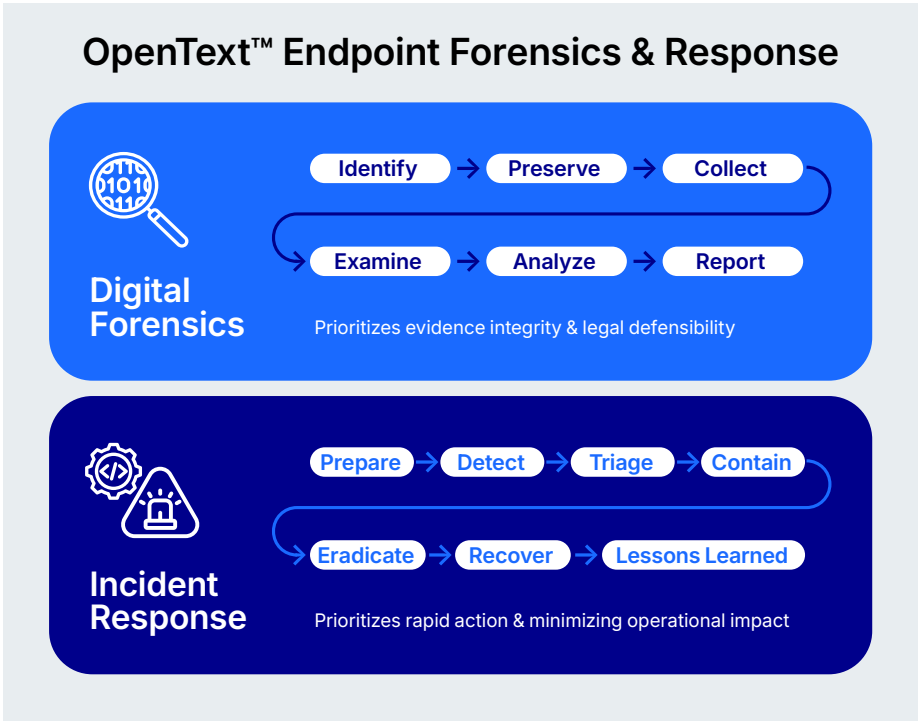
Cybersecurity Services ›



Automation and efficiency: Instead of operating in isolation or requiring manual handoffs, OpenText Endpoint Forensics & Response integrates with your existing SIEM, SOAR, and EDR tools, amplifying the effectiveness of your incident response playbooks. It extends automation across the endpoint layer, allowing teams to trigger evidence collection, isolate systems, and remediate threats directly within orchestrated workflows. This reduces manual effort, shortens response timelines, and ensures a more cohesive, context-rich investigation process.

Enterprise zero trust: OpenText Endpoint Forensics & Response is designed for organizations adopting zero-trust security models. It offers centralized control for managing evidence collection and response across distributed endpoints (both on and off the network) and integrates seamlessly into enterprise ecosystems. As a robust digital forensics and incident response tool, it ensures that security teams have the forensic visibility and near real-time response needed to detect, isolate, and investigate threats.

Collaboration and multi-user access: Unlike tools designed for individual analyst workflows which leave collaboration to occur as a post-analysis activity during the reporting phase, OpenText Endpoint Forensics & Response enables multi-user, simultaneous access, near real-time collaboration and centralized case management.



Resources

OpenText Endpoint Forensics and Response
Product Page ›

DFIR: The unsung hero of cybersecurity
Read the blog ›

A Day in the Life of a SOC Analyst ›

DFIR precision, speed, and forensic-grade integrity

Whether identifying the root cause of an incident, containing threats, or preserving court-admissible evidence, OpenText Endpoint Forensics & Response enables teams to reduce dwell time, accelerate remediation, and strengthen compliance, all while minimizing operational disruption. Recognized for its enterprise-first architecture that is purpose-built for scale, integration, and security, OpenText Endpoint Forensics & Response, brings organizations the DFIR precision, speed, and forensic-grade integrity needed to outpace today's threats and future-proof their cyber resilience.

Features	Benefits
Artifact-driven workflows	Speeds investigations by focusing only on relevant data, reducing noise, improving efficiency and analyst productivity, and improving response times
Deep-dive forensic investigation capabilities	Provides root-cause clarity, uncovers hidden threats, delivers court-admissible evidence, enables informed response and regulatory readiness, allowing security teams to move from chaos to control faster, smarter and with higher assurance
Endpoint isolation	Instantly contains threats while preserving forensic access, stops lateral movement, minimizes business disruption, boosts incident response confidence, and supports zero trust principles
File remediation	Enables SOC teams to act immediately, remotely deleting, quarantining or neutralizing malicious files, reducing dwell time, damage, and operational disruption
Process remediation	Immediately halts active threats, critical for minimizing attack impact
IoC scanning with YARA support	Proactively detects threats faster, automates investigations and reduces risk exposure, enhancing detection precision and breadth
Registry search & live remediation	Equips DFIR teams to identify and disable threats, preserve business operations, and boost security posture with zero downtime
Pivot directly from investigation to response	Gives security teams speed, clarity, and control, enabling faster, smarter decisions in high-stakes situations
Modern web UI	Delivers faster time to action, increased analyst productivity and support of remote and distributed teams, while reducing IT overhead, improving cross-functional collaboration and enhancing tool adoption
Integrated threat intelligence	Transforms DFIR operations into a smarter, faster, and more strategic function, helping organizations detect early, respond accurately, and evolve continuously in the face of evolving threats

opentext™