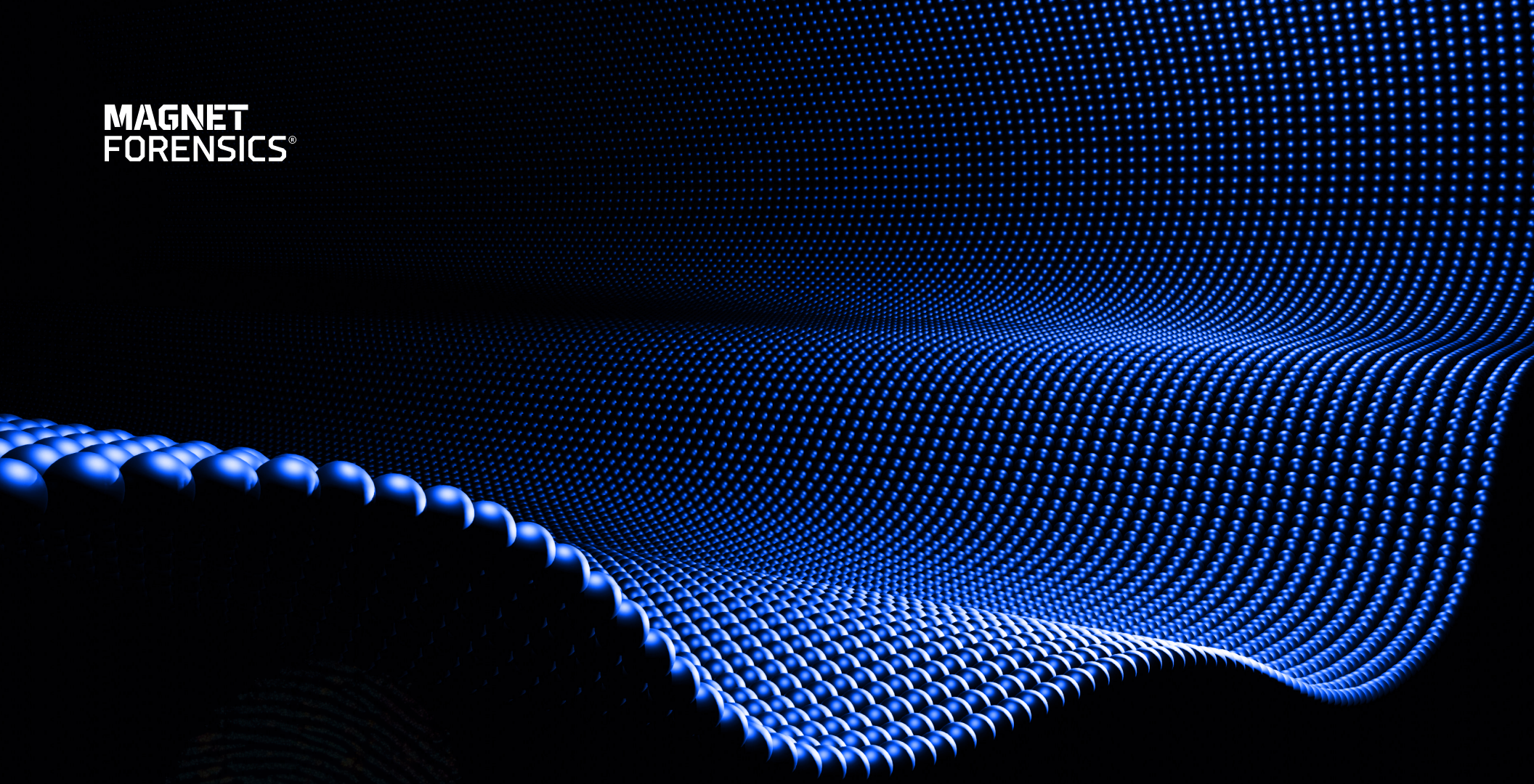
MAGNET FORENSICS®



Uncover the Value of DFIR

How digital forensics delivers an unbeatable ROI and enhances resilience

The unmet need for DFIR tools

The gap between digital forensics and incident response (DFIR) needs and the ability of existing toolsets to meet them results in post-incident investigations that are typically slow, costly, and, worse, incomplete.

Digital forensics functions are often handled by repurposing various security tools, such as endpoint detection and response (EDR) solutions and various open-source tools. These can be effective for alerting SOCs to an issue, but are a fragmented, largely manual approach that poses challenges and risks to organizations, such as compromising or destroying digital evidence and not identifying an incident's root cause.

The size and complexity of attack surfaces leave critical forensics information and evidence spread across disconnected systems and repositories. A lack of digital forensics solutions that take in all data sources, including volatile data, can leave a company exposed in the wake of a cyber incident.

Inability to identify the root cause of cyber incidents

Without understanding the cause of an incident, remediation tactics may only patch the immediate issue, leaving an organization at risk of future attacks exploiting the same vulnerability.

Compromised forensic data integrity

Internal IT teams without specialized tools and training can accidentally alter or destroy data, resulting in a non-defensible collection or missing important artifacts, such as metadata. Additionally, critical evidence can be lost quickly due to system reboots, log rotation, anti-forensic tools, or automated cleanup.

Regulatory, legal, and compliance exposure

Organizations that fail to identify and remediate the root causes of cyber incidents can miss notifications, leaving them at risk of fines, contract breaches, litigation, and harsh regulatory scrutiny.

> Stringent regulatory requirements and compliance standards have driven the adoption of digital forensics solutions to ensure the integrity and security of digital evidence."
>
> —
>
> **Grand View Research**
> Digital Forensics Market Size, Share & Growth Report

DISPARATE DATA SOURCES

- Cloud services
- SaaS applications
- Endpoints
- EDR telemetry
- Identity providers
- VPNs and remote-access gateways
- Privileged access management (PAM)
- Firewalls
- Network protocol analyzers
- Routers and switches
- Proxies and web gateways
- Web application firewalls (WAF)
- CDN logs
- IDS/IPS
- NDR
- Application servers
- Database servers
- XaaS
- Container platforms
- CI/CD
- Storage
- Backup systems
- Email
- SIEM
- DNS servers
- Physical security logs
- IoT, OT, and ICS devices
- Third-party audit logs

Costs of skipping post-incident digital forensics

Not conducting root-cause analysis after a cyberattack is expensive. Extended detection and containment times are among the largest contributors to multimillion-dollar breach costs, and both are directly impacted by the speed and completeness of post-incident investigations.

Beyond the immediate costs of losses and remediation, repeat incidents resulting from failure to identify the root cause drive long-term costs. According to the 2025 Cost of a Data Breach (COBD) Report by IBM and the Ponemon Institute, the average cost of a data breach in the United States is $10.22 million, almost 2.5 times higher than the global average of $4.44 million.

The cost of exposure from breaches grows every day that they are not resolved. Organizations continue to struggle to detect and remediate attacks. The COBD report also found that, on average, breached data stored across multiple environments took 276 days to identify and contain. Third-party vendor and supply chain compromise took 267 days, and malicious insider attacks took 260 days.

Ransomware remains a top financial threat because it combines operational disruption, ransom settlement costs, recovery expenses, and lost revenue, making ransomware incidents among the costliest individual breaches. The 2025 Barracuda Ransomware Insights Report found that 57% of organizations surveyed had experienced a successful ransomware attack in the past 12 months, and one in three victims were affected twice or more.

According to the 2025 Sophos State of Ransomware report, the average ransom payment was $1 million, and the average cost to recover from a ransomware attack was $1.53 million. Security gaps were cited as the primary cause of ransomware attacks, with 40.1% exploiting unknown gaps and 38.2% exploiting known security gaps that had not been addressed.

Failing to perform root-cause analysis delays recovery and can compound damage. From persistent threats, compliance violations, and reputational damage, the risks and associated costs can be catastrophic.

—

SOURCES:

IBM Cost of a Data Breach Report 2025
Barracuda The Ransomware Insights Report 2025
Sophos The State of Ransomware 2025

How digital forensics enhances cybersecurity and reduces risk

Digital forensics integrates two key disciplines to streamline investigations and speed up cyber threat detection and containment. Digital forensics goes beyond simple incident remediation and looks to uncover the root cause, understand the scope, mitigate damage, preserve evidence, and eliminate vulnerabilities that can be exploited in future attacks.

Digital forensics capabilities

By identifying the root cause of incidents, digital forensics allows security teams to:

- Uncover attack methods and motives to focus cyber defense fortification and enhance digital resilience.
- Understand the actual issue behind a cyber threat or attack rather than simply treating symptoms.
- Expedite isolation of affected systems after an incident to minimize financial losses and operational disruptions.
- Ensure compliance with regulatory requirements for cybersecurity and cyber risk management.
- Identify persistence and backdoor mechanisms to prevent future compromises.
- Share IOCs with proactive defenses, such as blocklists, SIEM, EDR, and NGFW policies, detection rules, and threat hunting playbooks.
- Use post-incident findings to update and optimize policies, processes, and training.

> DFIR isn't just about knowing that something happened—it's about understanding how, why, and what it impacted. That's the kind of insight that drives meaningful response—and prevents future incidents."

Why CISOs invest in DFIR

CISOs put DFIR into their tight budgets because they know that it is an invaluable resource to:

- **Respond to the complex and evolving threat landscape,** which is fraught with sophisticated attacks targeting an ever-expanding attack surface.
- **Meet increasing regulatory requirements** for cybersecurity and risk management with heightened scrutiny by regulators and costly penalties for violations.
- **Take a proactive approach to cybersecurity** by seeking out and eliminating the root causes of cyberattacks to minimize risk and prevent future incidents.
- **Gain valuable data to identify and understand security gaps,** demonstrate the business value of cybersecurity investments, and justify ongoing security budgets.
- **Lower cyber insurance premiums** by eliminating the root cause of risk and enhancing digital resilience.

Connecting detection, response, and investigation

Digital forensics as a practice and digital forensic solutions work with existing cybersecurity tools to create greater value and protection and improve digital resilience. When integrated with other tools and processes, digital forensics replaces noise with verified actions, reduces recovery time, and hardens systems against repeat attacks.

How digital forensics solutions work with cybersecurity tools

Detection and response (EDR and XDR)

An EDR alert flags suspicious activity on a host, prompting a DFIR analyst to perform a quick remote triage to capture context and decide whether to collect full memory and targeted disk artifacts. The forensic data is analyzed to identify any persistence mechanisms and IOCs to show the affected systems, impact, and root cause. With this information, the team can execute controlled containment actions while preserving evidence for future needs.

SIEM

SIEMs provide the centralized telemetry and correlation of log and alert data from endpoints, networks, cloud services, and authentication systems to detect and scope incidents. DFIR solutions use that telemetry plus targeted forensic collection to reconstruct the attack chain and zero in on the root cause.

SOAR

SOAR platforms orchestrate incident response workflows and can be integrated with digital forensics solutions that automate the collection, processing, and preservation of digital forensic evidence. The SOAR system triggers forensic playbooks that support digital forensics, such as gathering memory, disk, and log data, and attaching artifacts to incidents for analysts. This integration speeds investigations, ensures consistency, and preserves evidence integrity.

Results of digital forensics integrations

- **Rapid triage and response**
  Digital forensics validates alerts from other systems and records exact commands taken to preserve the chain of custody.
- **Deep investigation**
  Digital forensics reconstructs the timeline, identifies root cause and any persistence, extracts IOCs and TTPs, and preserves evidence.
- **Remediation and hardening**
  Digital forensics translates root-cause information into targeted fixes, verifies the removal of persistence, retests, and validates remediation.
- **Continuous improvement**
  Digital forensics shares vetted IOCs and TTPs, lessons learned, and improved detection rules and runbooks with other cybersecurity systems.

Measuring and demonstrating the value of digital forensics

Justifying cybersecurity expenses is essential because resources are finite and executives demand clear links between investment and outcomes. Budget requests should show how security controls improve digital resilience, reduce measurable risks, and support digital initiatives.

Calculating digital forensics ROI

While limiting the scope and duration of breaches and preventing future attacks cuts costs associated with cyberattacks, reducing their likelihood with insights gained from thorough post-incident analysis provides significant savings.

SAVINGS in event of a breach = (**Breach probability** − **Breach probability with DFIR**) × **Average cost per breach**

Example: If a breach would cost $10,220,000 (the average cost of a data breach in the U.S. per the Cost of a Data Breach report) and digital forensics cuts the breach probability from 10% to 5%, the expected loss reduction would be $510,000 versus $1,200,000 without digital forensics.

(NOTE: This scenario is only an example to demonstrate a model. The actual costs and probability will vary by organization.)

> The global digital forensics market growth has been driven by the rising number of cyberattacks and data breaches happening in recent years, owing to a surge in the number of connected devices."
>
> —
>
> **Straits Research**
> Digital Forensics Market Size & Outlook, 2025-2033

Other metrics to demonstrate DFIR value

- Reduction in incident response time and costs based on mean time to detect (MTTD), mean time to respond (MTTR), and mean time to contain (MTTC)
- Compliance cost avoidance based on penalties, and legal costs avoided due to the role of digital forensics in meeting regulatory requirements for cybersecurity and risk management
- Customer trust and revenue stability by preventing breaches, increasing response speed, and minimizing damage that impacts customers
- Insurance premium reductions and improved coverage due to enhanced security posture and risk reduction

Digital forensics for cybersecurity and beyond

> Anytime I'm doing a remote collection, nine times out of 10, I will attempt to use Magnet Forensics first. I can use it to get the data, then it automatically processes it, saving me an extra step."
>
> —
>
> **Jamie Stokes**
> Senior Digital Forensics Investigator

Cybersecurity use cases

Digital forensics plays an essential role in cybersecurity, allowing organizations to take proactive measures to respond to and defend against threats. To understand specifically how digital forensics bolsters cybersecurity efforts, consider the following use cases.

Ransomware

- Create an infected-host list, timeline, and IOCs
- Identify infected hosts
- Map encryption scope
- Validate remediation and clean restores
- Determine intrusion vector

Malware

- Analyze samples in sandboxes
- Classify malware
- Extract IOCs
- Create YARA signatures
- Produce detection signatures

Business email compromise (BEC)

- Trace fraudulent emails
- Reconstruct fraud timelines
- Create mailbox artifact package
- Support legal action
- Identify mailbox rules used to hide activity

Data breach

- Pinpoint systems and accounts used for entry
- Determine what was stolen
- Stop ongoing exfiltration
- Identify IOCs
- Define remediation steps

Malicious insiders

- Correlate file access, privileged sessions, and endpoint data
- Collect admissible evidence
- Create redacted evidentiary packet
- Recommended HR actions
- Maintain the chain of custody

Cloud breach

- Identify compromised cloud accounts and resources
- Check for new roles or keys
- Capture snapshots of VMs and containers
- Detect cloud-native persistence
- Verify tenant isolation integrity

Web compromise

- Review webserver logs, modified files, and access patterns
- Determine exploit type (e.g., SQLi remote code execution)
- Search for exploit requests
- Preserve webroot
- Identify malicious uploads or backdoors

Supply chain and third-party compromise

- Identify affected systems and software
- Investigate vendor artifacts for malicious indicators
- Update SBOMs (software bill of materials)
- Assess downstream impact
- Coordinate disclosures

Proactive detection

- Validate anomalous behavior
- Discover stealthy intrusions
- Search for vulnerabilities
- Create new detection rules
- Prioritize vulnerabilities for remediation

DFIR for cybersecurity and beyond

> The demand for digital forensics is fueled by the rise in cybercrime incidents, the complexity of digital services, and the legal necessity to preserve and present digital evidence with court-admissible standards. Digital forensics is no longer confined to courtrooms or crime scenes; it is now a strategic, operational, and reputational imperative."
>
> —
>
> **Precedence Research**
> Digital Forensics Market Size to Hit USD 47.9 Billion by 2034

Corporate use cases

While digital forensics is widely associated with cybersecurity, its value extends across organizations. The versatility of digital forensics systems gives them a remarkably high return on investment. Several of the many use cases for digital forensics, beyond cybersecurity, include the following.

Legal → eDiscovery

- Collect defensible electronic evidence
- Create ESI production set
- Produce chain-of-custody package

HR → Employee misconduct

- Verify misuse, data theft, or policy violations
- Create a redacted timeline
- Develop an evidentiary packet for HR.

Finance → Fraud

- Reconstruct system access tied to suspected fraud
- Reconstruct wire or transaction fraud
- Trace funds or responsible actors

Legal → IP theft

- Identify exfiltration vectors
- Recover artifacts pointing to stolen IP
- Create a provenance report

Mergers and acquisitions → Due diligence

- Identify latent compromises or data exposure
- Detect data leakage or compliance gaps
- Create a due diligence forensic report

Compliance → Audits and regulator requests

- Demonstrate who accessed regulated data and when
- Provide immutable evidence
- Demonstrate controls for auditors or regulators

Finance → Insurance claim validation

- Validate the authenticity of media (e.g., photos)
- Create insurer-ready forensic packet
- Produce chain-of-custody artifacts
- Preserve the chain of custody for evidence

Compliance → Breach notifications

- Verify exfiltration evidence
- Confirm the scope of exposed data
- Create a notification list and timelines

Operations → Physical incident correlation

- Collect CCTV and badge logs
- Align timestamps with device logs
- Extract artifacts from endpoints tied to a person or device

Considerations when assessing digital forensics solutions

> Magnet Forensics specializes in digital investigation solutions. These solutions assist in acquiring, analyzing, managing, and reporting evidence from numerous digital sources such as mobile devices, computers, IoT devices, and cloud services. It enables investigators in tackling crime, safeguarding assets, and upholding national security in more than 100 countries."
>
> —
>
> **Gartner**
> Cloud Investigation and Response Automation (CIRA) – Magnet Forensics profile

DFIR is a key element of digital resilience and cyber readiness when the tools align with an organization's needs and available resources. When evaluating solutions, be sure to assess the following capabilities.

☑ Data collection and preservation

Conduct thorough and reliable forensic investigations with targeted remote and off-network collections from Mac, Windows, and Linux endpoints, as well as acquire and analyze artifacts from single physical drives and volatile memory to get complete visibility. Additionally, use targeted locations to limit collection, processing, and analysis to only relevant information from computers, cloud services, mobile, IoT, and third-party sources. If a target goes offline and reconnects, collections should also automatically resume.

☑ Data review and analysis

Speed the correlation of all the artifacts in a case with automated visual analysis and AI analysis that uncover patterns, create timelines, and connect artifacts. Enable searches and deep-dive analysis from any location with broad artifact support and file system views for historical long-term investigations.

☑ Remote access and sharing

Share and collaborate on all aspects of an investigation, from the workload on case setup to artifact tagging and filtering, with anyone (e.g., examiners, non-technical reviewers, and other internal and external investigative team members.

☑ Mobile data extraction

Ability to gain consent-based, full file system access to iOS and Android device data, including deleted data. Additionally, access credential stores (e.g., Keychain and Keystore) to decrypt content. While logical or category-based extractions support targeted, compliance-driven collections, full file system access delivers the deeper, more comprehensive artifact and deleted-data visibility investigators need when the scope expands beyond what limited collections can surface.

☑ Automated workflows

Use templates or drag-and-drop capabilities to modify or build custom automated forensic workflows for end-to-end evidence processing. Save workflows for future use to ensure consistency.

☑ Integration

An investment in DFIR should cover a full suite of cybersecurity tools that can integrate with existing cybersecurity tools (e.g., XDR/EDR, SIEM, and SOAR), mobile data acquisition, and business system tools. Integration capabilities should also support automated collections and the ability to use custom scripts.

For more information about Magnet's enterprise digital forensics and incident response solutions, visit our Enterprise Solutions page:

magnetforensics.com/solutions-enterprise-forensics

Magnet Forensics is a developer of digital investigation software that acquires, analyzes, reports on, and manages evidence from computers, mobile devices, IoT devices, and the cloud used by over 4,000 public and private sector organizations in over 90 countries and has been helping investigators fight crime, protect assets, and guard national security since 2011.

MAGNET FORENSICS®

Magnet Forensics can help you and your organization with your digital forensics investigation needs. Please visit **magnetforensics.com** or contact **sales@magnetforensics.com**.

© 2026 Magnet Forensics Inc. All rights reserved. Magnet Forensics® and related trademarks are the property of Magnet Forensics Inc. and its affiliates and used in countries around the world. This Report is current as of the initial date of publication and may be changed by Magnet Forensics at any time without notice. The information contained in this Guide is for general informational purposes only, and is provided "AS IS", without any representations or warranties, express or implied. Magnet Forensics does not accept responsibility for any omission, error, or inaccuracy in the gBook, or any action taken in reliance thereon. To learn more about how.