Trellix

WHITE PAPER

Advanced Forensic Analysis with Trellix® EDR with Forensics (EDRF)

Part 1: Automated Triage and AI-assisted Investigation

Executive summary

Modern adversaries utilize obfuscation, fileless execution, and legitimate system tools to evade detection. Trellix Endpoint Detection and Response with Forensics (EDRF) addresses these challenges by integrating real-time detection with deep-dive forensic capabilities. This white paper is part one of a three-part series that provides a technical framework for conducting end-to-end forensic investigations using the Trellix ecosystem, detailing the transition from automated triage to granular artifact acquisition and analysis.

We have prioritized optimizing the most labor-intensive and complex phases of the security analyst's workflow, referred to as "phase 2" and "phase 3." This may seem unusual. However, the concept of mean ime to investigate (MTTI) is often the "long pole" across the lifecycle of threat detection, investigation, and response (TDIR), where most of the time and effort is put in, and is an area frequently overlooked by other vendors. In this paper, we will focus on how Trellix EDRF provides advanced capabilities in delivering critical security outcomes for:

1. **Deep-tier Forensic Visibility:** Unlike standard EDRs that provide ephemeral telemetry, Trellix EDRF delivers a "time machine" for the enterprise. It captures deep-system artifacts—including memory dumps and master file table (MFT) audits—ensuring that the root cause of a breach is never lost to system volatility.
2. **Expedited Investigations with Trellix Wise™:** We solve the "talent gap" by embedding a generative AI analyst directly into the forensic workflow. Gone are the chair pivots between disconnected tools and the manual time-consuming steps that drain analyst bandwidth. Trellix Wise automates alert investigations, reducing the mean time to respond (MTTR) by up to 50% and allowing junior analysts to perform at the level of senior forensic investigators.

Each one of these pillars—along with supporting every part of your environment and rooting out even the most advanced threats—is essential to align an organization's security operations with business objectives.

Enhancing business outcomes

In the modern threat landscape, maintaining business continuity against sophisticated attacks requires a shift from reactive recovery to surgical precision. This means moving beyond simply detecting and responding to threats—and toward proactively hardening systems against future attacks and emerging variants. Trellix EDRF helps ensure that while security teams dive deep into investigations, business-critical assets remain operational and compliance standards stay rigorous. It also frees the security operations center (SOC) from the burden of manual triage, allowing teams to focus on delivering timely responses to identifying a threat and proactive defense, as shown by the diagram below.

The Trellix EDRF architecture

The Trellix EDRF architecture is designed for continuous visibility. Trellix EDRF is unlike standard EDRs that provide ephemeral telemetry based on transient data that resides primarily in memory (RAM), temporary files, or volatile network connections, making it crucial for real-time investigation but difficult to capture after the fact. Trellix EDRF instead delivers a “time machine” for the enterprise. It captures deep-system artifacts—including memory dumps and master file table (MFT) audits—ensuring that the root cause of a breach is never lost to system volatility.

Trellix EDRF utilizes a multilayered approach:

- **Threat Detection:** It collects and analyzes data quickly to surface advanced and targeted attacks.
- **The Forensics Engine:** It enables automated and on-demand, non-persistent data collection, allowing for the acquisition of deep-system artifacts like memory dumps and full disk images without requiring remote shell access.
- **Threat Hunting:** It collects data locally and enables connected systems to be queried near real-time. It continuously streams endpoint telemetry (processes, network flows, registry changes) to a centralized Telemetry Store for historical search.
- **Rapid Response:** It doesn’t stop at detection. It also enables enterprises to respond quickly and at scale to stop an ongoing attack, collect data, and isolate affected systems.

From here, we will dive into phase 2, the forensics engine, automated investigative capabilities, and AI-driven threat hunting.

The forensic workflow: A technical deep dive

Traditionally, when an EDR solution detects an alert, it grabs artifacts and behaviors necessary to determine there may be a threat. These artifacts and behavioral indicators are collected and returned to the analyst as a correlated alert.

For each alert generated, an investigation of the alert elements is performed by an analyst to determine the validity of the alert as a threat, if additional investigative actions such as forensic data collection should be taken, and what, if any, response is required to isolate or eliminate the threat.

In many cases, each alert can generate dozens of individual artifacts that need to be researched. An alert investigation can take hours to complete. The analyst needs to be able to identify quickly when additional data is needed and a response action needs to be taken to stop an ongoing attack, reduce exposure, or remediate the affected system. Any delay in analysis increases the likelihood of broader impact and may also result in the loss of artifacts that could have contributed to the forensic understanding of an attack.

Figure 1. Process timeline view of an alert with over 500 individual events.

Trellix Wise and Trellix EDRF triage automation help to reduce the time challenges involved in alert review and reduce the risk of losing volatile artifacts related to the threat.

Trellix Wise

Trellix Wise is an AI assistant that accelerates alert review by analyzing all of the collected events into an easy-to-understand narrative of the event. With Trellix Wise, an analyst can request a summary or interact with the LLM to ask questions about the data collected. Figure 1 is an example of a process timeline for a single alert with over 500 related events. Figure 2 shows the power unlocked with Trellix Wise to review over 500 events in under a minute and consolidate them into a straightforward summary of the alert.

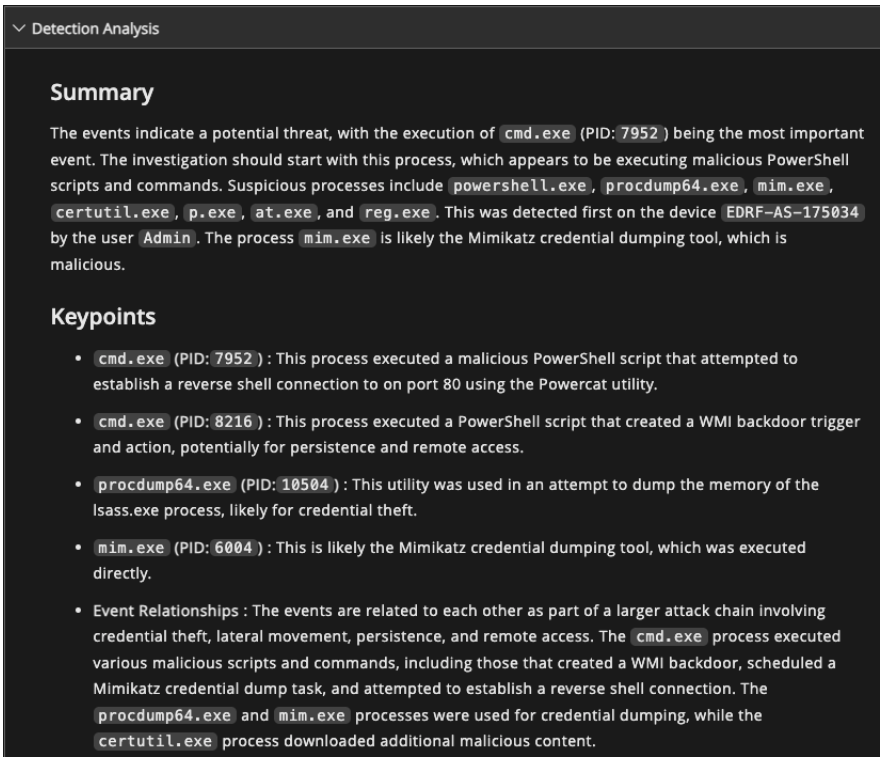

Figure 2. Trellix WISE AI summary of the events in Figure 1.

Additionally, Trellix Wise provides an analyst with the ability to research more details about the alert—such as related global breaches, MITRE ATT&CK tactics and techniques, and more details related to the specific alerts.

Trellix Wise will also provide the analyst with recommendations for what to do next, including what actions to take on the target system, real-time search queries, and forensic data collection. Figure 3 shows the suggested action specific to the alert summarized by Trellix Wise in Figure 2.

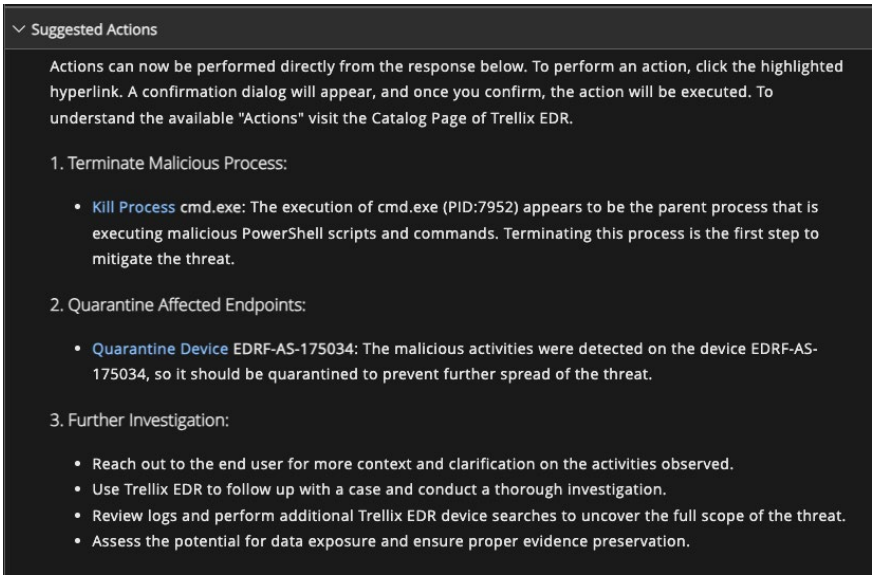

Figure 3. Trellix Wise accelerates response by guiding the analyst to perform certain actions.

Triage automation

Detection is only the starting point. A single alert rarely tells the full story—effective investigation demands broader context, deeper artifacts, and the ability to collect data quickly without disrupting the analyst's workflow. This is where automated triage data collection becomes the force multiplier for SOC teams.

With many solutions, forensic data collection involves manually deploying a package of scripts to collect data for review. Often, this represents a delay from the time an alert occurred and the time the data was collected. Forensic data elements can be volatile; data that lives in memory, scripts that have run, or clean-up actions taken by a threat actor can go undetected even in forensic collection if the collection isn't triggered soon enough.

Trellix EDRF includes forensic automation through triage. When Trellix EDRF detects an alert, it can automatically trigger the collection of full investigative data. This preserves more artifacts, provides a more complete understanding of what happened before and after an attack, and accelerates the ability to fully understand the impact of a threat.

Analysts can design their own baseline of forensic data collection using the built-in script builder, without the need to write code, and then define the automation triggers.

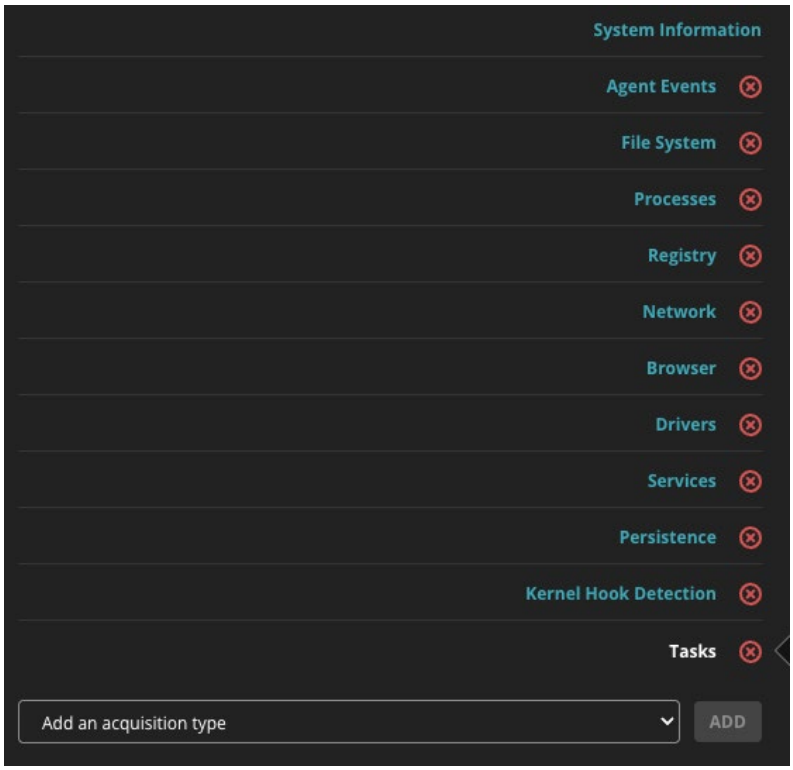

Figure 4. Users can define the forensic elements they want automatically collected.

While collecting forensic data is an important investigative step, it can also be overwhelming. Trellix EDRF not only provides the power of expediency, it also provides the power of forensic data analysis. Triage summary within the platform enables an analyst to quickly see the timeline of collected events, allowing them to quickly search for root cause, lateral movement, and changes to the host made by the attacker.

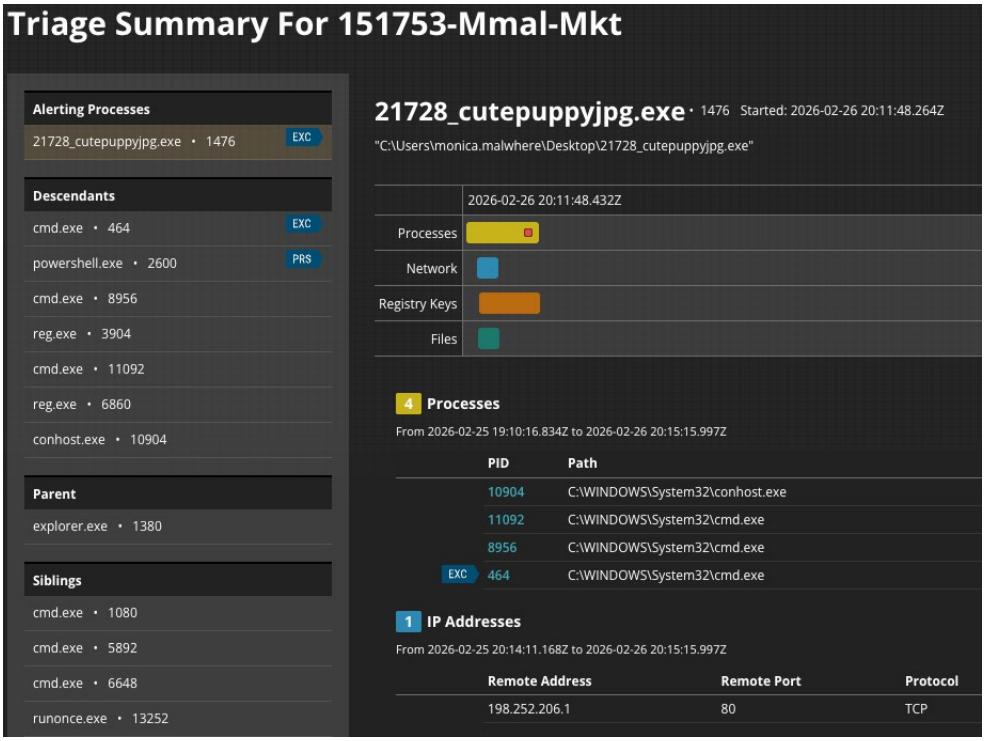

Figure 5. Triage collection of forensic data organized by timeline and artifact type.

Additional data acquisition strategies

Beyond full forensic capture, analysts have the flexibility to perform more granular data collection on a host. Some examples of a more-targeted approach include:

1. **File Acquisitions:** Targeted retrieval of specific files (e.g., a suspicious .ps1 script or a locked database file).
2. **Data Acquisition (Full Disk/Memory):** For cases requiring deep-dive analysis (e.g., rootkit detection), Trellix EDRF can perform a full memory dump or partial/full disk image capture.

Logon Tracker: Visualizing lateral movement

Logon Tracker visualizes historical logon activity and automatically alerts analysts to malicious remote desktop login attempts—providing the timeline context needed to separate routine access from adversarial movement. This can be utilized as an enricher for login context, or as an investigative tool to search/filter logs that matter. This module enables the investigation of lateral movement within Windows Enterprise environments.

Logon Tracker improves the efficiency of investigating lateral movement by aggregating historical activity and monitoring new activity. This data is presented in a user interface designed for analyzing investigative leads (e.g., a compromised account) and hunting for suspicious activity (e.g., RDP activity by privileged accounts).

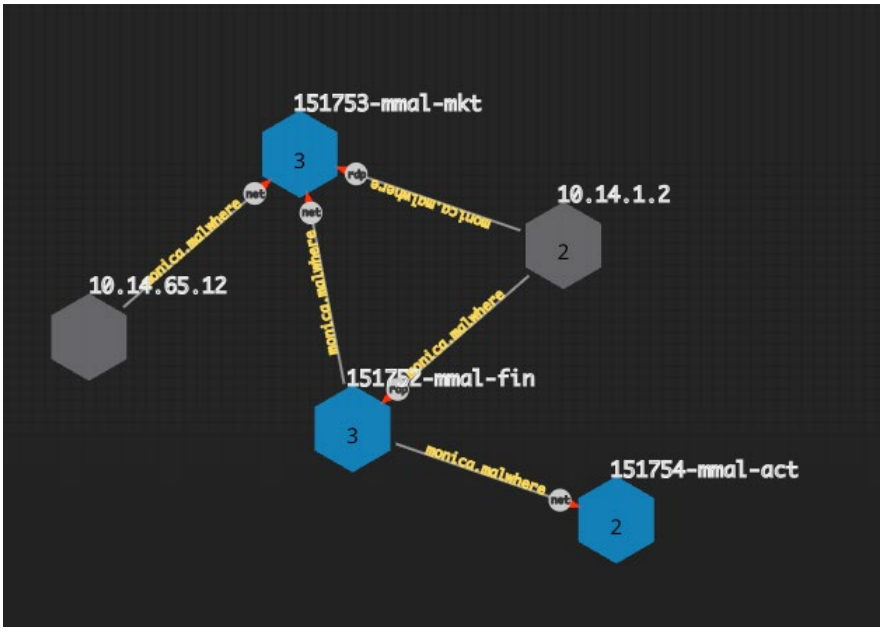

Figure 6. Quickly identify lateral movement by identifying every host a suspicious account has connected to.

Process Tracker

Process Tracker monitors and records all process execution activity on an endpoint, automatically alerting analysts to malicious events and capturing a detailed history of unique file executions for deeper investigation. An analyst can quickly identify when and where a suspicious process has executed. This helps to identify other affected systems as well as patient zero, where the threat is executed for the first time.

Process Tracker Events

Start Time	Process Path: cutepuppyjpg.exe	User	Creation Time	Hostname
2026-02-11T20:33:25.594Z	C:\Users\monica.malwhere\Desktop\6133_cute...	SELABS\monica.malwhere	2026-02-11T20:33:07.272Z	151753-mmal-mkt
2026-02-25T19:17:05.291Z	C:\Users\monica.malwhere\Desktop\115_cutep...	SELABS\monica.malwhere	2026-02-25T19:11:43.132Z	151753-mmal-mkt
2026-02-25T20:02:45.976Z	C:\Users\monica.malwhere\Desktop\21092_cut...	SELABS\monica.malwhere	2026-02-25T19:49:46.876Z	151753-mmal-mkt
2026-02-26T20:11:48.264Z	C:\Users\monica.malwhere\Desktop\21728_cut...	SELABS\monica.malwhere	2026-02-26T19:48:49.181Z	151753-mmal-mkt
2026-03-02T02:25:46.009Z	C:\Users\barty.bushes\Desktop\9612_cutepup...	SELABS\barty.bushes	2026-03-02T02:17:36.425Z	151831-bbus-mkt
2026-03-02T02:32:45.133Z	C:\Users\barty.bushes\Desktop\23942_cutepu...	SELABS\barty.bushes	2026-03-02T02:30:10.788Z	151831-bbus-mkt
2026-03-02T02:50:14.717Z	C:\Users\barty.bushes\Desktop\23195_cutepu...	SELABS\barty.bushes	2026-03-02T02:47:58.058Z	151831-bbus-mkt
2026-03-02T02:59:21.893Z	C:\Users\barty.bushes\Desktop\32006_cutepu...	SELABS\barty.bushes	2026-03-02T02:58:10.129Z	151831-bbus-mkt
2026-03-02T15:08:40.005Z	C:\Users\monica.malwhere\Desktop\19908_cut...	SELABS\monica.malwhere	2026-03-02T14:29:32.540Z	151753-mmal-mkt

Figure 7. The ability to query for a suspicious process and sort by time stamp helps to identify the first affected host.

Phase 3: Historical and real-time hunting

During the course of an investigation, as attack indicators are discovered, the ability to quickly hunt current and historical data across the enterprise is critical to understand active attacks and prior events that may have gone undetected. Trellix EDRF includes both real-time and historical search functions to aid the analyst in the identification of other affected systems.

Real-time search

The Trellix EDRF client collects 32 data elements out of the box and stores them in a data store on the host. The 32 out-of-the-box elements include:

WinRegistry	User profiles	USB storage	Twin files
Startup	Software	Services	Scheduled tasks
Process history	Processes	NSACrypt events	Network shares
Network sessions	Network flow	Logged-in users	Local groups
Loaded modules	Interactive sessions	Installed updates	Installed drivers
Installed certificates	Host info	Host entries	Files
Environmental variables	DNS cache	Disks and partitions	Current flow
Network interfaces	Command-line history	Browser history	Browser download

In addition to the 32 out-of-the-box collectors, enterprises are able to create their own custom collectors. Collectors can be created for Windows, Mac, and Linux operating systems and support common scripting languages such as OS commands, Python, Bash, PowerShell, and VBScript.

As data on the end client changes, the data is refreshed in the local data store and is searchable from the Trellix EDRF console. Using the underlying Trellix EDRF data exchange layer, an analyst is able to query thousands of connected systems and gain a near real-time understanding of what is happening in the active and connected network.

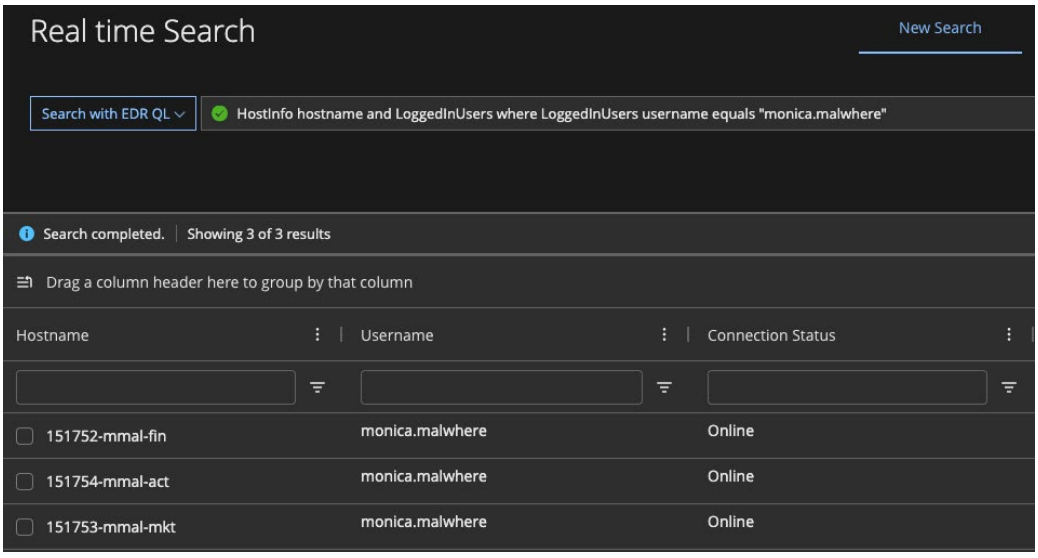

Figure 8. An analyst search for a suspicious user account shows three active connections on three different hosts.

Historical search

As a function of the behavioral threat detection capabilities, Trellix EDRF continuously collects telemetry data, referred to as trace within the platform. Trace collection includes over 70 different telemetry elements, including those collected for real-time search.

Top-level trace categories include:

Process activity	File manipulation	User account activity	Network activity	File system activity
Registry activity	Kernel mode events	Driver/module activity	Group policy modifications	File hashes
Named-pipe activity	Device operations	PowerShell activity	API calls	

Trace data is retained for up to 90 days by Trellix EDRF SaaS and made searchable as part of the historical search module. With the introduction of the Trellix Telemetry Store, enterprises can now extend the retention period of their historical data to meet the needs of their business, by scaling and hosting their own virtual telemetry system.

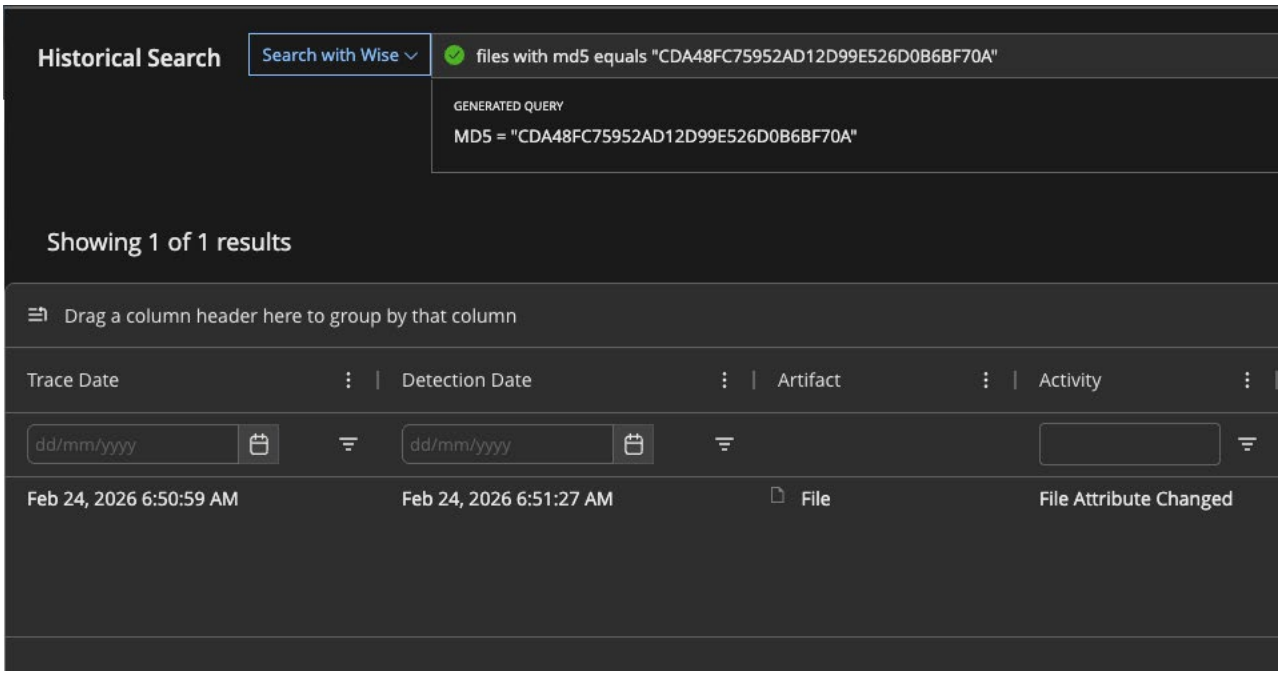

Figure 9. An analyst's 30-day historical search revealed a suspicious file executed on 31 systems.

Threat-hunting Trellix Wise integration

Threat-hunting tools often rely on proprietary query syntax, forcing analysts to spend valuable time crafting the right query rather than acting on findings. We integrate Trellix Wise AI into real-time search and historical search to enable natural language query capabilities. This automatically converts natural language questions into Trellix Query Language, simplifying and accelerating the threat-hunting process.

The Trellix EDRF competitive edge

Trellix EDRF delivers a uniquely powerful combination of best-in-class EDR and deep forensic investigation in a single, integrated platform—purpose-built for the demands of modern SOC operations, giving security teams the depth, speed, and accuracy they need to stay ahead of modern threats. Built around real-world SOC workflows and backed by flexible deployment options, Trellix EDRF enables organizations to reduce tool sprawl, streamline investigations, and respond with confidence at enterprise scale.

- Trellix EDRF provides forensic depth that rivals point tools by combining FireEye-proven investigation capabilities with Trellix's integrated telemetry, enabling incident responders to uncover root cause, lateral movement, and attacker tradecraft with a level of precision many competitors cannot match.
- It delivers true deployment flexibility—supporting diverse architectures, regulatory environments, and modernization journeys—so customers can adopt Trellix EDRF on their terms, where competing solutions often lock organizations into rigid, single-path implementations.
- Unlike point solutions that lock you into a single deployment model, Trellix EDRF's optional hybrid delivery gives SOC teams the flexibility to consume the platform the way their organization requires—whether on-premises, cloud-delivered, or both—without sacrificing forensic depth or detection capability.

Conclusion and next steps

Trellix's combination of detection accuracy, forensic automation, response at scale, and deployment flexibility is unmatched by other EDR providers.

To continue the series and learn more about Trellix EDR with Forensics and its deployment flexibility and threat detection capabilities, check out our white paper, "Advanced Forensic Analysis with Trellix EDR with Forensics (EDRF) Part 2: Multi-deployment Capabilities for Discovering Advanced Threats."

To read the final part of the series and learn more about our unmatched capabilities for remediation, check out our white paper, "Advanced Forensic Analysis with Trellix EDR with Forensics (EDRF) Part 3: Eradication of Threats with Precision Response."

Request a demo.
Learn more about Trellix EDR with Forensics at trellix.com.