Trellix

DATA SHEET

Trellix® Endpoint Detection and Response with Forensics (EDRF)

Surface deeply hidden threats, increase detection accuracy, and streamline investigation and response with AI

Key Benefits

- Provides high-quality actionable threat detection without the noise
- AI automatically correlates alerts and attacker TTPs to previous breaches
- Uses AI-guided investigations to provide analysts with machine-generated insights into attacks
- Enables forensics data collection to surface and eliminate hidden threats
- Enables analysts to investigate past incidents and proactively hunt for threats by querying a centralized repository of deep forensic data from all their devices
- Enhances compliance with regulations such as GDPR, PCI-DSS, and HIPAA
- 1-click report generation, so analysts can close investigations fast
- Simplifies deployment using Trellix® ePO software or SaaS-based ePO
- Enables analysts to focus on strategic incident response without burdensome administrative overhead

Overview

Endpoint detection and response (EDR) helps organizations identify, contain, and remediate threats, minimizing damage. EDR solutions capture and analyze behavior on endpoints for suspicious activity, working side-by-side with traditional signature-based detections to identify threats. They can also perform automated actions to contain threats and alert security teams for further investigation. However, sophisticated threat actors often bypass many EDR solutions, leaving minimal trace.

Attackers can hide the initial compromises and/or root cause of an attack, creating a foothold to penetrate organizations deeply and find critical data. They often camouflage actions within trusted components. Even when security teams limit an attack, hidden exploits can remain, leading to a resurgence or even enabling an attack variant. This lack of full understanding leaves organizations vulnerable. A new approach is needed to simplify endpoint security, providing comprehensive and accurate detection and protection against advanced threats.

Fully extinguishing the fire: Trellix EDR with Forensics

Trellix Endpoint Detection and Response with Forensics (EDRF) extends and enhances current EDR capabilities to provide a new level of visibility and relevant context needed to detect, investigate, and respond to deeply rooted and obfuscated threats, in addition to “patient zero.”

With the ability to collect forensic data critical to investigations, Trellix EDRF reduces mean time to detect and respond to threats by providing the context needed for analysts of any skill or experience level to understand alerts, fully investigate, and quickly respond.

As an integrated part of our EDR solution, Trellix forensics offers always-on data collection and multiple analytic engines throughout detection and

investigation stages. It helps analysts accurately surface suspicious behavior, make sense of alerts, collect forensic data, and take informed action.

Endpoint telemetry is analyzed both on the client and in the cloud, providing multiple threat-detection mechanisms. Endpoint information is available for immediate inspection and real-time and historical search.

On-demand and automated forensics

To support investigations, Trellix EDRF can take a snapshot of an endpoint, capturing a comprehensive view of active processes, process memory, driver memory, network connections, services, registry keys, and autorun entries. Integrated forensic data collection allows security teams to capture and store files, memory, and process, as well as partial and full disk images for further analysis and investigation. Unlike other, overly intrusive solutions, all forensics actions can be performed remotely without requiring remote shell access to the endpoints.

Forensics continues to capture data both in online and offline mode. Enabled by a nonpersistent data collection tool, snapshots can be captured on both monitored and unmonitored systems.

Our forensics actions offer extensive customization to meet specific user needs. We support the collection of approximately 11 event types, allowing users to select the specific attributes they wish to gather.

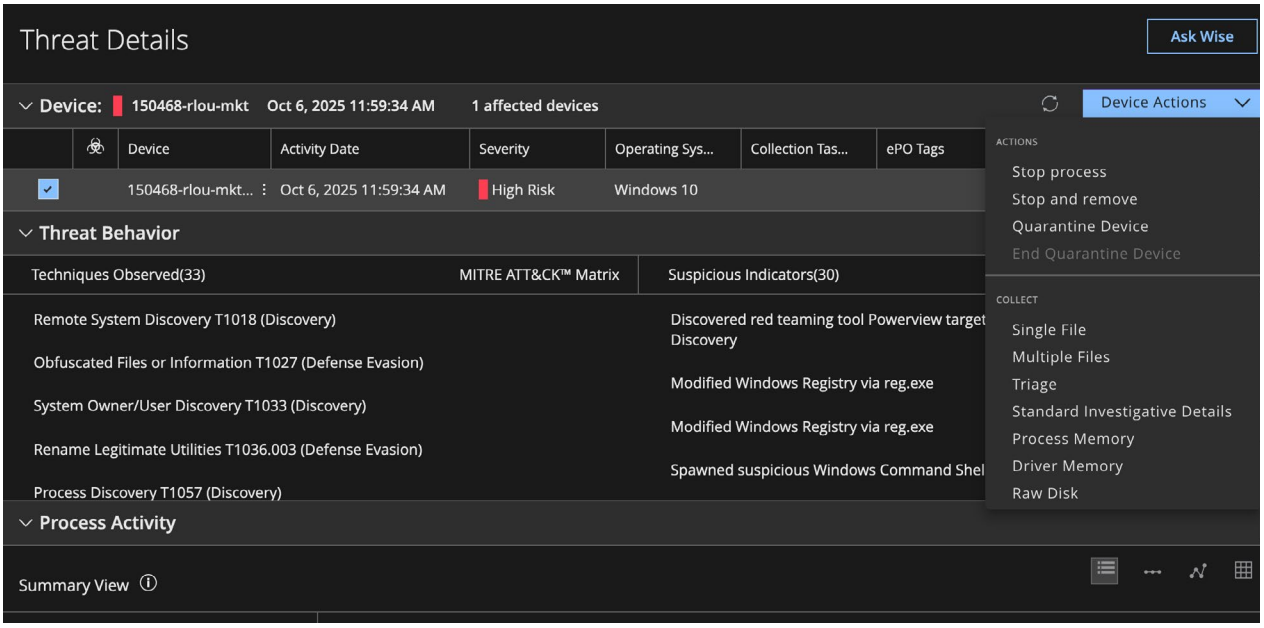

Figure 1. Trellix EDRF allows security teams to immediately collect forensic data associated with a threat for further analysis.

Think like an attacker
Behavior-based detection results map to the MITRE ATT&CK® framework, supporting a more consistent process to determine the phase of a threat and its associated risk, and to prioritize a response.

Powerful cloud-based analytics
Analytics engines inspect endpoint activity to uncover a broad spectrum of suspicious behavior and detect threats—from file-based malware to fileless attacks—that have slipped by other security defenses. Cloud-based deployment enables rapid adoption of new analytics engines and techniques.

Support for on-premises–only and air-gapped environments
There are circumstances where it is important to keep your data isolated from the internet and the cloud, making it less susceptible to remote hacking attempts, malware, and cloud-based exploits. In addition, organizations can have tighter controls regarding where data is stored and kept secure.

This is extremely important for businesses concerned with data protection and privacy regulations such as GDPR, PCI-DSS, and HIPAA. Trellix EDRF has the capability to offer enhanced forensics for these types of deployment requirements.

Streamlined navigation
Alert ranking further helps analysts understand risk severity and formulate an appropriate response. Flexible data display and visualization at this stage help analysts with different levels of experience easily navigate the data to quickly understand why an alert was raised and determine next steps: dismiss, respond, or investigate.

How Trellix EDRF with AI uplevels your team and speeds response times

To completely eradicate the full scope of an attack and understand all facets of a complex threat or campaign and its associated risk, security analysts must go beyond what a typical EDR solution provides and manually gather additional data during investigations.

However, organizations often struggle with limited resources and to retain experienced analysts. Higher-level analysts lack time for numerous alerts, while inexperienced analysts may escalate prematurely, overburdening Tier 3 analysts and hindering proactive threat hunting.

Trellix EDRF with Trellix Wise™ artificial intelligence (AI) reduces the expertise and effort needed to perform investigations and increases the speed with which analysts can determine the risk of an incident and its root cause by enabling guided investigation, alert correlation, and report generation.

Trellix EDRF with Wise automatically collects and correlates related breaches, artifacts, network connections, and more into a visual graph to accelerate investigations. In addition, Trellix Wise provides detailed recommendations of next steps to take based on the nature and severity of the threat identified, cutting down response time. It also provides one-click report generation so analysts can focus on security instead of paperwork.

Trellix EDRF helps to respond to threats in real-time with direct command-line access to impacted devices. This full visibility and control significantly reduces the time it takes to contain and remediate security incidents.

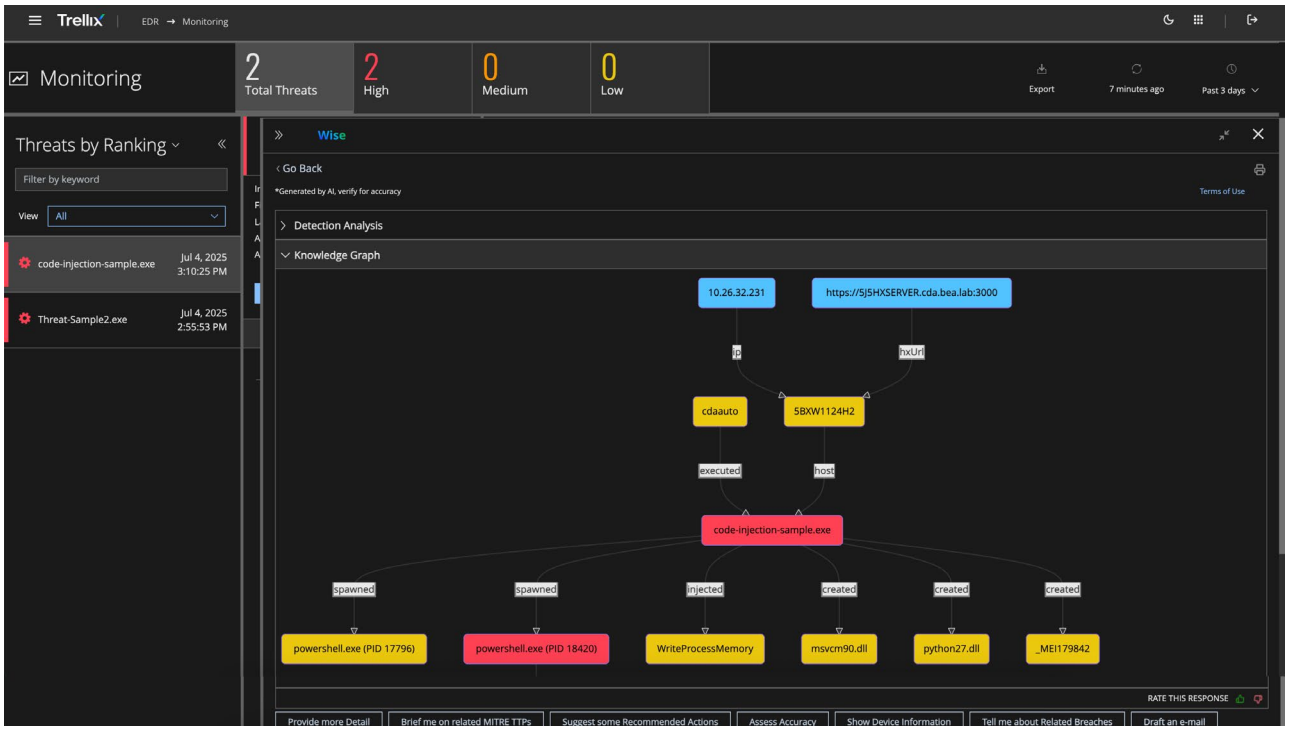

Figure 2. Trellix EDRF with Wise investigates for you. It automatically collects artifacts and presents the key findings. This visualization clarifies relationships and speeds analyst understanding.

Dynamic investigation guides

By combining the expertise of Trellix incident responders and Trellix Advanced Research Center with AI, investigation guides in Trellix EDRF force multiply the investigation process. Unlike playbooks that automate scripted tasks for known threats, investigation guides dynamically adjust

to each case, combining different investigation strategies and data. Trellix EDRF automatically gathers, summarizes, and visualizes evidence from multiple sources and iterates as the investigation evolves.

In addition to guided investigation, analysts and threat hunters can use the powerful Trellix EDRF search and data collection capabilities to expand inquiries across systems.

Prioritized investigations with Trellix Insights

Unique to Trellix EDRF is Trellix Insights, the first technology to proactively prioritize threats before they affect your organization and simultaneously predict if your countermeasures will stop them.

With Trellix EDRF, custom indicators of compromise (IOC) occur directly at the endpoint level. Trellix EDRF collects IOCs at the endpoint itself; however, to improve investigations, we offer broad IOC customization that supports six event types. These include process, file, image load, registry key, IP, DNS lookup, address notification, and URL, with over 94 attributes available for customization.

Through these customizable IOCs we can provide greater context that can help security analysts better prioritize events specific to their environment as part of the attack campaign.

Broad data collection and local relevancy

The AI-powered investigation engine gathers and processes artifacts and complex event sequences—from endpoints, security information and event management (SIEM) systems, and Trellix Insights, to make sense of alerts. Trellix EDRF compares evidence against known normal activity for each organization and threat intelligence sources to improve local relevancy and reduce false positives. Trellix Wise automatically correlates alerts, related breaches, and attacker TTPs and provides recommended next steps.

Historical search

The comprehensive and always-on data collection feature streams endpoint event information—including process activity, file changes, network connections, DNS queries, and command line activity from all monitored systems. Unlike other solutions, Trellix historical search can be performed either on-premises or in the cloud with little to no performance impact. Analysts can search this centralized data—regardless of online or offline status of endpoints—to find IOCs and indicators of attack that may be present along with deleted files. The activity history is preserved and available, and the search window can span weeks or months, ensuring you have the historical context needed for thorough investigations.

Real-time search
For active incident inquiries, real-time search reaches out to endpoints across your estate to quickly query for up-to-the-moment information. Flexible syntax enables capabilities like simple queries for searching workstations.

You can also run more complex searches that return more data from the workstation, such as identifying a user at the time of event, command-line execution, and when the suspected application was started. Trellix EDRF can easily scale queries across the enterprise to tens of thousands of machines.

Trending campaigns
Orchestrated and targeted attacks (based on region or industry) are alerted upon, identifying IOCs to search for with Trellix EDRF. This empowers the analyst to execute proactive searches before the attacks occur.

Leveraging Trellix end-to-end security for maximum visibility and protection

Trellix EDRF is a key component of an integrated security ecosystem. It extends endpoint protection capabilities and visibility while supporting the workflows and processes of the security team. You can also use the solution to help reduce mean time to detect and respond and increase operational efficiency.

Correlate data from across the enterprise for complete visibility
Collaboration and easy integration with data sources beyond the endpoint are key to closing data gaps for multifaceted threat investigations. Trellix Helix Connect unites threat events from multiple controls, including Trellix EDRF, so you can get the full story of an attack and reduce pivots across tools.

It provides automation that is accessible to analysts of any level and GenAI that investigates, surfaces insights and speeds incident response. Events are prioritized by severity, with 50% to 70% of false positives already removed.

Built-in automation also removes routine threats and performs tasks like data enrichment, device containment, disabling users, and creating incidents for ticketing systems and hundreds more third-party components.

Tight integration with network solutions, such as Trellix Network Detection and Response (NDR) and Trellix Intelligent Virtual Execution (IVX) sandbox, enables Trellix EDRF to expand investigation capabilities and insights. It does so by correlating endpoint artifacts with network information and other data collected, including support for IPv6.

Support team collaboration and workflows
Trellix EDRF plugs into current security operations workflows and supports collaboration by sharing investigation data and updates through security incident response platforms.

Scalable, simple deployment
Trellix EDRF is available as a software as a service (SaaS) application. Management with Trellix ePO—the industry's foremost centralized security management platform—simplifies deployment and ongoing maintenance of Trellix EDRF and your entire security infrastructure. Available both on-premises and in the cloud, Trellix ePO offers management flexibility to fit diverse organizational needs.

Overburdened team? Trellix MDR can augment your organization.

Constrained resources and constant workforce movement leaves organizations understaffed and overburdened when it comes to having enough experienced "eyes-on-glass" to monitor, detect, investigate, and respond to threats. Our MDR security service works 24/7 to help you by performing a range of fundamental security activities.

Trellix MDR services combine advanced analytics, threat intelligence, and human expertise in incident investigation and response deployed at the host and network levels. Our certified partners offer 24x7 critical alert monitoring, managed threat hunting, advanced investigations, and response to significantly improve your security posture.

To learn more about Trellix, visit trellix.com.