Trend Vision One™ - Forensics

Frictionless investigation of critical incidents directly within the Trend Vision One™ platform

As security teams take on more and more tools to deal with increasingly sophisticated threats, they're also building up operational complexity that makes their jobs even harder. That's especially true when it comes to standalone, out-of-the box incident response tools, which lack built-in threat intelligence and require manual intervention. With digital forensics and incident response (DFIR) talent in short supply, any need for human attention just bogs teams down further.

What's really required is a tool that lets incident responders do more with less.

Trend Vision One – Forensics answers that call by providing a frictionless way for security operations center (SOC) analysts and DFIR specialists to conduct security investigations right from inside the Trend Vision One console.

Part of the Trend Vision One platform, Trend Vision One – Forensics makes it easy to collect and organize evidence when critical events happen, enabling thorough investigations and effective responses that help prevent the same incidents from occurring again.

Trend Vision One – Forensics lets teams gather digital evidence from endpoints, organize data in workspaces, and triage endpoints quickly using osquery and YARA scans. It has no deployment requirements and adds zero operational complexity, working seamlessly with Trend Vision One™ - EDR/XDR for endpoint, server and cloud workloads.

Seamless, end-to-end incident response

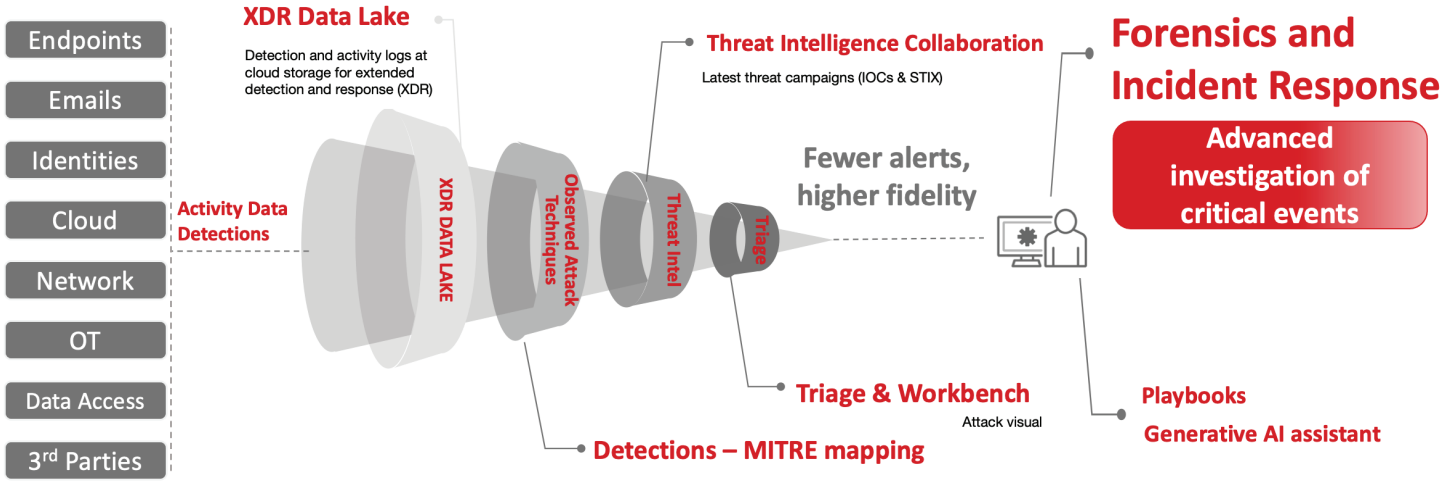
Simplifying and converging security operations starts with a single platform. Trend Vision One supports diverse, hybrid IT environments, automates and orchestrates workflows, and delivers expert cybersecurity services to help organizations stop adversaries faster and take control of cyber risks.

Trend Vision One – Forensics empowers teams to manage incidents, collect evidence and artifacts, investigate and analyze evidence, and respond to incidents all in the Trend Vision One console. Manage security holistically with comprehensive prevention, detection, response, and forensics capabilities powered by leading threat research and intelligence.

The benefits of integrated incident response

- **One platform for detection, investigation, and response** – From a single console, security teams can carry out advanced forensics and analytics with no need for separate DFIR tools. This minimizes operational complexity, improves incident response, and prevents future attacks.
- **Zero deployment** – As a built-in capability of Trend Vision One, there are no deployment steps to get Trend Vision One – Forensics up and running, saving precious time and getting teams to incident interrogation faster.
- **Faster, more effective incident response** – Native threat intelligence analytics, AI capabilities, live forensics, and automatic endpoint detection and response (EDR) data-pulling help teams find the proverbial "a needle in a haystack" faster, with less effort. Automatic, built-in artifact collection and incident response report generation speed things up even further.

Trend Vision One - Forensics as part of the connected security operations workflow



Trend Vision One - Forensics: Frictionless capabilities

Evidence and Artifact Collection

- Snapshot full artifacts/evidence on endpoints at any time
- Request batch evidence collection through centralized console
- Collect artifacts based on automatic trigger conditions

Native Threat Intelligence

- Run threat intelligence queries when specific conditions are met
- Leverage AI technology for faster evidence tagging
- Pull EDR telemetry and detections into view automatically

Incident Management War Room

- Create workspaces during incidents
- Scope the affected endpoints
- Manage incidents through a centralized console

Live Investigation from Anywhere

- Run YARA queries for typical memory and artifact exploration
- Review running processes and sub-processes live
- Run native commands such as whoami and netsat with osquery for live investigation

Respond in Super Timeline View

- Generate a Super Timeline with expert Trend Micro pre-generated and built-in threat knowledge
- Take advantage of holistic forensic data and heuristic analyses

Easier investigations and faster responses with automatic threat intelligence

Trend Vision One – Forensics rounds out the comprehensive capabilities of the Trend Vision One platform by integrating collected evidence and threat intelligence analytics. The screen capture below shows how the Trend Vision One – Forensics Evidence Report and Super Timeline views incorporate in-house and third-party threat intelligence for robust, automated analysis—highlighting critical risks when detected.