Platform Overview

Praeventra is a near real-time and continuous Digital Forensics and Incident Response platform designed to help organizations detect, investigate, correlate, and respond to security incidents while endpoint activity is still happening. Instead of starting the forensic process after an incident, Praeventra continuously collects forensic and security-relevant information from client machines and turns this data into actionable intelligence through predefined IoCs, advanced rules, graph-based correlation, and automated workflows.

Platform Intelligence

Praeventra is built to transform endpoint activity into meaningful forensic context. The platform currently includes more than **1,800 predefined Indicators of Compromise**, helping security teams detect suspicious behavior, known attack patterns, and policy-relevant activity faster.

In addition to IoC coverage, Praeventra collects a wide range of endpoint forensic data points, including process activity, system behavior, file-related events, network indicators, user activity, and other security-relevant signals. These data points provide the foundation for detection, investigation, correlation, and response.

As the platform grows, these intelligence assets can be expanded with new IoCs, additional forensic data points, custom rules, customer-specific detection logic, and AI-supported investigation capabilities.

Predefined Indicators of Compromise	**1,800+ IoCs**	Helps detect suspicious behavior, known attack patterns, and policy-relevant activity faster.
Client-Side Data Points	**70+ Data Points**	Provides broad endpoint visibility across forensic and security-relevant activity collected from client machines.
Response Actions	**100+ Actions**	Enables flexible workflow-based response, from notifications and investigation steps to controlled containment actions.

Customer Value

Praeventra helps organizations stay ahead of incidents with near real-time and continuous forensic readiness. Instead of waiting until after an attack to search for evidence,

Praeventra continuously collects, structures, and connects endpoint information while activity is still happening.

This gives security teams faster visibility, stronger evidence, and a clearer path from detection to response. With Praeventra, organizations can reduce investigation time, preserve critical forensic data, and understand the full context of an incident across users, machines, processes, files, and events.

By combining advanced rules, graph-based correlation, and workflow automation, Praeventra helps analysts focus on what matters most. The platform turns disconnected endpoint data into actionable intelligence, enabling faster decisions, more consistent response, and stronger operational control.

Praeventra delivers value where it matters: better preparedness before an incident, faster investigation during an incident, and more confident response after detection.

Key Benefits

Praeventra helps organizations improve forensic readiness by continuously collecting endpoint evidence before critical information is lost, modified, or deleted. This gives security teams richer investigation context, stronger evidence quality, and a clearer understanding of suspicious activity as it develops.

The platform improves detection and response speed by using predefined IoCs, advanced rule logic, and customer-specific detection policies. When suspicious behavior is identified, Praeventra can generate alarms, enrich them with context, and trigger investigation, notification, containment, or automated response workflows.

Praeventra also helps reduce the risk and impact of operational downtime. Security incidents can spread quickly across endpoints, disrupt business operations, and force teams into broad manual containment. With near real-time visibility, graph-based correlation, and workflow-driven response, Praeventra helps teams detect incidents earlier, contain affected systems faster, and reduce the potential impact on business continuity.

Another key benefit is connected investigation. Praeventra does not treat every alarm as an isolated signal. By using a graph database, the platform connects endpoints, users, processes, files, events, and alarms to reveal relationships, attack paths, and wider incident patterns.

Praeventra also improves operational efficiency by helping security teams standardize and automate response processes. Analysts can reduce repetitive manual work, focus on high-priority incidents, and use workflow-based actions to respond more consistently and with greater confidence.

Card View :

Stronger Forensic Readiness
Continuously collect endpoint evidence before critical information is lost, modified, or deleted.

Faster Detection and Response
Use IoCs, advanced rules, and customer-specific policies to identify suspicious activity and trigger response workflows.

Reduced Downtime Risk
Detect incidents earlier, contain affected systems faster, and reduce the potential impact on business continuity.

Connected Investigation
Correlate users, machines, processes, files, events, and alarms through graph-based relationships.

Operational Efficiency
Automate repetitive actions, standardize incident handling, and help analysts focus on the incidents that matter most.

What Makes Praeventra Different

Praeventra brings digital forensics into the live security operation.

While conventional forensic tools are often used after an incident has already happened, Praeventra is designed to run continuously and support investigation before, during, and after suspicious activity occurs. It helps organizations collect and preserve forensic evidence while endpoint activity is still happening, reducing the risk of missing critical context when an incident is discovered.

Praeventra combines capabilities that are often handled separately. It brings together continuous endpoint collection, IoC-based detection, advanced rule processing, graph-powered correlation, workflow automation, and controlled response actions in one DFIR platform. This allows security teams to move faster from signal to investigation, from investigation to understanding, and from understanding to action.

Unlike tools that focus only on alerts or only on post-incident analysis, Praeventra connects the full incident story. The platform links users, machines, processes, files, events, alarms, and response actions through a graph database, helping analysts understand not just what happened, but how each activity is connected.

Praeventra also supports action when speed matters. With more than 100 response actions, the platform can trigger notifications, support investigation workflows, provide structured data to AI agents, isolate machines, terminate suspicious processes, shut down systems, or control network interfaces based on customer-defined policies. These

actions can be manual, approval-based, or automated depending on operational requirements.

The result is a near real-time and continuous DFIR capability that helps organizations improve visibility, preserve evidence, reduce investigation time, and respond before incidents create wider business impact.

Shortened Version:

Praeventra is not just a forensic tool. It is a continuous DFIR platform built for live security operations.

It collects endpoint evidence before it disappears, detects suspicious activity through IoCs and advanced rules, connects related events through graph-based correlation, and enables workflow-driven response when action is required.

By combining forensic collection, detection, correlation, and controlled response in one platform, Praeventra helps security teams move from reactive investigation to near real-time forensic readiness.

Component Overview

Endpoint Agent

The Praeventra endpoint agent runs continuously on client machines and collects forensic and security-relevant information. It provides the foundation for continuous visibility by capturing endpoint activity that may be important for detection, investigation, and evidence preservation.

Event Engine

The event engine processes collected endpoint data using advanced rule logic. It evaluates incoming events against predefined IoCs, detection rules, and customer-specific policies. When suspicious or policy-relevant activity is detected, the event engine creates alarms and enriches them with useful context.

Indicator of Compromise Library

Praeventra includes more than 1,800 predefined Indicators of Compromise that help identify suspicious activity and known threat patterns. This IoC library strengthens the platform's detection capability and can be expanded over time with new intelligence and customer-specific indicators.

Graph Database

The graph database stores and connects forensic entities such as endpoints, users, processes, files, events, alarms, and relationships. This allows Praeventra to analyze security activity as a connected structure instead of isolated records.

Correlation Engine

The correlation engine uses graph relationships and correlation rules to identify links between events, alarms, systems, users, and processes. It helps analysts understand whether an event is isolated or part of a broader incident chain.

Workflow Engine

The workflow engine turns detection and correlation results into action. It can trigger notifications, investigation tasks, AI-agent support, containment steps, or controlled response actions based on predefined policies and customer configuration.

AI-Powered Investigation

Praeventra brings AI into the investigation process by combining forensic data, graph-based relationships, and workflow-driven intelligence. The platform uses the graph database to navigate connected security context across users, endpoints, processes, files, events, and alarms, helping analysts understand incidents faster and with less complexity.

With AI-supported analysis, Praeventra can summarize incidents, surface critical relationships, highlight possible attack paths, and guide analysts toward the evidence that matters most. Through workflow integration, Praeventra can also provide structured forensic context to AI agents for deeper analysis, reporting, and response recommendations.

This creates a practical and intuitive investigation experience that helps security teams move from data overload to clear, actionable insight.

Platform Outcome

Praeventra gives organizations a continuous and real-time DFIR capability that connects forensic collection, detection, correlation, and response in one platform. It helps security teams preserve evidence, detect threats faster, understand incident relationships, and respond with greater confidence.

By combining endpoint agents, more than 1,800 predefined IoCs, advanced rule processing, graph-based correlation, and workflow automation, Praeventra helps organizations become better prepared before, during, and after security incidents.