OpenText Endpoint Investigator

Uncover the truth faster with forensic investigation results you can trust

Benefits

- Collect anything, anywhere, anytime, of any size
- Scale to >1,000,000 endpoints for enterprise investigations
- Automatically deploy agent to clients
- Align with zero-trust security models

Deployment options

Extend your team

- On-premises software, managed by your organization or OpenText

Cybersecurity in enterprise organizations is driven by increasing cyber threats, regulatory changes, and digital transformation. Digital forensics and incident response have taken a critical role in helping organizations investigate, analyze, and respond to security incidents.

OpenText™ Endpoint Investigator enables organizations to conduct discreet, comprehensive internal investigations—helping to prevent financial loss, reputational damage, and legal exposure. Designed for modern enterprises, it allows seamless investigations of laptops, desktops, servers, and mobile devices, whether employees are on-site or remote. Most importantly, it does so without disrupting workforce productivity.

Zero trust compliance

OpenText Endpoint Investigator conducts network collections, both on and off the VPN, without exposing sensitive data. This isolation is in line with zero trust principles, ensuring that even in the event of a breach, investigation processes remain secure.

Flexibility needed for enterprise investigations

No enterprise is the same, nor are its investigation requirements. The type of data you need to collect, where you need to collect it from, when you need to collect it, or how much you need to collect can all vary. Enterprises need the flexibility to collect any digital evidence, anywhere, anytime, and of any size in order to perform the most effective investigations.

With OpenText Endpoint Investigator, investigators can simply specify the data they need collected from each endpoint and the appropriate collection methodology is automatically deployed.

"I have about 100 different duties to perform on an annual basis. With OpenText Endpoint Investigator, I'm able to take care of 80 percent of my workload in 48 hours."

Deputy Director
IRM Office and ISSO
U.S. Federal Agency

Resources

Read the blog ›
Learn more ›

Fast and efficient investigations

The ability to gain early insights, optimize resources, and focus on critical data is key to successful forensic analysis and incident response. In addition to its deep dive forensic capabilities, OpenText Endpoint Investigator utilizes an artifacts-based workflow to enhance speed, efficiency, and relevance in digital forensic investigations.

This artifacts-based approach allows users to prioritize and target artifacts to quickly extract actionable intelligence without scanning entire disks or memory dumps, making evidence analysis more manageable.

Increase investigation accuracy and expertise

Collaboration in digital forensic investigations leads to faster, more accurate, and legally sound results. It enables better expertise utilization, workload distribution, and real-time intelligence sharing, making it an essential tool for handling modern cybercrime cases effectively.

Utilizing OpenText Endpoint Investigator's centralized database, multiple users can collaborate on case details and get to the truth faster.

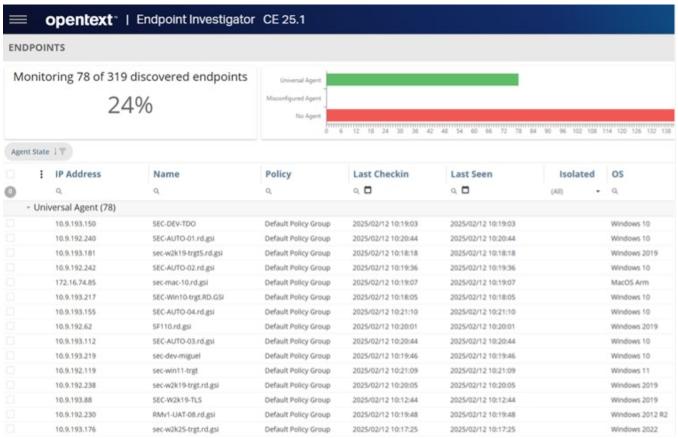
Boost productivity

The OpenText Endpoint Investigator web-based interface is about more than ease of use. Investigators get remote access and can perform forensic analysis on remote Windows® and macOS® systems. Teamwork is improved by allowing multiple investigators to work on a case simultaneously, viewing and analyzing evidence in real time. Because all case data is stored in a centralized location, investigators benefit from better organization and tracking of forensic evidence.

Designed for enterprise investigations, OpenText Endpoint Investigator can easily scale to handle multiple cases, large datasets, and distributed forensic investigations. Additional benefits include enhancement updates and maintenance, secure access controls, seamless integration with other tools, more efficient resource utilization, and improved reporting and visualization.

OpenText Endpoint Investigator empowers organizations to uncover the truth faster with forensic investigation results they can trust. By delivering accurate, comprehensive, and tamper-proof evidence, OpenText Endpoint Investigator enables security teams to rapidly identify threats, minimize business disruption, and ensure compliance with regulatory requirements. With advanced automation, AI-driven analytics, and streamlined workflows, OpenText Endpoint Investigator accelerates incident response, reduces investigation complexity, and provides actionable insights—helping organizations strengthen cyber resilience, protect their reputation, and make informed decisions with confidence.

Features	Description
Enhanced web-based user interface	Easily transition between preview, collection, and response functions while streamlining collaborative investigations.
Automated large-scale collections	Scale to > 1,000,000 endpoints. Specify the data required from each endpoint and the appropriate collection method will automatically be identified and deployed.
Single enhanced universal agent	Benefit from uniform capabilities across Windows and macOS for simplified deployment and faster data collection.
Collection APIs	Automate evidence collection with API-driven snapshots, file collections, memory capture, and timeline generation.
Integrated threat intelligence	Leverage a global network of sensors to detect emerging threats, allowing investigators to prioritize them for immediate action.
Artifact-based workflows	Enhance investigative efficiency by quickly identifying relevant forensic artifacts alongside deep-dive forensic capabilities.
Automated agent deployment	Ensure a frictionless approach to data collection with agents that are automatically pushed out, delivering endpoint check-ins every five minutes.
Enterprise endpoints dashboard	Gain a comprehensive view of enterprise endpoints, offering visibility into agent deployment status and communication readiness.
Zero-trust compliance	Ensure reliable data collection and analysis while aligning with zero-trust security models.



Monitoring 78 of 319 discovered endpoints

24%

Universal Agent (78)

IP Address	Name	Policy	Last Checkin	Last Seen	Isolated	OS
10.9.193.150	SEC-DEV-TDO	Default Policy Group	2025/02/12 10:19:03	2025/02/12 10:19:03		Windows 10
10.9.192.240	SEC-AUTO-01.rd.gsi	Default Policy Group	2025/02/12 10:20:44	2025/02/12 10:20:44		Windows 10
10.9.193.181	sec-w2k19-trgt5.rd.gsi	Default Policy Group	2025/02/12 10:18:18	2025/02/12 10:18:18		Windows 2019
10.9.192.242	SEC-AUTO-02.rd.gsi	Default Policy Group	2025/02/12 10:19:36	2025/02/12 10:19:36		Windows 10
172.16.74.85	sec-mac-10.rd.gsi	Default Policy Group	2025/02/12 10:19:07	2025/02/12 10:19:07		MacOS Arm
10.9.193.217	SEC-Win10-trgt.RD.GSI	Default Policy Group	2025/02/12 10:18:05	2025/02/12 10:18:05		Windows 10
10.9.193.155	SEC-AUTO-04.rd.gsi	Default Policy Group	2025/02/12 10:21:10	2025/02/12 10:21:10		Windows 10
10.9.192.62	SF110.rd.gsi	Default Policy Group	2025/02/12 10:20:01	2025/02/12 10:20:01		Windows 2019
10.9.193.112	SEC-AUTO-03.rd.gsi	Default Policy Group	2025/02/12 10:20:44	2025/02/12 10:20:44		Windows 10
10.9.193.219	sec-dev-miguel	Default Policy Group	2025/02/12 10:19:46	2025/02/12 10:19:46		Windows 10
10.9.192.119	sec-win11-trgt	Default Policy Group	2025/02/12 10:21:09	2025/02/12 10:21:09		Windows 11
10.9.192.238	sec-w2k19-trgt.rd.gsi	Default Policy Group	2025/02/12 10:20:05	2025/02/12 10:20:05		Windows 2019
10.9.193.88	SEC-W2k19-TLS	Default Policy Group	2025/02/12 10:12:44	2025/02/12 10:12:44		Windows 2019
10.9.192.230	RMv1-UAT-08.rd.gsi	Default Policy Group	2025/02/12 10:19:48	2025/02/12 10:19:48		Windows 2012 R2
10.9.193.176	sec-w2k25-trgt.rd.gsi	Default Policy Group	2025/02/12 10:17:25	2025/02/12 10:17:25		Windows 2022

Figure 1. Monitoring endpoints activity is crucial for detecting threats, collecting evidence, identifying attack vectors, ensuring compliance, and accelerating incident response.

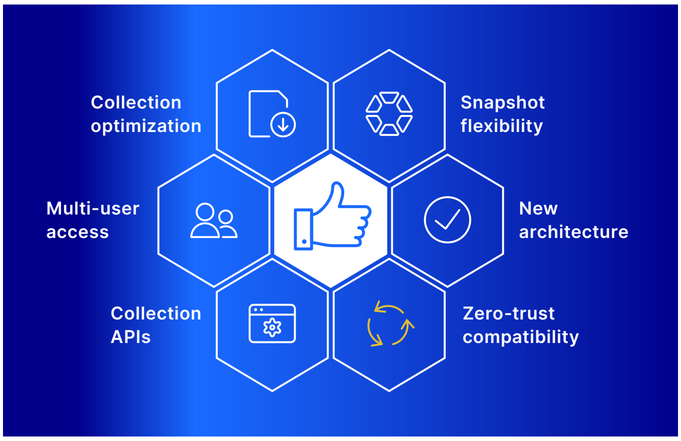


Figure 2. OpenText Endpoint Investigator help organizations quickly and efficiently analyze endpoints for potential security incidents, data breaches, or internal threats.