Faster, smarter, compliant: Why OpenText Endpoint Investigator CE 26.1 changes the game

Enterprise-grade performance with integrated investigation and endpoint response, providing organizations with the clarity and results they need when it matters most

Modern cyber incidents demand more than traditional forensics. Security teams need to investigate rapidly across large environments and be able to take decisive action without delay.

Staying on older versions of OpenText™ Endpoint Investigator can limit your team's speed, visibility, and effectiveness. Upgrading to the enhanced CE 26.1 release empowers security teams to investigate faster, scale across the enterprise without disruption, and respond to incidents more effectively. The outcome: stronger cyber resilience, reduced investigation fatigue, and confidence that your digital forensics capabilities are ready to meet today's complex threat landscape.

Capability	Legacy	Modern (CE 26.1)
Off-VPN check-in	• Limited scalability • DMZ placement • Custom port and firewall configuration	• Validated to more than one million endpoints • Standard port (HTTPS) • Zero-trust friendly • Behind firewall
User experience	• Thick-client only • Limited to one user per case • Click-intensive • Accessed on a physical or virtual asset • Steep learning curve for new users	• Modern web interface • Fewer clicks • Collaborative multi-user case access • Access anywhere • Intuitive user interface
Accelerated collections	• Not available	• Smarter unified agent • Chunk collections • AFF4 evidence file format • Fastest collection method to date • Full logical collections, even off network
Compliance and security	• Manual cryptographic key pair administration • Integrated Active Directory • Little to no audit capability	• Active Directory integration • New case auditing with the ability to export

Capability	Legacy	Modern (CE 26.1)
Snapshot functionality	• Manual process • Required job configuration for desired results • Time-consuming process	• Off-network support • Automated process • Greater contextual information • Snapshot comparisons • Intelligence-driven clarity • Whitelist/blacklist processes, connections, and DNS cache
Integrated threat intelligence	• No threat intelligence enrichment	• Automatically identify threats as part of the snapshot process • Enhanced visibility into the state of the target
Collection and endpoint response APIs	• No API	• Fully or partially automate forensic or response tasks • Integrate with ticketing systems, SIEM, SOAR, etc.
Endpoint agent visibility	• Not available	• Gain real-time visibility into agent deployments • Includes details on each target
Licensing	• Cumbersome and inflexible • Locked out when license expires	• More forgiving licensing • License expiration awareness • Drag-and-drop licensing
Timeline	• Not available	• Retrospective visibility • Visualization and filtering • Records all processes, DLLs, IP connections and DNS cache over time, curated into a single view for searching • Accelerates root-cause analysis
Rapid triage	• Not available	• Off-network support • Bypass time-consuming parsing of MFT • Near instantaneous access to target disk viewing • Pivot between forensic and new add-on response functions with ease
Case job activity	• Not available	• See the status of case jobs in near real time • Job error tab for troubleshooting • JSON output of job configuration for legal matters

And that's not all. When you upgrade OpenText Endpoint Investigator from legacy to modern architecture, you can take advantage of a free, 45-day trial of OpenText incident response capabilities. If you decide you want to make the "IR" of DFIR a permanent solution within your SOC, our team is ready to help with a seamless upgrade to OpenText™ Endpoint Forensics & Response.

Now is the time to upgrade and unlock the full potential of your digital forensic investigations. Watch this demo to learn why you should upgrade to OpenText Endpoint Investigator CE 26.1.

Contact us to learn more ›

opentext™