Top reasons to upgrade to OpenText Core Endpoint Detection and Response

Complete visibility for detection, investigation, and remediation of endpoint threats

Existing OpenText™ Core Endpoint Protection customers and MSPs:
Can upgrade to OpenText Core Endpoint Detection and Response with no redeployment or script changes.

Quick time to value:
Seamless integration with over 500 technology stack in the MSP infrastructure

Includes SIEM at no additional cost:
Enables log ingestion, event correlation, triage, search, and reporting.

Includes SOAR at no additional cost:
For automated remediation via canned and customizable workflows.

Helps meet SMB cyber insurance and compliance requirements:
Such as NIST, PCI, and SOC-2.

Advanced threat detection:
More advanced threat detection capabilities compared to OpenText Core Endpoint Protection.

Forensic capabilities:
Detailed forensic can be used to investigate security incidents, including information on the attack vector and the scope of the breach.

Automated response:
Can isolate compromised endpoints, kill malicious processes, and take other actions to contain threats.

Competitive differentiation:
MSPs can offer higher margin services (e.g. managed Endpoint Detection and Response) to boost revenue

Improved client trust and satisfaction:
MSPs can provide a higher level of security, which can improve client trust and satisfaction.

To learn more about OpenText Core Endpoint Detection and Response (EDR) or to schedule a demo, contact your OpenText account representative or visit our website:
cybersecurity.opentext.com