Endpoint security software is no longer optional. Banks require deep visibility to secure endpoints and investigate potential threats.

The best detection and response solutions provide greater localization and contextualization of security events for more informed decision-making, faster triage and effective remediation of threats.

Cybersecurity, risk and compliance: Top priority for banks in 2020

$18.4M
Average cost of a cyberattack for financial organizations²

37%
Consumers say their financial information was compromised³

36%
Breaches were caused by internal actors³

$17B
How it works

Investigation software enables over-the-wire examination of a suspected compliance violation.

Step 1 Investigation team is alerted to the suspected intrusion.

Step 2 Investigation team collects and analyzes potential evidence with high-fidelity applications and techniques.

Step 3 The software generates a report to determine whether an intrusion occurred, which can be remediated based on organizational policies and procedures.

Discover, identify, remediate and investigate

Greater automation and contextualization ensures more informed decision-making, faster triage and effective remediation.

Organizations employing remote investigation solutions reduce investigation time by 75%⁶

Investigation software enables over-the-wire examination of a suspected compliance violation.

Compliance, detection and response

Address endpoint security and digital investigation needs with industry-leading endpoint detection and remediation for compliance, detection and response.

Fearlessly protect your organization and remediate any threats—anywhere, any time—on any platform with OpenText EnCase® Endpoint Security 6.07.

Learn more