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

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 automation and contextualization of security events for more informed decision-making, faster triage and effective remediation of threats.

$18.4M
Average cost of a cyberattack for financial organizations

37%
Consumers say their financial information was compromised

36%
Breaches were caused by internal actors

56.8%
Organizations cited shortage of staffing as an impediment to effective IR

$17B
Saved annually if global enterprises reduce the cost of breaches by 10%

Discover, identify, and remediate

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

Organizations employing remote investigation solutions reduce investigation times by 75%.

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 help determine whether an intrusion occurred, which can be remediated based on organizational policies and procedures.

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 threat—commodity or advanced—with OpenText EnCase Endpoint Security 6.0.

Learn more