REMOTE TESTING SECURITY CHECKUP

UNDERSTANDING THE STRENGTHS AND WEAKNESSES OF YOUR REMOTE TESTING SOLUTION

KNOWLEDGE IS POWER

The online, remote testing environment provides fertile ground for many types of cheating and content theft. Caveon's Security Checkup provides layers of valuable insight into the health of your remote testing program, helping your team address questions such as:

1 Do your items appear compromised?

By uncovering exposed exam content and running statistical analyses of your test data, Caveon experts can find evidence about whether your items and tests have been compromised.

2 Is your test content on the internet?

Caveon's experienced Web Patrol™ experts can check internet hotspots for stolen test content, including public and private social media, forums, chat rooms, and prep sites.

3 Are your proctors doing a good job?

Caveon's test administration monitoring experts can stress-test your proctoring policies and procedures by posing as test takers to get an insider's perspective of the exam experience.

4 Is your intellectual property at risk?

Once the internet has been scoured for signs of your test content, the web patrol team can provide feedback on your program's unique risk of exposure to theft.

5 Are examinees using pre-knowledge?

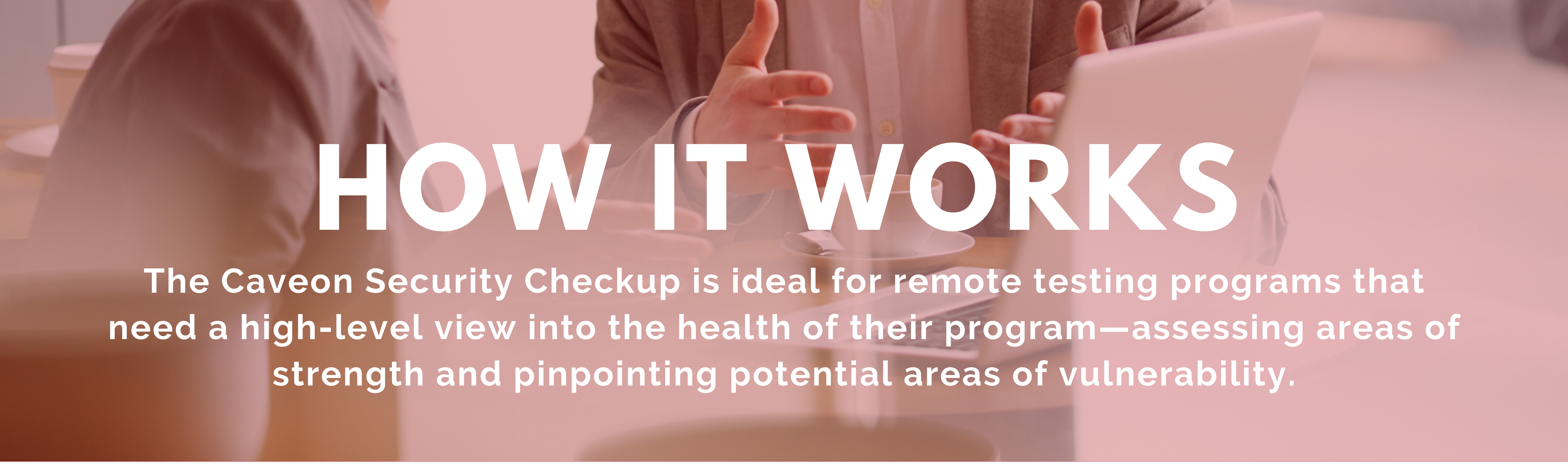
Data comparisons, such as M4 Similarity and Identical Test observed over time, can help to determine whether examinees are using pre-knowledge to gain an advantage.

6 Are your security policies strong?

Caveon's test security experts can provide a multi-faceted view into the strengths, weaknesses, and effectiveness of your security protocols, policies, and practices.

7 How can you improve in the future?

Leverage the knowledge and feedback you gain from the Security Checkup to modify your security practices, keeping your tests and scores valid for years to come.



HOW IT WORKS

The Caveon Security Checkup is ideal for remote testing programs that need a high-level view into the health of their program—assessing areas of strength and pinpointing potential areas of vulnerability.

Caveon's powerful Data Forensics℠, Monitoring, and Web Patrol teams provide deep and meaningful insight into highly-specialized silos of security. Now, they're teaming up to deliver a multi-perspective view of your remote testing security. When used together to locate, monitor, and investigate security threats, Caveon's tried-and-tested test security services can provide valuable insight into the health of your testing program.

LOCATE
stolen content

MONITOR
tests for unusual behavior

INVESTIGATE
testing data for answers

WHAT'S IN THE CHECKUP?

DATA FORENSICS

Caveon's experienced Data Forensics team will analyze your test data using a suite of powerful threat-detecting statistics. These analyses will help you locate threats and eradicate fraud impacting your program.

You'll learn:

- Whether your content shows evidence of being stolen and used
- If examinees show evidence of using prior knowledge of tests
- Whether security threats appear to increase through the date range of the testing window

REMOTE MONITORING

Remote monitoring provides a window into your test taker and proctor behavior. First, select whether you'd like us to perform recorded test session audits or remote proctoring quality assurance, then Caveon's trained and experienced monitors will evaluate your testing processes.

You'll learn:

- If your remote proctoring vendors are enforcing policies and procedures
- If test takers display unusual behavior that could signal the need for a deeper investigation

WEB PATROL

Caveon's Web Patrol experts provide a high-level analysis of your online threats and vulnerabilities. You'll receive a letter grade of current online exposure levels and a hierarchical graphic breakdown of potential areas of vulnerability for your intellectual property.

You'll learn:

- What social media apps or online hotspots have the highest potential for leaked content
- Where you're at risk for any other types of online exposure