

7 REASONS to Automate CIS Benchmarks in Higher Education

Strengthen cybersecurity across complex campus environments without adding more manual work to your IT team.

1. IMPLEMENT CIS BENCHMARKS FASTER

Automate CIS Benchmarks scanning and remediation across large numbers of endpoints to accelerate implementation and reduce repetitive manual hardening.

2. REDUCE MANUAL WORK

Reduce recurring policy deployment, scanning, remediation, and validation work so limited IT staff can focus on security priorities that require their expertise.

3. ENFORCE CONSISTENTLY

Centrally manage approved policies and automate enforcement across campuses, departments, remote systems, and cloud environments, including connected and disconnected endpoints.

4. CUSTOMIZE WITH CONTROL

Adapt CIS Benchmarks to institutional requirements, document necessary exceptions, track policy changes, and validate systems against the institution's approved baseline.

5. CORRECT CONFIGURATION DRIFT

Continuously validate configurations, identify drift caused by updates and routine changes, and automate remediation before security gaps accumulate.

6. IMPROVE VISIBILITY

Gain centralized visibility into configuration status, policy enforcement, findings, and remediation activity across managed endpoints to identify issues and demonstrate progress.

7. PROTECT CRITICAL OPERATIONS

Test and customize policies, manage exceptions, and roll back changes when necessary to strengthen security without disrupting teaching, research, or administration.

Make CIS Benchmarks Security Sustainable

ConfigOS unifies the work required to implement and maintain secure configurations across higher education environments. Move beyond one-time hardening with CIS Benchmarks automation built to keep pace with your institution.