SteelCloud

Centralizing and Automating CIS Benchmarks Hardening Across 20+ Community Colleges

CHALLENGE: Strengthening Security Posture with Existing IT Teams

The Virginia Community College System (VCCS) oversees 20+ community colleges with widely varying IT resources. Some colleges have substantial IT teams, while others rely on a single IT professional to handle everything from user support and networking to server administration and security.

VCCS had been using ISO 27000 as its security framework, Tenable for vulnerability scanning and manual processes to remediate more than 900 endpoints, largely Windows servers and workstations. However, when Tenable scanned VCCS systems against CIS Benchmarks, the results showed only 40% alignment. In practical terms, the audit revealed that too many default settings remained enabled, increasing the number of potential entry points attackers could exploit.

The message was clear: VCCS needed to apply stricter security benchmarks across its environment without creating additional manual work for already-stretched IT teams. That meant finding an approach that could scale across 20+ campuses, support distributed campus IT resources and give the system office centralized oversight without requiring a large security staff.

Finally, VCCS also needed greater visibility across the system. Individual colleges could have different requirements, exceptions or policy variations, making centralized oversight difficult when compliance information was spread across separate environments. Addressing those challenges would require more than a new framework. VCCS needed a way to automate CIS Benchmarks hardening, centralize policy management and scale the process organization wide.

SOLUTION: Automating CIS Benchmarks Hardening Across 20+ Campuses

VCCS decided to move to CIS Benchmarks as their framework. CIS Benchmarks is a globally recognized, consensus-based,standardized framework that is widely used in higher education. It provides a clear roadmap as to the services and settings to turn off for a more secure system, as well as how to do it.

More importantly, CIS Benchmarks can be automated, reducing manual effort, minimizing the risk of human error and helping teams identify unnecessary services and functionality to turn off and significantly reduce the attack surface across the system.

To do that, VCCS chose ConfigOS MPO. The long-proven, unified solution is purpose-built to scan, remediate, verify and report from a single dashboard, giving VCCS a practical way to automate CIS Benchmarks hardening across the system.

ConfigOS also helped VCCS centralize operations. Instead of requiring each college to create and maintain its own policies, the system office established baseline policies while still working with individual colleges on tailored configurations when needed. The platform also gave VCCS a centralized view of hardening progress across all 20+ colleges.

Notably, the platform automates the remediation process. Instead of engineers manually making registry and configuration changes on individual systems, ConfigOS applies the required changes directly, including customized policy needs.

Four features of the solution became particularly instrumental in VCCS' selection of ConfigOS:

Centralization: ConfigOS gives VCCS centralized visibility into hardening progress across all colleges while allowing individual colleges to connect back to a central server. This eliminates the need for each college to maintain its own instance or manage hardening independently.

Ease of Use: Because many college IT staffs experience high turnover, VCCS needed a solution that was easy to learn and maintain without requiring extensive training on a complex tool.

Policy Customization: ConfigOS allows individual colleges to implement policy exceptions or differentiated configurations when needed, while keeping that information centralized for system office oversight and audit inquiries.

Rapid Policy Debugger (RPD): RPD helps VCCS troubleshoot policy issues more quickly, especially when identifying controls that may be negatively affecting an endpoint. Issues that previously took days to isolate can now be identified in as little as 10 to 15 minutes.

The transition to ConfigOS and CIS Benchmarks was deliberately phased. VCCS began with a pilot at a single, minimally staffed college, using that implementation to validate the approach before expanding further. Once the pilot was complete, ConfigOS was rolled out in groups of approximately four or five colleges at a time, with implementation meetings held weekly or every other week to support multiple colleges simultaneously. In total, VCCS implemented the solution across all 20+ colleges in approximately two months after the pilot.

OUTCOME: Improving Audit Scores from 40% to 80%+

The biggest outcome for VCCS has been the transformation of system hardening from a labor-intensive manual process into an automated and centrally managed capability. Systems that previously required hours or days of manual work can now be scanned and remediated in minutes, subject to VCCS's normal change-management process.

The security improvement was also measurable. When VCCS began the effort, servers were initially returning CIS Benchmarks alignment results around 40%. That figure subsequently moved into the 80%+ range.

At one smaller western Virginia college, a single IT administrator was able to implement ConfigOS, automate the hardening process and then let the software do all the work, checking periodically to make sure the processes continued to operate. Now, hardening doesn't have to compete with every other operational priority for already constrained IT resources.

For VCCS, ConfigOS delivers value beyond individual configuration changes. It gives the system office a practical way to operationalize CIS Benchmarks hardening across a complex, distributed higher-education environment. Most importantly, VCCS has strengthened its security posture without adding burden to the IT teams responsible for keeping 20+ colleges running.

ConfigOS Key Outcomes

- ✓ 20+ community colleges and more than 900 endpoints brought into alignment with CIS Benchmarks
- ✓ Automation that scans and remediates the entire enterprise in minutes, instead of weeks
- ✓ From 40% CIS Benchmarks alignment to over 80%, system wide
- ✓ Centralized policy management and visibility across the system
- ✓ Approximately two months to roll out ConfigOS across all colleges (after the pilot)
- ✓ Continued support and training throughout implementation

> "We went from **40% alignment with CIS Benchmarks to over 80%**. And we didn't achieve that by adding more people or putting more stress on our team. We did it by using a ConfigOS automation and the people we already had."
>
> —**Brian Hicks**
> Information Security Analyst, VCCS