Ohio | Benefits Program

DRAWING THE LINE & HOLDING THE LINE

May 2023

State: State of Ohio

Agency: Department of Administrative Services

Award Category: Cybersecurity

Project Title: Drawing the Line & Holding the Line: Maintaining a Robust Security Baseline for Ohio Benefits

Project Dates: April 2022 – January 2023

Contact: Kristina Hagberg, Deputy State Chief Information Officer, Kristina.Hagberg@das.ohio.gov

Executive Summary

Maintaining a large environment comes with challenges as many government organizations and commercial entities can attest. How do you keep things compliant? How do you prevent configuration drift or detect and correct it quickly when it occurs? How do you prevent a vicious cycle of introducing vulnerabilities and remediating them? It all comes down to establishing and maintaining a robust security baseline. In other words, **drawing the line and holding the line**.

The Ohio Benefits Program initiated a project in 2022 to improve compliance and instill strong discipline to make sure things stay compliant, stable, and secure. It was clear from the onset that this was as much about process as it was about technology. Technology investments were not needed; the required tools were already in place. It came down to dedicating the time and effort needed to drive the improvements and sustain them once the project's objective was met.

The successful outcome of the project was based on five key parts:

1. Identify and set a solid standard. For the Ohio Benefits Program system, this was the Center for Internet Security (CIS) Benchmarks.
2. Use a policy scanner to verify compliance against the standard.
3. Instill ongoing process discipline through daily compliance scans, reviews, and, if needed, corrections.
4. Track security exceptions for specific configurations where compliance is not feasible or where the scanner is unable to determine compliance and gives 'false positives.'
5. Stay current on security best practices by adopting new benchmark versions.

Ohio Benefits was able to maximize compliance across multiple technology areas, resulting in a stronger security posture overall. The consistency in configurations also makes it easier to manage the environment and assess proposed changes. The program is also experiencing less rework where changes reintroduce vulnerabilities, on some servers, that then need to be addressed again. It is also easier to support external audits with unmistakable evidence of configurations and documented security exception decisions.

IDEA

The Ohio Benefits Program system is an integrated eligibility solution that delivers critical services to millions of Ohioans. The system facilitates online benefit applications, eligibility determinations, and benefits administration for programs like Medicaid, Supplemental Nutrition Assistance Program (SNAP), Temporary Assistance for Needy Families (TANF), and Child Care. The Ohio Benefits Program is entrusted with Ohioans' sensitive data and with making sure that the funds for benefits are used appropriately and efficiently. This raises the stakes for information security at all levels and in all aspects.

In technology environments like that of Ohio Benefits, with hundreds of servers, it is easy to get configuration drift. Even when servers are built from the same template, settings may be unintentionally altered while installing applications. It is just the nature of how various vendor software solutions behave. At the same time, there may be legitimate reasons for certain servers to be configured differently, due to their specific function or as required by the software they host.

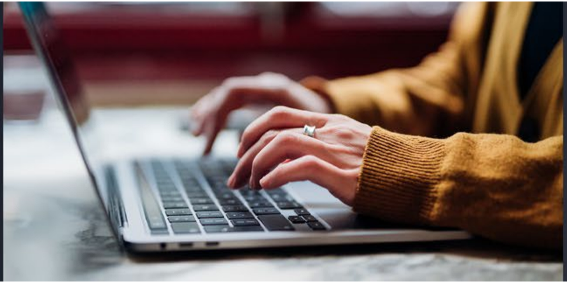
The result of all this is an environment with a suboptimal security posture:

- **Unnecessary vulnerabilities.** Certain settings are configured too liberally to avoid interference with application functions, even on servers where a stricter configuration is desirable and feasible.
- **Remediation causing impacts**. Attempts to tighten things down result in configurations that interfere with the normal operation of some applications, which in turn triggers business impacts.
- **Rinse and repeat.** There is a likelihood of getting into a cycle where system and operational activities reintroduce previously remediated vulnerabilities. This is not only a security concern, but also a waste of resources.

Ohio Benefits experienced each of these scenarios to varying degrees in its legacy infrastructure. They are challenges faced by many organizations, government entities, and private companies alike. The Program saw a broad technology refresh as an opportunity to address this challenge and improve security, compliance, stability, and support efficiency. After all, what better way than to start again with a freshly built infrastructure. Of course, security and vendor hardening guidelines were a priority when building the new infrastructure, but it was clear from the initial scans that things were not where the Ohio Benefits Program team wanted them to be. Installation of commercial-off-the-shelf software often leads to unexpected changes in server configurations. Likewise, the complexity of technology and the ever-expanding array of configuration options (with sometimes varying opinions on the best settings) make it highly likely that certain settings are not optimized or consistent, unless standards are enforced.

As the Ohio Benefits Program team set out to solve the problem, it was quickly realized this was as much a process issue as it was a technology issue.

IMPLEMENTATION

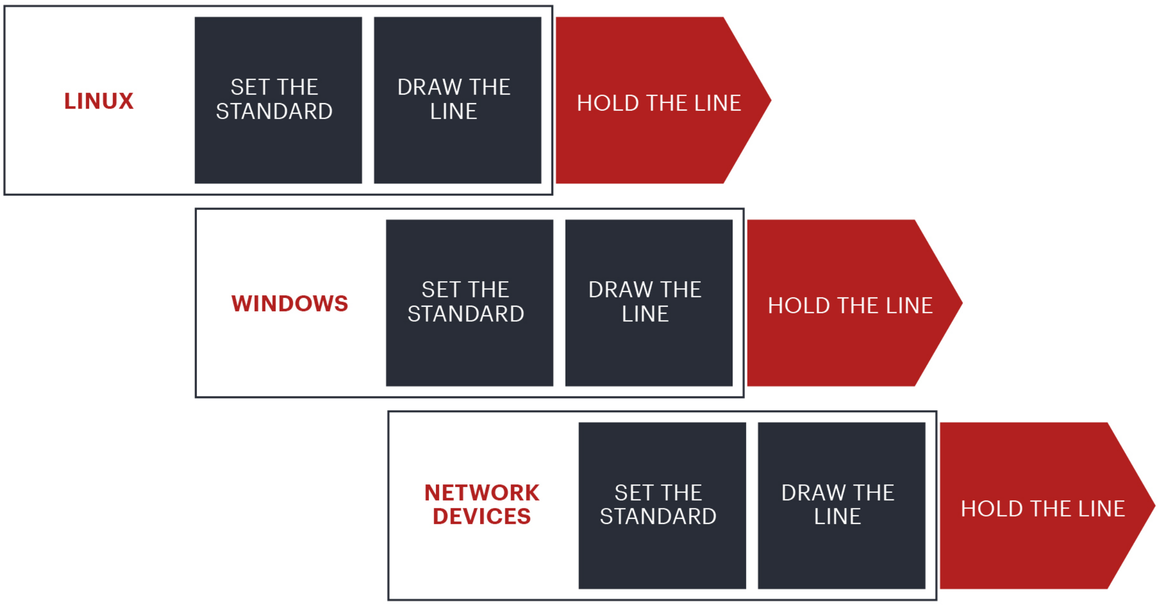


There were five key parts to the desired solution:

1. **Solid standard.** CIS Benchmarks were adopted for several technology platforms.
2. **Policy scanning.** A vulnerability and policy scanning tool was used that could verify compliance against the benchmarks.
3. **Process discipline.** Compliance is not a one-and done deal. Scans needed to be run daily and drive corrective actions when needed, either automated or manually.
4. **Security exception process.** There is inevitably some noise on the scan reports due to configuration settings that are either not relevant or with which some servers simply cannot comply.
5. **Stay current.** New benchmark versions are published from time to time. It is important to stay current with the latest security best practices.

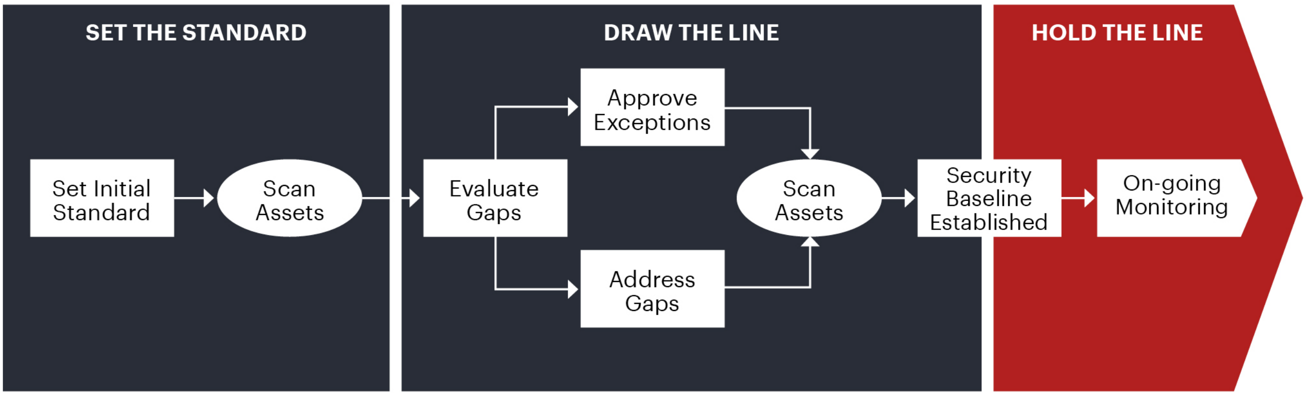
The up-front investment was limited since a suitable scanning product was already in place as well as scripting tools to apply configurations at scale, so this was purely a time investment. Most of the time was spent on researching required settings to assess their potential impact, building out playbooks to roll out configuration settings, and investigating situations where scan results did not match the compliance assessment for specific settings. The latter was caused by the scanner lacking the flexibility to recognize that there were multiple ways to set up a compliant configuration.

The project approach included overlapping tracks where each track covered one specific technology area. Once one track was close to reaching the target state, the next track kicked off. This allowed the Ohio Benefits Program team to better manage its resources. For each track, there was a team of security administrators (responsible for scanning), system administrators (responsible for the configuration of their technology area), and leadership to manage the project.



Each track consisted of three phases:

1. **Set the Standard**. The Ohio Benefits Program team selected the appropriate CIS Benchmarks version and level and performed an initial scan to measure the starting position.
2. **Draw the Line.** After evaluating where scanned assets did not meet the standard, the Ohio Benefits Program team either took action to address the deficiency or, after proper review, documented and approved a security exception to avoid these items from being flagged as non-compliant. Another scan would help confirm progress. Often, multiple rounds like this were performed to reduce the amount of change introduced at once. This was repeated until clean scans were achieved across all in-scope assets.
3. **Hold the Line.** Once the scan was clean, a security baseline was established for the respective asset class, allowing the Ohio Benefits Program team to move into regular maintenance mode. The expectation from this point forward is that every scan has the same outcome, ensuring ongoing compliance. When deviations are discovered, the gaps are to be addressed and the root cause is identified to prevent future configuration drift.



IMPACT

The direct impact of this project is easily quantified by the compliance scores. The table below illustrates the before and after compliance scores across different technology areas.

ASSET TYPE	BEFORE	AFTER		
	COMPLIANCE	COMPLIANCE	MET	EXEMPT
WINDOWS SERVERS	74% – 83%	100%	92%	8%
LINUX SERVERS	81% – 87%	100%	93%	7%
NETWORK DEVICES	62% – 74%	100%	77%	23%

The ranges for the before values reflect the inconsistencies that existed across similar assets and exceptions that were not adequately documented or even recognized. Each of the technology areas was brought to maximum compliance with CIS Benchmarks, while keeping security exceptions at a minimum, as shown in the after values.

Examples of common and justifiable exception scenarios are:

- Some servers require settings that contradict the CIS Benchmarks but are needed for their applications to function (e.g., X11 is needed for the administration of some applications).
- In some cases, the scans checked for specific configuration values related to securing capabilities that were not enabled or even installed, resulting in 'false positives.'

Of course, there is also an indirect impact that is much harder to quantify. Higher compliance results in a stronger overall security posture. The consistency in configurations makes it easier to manage the environment and assess proposed changes, and we are seeing less rework where changes reintroduce vulnerabilities on some servers that then need to be addressed again.

The results of this compliance project are now baked into the operational processes. The Ohio Benefits Program team scans for compliance daily, addresses gaps where needed, and reviews and introduces newer versions of the CIS Benchmarks as they become available. Exceptions are evaluated annually to determine if there is a continued need for the deviation. When new systems are introduced into production, they are built to standard and reviewed for compliance before being put into use. This ensures an elevated level of compliance going forward that is also easier to demonstrate to external auditors with unmistakable evidence of configurations and documented security exception decisions. Overall, this project delivered a mindset and a way of working that are now engrained in Ohio Benefits Program daily operations.