SteelCloud

WHITE PAPER

The Unified Automation Advantage for 2026 Cyber Readiness

Unified Compliance Automation—A Force Multiplier for Cyber Readiness

EXECUTIVE SUMMARY:

How to Achieve Cyber Readiness in 2026

Each year, bad actors up the ante. They find new vulnerabilities to exploit. They increase the number and types of attacks. And, more and more, they leverage AI to multiply their efforts.

If AI is their force multiplier, what is yours?

In agencies and organizations across America, many are still bringing manual methodologies to a bot fight. Most have automation tools, like scanners, to help ease the burden. But remediation and reporting often still require significant manual intervention. Moreover, cobbling together a solution of fragmented, siloed tools inevitably creates drift, rework and unnecessary risk.

Today's cyber readiness is marked by speed, consistency and the ability to sustain operations under pressure. Every industry—not just sensitive areas of the Department of Defense—now requires a STIG-level security mindset. A "my bot can immobilize your bot" mindset. A unified automation mindset.

Discover the force—and readiness—multiplier of unified automation.

Unified automation (or unified compliance automation) is today's most powerful approach to cybersecurity—the only reasonably sustainable way to combat the threats that continue to grow year after year.

"Unified automation" refers to a single, purpose-built solution that automates the scanning, policy implementation, remediation, ongoing maintenance and reporting required to fulfill or comply with cybersecurity standards. It automates cybersecurity compliance and audit-readiness, eliminating errors, rework and inconsistencies. It also ensures your readiness isn't achieved in silos, but applied across the entire enterprise by unifying content as well as implementation.

From STIGs and CIS Benchmarks to RMF/Cyber Security Risk Management Construct (CSRMC), and CMMC, no other approach does the job as quickly, as affordably, as effortlessly and as well. Unified automation is the force multiplier that makes it possible for your team to finally address those other cybersecurity initiatives they never get around to, strengthening your overall security. And it's the readiness multiplier that delivers on the promise of today's most comprehensive frameworks.

What Cyber Readiness Means in 2026

If the fruits of cybercrime were measured against the most successful nations, it would be the world's third largest economy with damages totaling $10.3 trillion in 2025 (up from $3 trillion in 2015).

Another way of looking at it is that 97% of companies report Gen AI security issues and breaches each year. And the World Economic Forum reports that more than 70% of cyber leaders believe that small businesses have reached a point where they can no longer adequately secure themselves on their own.

Simply put, the threat tempo is on the rise. Adversaries are moving faster, automating more and weaponizing more rapidly. Readiness must be continuous to protect your systems and data from these threats.

We see a lot of organizations struggling so much to achieve a secure baseline and keep up with updates that they don't have time to police everyday drift. Meanwhile, perpetrators with relentless bots are just waiting to find a vulnerability to exploit. Your security needs to be just as relentless, which is why continuous compliance is now becoming requisite.

Learn why manual means can no longer keep up.

There was a time when organizations could use manual means to protect their systems. But in a world where 65% of C-suite cyber leaders say they've been hit by a successful cyberattack in the past year, those days are gone. Here are a few of the reasons why:

- ✓ **Modern environments are too complex for manual control.** Today's hybrid, multi-cloud and classified environments increase configuration volume and the risk of drift. The more systems you have, the more variables you have and the more opportunities for misconfiguration by manual means.
- ✓ **Staffing shortages and burnout limit what you can accomplish.** In the US alone, there are only 74 workers for every 100 available cybersecurity jobs. And these are expensive positions to fill, especially if you are asking one of these experts to manually STIG as their career. As a result, whether you're working in government or industry, you're asked to do more with less—and at an unsustainable pace. So teams are always behind the 8 ball. And the resulting burnout and stress translates to more errors, more job dissatisfaction and a near zero likelihood of maintaining continuous compliance through manual efforts.
- ✓ **Compliance debt causes a significant amount of operational risk.** Missed updates, outdated STIGs and incomplete CIS Benchmarks controls create silent vulnerabilities in your system. Using manual means or fragmented automation tools to secure your system can introduce inconsistencies and blind spots in your security. Aside from these vulnerabilities, if you are subject to audits, you could be fined or lose contracts by not being able to keep up. Unified automation is not just critical to your security, but also to your continued operations.

The cadence of attacks is only going to increase. Your IT environment is only going to get more sophisticated. Your readiness will remain directly related to what your people are able to accomplish. And your operational risks will continue to rise.

You simply cannot continue to achieve the vision of STIGs, CIS Benchmarks and other standardized frameworks using the approaches you are using today. It's an operational tempo challenge. You are limited by the amount of manpower you have and the amount that's available in the marketplace when you rely on manual and even hybrid means. Even if you are able to keep up right now, threats and vulnerabilities are intensifying. Using an end-to-end, fully integrated, purpose-built unified automation solution is quickly becoming the only way to maintain both continuous compliance and your sanity moving forward.

Standardized Frameworks Deliver Discipline at Scale

Standards form the foundation of today's world-class cybersecurity efforts. You don't have to follow standards unless they are mandated or otherwise contractually required. But what the standards offer you is something that's nearly impossible to achieve on your own.

Standards distill global experiences into a prescribed roadmap you can follow to secure your systems against all known vulnerabilities. They combine what you know with the "what you don't know can hurt you" aspects of cybersecurity for 360-degree system security.

Find out which standards make sense for you.

While generally prescribed for the government and their contractors, today's leading standards can be used by any industry. Standardized frameworks bring structure, discipline, repeatable practices and measurable expectations to the table. By issuing regular updates, they also keep you secure against emerging threats.

Today's three leading frameworks are:

- ✓ **NIST.** The National Institute of Standards and Technology (NIST) standards are used widely across government and industry to provide a cybersecurity framework and best practices for organizations to follow. NIST SP 800-153 and 800-171 are the two leading publications in this framework and they provide the basis upon which STIGs and CIS Benchmarks are modeled. While mandated in some places, NIST standards are often adopted voluntarily, and they provide a solid roadmap for most organizations to follow. They are updated as needed.

- ✓ **CIS Benchmarks.** Developed by the Center for Internet Security (CIS), CIS Benchmarks provide prescriptive configurations for more than 25 vendor product categories. They are based on NIST guidelines and represent the consensus of global cybersecurity experts on how and where to best protect systems against threats. CIS Benchmarks are mandated or voluntarily adopted throughout government, across the government supply chain and in private industry. They are updated as needed.

- ✓ **STIG.** With hundreds of Security Technical Implementation Guides designed for specific, off-the-shelf software, routers, operating systems and devices, STIGs represent the highest level of security achievable. They are often used in the most sensitive government agencies, such as the Department of Defense and Department of Energy, as well as among some of their vendors and partners. They are usually mandated, though voluntary adoption is becoming more and more common. They are updated quarterly, which is generally the most often of all the standards.

In many cases, these frameworks are enforced by audits such as Cybersecurity Maturity Model Certification (CMMC) or the Cyber Operational Readiness Assessment (CORA). Audits add another layer of stress to the equation because they often happen on short notice.

Here, your need to be continuously compliant translates to continuous audit readiness. In the government, a failed audit is shame on your agency. In the supply chain, it could cost you your contract. So there is incentive—and often a mandated requirement—to be fully in compliance at all times.

See how the cybersecurity mindset is changing and how it impacts logistics.

It is important to research the standards and apply whichever works best for your industry and your risks. A few years ago, you didn't hear of STIGs too much outside of DoD applications. But that is changing.

A DoD level of rigor—a STIG mindset—is becoming more necessary because adversaries don't care what business you're in. More of them are looking to hold your data ransom than to steal it for nefarious means. And ransomware is a great equalizer. It makes a chain of daycare centers nearly as attractive to infiltrate as our nuclear stockpile.

Having a STIG-level mindset means maintaining strict security discipline. It means continuously monitoring for when the system drifts from its secure baseline. Drift can start innocently enough just from performing daily system maintenance, adding users, endpoints and software updates. Then suddenly there's a vulnerability for bad actors to exploit.

Beyond that, it's also about instilling discipline among your users. It probably won't surprise you to know that phishing is the most common way to breach a system. So a STIG-level mindset is also about instilling a Zero Trust mindset throughout your enterprise where no email, no link, no device, no login/log out—nothing—is trusted.

That's why standards are so valuable. They provide fixes for all the minutiae we might overlook in our security strategies—all the app functionalities, all the current threats and all the hacker tradecraft that makes our systems vulnerable to attack. They tell us what to address to cultivate readiness.

Unified automation operationalizes standards and helps us with the "how"—how to implement them efficiently, consistently, effectively, affordably, continuously and to the great frustration of our adversaries. Working together, standardization and automation provide the most powerful defense against a rapidly evolving threat.

How Manual Processes Impede Readiness

So far, we've been talking about manual processes like they should be eliminated altogether. To be clear, if you only have a handful of endpoints and perceive you have a low risk of attack, your manual efforts are probably sufficient. If you have hundreds or thousands of endpoints and an army of cybersecurity pros, that may also cover you. But not likely.

The reason that no number of willing hands will get you where you want to go is due to shortcomings inherent in the manual process:

- ✓ **Inconsistency.** Manual processes lead to error, inconsistent implementations, incomplete documentation, unpredictable outcomes and a lack of repeatability and consistency across the enterprise if efforts are siloed. It's a form of chaos that we've come to accept. We think this is the only way it's done until we have the opportunity to see a different way.
- ✓ **Burnout.** Mental health is the elephant in the room when it comes to manual implementation. Spending long hours patching, checking, verifying and redoing work leads to burnout. And it's usually senior engineers doing this repetitive work as they see other mission-critical priorities set aside for STIGs or CIS Benchmarks. It's a monotonous job that never ends and leads to everything from burnout to depression.
- ✓ **Added risk.** With manual efforts, drift accumulates from lack of visibility into the state of your compliance. Audits reveal issues too late. Vulnerabilities go unpatched. And all of this puts your system at risk. Conversely, unified automation is always on the job with a watchful eye, sharing progress through dashboards, implementing updates with little intervention and continually updating records for reports.
- ✓ **Fragmented effort.** When you combine fragmented tools with manual effort, you get fragmented results. Siloed scripts, local automation and point solutions create uneven security. Without unified automation, implementation varies by team, system and environment. With this sort of approach, you are unable to scale and your teams are on different pages at different times, creating cracks that can be exploited.

Unified automation addresses all these issues compromising your readiness. It creates an opportunity to unify your policy and implementation across your enterprise, rather than having five teams doing the same work five times over. It eliminates human error, is easily scalable and delivers predictable, fully documented results. It keeps drift at bay with little intervention and lets you know when intervention is needed. In short, it brings sanity to security.

Multiplying Readiness With Unified Compliance Automation

Readiness isn't a destination. It's a journey. Because as soon as you achieve readiness—for compliance, for audits, for defending your system and for whatever comes next—a new update is posted, an inconsistency is found or new attack vectors are discovered.

Unified automation is considered a readiness multiplier because it eliminates all the variables that inhibit readiness. It eradicates inconsistencies and the risk of drift because it applies controls the same way, every time and across every system. It's always on the job. And it automatically performs updates with minimal intervention.

It's really a no-brainer. Some will be hesitant to implement unified automation because it means leaving the familiar, even if the familiar is fraught with frustration, repetition and the questioning of one's existence. But that is the only drawback, and it's a false one at that, because within a couple hours of training you'll be up to speed and wondering why it took you so long to make the switch.

97% of companies report **Gen AI security issues & breaches** each year

Turn readiness into something repeatable.

Unified automation is not just a tactical or logistical convenience. It's also a strategic blueprint for implementing the highest—and most friction-free—standards of security. Beyond strengthening your readiness, unified automation delivers benefits and capabilities that make it worthy of your mission:

- ✓ **Improve operational tempo.** With manual means, you think of compliance in terms of taking weeks and months to achieve. With unified automation, once policy is set, the same steps take hours and, on the outside, days to complete. So frameworks are implemented faster, new software or devices are available sooner, POA&M timelines are shorter and remediation is rapid and hands-off. On average, users report a 70%-90% reduction in effort with unified automation.
- ✓ **Achieve precision at enterprise scale.** Open-source scanners and tools go a long way in expediting compliance. But they are not built for each other—they are not natively created to work together. As such, they don't integrate smoothly into a solution that is reliable or consistent. With unified automation, consideration of every step of the process is purpose-built into each functionality for a holistic and unified approach to getting the job done. Every environment and every team follows the same authoritative control logic.
- ✓ **Gain real-time visibility and assurance.** When everything is intentional and integrated in your compliance approach, it's easy to see what's going on. Your compliance posture suddenly becomes measurable in real time. Dashboards give you insight into the process. Data is collected to issue reports without any lag time. And leaders no longer have to guess where they stand in the compliance process—it's right there in front of their noses.
- ✓ **Attain continuous compliance.** Continuous compliance is the holy grail of STIG, NIST and CIS Benchmarks compliance. It means there is no drift. No vulnerabilities to exploit. And no updates waiting for you to find time to implement. Humans can't have their eyes on every element of your framework cybersecurity 24/7/365, but unified automation can.
- ✓ **Get more done with less.** Users of unified automation routinely save about 70% of the costs of compliance, based on the time and manpower savings, as well as the cost of tools. And that manpower is now available to get to that patching you've been putting off, the Zero Trust initiative that never gets off the ground and whatever pet projects you've been meaning to initiate when you have time. You won't need to hire any expensive, hard-to-find experts to up your cybersecurity game. The staff you have on hand will now be able to achieve a much bigger vision for your mission.

How Frameworks Interact With Each Other

Readiness is not about which framework you choose. STIG, CIS Benchmarks, and NIST 800-53 all demand disciplined, repeatable controls. But it's about how consistent you are in implementing and maintaining those controls. That's what unified automation does better than any other approach.

Because all these frameworks are based off the same controls, the different standards, audits and mandates reinforce each other and have some crossover. For example, STIGs inform the RMF/Cybersecurity Risk Management Construct, establishing baseline compliance for both. And all the frameworks—CIS Benchmarks, NIST and STIG—can help make you CMMC-ready.

The frameworks are not limited to any one industry, either. CIS Benchmarks, for instance, improves auditability across SLED and regulated industries, as well as any organization. And if you are subject to audits like regulated industries, unified automation ensures you are always audit-ready.

In other words, unified automation is the connecting fabric across frameworks, requirements, expectations and industries. It standardizes the standards and frames the frameworks as it reduces work, drift and documentation burdens. It turns your compliance efforts into a cohesive readiness strategy.

Building Your Readiness-First Security Program in 2026

If the stress and tension around cybersecurity and compliance was hot in 2025, you can expect it to get even hotter in 2026. And again in 2027. Adversaries are getting more sophisticated every year and so should you.

Cybersecurity maturity in the latter half of the 2020s means moving away from an "audit prep" mindset into an "always ready" mindset. Audits and certifications are secondary to being secure in the first place. And if you are properly secure with continuous control enforcement and validation from unified automation, you are always audit-ready.

Join the readiness culture.

Readiness isn't a destination or a checklist item. It's a culture. It's an ongoing journey. Unified automation is the vehicle that will take you on the journey. It will empower your teams with ease, repeatability and clarity. And it will finally align leadership around the operational outcomes you strive for every day, as opposed to just audit results.

Readiness covers many areas—audit-readiness, compliance readiness, and response readiness if a breach occurs. But perhaps most relevant is being ready for what comes next…whatever that may be.

The future will definitely bring more control updates. It will likely include more audit scrutiny. There will be a growing interest in automation evidence and artifacts. And each year already brings more complexity to your enterprise.

Unified automation puts you in a strategic position to mature your cybersecurity position and address future challenges with little to no retooling of your processes and procedures. It is likely the last new approach you'll need to adopt for compliance because unified automation solutions are built with that type of agility in mind.

CONCLUSION:

Unified Compliance Automation Delivers Readiness for 2026 and Beyond

If you want security, compliance and readiness, unified automation is the best, most efficient (and quite possibly the only) way to achieve it.

Threats are accelerating at an alarming pace. The staffing shortage in the industry is growing. Standards are evolving and getting more complex. Frameworks are converging. And environments are growing more complex. This is no longer a job humans can handle on their own…even with the help of disparate tools…even if they are really good at what they do.

Unified automation is the only approach that can keep up with what's happening today and scale to greet what tomorrow might bring. It's more than a tool. It's an end-to-end solution that can enforce standards, reduce drift and sustain readiness at scale, changing business as usual in some of the very best ways.

The only catch is that, while it's easy to find one-off tools, it's hard to find a true, unified solution. And even harder to find one that's been proven over countless implementations. To learn more about unified automation, see it action and discover how to find a solution that's customized to your organizational needs and policies, visit www.steelcloud.com.

About SteelCloud

SteelCloud develops innovative software that delivers near-impenetrable endpoint security with minimal effort. Our patented ConfigOS platform is the industry leader in optimizing readiness by automating the implementation of NIST (National Institute of Standards and Technology) and STIG (Security Technical Implementation Guide) security controls and CIS (Center for Internet Security) Benchmarks.

ConfigOS has been proven over more than a decade to streamline and accelerate the hardening process by automatically detecting vulnerabilities and remediating issues—eliminating the complexity traditionally associated with endpoint hardening.

What once took weeks of manual effort is now completed in about an hour. ConfigOS and ConfigOS MPO make it effortless to maintain secure baselines in any environment, laying a critical foundation for Zero Trust architectures and other advanced cybersecurity strategies.

SteelCloud can be reached at 703.674.5500. Additional information is available at www.steelcloud.com or by email at info@steelcloud.com.