

# Testing & Validating

the Maturity of  
Cybersecurity  
Programs

## CONTRIBUTORS:



**Aaron McIntosh**  
Director,  
Product Marketing



**Adam Mansour**  
Virtual CISO &  
Head of Sales Engineering



## 1 Introduction: the allure of complacency

It is easy enough for an IT department to *create* a cybersecurity apparatus: buy this piece of software, announce that policy, and you have built yourself a security framework. However, *validation and testing* of these programs are not always quite as rigorous as the initial construction efforts that went into them, as the very act of “construction” can lead some IT professionals into feeling they have something viable just because they’ve taken action. One major contributor to this inadvertent complacency is that the success of a security program is most easily judged by the absence of a negative outcome. So long as it hasn’t been breached, the program can be deemed a “success,” regardless of its true integrity, and busy IT departments are free to focus on their many other tasks.

As too many headlines have made clear, simply reacting to threats is no longer good enough to protect a business. The capabilities and tactics of threat actors are advancing all the time, and the rise of long-cycle attacks that leverage “living off the land” tactics means that attackers can penetrate deeper into systems before exposing themselves (we discuss long-cycle attacks in more detail in our white paper “[The Rise of Ransomware as a Service](#)”). As attacks grow in scope and sophistication, the cost of a single breach is also rising. By 2020, the average sum paid by victims of ransomware attacks had ballooned to over **\$178,000**. This expenditure and the resulting reputational damage can be especially devastating to smaller businesses: [a February report from telecom giant Vodafone](#) estimated that in the U.K. alone, 1.3 million small to mid-sized enterprises would be “incapable of surviving” a successful cyberattack.




Since threats are continuously evolving, solutions must do the same – and with the price of failure so high, there’s no better solution than a solid and *proactive* cybersecurity strategy. In this white paper, we will guide readers on how to harden their systems without the need for additional services and tools. Rather than an approach of “buy this and buy that,” **we offer expert advice on configuring and optimizing the OS and software you already have, to strengthen your security posture through toolless defense strategies.**

The white paper will also assist you in assessing your systems so as to identify shortcomings before they are discovered the hard way. Has your carefully constructed security program matured along with iterations of threats and the capabilities of malicious actors? We discuss the Cyber Maturity Model Certification (CMMC), the modern regulatory framework that we consider the gold standard of cybersecurity compliance. Since the CMMC process can take months, we’ll introduce you to ActZero’s [Security Maturity Model](#) – a quick and free way to assess where your business currently stands. Ultimately, the strategies outlined herein should help ensure you’re not coasting on a false sense of security rooted in overconfidence.

## 2 The trap of the buy/build mentality

IT leaders are builders who often pride themselves on their constructive efforts and projects when developing their environment and infrastructure – and the work they put in to secure it all. Add a strategically driven and comprehensive plan into the mix – architected by competent experts and augmented by tier-one vendors and many IT leaders rest confident in their security coverage. However, there are significant technical drawbacks to overconfidence in constructionist security programs, no matter how brilliant their architects. (And if they're reading this paper, we know they're pretty smart!)

CSO reports that 60 percent of breaches in 2019 involved vulnerabilities for which a patch was available but not applied, demonstrating that it's insufficient to “set it and forget it.”




When a security approach is dictated by a buy/build mentality, risk mitigation is only as comprehensive as the vectors that have already been covered. As an IT team pieces together protection across the attack surface – its hardware, email, cloud, and so on – they can find themselves **building a SOC without even knowing it**. This is an expensive way to proceed, as each new technology added to an environment needs to be secured anew. Having an “incomplete SOC” that lacks the people, processes, and security technology to protect every category of business-enabling technology means **an organization remains vulnerable to attacks that exploit categories outside those it has defended**. In short, no single piece of prevention technology will be sufficient to protect every vector, so a company building its own SOC – be it intentionally or inadvertently – will never be able to safely *stop* building.

Another challenge facing IT security builders is that after they progress beyond purely preventive strategies like anti-virus and firewall into technologies that enable/require an active response, they will also need dedicated and qualified cybersecurity personnel to operate them. For once something is built, it must be maintained to be fully effective: *CSO* reports that **60 percent of breaches in 2019** involved vulnerabilities for which a patch was available but not applied, demonstrating that it’s insufficient to “set it and forget it.”

Even if a company makes a large investment into technology stacks that generate alerts, analysis (that, at scale, leverages data science) is necessary to garner insight from them – and to dictate action. Such tech can generate logs at a blistering rate no human could possibly keep pace with. A Security Information and Event Management (SIEM) program can assist in aggregating and funneling these alerts – which can number into the billions per day and come in 24 hours a day – but can still generate **false positives and a bloated collection of irrelevant logs**.

This leads to another critical drawback to the buy/build approach: **finding top-tier security talent to manage such technology is already hard enough**. Last year, *Forbes* reported that “the U.S. has less than half the cybersecurity candidates that it needs to handle increasing demand.” And overburdening the IT resources you do have by trying to satisfy 24/7 monitoring demands internally risks the danger of them becoming desensitized or burnt out from too many alerts. For businesses that have built a SOC, yet lack the resources to sustain or grow it, the solution is incorporating artificial intelligence and machine learning into your security operations. This gives you the capability to have more intelligent output and to automate away the need for human threat hunters to look after endless low-level alerts all day. (Read more about that in our post [“The Traditional SOC Is Dead, Long Live the Remote SOC.”](#))

### 3 Hamper cyberattacks through toolless defense strategies



Before you spend any more money tacking on to your existing security stack – or outsourcing management of it entirely – ActZero’s security engineers have some simple, inexpensive suggestions to fortify your systems just by properly configuring your existing technology and fully using the tools that come with your operating system or hardware. Note: we are not saying that these included tools are as good as purpose-built or premium solutions. As you add premium options, your coverage will improve. We are also not saying that standing these up in a ‘one-and-done’ fashion will have the desired preventative effect. The whole is more than the sum of its parts. Somebody must bring these tactics together into a cohesive strategy to configure for security, either on your own or with external help. With those caveats, here are four steps you can take immediately.


#### Introduce a Software Restriction Policy (SRP)



This is part of Microsoft’s Group Policy, so it’s built into Windows, the operating system used by roughly **80 percent of all desktop computers** worldwide. An SRP allows you to limit which scripts, applications, and other technologies are authorized on the OS, and it’s available to you whether you’re running one machine – or one thousand. Since almost all malware depends on being able to use some kind of executable or script to abuse the system, by locking down your endpoints in this manner you can close many of the avenues available for an attacker to successfully break in.

By using an SRP, you’re also following many of the best practices of security maturity – the experts behind the CMMC are expecting you’ll do this. Applying this policy also grants application whitelisting, which will go a long way to enforcing the culture and awareness the users have to play in order to diligently enforce your standards. Utilizing a **Software Restriction Policy** should be every Windows administrator’s first order of business when hardening your systems, as it is an economical way to defend against a wide assortment of malicious techniques.

“ In order to do damage at a wide scale, an attacker needs to control multiple machines – and they’re only able to control multiple machines if the accounts they’re using are allowed to control them.





## Create a host firewall policy

Virtually any operating system you manage, be it Windows, Mac, or Linux, will have an inherent firewall capability. This is one of the more powerful defenses available on workstations and servers, and also one of the more overlooked, as people frequently find it a nuisance and turn it off. It's worth the inconvenience, however, as attackers depend on this capability being disabled or defeated to gain remote control of a system. Be your own traffic cop, and don't allow any applications you don't need going in, while severely restricting the applications that can go out. Controlling your own network right at the host level will dramatically improve your security posture – for free.

## Institute a restricted groups policy


There exists a widespread misbelief, especially in the Windows community, that a domain administrator should be responsible for controlling every machine on the domain. In truth, [the admin was never intended for such wide-ranging privileges](#), and when networks are put together like this an attacker only needs to steal one set of credentials to gain the keys to everything else.

In order to do damage at a wide scale, an attacker needs to control multiple machines – and they're only able to control multiple machines if the accounts they're using are *allowed* to control them. To put it bluntly, **having one account control your entire enterprise is a very high-risk move, and almost certainly unnecessary**. Instead, you can enact a restricted groups policy that ensures no single account has access to multiple systems, and limits which accounts can access each system.

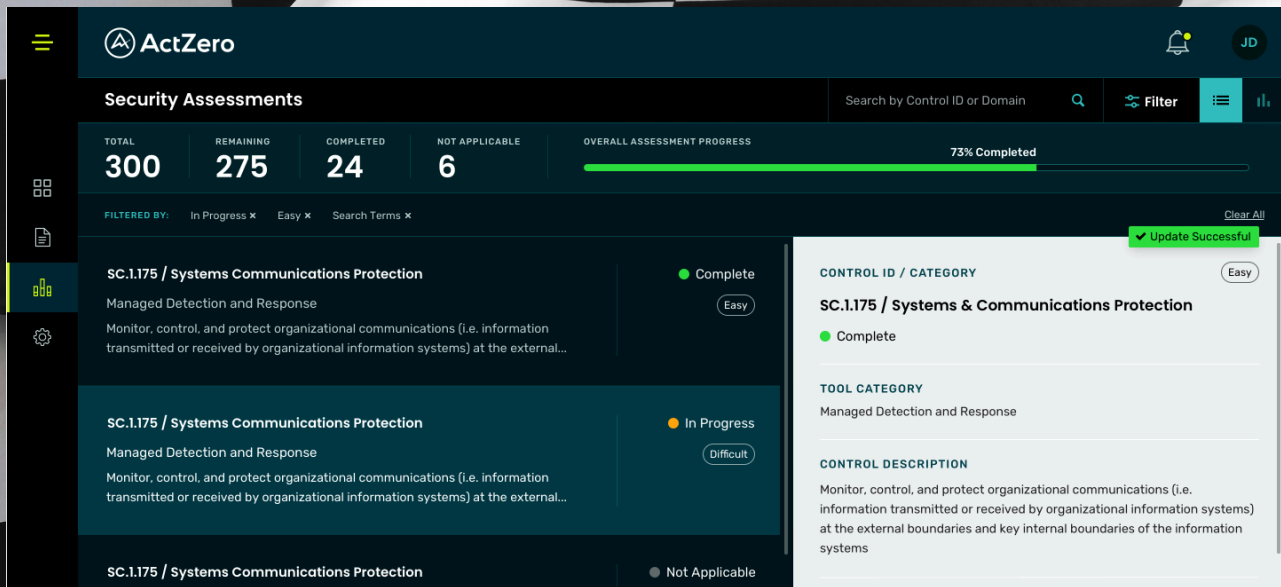


## Leverage the anti-virus software already on your OS

Windows comes with Microsoft Defender, and Macs come with Gatekeeper. These are free tools, so make sure they're turned on! They might not be enough to stop cutting-edge ransomware, but they're certainly better than running nothing at all – especially in terms of identifying and blocking *known* threats. (We'll talk more about the challenges associated with polymorphic, unfamiliar threats shortly.) PCMag recently [reviewed and tested other free anti-virus tools](#), and offers other decent options. A caveat: the publication cautions that "the best paid anti-virus software does offer more and better protection," and that people looking to protect their business "should probably consider upgrading." At a certain point, you get what you pay for. Beyond moving from included to purpose-built anti-virus solutions, is considering a categorical improvement in next-generation anti-virus (NGAV).



Taking these steps won't make your network invincible. However, utilizing all four could force long-cycle attackers to spend months or even years reconnoitering what accounts, scripts, and protocols are allowed on each system in order to coordinate an enterprise-wide assault. With so many hoops to jump through, a would-be hacker may just move on to an easier target.



## 4 Don't expect, inspect: the need for a rigorous testing strategy

The CMMC is designed to validate your security posture. Before (and, after) undergoing this difficult process, it only makes sense to thoroughly test yourself. Imagine you hoped to get your driver's license: would you learn to drive during the road evaluation, with your examiner in the car beside you? This would only waste time and money, and cybersecurity is no different. It's far better to uncover weaknesses now, rather than during a formal audit – or worse yet, during an attack from an active adversary. A strong approach is one that proactively **battle-tests "hardened" security programs, to see whether they stand up** – and, more importantly, **where specifically they fall down**. Once you've put in place the four strategies we discussed previously, there are easy ways to run preliminary penetration tests without even hiring a consultant.

Windows admins can appraise an SRP by attempting to run PowerShell scripts and Batch files from different places, or if these are blocked, a test program like [putty.exe](#). Pretend you're an attacker, think of what you've whitelisted, and try running the scripts from there. Check the Event Viewer to see if violations were successfully blocked – when something doesn't run, it will create a log for you. This is also a good chance to assess your log analysis capabilities: how are they funneled and who is responsible for monitoring them?

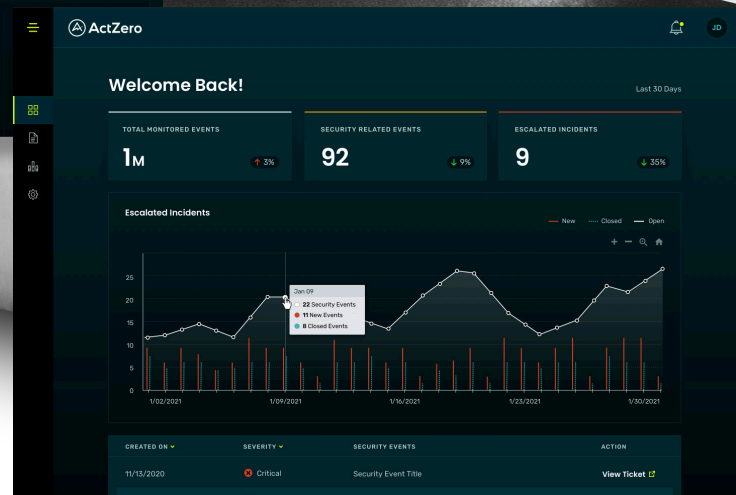
To test a firewall, the easiest way is to use the port and protocol scanner [Nmap](#). Let it run for a couple of days and see everything that's open. More ports mean more opportunities for a breach, and restricting access by IP should become apparent.

Trialing your restricted groups policy is also simple: download the tool [PDQ Inventory](#), enter your administrative credentials, and hit scan. Every machine it finds can be controlled from this one account, and is thus vulnerable to a ransomware attack from it. Ask yourself: does this user account truly need access to all these systems?





To see the guidance you receive through our Customer Portal, **request a demo** of our service today.



Assess your anti-virus software with harmless test viruses like [EICAR](#) and [WildFire](#). Try to download them through your browser and email, and to the local machine. If the anti-virus is working, it should get blocked immediately.

You should also assess the human components of your security posture. Educate employees about phishing emails, and send them benign ones. Consider who will be involved in a real-life security incident, as they should be included in “fire drills.” (Also consider drills with them excluded, to ensure your plan still functions when they’re on vacation.) Do you have a team that is prepped, ready, and easily accessible on your call tree to respond to, say, a Trojan pushing ransomware to your machines? A coherent response might require coordination with business management, endpoint and network admins, legal, HR, PR, and law enforcement. (Read more about this in our post [“Preparing For A Security Incident: Six Decisions You Must Make.”](#))

These strategies and tests are a great start, but another caveat is needed here. Ultimately, a mature approach to cybersecurity must account for more than just known threats. Technologies are always evolving, and so are the capabilities of bad actors. Additionally, modern malware is polymorphic and capable of iterating endlessly. “By 2017, around 96 percent of all malware files detected and blocked by Windows Defender were detected only once on a single computer and never seen again,” writes Cybercrime Magazine in a [recent report](#). Malicious programs can automatically change their attributes in order to bypass pre-existing rules on how to access an operation system, so systems shouldn’t be considered fully secure just because you stopped a test virus. Relying on anti-virus as the last line of defense is an “immature” approach for this reason.

## 5 Next steps: increase your security maturity

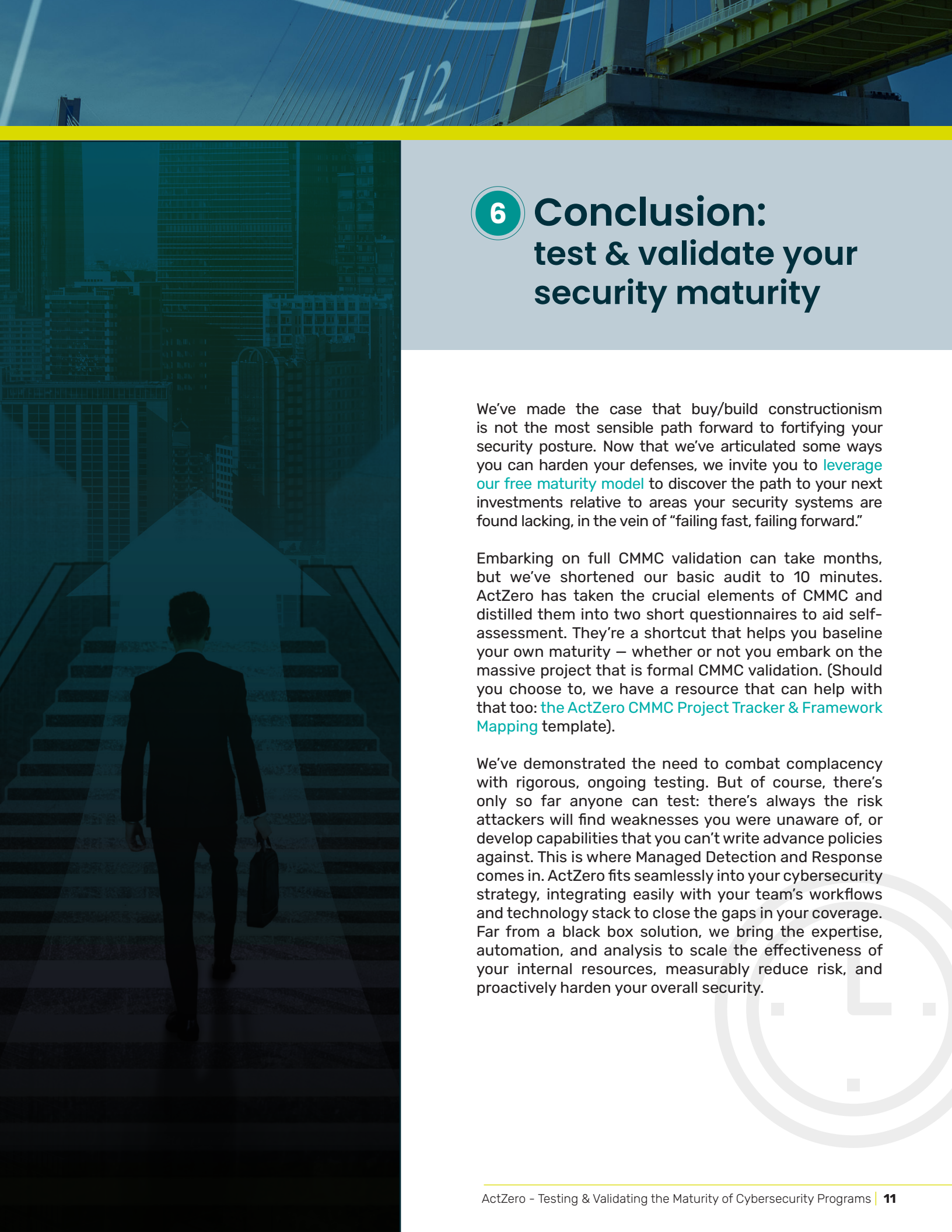
Security compliance standards have typically not kept pace with the true need for companies to upgrade their security stance. But new regulations and dramatically increased penalties for data breaches mean big changes are emerging. (Our [2021 Cybersecurity Predictions](#) white paper discusses new laws in greater detail.)

U.S. lawmakers are seriously considering a [national breach notification law](#). No longer can companies simply write policy documents, maintain the status quo until a fine or warning is issued, and then figure out the easiest and cheapest way to tick the right proof boxes to comply. Customers are demanding answers to security questions, and new risks are emerging as teams adopt new cloud-based systems, such as remote collaboration tools.

There is no more room for guessing; businesses need to understand their security maturity and be ready to demonstrate their best practices to auditors, customers, and prospects. The CMMC was released in 2020 by the U.S. Department of Defense as a requirement for all private-sector businesses that serve the defense industry – not to mention the businesses that serve them. Striving for maturity validation is a sound business decision, and ActZero has used the CMMC regulatory framework and others as the underpinning of our own [Security Maturity Model](#). With many compliance standards, including CMMC, the real consequence of noncompliance is not that fines are levied, but rather contract ineligibility. In an increasingly competitive landscape, this is a gamble most businesses shouldn't take – why exclude yourself from future government contracts?

Even if your organization doesn't plan to do business with the DoD or those servicing/supplying it, we believe it's prudent to meet contemporary maturity standards, and see CMMC in particular as the gold standard (discussed further in our playbook [Why You Need a Modern Regulatory Framework](#)). Systems and data security should be viewed the same way as any insurance policy: it may not protect you from everything, but you still want to be covered for as many eventualities as possible. We all know how devastating modern-day breaches can be, and it only makes sense to take every proactive measure feasibly available in order to avoid one.

We've modeled our own Security Maturity Model after the high standards demanded by the CMMC because we believe them relevant to virtually every business, not just those connected to supply chains around sensitive areas. Hackers don't distinguish between essential government organizations and private manufacturers with their attacks, when there is an ultra-valuable Bitcoin ransom to be made. It's probably wishful thinking to hope every business in the nation achieves the highest levels of maturity – but if they *did*, it would immediately deprive the bad actors of their endless stream of soft, lucrative targets. We must collectively put an end to the runaway success experienced by these cybercriminals; the current state of affairs is frankly no way to do business.



## 6 Conclusion: test & validate your security maturity

We've made the case that buy/build constructionism is not the most sensible path forward to fortifying your security posture. Now that we've articulated some ways you can harden your defenses, we invite you to [leverage our free maturity model](#) to discover the path to your next investments relative to areas your security systems are found lacking, in the vein of "failing fast, failing forward."

Embarking on full CMMC validation can take months, but we've shortened our basic audit to 10 minutes. ActZero has taken the crucial elements of CMMC and distilled them into two short questionnaires to aid self-assessment. They're a shortcut that helps you baseline your own maturity – whether or not you embark on the massive project that is formal CMMC validation. (Should you choose to, we have a resource that can help with that too: [the ActZero CMMC Project Tracker & Framework Mapping](#) template).

We've demonstrated the need to combat complacency with rigorous, ongoing testing. But of course, there's only so far anyone can test: there's always the risk attackers will find weaknesses you were unaware of, or develop capabilities that you can't write advance policies against. This is where Managed Detection and Response comes in. ActZero fits seamlessly into your cybersecurity strategy, integrating easily with your team's workflows and technology stack to close the gaps in your coverage. Far from a black box solution, we bring the expertise, automation, and analysis to scale the effectiveness of your internal resources, measurably reduce risk, and proactively harden your overall security.



**Ready to get started?**

**Visit our Maturity Model Self-Assessment tool** now to start yourself on the path of leveling-up your security maturity.



**TORONTO**

207 Queens Quay, Suite 820  
Toronto, Ontario M5J 1A7

**MENLO PARK**

2882 Sand Hill Road, Suite 115  
Menlo Park, California 94025

**SEATTLE**

925 4th Ave., 20th Floor  
Seattle, Washington 98104



ActZero



ActZeroAI



ActZero.ai