ActZero

The Collaborative Approach to Cybersecurity

CONTRIBUTORS

Adam Mansour
Chief Security Officer

Gwen Way
Manager, Technical
Account Management

Jeffrey McMillan
Manager,
Customer Success

Introduction

"How do we know when we're getting security right?"

The context in which modern organizations find themselves calls for a change in our thinking about what exactly "cybersecurity readiness" means. To be effective, our approach needs to go beyond tactics and point products to consider the total culture and mindset shift that the cybersecurity landscape demands today.

The fallout from every breach and ransom goes beyond the purview of IT or security teams. Yet many leaders still fail to recognize that cybersecurity is a business problem, not a technology one. It calls for close, persistent attention from everyone in the organization as well as from the security providers and partners outside it.

Expecting IT or security teams to handle the problem, or spend their way out of it, simply doesn't work. As the news reminds us daily, the cost of failure is too high to ignore.

So, how do we reach the state where we can be sure our approach is working?

Getting to zero takes technology plus teamwork

In cybersecurity, our goal is simple: Get to zero breaches, zero compliance issues and zero critical vulnerabilities. To get there, first we need to bring the vulnerabilities that cause breaches to zero. Technology can't get us there alone. In our experience, a cybersecurity program defined and driven by the purpose of reaching zero vulnerabilities that remains sensitive to evolving risks, depends on two tenets:

- **Shared responsibility** for collaborative action in pursuit of zero, between internal business, IT and security stakeholders, and external partners where necessary, working together within a holistic framework.
- **Measurement of progress** toward that goal, including a clear and agreed upon definition of success and the metrics or KPIs to assess performance against it.

For many leaders, it's been difficult to reach this understanding. Too often, IT and security teams pursue other less relevant or misleading objectives and KPIs. The need for proactive, consistent action toward the goal of zero vulnerabilities overwhelms strained or lean teams. Divided responsibility without accountability creates gaps and leads to finger-pointing when something goes wrong. The potential to do better is there, but the signal can get lost in the noise.

Cybersecurity is a difficult mountain climb: You can't go it alone.

We liken the journey toward zero breaches, compliance issues and vulnerabilities to a potentially deadly mountain climb. Even the best climbers don't make the ascent alone. Nor do they simply charter a helicopter ride to the peak. Instead, they work together, and rely on experienced guides, to reach the summit safely.

In this guide, we'll examine the need for a collaborative approach, what gets in the way and how ActZero and the Guide program are positioned to help you reach the summit, intact.

Why cybersecurity fails without a collaborative, proactive effort

"Who's responsible for security, exactly?"

The responsibility for security falls to everyone. The breadth of the threat to data, assets and intellectual property makes this non-negotiable. When a breach happens, whether IT, security or a vendor is at fault, the damage is the same.

The right approach is a partnership model based on clearly defined roles both inside the company and with its external security partners. Getting there requires an organization to shift its culture and mindset. This isn't easy to accomplish and it doesn't happen overnight. Most organizations fail because they don't understand the requirement for co-ownership.

In too many cases, leadership sees security as a separate function sectioned off from the rest of IT, or leaves it to IT generalists who aren't equipped for it. Legacy thinking at the organizational and individual levels paint security as a distraction from business value-creating projects. In other cases, it's viewed as a one-and-done investment: IT installs the tools to detect and alert them of threats, or hands this work to an external provider. Either way, the transaction is complete and the business is "secure." Except, it isn't.

In the worst scenarios, IT and security can become adversaries, competing for resources and working at cross-purposes. Management doesn't understand the problem or fails to unite these groups behind a common purpose. When an attack lands or a ransom gets paid, each group blames the other, or the external vendor whose solution failed. The climbers argue, separate and get lost as they each insist on taking their own way up the mountain.

Lack of clear accountability for continuous action to find and remedy vulnerabilities leaves gaps in the IT infrastructure for attackers to exploit. Secure just one vector and hackers move onto the next.

The right approach is also proactive, from the start

It's much easier to remain secure when you've engineered for security from the beginning. Asking questions and challenging assumptions early on pays dividends. This results in good security hygiene from day one. It also means time, money and effort saved that would otherwise have gone to restoring operations and retrofitting applications and systems if a problem developed later.

When the collaborative approach is missing, security is often an afterthought or unwelcome necessity brought on just to satisfy regulatory compliance or cyber insurance standards. Worse, it only gets the necessary attention after an attack has already happened. At the same time, the era of the one-year gap analysis and the security consultant that presents a plan and then hands over the keys is over. The nature of the threat changes constantly. The capacity to anticipate and adapt is essential to survival.

The essence of a collaborative approach

The culture shift needed to reach and sustain a state of zero critical and high severity vulnerabilities demands that leaders rally their people and give meaning to their efforts. To do this, they must reach past tactics and tools to address three needs:

Purpose: Whether it's to achieve a positive outcome (e.g., win more business with clients that have strict regulatory requirements) or prevent a negative one (e.g., reduce operational impact), the whole organization needs to understand the purpose or goal motivating its security efforts. After all, it's hard to reach the summit if you can't see it or even agree on where it is. Maintaining purpose can be difficult, however, as IT teams find themselves pulled away from the big picture by daily routine tasks and sporadic firefighting. Nonetheless, a strong sense of purposes makes priorities clear and alignment easier to achieve.

Autonomy: Often, the process of fulfilling our purpose presents problems we haven't experienced before. In response, we need autonomy, the freedom to apply our ingenuity, try multiple avenues and reshape the environment as necessary. We also need the tools, people, information and expertise to draw on as we go about solving these problems. In the context of cybersecurity, this freedom is curtailed by the need for balance between transparency and trust. It only works if those working toward security purposes clearly understand their roles and responsibilities.

Mastery: As the obstacles get more challenging, achieving our purpose demands mastery of the necessary actions. This mastery only comes from growth and continuous improvement. How do we determine whether and how far we've made it? To be its most effective, a cybersecurity program needs tangible measurements of progress toward its goals. However, relying on narrow KPIs or milestones can cloud understanding of that progress. Checking off one milestone means we're making progress. But this doesn't help us if our risk hasn't meaningfully decreased.

While these core concepts apply across all aspects of IT leadership, there is a fourth that underpins the collaborative approach to cybersecurity: **Community.** To make the tough, often draining journey up that mountain, security stakeholders need to know they're not alone in their efforts. The community aspect provides the organization with people to fall back on when the going gets tough and to provide the guidance, resources and experience to make sense of things and get them back on the path to zero.

This community aspect inspires and informs our Guide program, which bridges our proprietary AI-based platform and full-stack visibility with a collaborative approach to cybersecurity.

Case Study

Collaboration for Compliance

Overview:

An enterprise long term care and insurance provider was looking to improve security and guidance to achieve NIST 800-171 and HIPAA compliance.

Solution:

ActZero was able to guide the customer to full compliance and improved security through controls audits, controls mapping across previously addressed frameworks (including summarizing techniques to cover gaps and avoid exploits), information gathering to help source tools like trackers, running incident response tests and pen tests. Because they were on the path to compliance, threat hunters were able to find and guide the long term care provider through a DDOS attack without downtime or impact to its clients. Because action was taken swiftly, it resulted in zero day offline.

Lessons Learned:

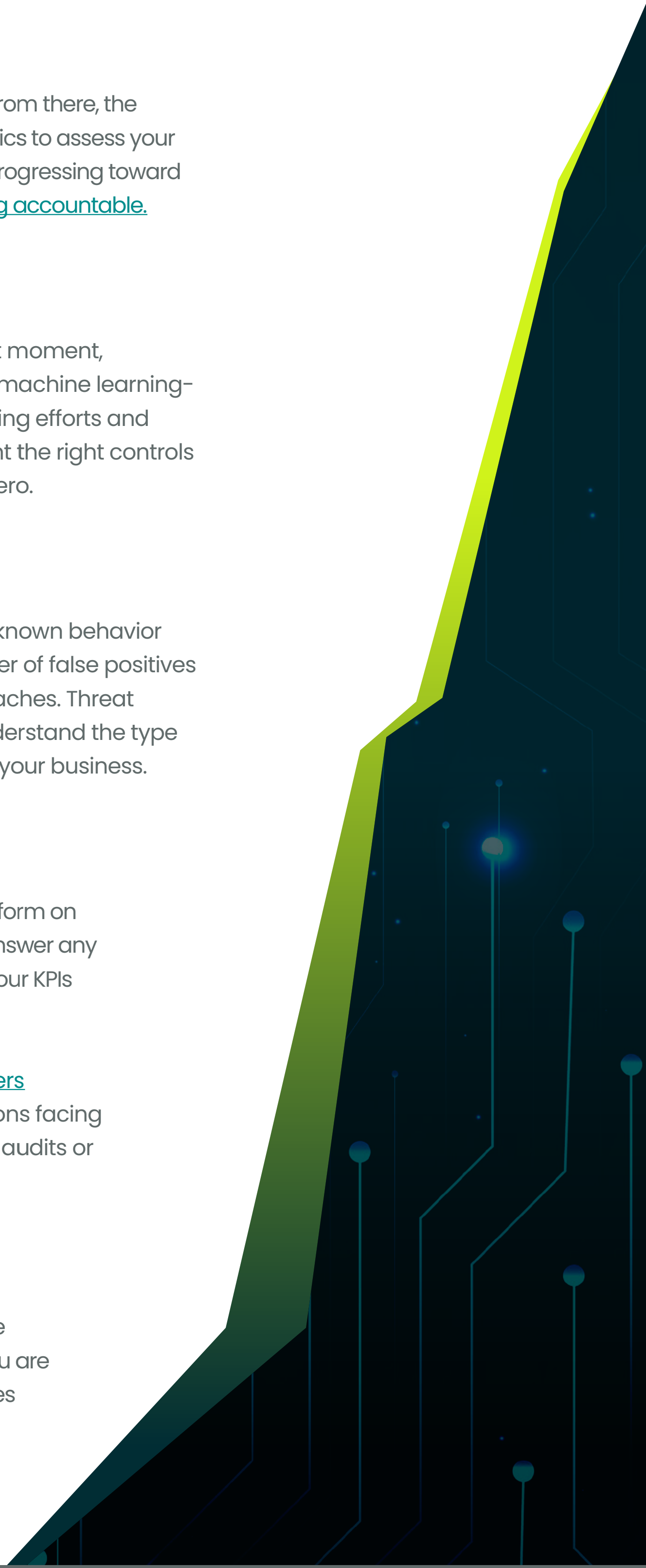
Taking on a massive compliance project while upgrading overall security can be incredibly challenging if going it alone. Being able to tap into expert knowledge and advice can not only help you reach full compliance, but also protect you from potential threats.

The role of the guide program in ActZero

“If you fail, we all fail.”

In many ways, ActZero guides help you plan ahead and stay focused as you define your purpose, pursue mastery and grow your autonomy in the mountain climb of cybersecurity. The guides are backed by a constantly learning platform, enacting ActZero’s foundational purpose of augmenting human ingenuity with the best technology available.

Scaling the Cybersecurity Mountain with ActZero



1 Chart the Path to Summit

ActZero's Defense : Setting KPIs

We recommend every activation start with a threat modeling exercise. From there, the guide works with you to establish clear cybersecurity goals and the metrics to assess your progress toward them. These include KPIs measuring how fast you are progressing toward the key outcomes of providing visibility, proving effectiveness and staying accountable.

2 Getting to Base Camp

ActZero's Defense : Complete Onboarding

Once onboarding is complete, ActZero agents are installed. From that moment, endpoints are protected by a combination of prevention-based and machine learning-powered detection and response. At this point, you can begin hardening efforts and compliance to help you separate the signal from the noise, implement the right controls to improve mean time to remediation (MTTR) and reach the goal of zero.

3 Bridging Pitfalls

ActZero's Defense : Threat Hunting

Our threat hunters, with the help of our AI, analyze event logs against known behavior patterns and threat intelligence feeds. This greatly reduces the number of false positives that require attention and allows them to stay on top of potential breaches. Threat hunters study advanced attack techniques, empowering them to understand the type of attack and when/how to take action without negatively impacting your business.

4 Navigating the Changing Path

ActZero's Defense : Report Reviews/Meetings with Guides

We conduct monthly meetings to assess the ongoing impact of the platform on your vulnerabilities and on CMMC controls, recommend changes and answer any questions. This provides you with up-to-date data on progress toward your KPIs over time.

Along with your guide, ActZero Virtual Chief Information Security Officers (vCISOs) are available to provide on-demand expertise to organizations facing regulatory compliance requirements, client/partner/supplier security audits or implementing security policies and programs.

5 Reaching the Summit

ActZero's Defense : Ongoing maintenance

You are now practicing a collaborative approach to cybersecurity. You're ready to pursue business objectives freely, safe in the knowledge that you are adhering to a proactive, collaborative cybersecurity program that evolves along with the risks.

Case Study

When You Fail We All Fail

Overview:

A mid-sized organization encountered a ransomware attack.

Problem:

ActZero's agent was not installed on all the customer's endpoints.

Solution:

While ActZero was able to stop the attack, there were about 50-75 endpoints that did not have our agent installed. These devices needed to be pulled offline and quarantined before the issue was resolved. This company was lucky because the infected devices were not critical to day-to-day operations, though the sheer number of devices out of service had the potential to create serious service disruptions.

Lessons Learned:

When responsibilities aren't shared across both your organization and your external parties, everyone fails. Opportunities for hackers persist, and these vulnerabilities are not only critical because of the damage they can do but also because of where they exist in your environment.

Playing your part in reaching the cybersecurity summit

In principle, managed detection and response (MDR) is about helping you avoid disaster. This is where the concept differs from traditional "bolt-on" security solutions that provide you with the tools and leave you with the responsibility for using them.

We work alongside you to provide the best security visibility possible and act on your behalf to remediate vulnerabilities on the path to zero. However, for the journey up the mountain to succeed, both guides and climbers must do the work.

Your guide is here to help you with templates to inform your security policy and with selection, procurement and configuration of security tools. You have to train, do as the guide instructs and take advice from the experts seriously. The risk is too high otherwise.

Your responsibilities under the collaborative approach to cybersecurity necessarily include:

- Proactively training the security stakeholders across your organization
- Providing environment data and installing agents as directed at the onboarding stage
- Implementing controls as per curated frameworks provided by your guide/vCISO
- Taking the prioritized remediation actions recommended in the portal

Just as a skilled guide's approach differs for climbers of varying experience, the guide program adapts to your organization's size and level of cybersecurity maturity.

For mid sized enterprises:

Working with an ActZero guide helps your team to prioritize proactive remediation actions and bring together disparate tools.

For small and medium businesses:

Working with an ActZero guide supports your team with security guidance, templates, frameworks and configuration.

Conclusion:

Cybersecurity readiness has grown past traditional boundaries between IT, security and business to become an organizational concern. The extent of what's required beyond installing point solutions and running monthly or quarterly scans is still misunderstood. Reaching the state of zero breaches, zero compliance issues and zero critical vulnerabilities takes a concerted, well-prioritized, collaborative effort.

To achieve this, every organization needs to take steps to:

- Establish a working security model that emphasizes collective responsibility for action and makes every stakeholder aware of roles, success criteria and associated metrics.
- Understand and act on the need for a proactive approach to security that supports good practices from the outset and stays ready to adapt to evolving threats.
- Ensure external security providers are consistently offering the information, guidance and capabilities you need to make this approach work.

Are your security stakeholders ready to acknowledge and enact their role in a proactive program based on shared responsibility? Are your providers today giving you the data, guidance and focus you need to pursue your security goals to mastery and the autonomy to do so freely? Do you have everything you need to answer the question, "is our approach to security working?"

It's a precarious climb, but you've seen how others have made it and, with the right guidance, you can, too.

Reach out to learn more about the Guide program!

info@actzero.ai
+1.855.917.4981

ActZero

TORONTO
5045 South Service Road, Suite 300
Burlington, Ontario
L7L 5Y7

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

SEATTLE
Hawk Tower
255 South King Street, Suite 800
Seattle, Washington
98104

in ActZero

f ActZeroAI

t ActZero