Beyond Cybersecurity: The Role of Cyber Resiliency in Network Defense

Is your organization’s security strategy prepared to face modern cyber threats? Cyber threats are evolving at an unprecedented pace, demanding organizations to align their security strategies accordingly. Traditional security methods prove ineffective against advanced threats and sophisticated attacks. Despite implementing new security measures, cybercriminals consistently outpace defenses, leveraging advanced technologies like AI/ML, deepfakes, and as-a-service malware and ransomware delivery. Make cyber resiliency your organization’s top priority and actively safeguard your network from potential threats.

According to the National Institute of Standards and Technology (NIST), cyber resilience is: “the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.” The key here is to anticipate and be proactive in protecting data and IT assets, regardless of what happens, so that network operations continue as normal.

Proactive Cyber Defense is Gaining Traction

At Fidelis Security, we recently surveyed over 11,000 of our LinkedIn followers and found that an increasing number of organizations are adopting a proactive approach to cybersecurity. And it’s a good thing!

Proactive cyber defense means that you’re focused on getting ahead of attacks and reclaiming the advantage over adversaries. Those proactive measures are a natural step toward building a more resilient network.

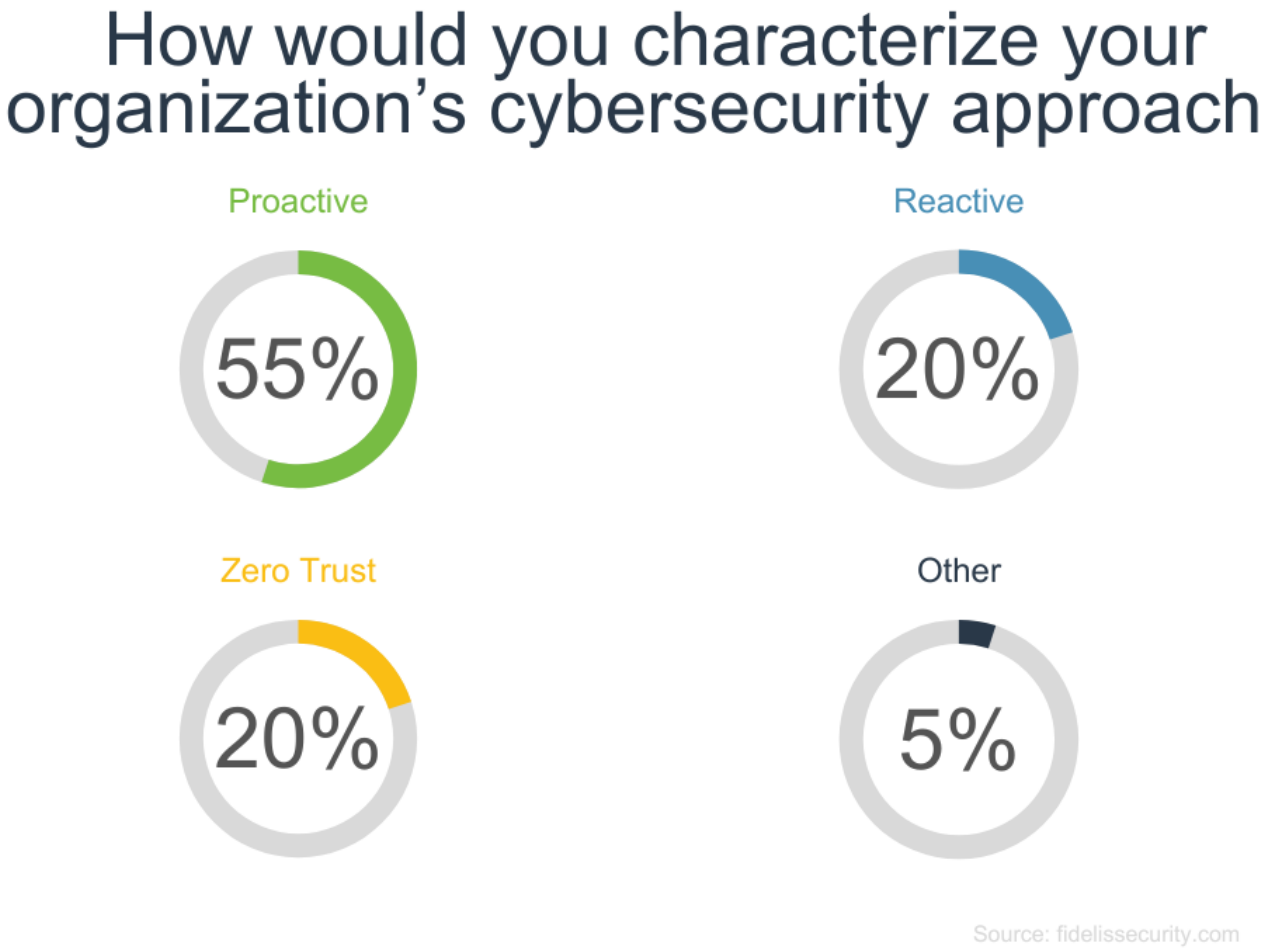

Figure 1: Survey results – How organizations approach cybersecurity in 2023.

Cyber Resiliency is All the Rage

In 2020, the world underwent an overwhelming period of rapid digital transformation. By the end of that year, IDG revealed that 78% of cybersecurity leadership lacked confidence in their organization's security posture. Shortly thereafter, IDC predicted a surge in cyber resiliency spending. Ever since, consumer and government groups have committed to collective actions on cyber resiliency, including:

- Global oil companies at The World Economic Forum, May 2022
- CISA, in their Strategic Plan for 2023-2025
- The United States White House's national security strategy, March 2023

And those are just a few examples that the world is moving away from talking solely about security, turning instead toward building resiliency.

Cybersecurity vs. Cyber Resiliency: What's the Difference?

If you're like us, you've spent your entire career focusing on keeping your organization *safe* from cyber threats. But recent high-profile attacks, demonstrate that our focus on "security" isn't working. One could assume that, had these organizations placed more emphasis on resiliency, they might have been better prepared to withstand and recover from these adversities.

Let's explore the reason behind this.

Security is binary in nature. Something is secure, or it's not. It focuses on keeping bad actors out and responding if-and-when a breach takes place. However, as we all know, attackers find their way inside regardless. Or they originate as inside threats–even if they're just innocent users accidentally clicking an infected link.

Resilience takes on the "what-if" questions and picks up where security leaves off. It adapts to the chaos of our rapidly changing cyber landscape and acknowledges that a successful cyber-attack or accidental breaches a matter of "when", not "if". It solidifies the tools and processes required for rapid post-breach detection and response, surpassing traditional defensive security solutions.

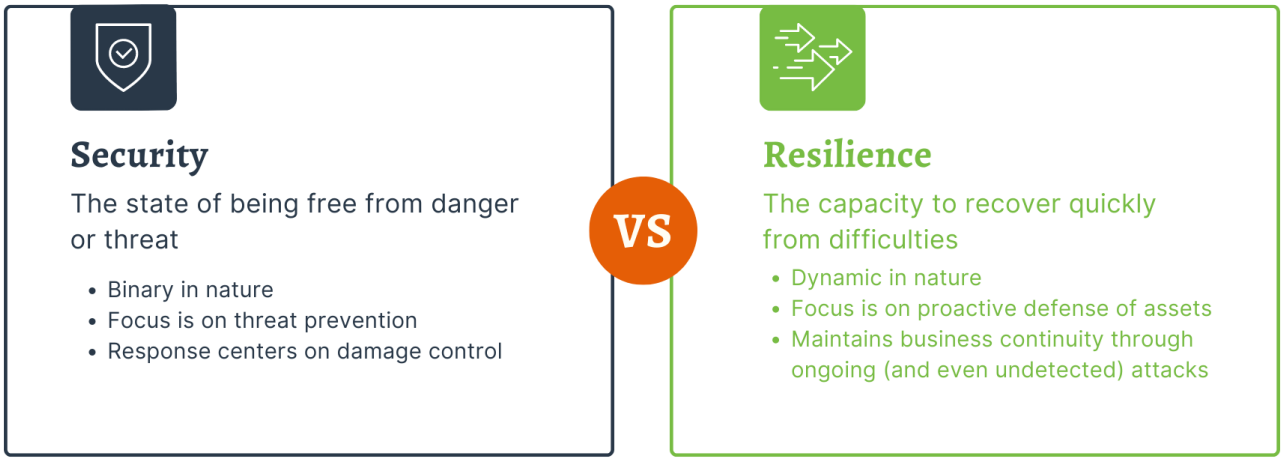

Figure 2: security vs. resilience.

Organizations must continuously assess and update their security measures, identify potential vulnerabilities, and train their employees to recognize and respond to cyber threats. The failure to prioritize to do so can result in significant financial losses, reputational damage, and legal liabilities as demonstrated above.

Hope for the Best; Plan for the Worst

About now, you might be thinking that the days of cybersecurity are over. It's true that, to outmaneuver threat actors and promote business continuity, organizations must prioritize resiliency but not at the cost of security.

Security-focused strategies hope for the best. They aim to keep adversaries out by building strong defenses and keeping track of all the data, assets, users, connections, and potential risks inside. Resiliency plans for the worst. A resiliency strategy assumes that the threat actor is already inside and aims to shorten the attack lifecycle while placing a strong emphasis on continuity.

A highly automated, proactive cyber defense is the sweet spot between security and resiliency. It hopes for the best and plans for the worst at the same time.

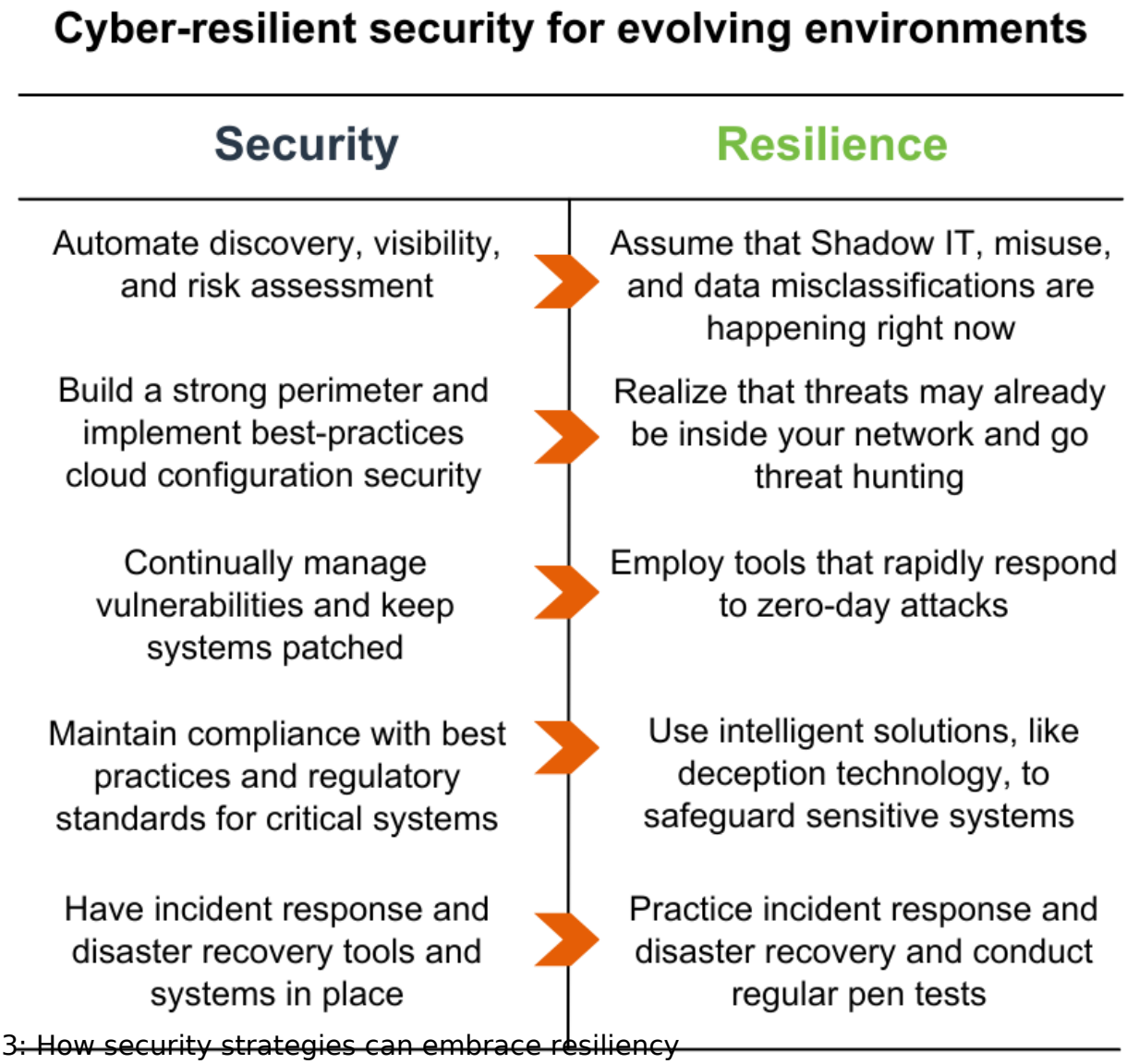

Figure 3: How security strategies can embrace resiliency

Adversaries focus on exploiting the weakest link in the system, penetrating deeper, staying longer, and causing lasting damage once they bypass defenses. Balancing resiliency with security provides two critical benefits:

1. You'll catch the adversary as early in their attack lifecycle as possible—before the damage is done, and
2. You'll provide critical intelligence into attacker movements so that security becomes a process of continuous improvement.

With the right balance in place, organizations can effectively mitigate risk, respond quickly to post-breach attacks, and distract adversaries to protect critical data and systems, all while keeping assets available through and beyond a breach.

Navigating Cyber Resiliency Together

At Fidelis Security, we are proud to say that we are ahead of the cyber resiliency trend. Our technology is designed for proactive cyber defense, providing customers with deep insights into threat actors' movement within their network. Our platforms couple intelligent deception technology with active threat detection to distract post-breach attackers, shorten the attack lifecycle, and keep data and assets safe before, throughout, and beyond an attack. With strong

resiliency-based solutions, we help customers protect, detect, respond, and neutralize threats faster so that they can minimize the impact of any breaches and keep networks running strong.