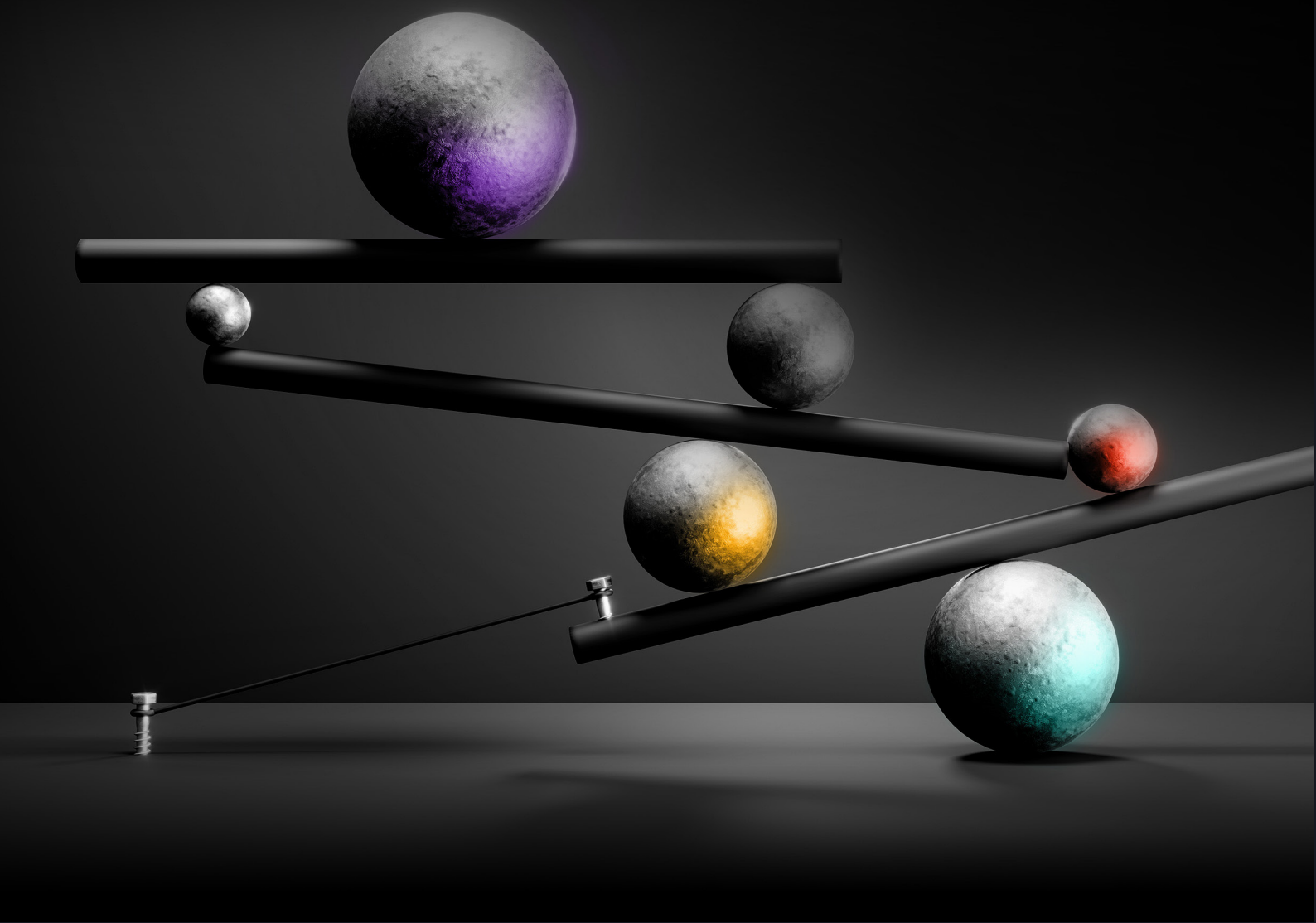
The CISO Circuit by
YL VENTURES

Top CISO Insights Edition 9

The Down Market's Downmarket Effects on CISOs



About YL Ventures

YL Ventures funds and supports Israeli tech entrepreneurs from seed to lead. Based in Silicon Valley and Tel Aviv, the firm currently manages over $800 million and exclusively invests in cybersecurity.

YL Ventures is uniquely focused on supporting the U.S. go-to-market of early-stage Israeli companies and leverages a vast network of industry experts, Chief Information Security Officers (CISOs) and U.S.-based technology companies as advisors, prospective customers and acquirers of its portfolio businesses. The firm's focused strategy allows it to conduct rapid and efficient evaluations for early-stage entrepreneurs and guide founders through their ideation processes pre-investment. The firm is also dedicated to providing unmatched, hands-on value-add support to each of its portfolio companies, both strategically and tactically, across multiple functions post-investment.

The firm's global network and footing in the U.S. have always counted among its most powerful assets. YL Ventures bridges the gap between Israeli innovation and the U.S. market. The firm has formalized and amplified this core competitive advantage through the launch of YL Ventures' Venture Advisory Board.

YL Ventures' Venture Advisory Board is composed of over 100 security professionals from leading multinationals, including Microsoft, Google, Amazon, Intuit, Hearst, Kraft-Heinz, Walmart, Netflix, Nike, Spotify and Zendesk. The firm's relationship with its advisors, as well as its extended network, is symbiotic in nature. The advisors bolster the YL Ventures investment due diligence process and provide the firm's portfolio companies with continuous support across a multitude of functions throughout their life cycles. In return, network members benefit from introductions to pre-vetted Israeli cybersecurity innovations and receive direct exposure to a market second only to the U.S. in cybersecurity innovation.

Portfolio

Spera Identity Security Posture Management **www.spera.security**	opus Cloud Security Orchestration & Remediation **www.opus.security**	eureka Data Security Posture Management **www.eureka.security**	PIIANO Data Protection **www.piiano.com**	valence Collaborative SaaS Security Remediation **www.valencesecurity.com**
grip SaaS Security Control Plane **www.grip.security**	satori Secure and Automated Data Access **www.satoricyber.com**	cycode Application Security Platform **www.cycode.com**	orca security Cloud Security Platform **www.orca.security**	HUNTERS SOC Platform **www.hunters.ai**
VULCAN. Cyber Risk Management **www.vulcan.io**	Karamba Security Embedded Security for Connected Systems **www.karambasecurity.com**	RIDEVISION Predictive Vision for Motorcycles **www.ride.vision**		

Acquisitions

enso Acquired by snyk	MEDIGATE Acquired by CLAROTY	build.security Acquired by elastic	AXONIUS Exited to late-stage investors	Twistlock Acquired by paloalto	HEXADITE Acquired by Microsoft
FIRELAYER Acquired by proofpoint	Seculert Acquired by radware	BlazeMeter Acquired by ca technologies	Clicktale Exited to Amadeus Capital Partners	AcceloWeb Acquired by Limelight Networks	UPSTREAM COMMERCE Acquired by Walmart

About the CISO Circuit

YL Ventures frequently confers with an extended network of prominent cybersecurity professionals, including our Venture Advisory Board and industry executives, to assess our portfolio prospects, inform market predictions and cultivate portfolio company business development. As such, we have established direct lines of communication with the global market's preeminent CISOs and cybersecurity experts for ongoing insights into their thoughts, priorities and opinions about the state of their organizational cybersecurity.

We recognize the value this information presents to entrepreneurs, especially those wishing to enter the U.S. cybersecurity market, and to the cybersecurity community as a whole. For this reason, YL Ventures launched "The CISO Circuit", an initiative under which we publish reports containing gathered intelligence for general use.

We hope the observations compiled in this report will prove useful to aspiring cybersecurity entrepreneurs and the rest of the cybersecurity community.

Table of Contents

Introduction

In this report of the CISO Circuit, our team set out to understand the challenges that current down market conditions present to enterprise security leaders. Over the course of 40 interviews with distinguished cybersecurity executives hailing from a wide spectrum of verticals and company sizes, we collected responses to a series of questions (see Appendix) about how their budgets have been impacted, what this means for their interactions with vendors and how security strategies have evolved in response.

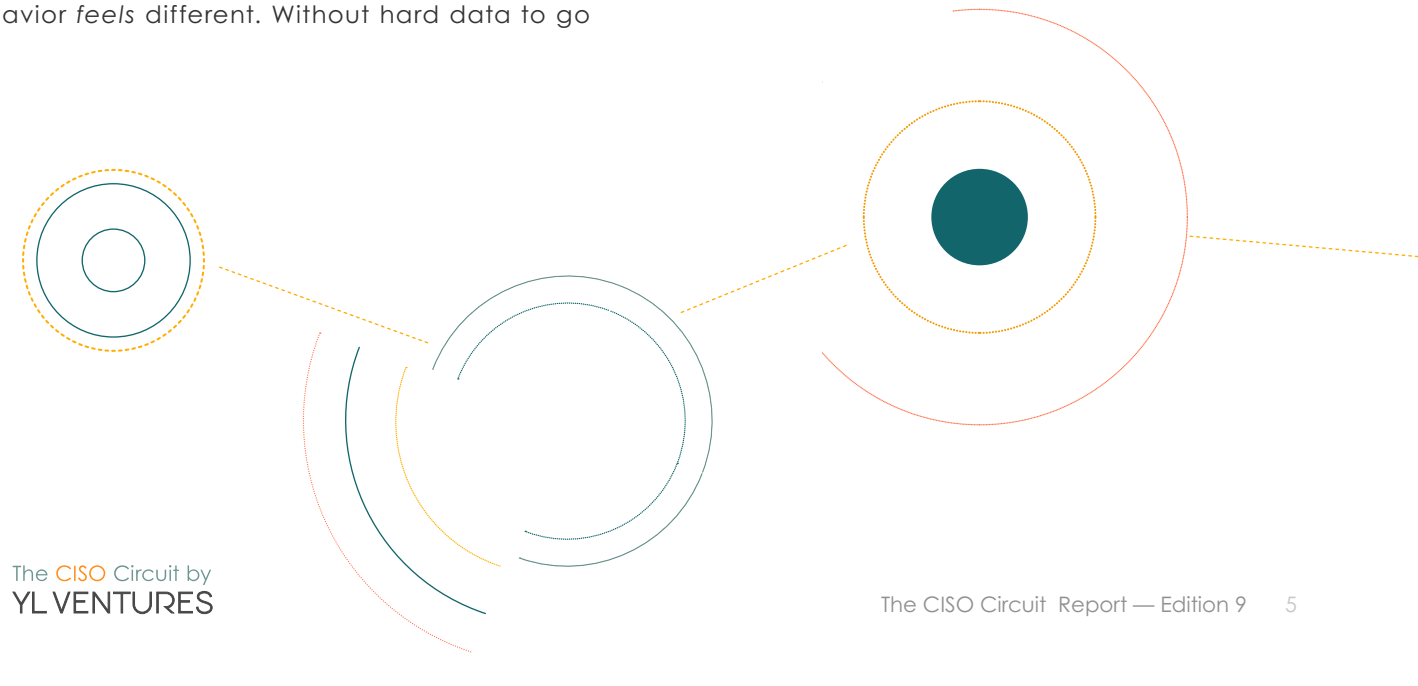
Three years ago, when a global pandemic confounded–and confined–the world, the global economy went into flux. As geopolitics added its own pressure onto global trade, economists, venture capitalists and other market experts awaited a surefire recession with bated breath. Rather than a quick, dramatic dip, the economy fizzled into today's "market downturn".

Cybersecurity's relatively safer status as a market necessity has not isolated the industry from the market downturn's ramifications–though what these ramifications are has been up for debate. What we do know is that 2023's overall enterprise budgets are shrouded in cross-board austerity, bringing up legitimate questions around whether or not–and how–allocations for cybersecurity may have been impacted. From reports on vendor experiences and in discussions with our extensive network of CISO advisors, we also know that CISO buying behavior *feels* different. Without hard data to go by, cybersecurity vendors and startup founders find themselves readjusting their footing in the dark. Our endeavor in this CISO Circuit is to definitively quantify new behavior and decision-making with data pulled directly from CISOs themselves.

Our research confirms that while CISO buying behavior has indeed changed, the majority of their budgets have not decreased and at least half can accommodate new solutions. We have also quantified how, due to new, company-wide cultures of austerity, demonstrable ROI has become top priority as all departments focus on cost-effectiveness. In turn, these newly prioritized goals have significantly narrowed the pool of vendors that make sense for cybersecurity decision makers to meet. The door remains open mostly to those that closely align with business objectives that often come down to cost effectiveness.

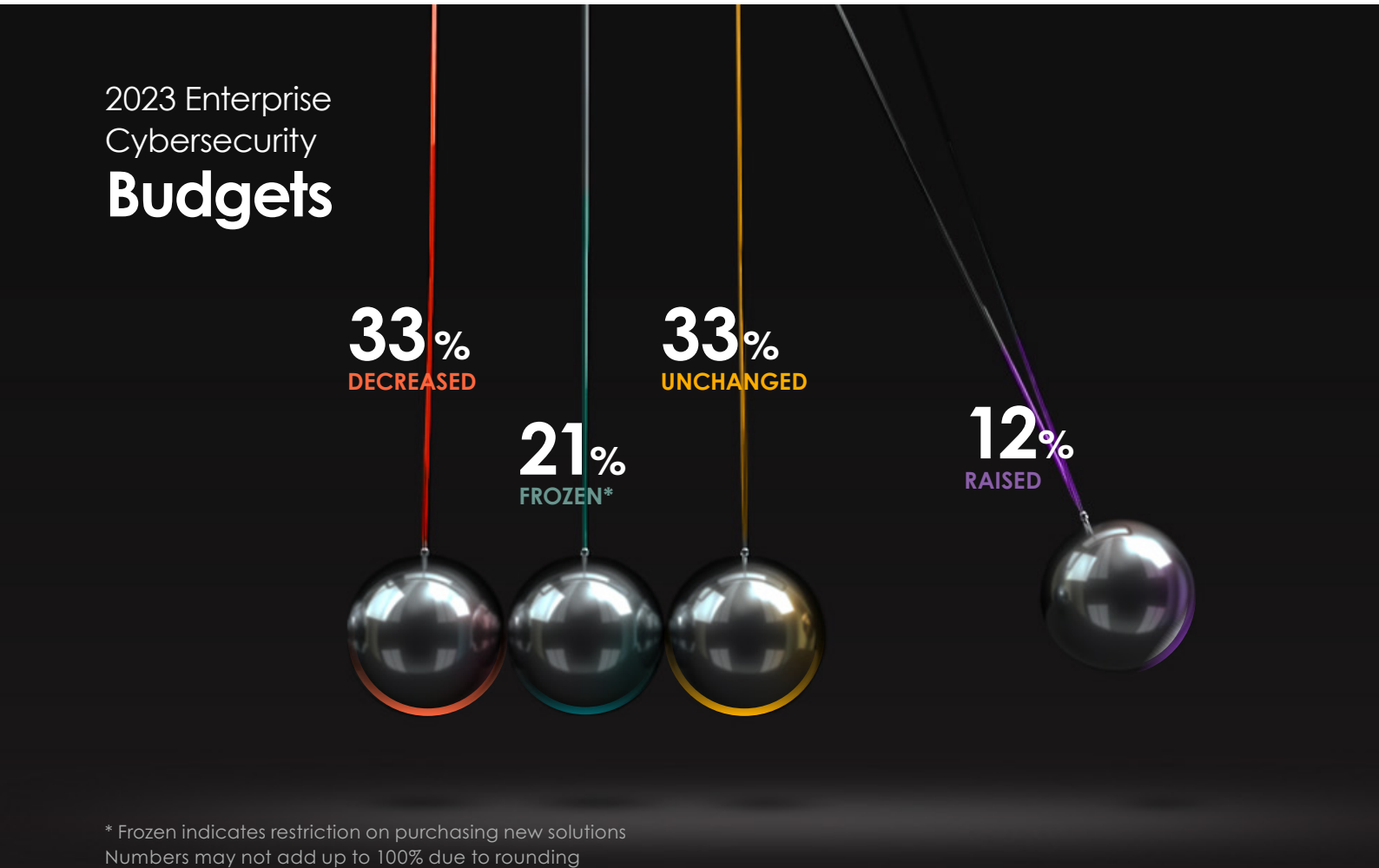
This edition's respondents also helped us learn which sectors are topping Fortune 1000 cybersecurity budgets in today's macroeconomic conditions. Our analysis concludes that CISO roadmaps are ramping up consolidation with a focus on securing the basics, as today's CISOs concentrate their spending on Cloud Security, Data Security, Application Security (AppSec) and Governance, Risk and Compliance (GRC).

Finally, thanks to the candidness of our respondents, we have collected insights on how vendors and aspiring cybersecurity founders can best cater to these newly emerged, budget-driven needs when communicating product value propositions. We hope this information will be of use to the cybersecurity community.



Down Market Impact on CISO Budgets

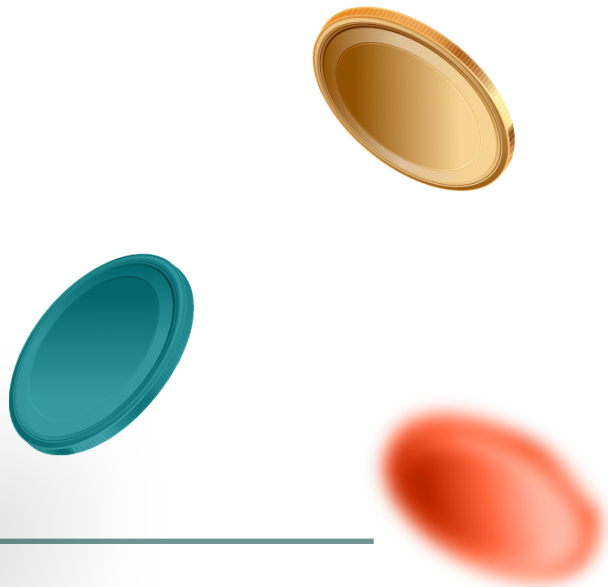
The cybersecurity sector has proven a compelling outlier and hallmark of resiliency in the recent macroeconomic environment. As we have noted in the past, much of this has to do with the critical nature of cyber threats on business continuity in today's digital age. Today's enterprises simply cannot compete without an arsenal of digital capabilities to drive innovation and productivity, which introduce myriad vulnerabilities and cyber attack vectors for bad actors to exploit. As enterprises grow evermore reliant on technology, cybersecurity has become an absolute necessity to counterbalance associated risks.



* Frozen indicates restriction on purchasing new solutions
Numbers may not add up to 100% due to rounding

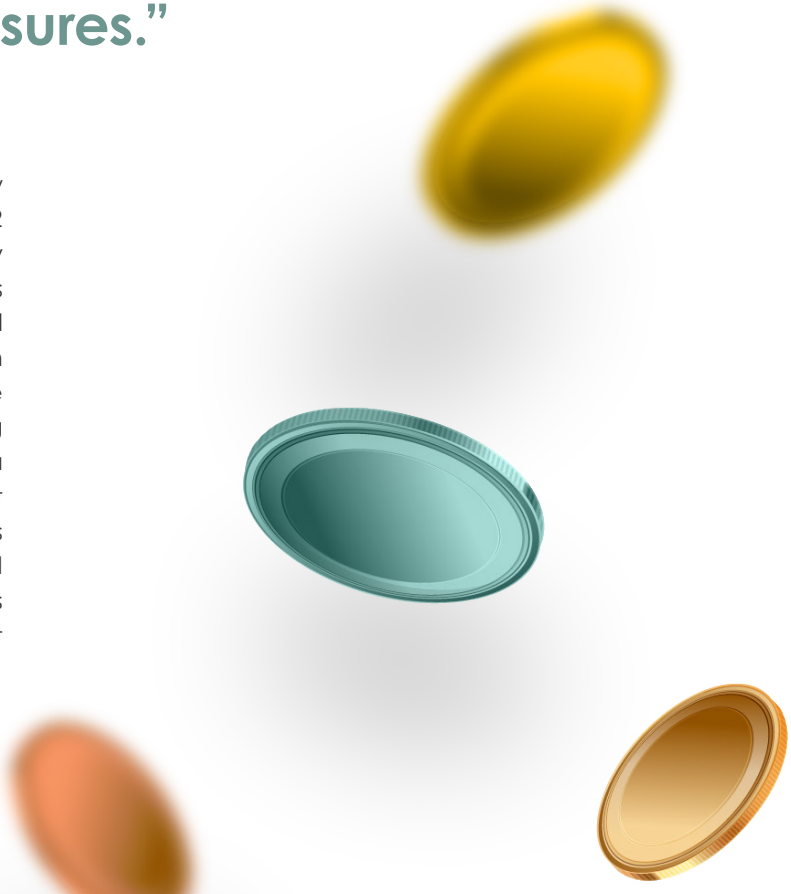
Having grown into a C-Suite priority, the fallout of cyber attacks are well known and represent massive risks to business continuity. This has secured reliable budgets for CISOs and other security leaders, which in turn has kept the B2B cybersecurity sector mostly safe from market fluctuations.

However, it is clear that cybersecurity does not enjoy full immunity from the impact of market conditions on buyer behavior. The down market has decreased the overall buying power of enterprises across many industry verticals, triggering more heavy losses in turn. Around the world, companies were pigeonholed into painful downsizing and forced to adopt new, austere budgetary measures. It is only natural that cybersecurity sales have been impacted as a result.



> **Around the world, companies were pigeonholed into painful downsizing and forced to adopt new, austere budgetary measures."**

According to our survey, a third (%33.3) of cybersecurity leaders have experienced budget cuts while %21.2 now oversee frozen budgets, meaning that new spending is not possible. This is hardly insignificant, as these numbers indicate that vendors have and will continue to contend with a significant decrease in CISO purchasing power. As we will discuss later in the report, however, even CISOs with decreased spending capacity are not closing their doors entirely; getting a foot in is simply a matter of vendors needing to adapt and update their strategy. Another third of respondents (%33.3) report unchanged budgets and %12.2 indeed saw their budgets raised. The overall picture does present a more challenging environment for sales–but not a hopeless one.

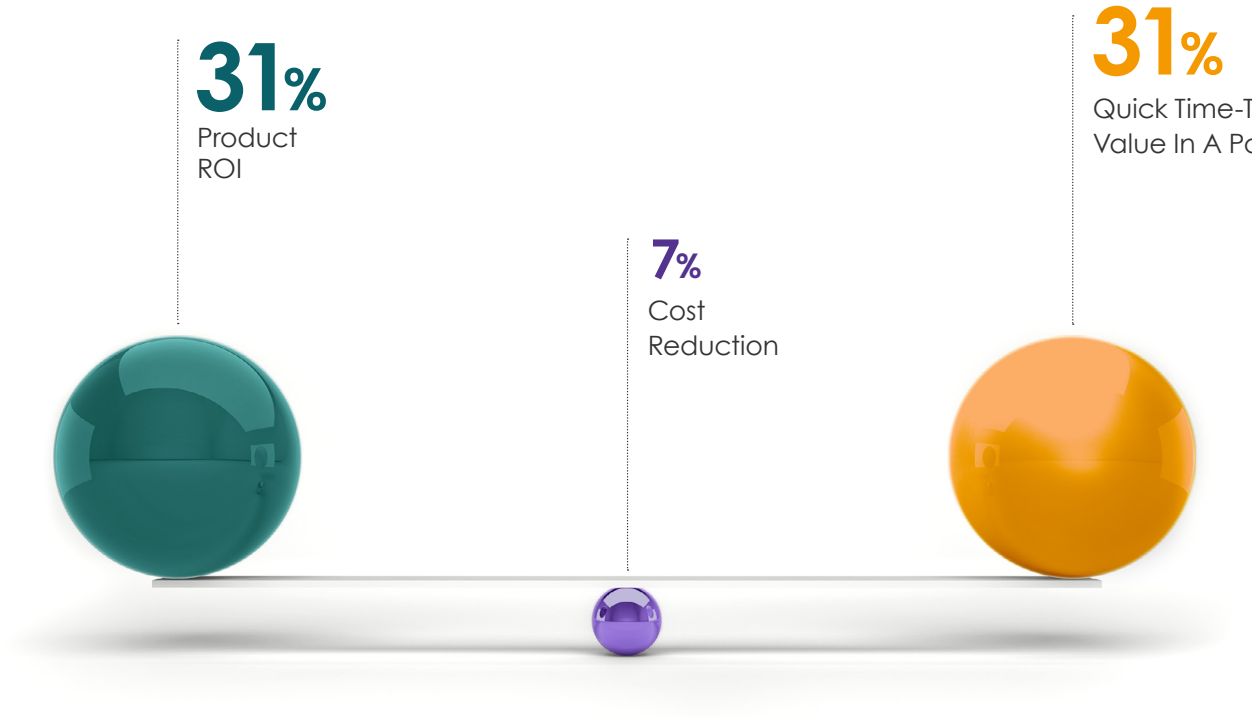


CISO Purchasing Response

Sound purchases focus on demonstrable value and such has always been the case for cybersecurity leaders. Many CISOs remember having to fight in the early days of the industry for every dollar spent. This fight became less ferocious as cybersecurity climbed its way up the list of enterprise priorities and became widely acknowledged as a need. The industry experienced its heyday, and innovation became another major driving force of sales.

> **The market downturn has since brought back the burden of proving a solution's value in fuller force, whether through ROI, cost reduction or how much time it takes to generate meaningful risk reduction."**

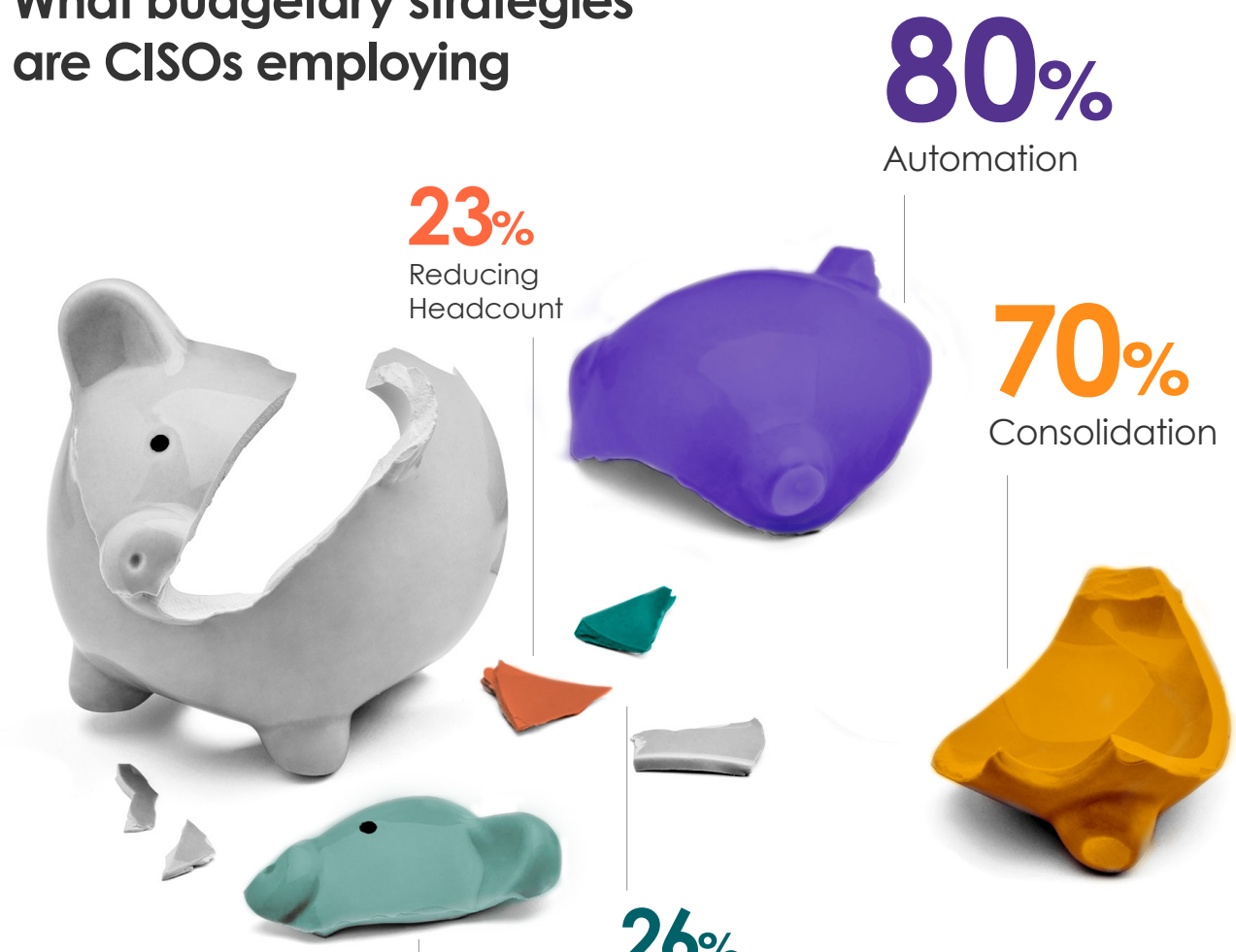
Top Three Vendor Criteria for CISOs



The market downturn has since brought back the burden of proving a solution's value in fuller force, whether through ROI, cost reduction or how much time it takes to generate meaningful risk reduction. When given the option to share what criteria they need to know most about new solutions–of which they could share more than one–our respondents consistently referred to these three.

We have long noted, since the first edition of the CISO Circuit, that cybersecurity leaders are looking to simplify their security stacks to streamline operations. Budgetary pressures are forcing them to double down on this strategy. Accordingly, today's CISOs are placing greater emphasis on cutting costs where they can. %80 of respondents are looking to consolidate their cybersecurity stacks and %43.3 have indeed ended at least one customer contract. %70 are hoping to save on labor with automation and %23.3 have had to lay off personnel. Until the market storm settles, %26.7 of respondents are relying on free trials as stopgap solutions.

What budgetary strategies are CISOs employing

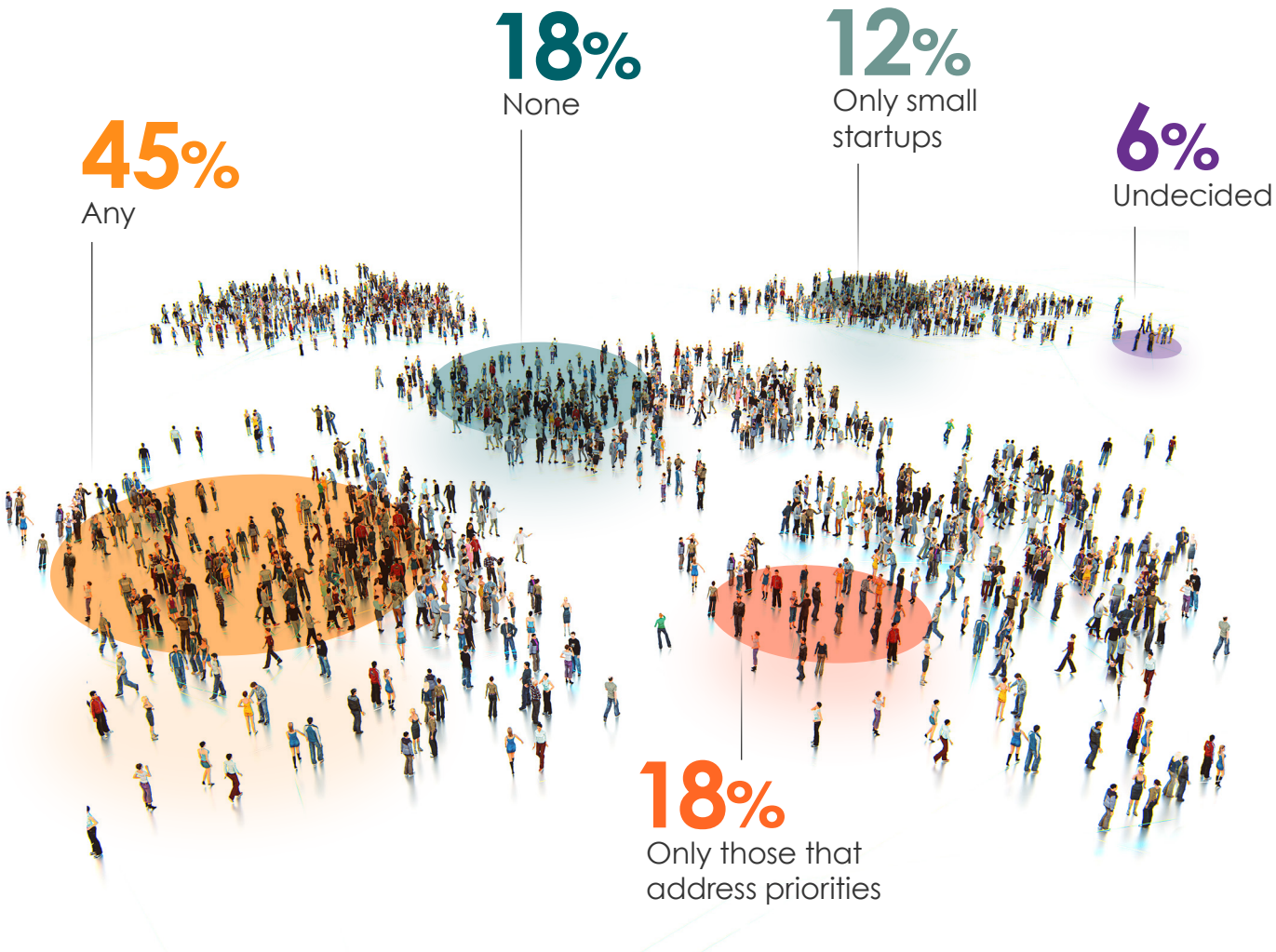


***multiple responses permitted
Numbers may not add up to 100% due to rounding

Proposed Vendor Strategies

Vendors should take heed that the majority of CISOs are still interested in hearing from them, simply in different capacities than before. Paired with a genuine curiosity and a desire to learn about innovation, CISOs see a great deal of value in meeting with vendors even if it is just to keep up with the industry. Cybersecurity vendors are capable of helping CISOs understand the landscape's new risks and distill highly technical information. However, the stresses brought on by the market are orienting these conversations away from direct sales opportunities. Indeed, 63% of respondents reported that they require more time to evaluate vendors and sales processes than before.

Which new vendors are CISOs meeting?



Numbers may not add up to 100% due to rounding

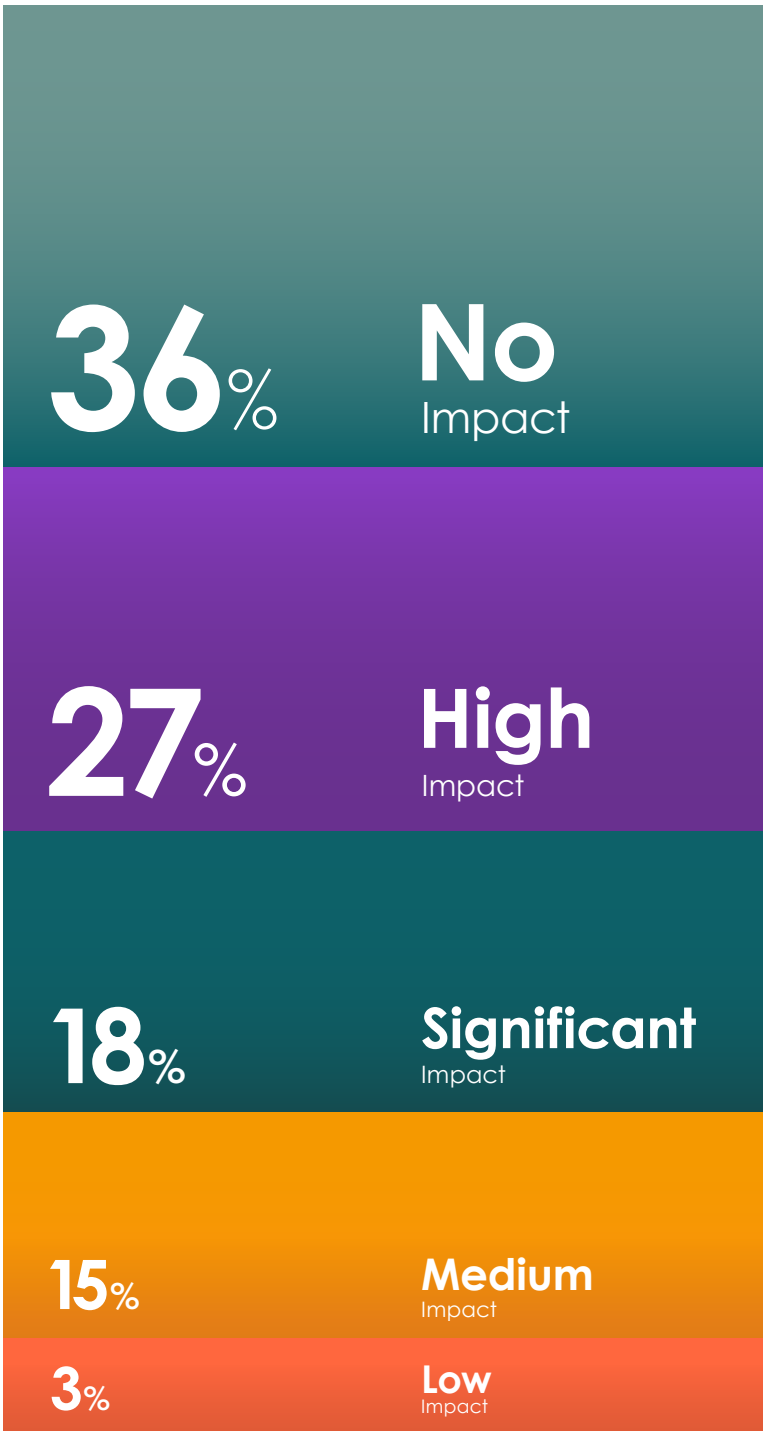
Smaller and earlier stage startups have an advantage in this today's macroenvironment. They are viewed more favorably by CISOs who believe these types of companies can offer more advantageous licensing costs and design partnerships relative to their larger counterparts. By engaging only with smaller companies, respondents are hoping to understand and find more effective solutions than what they currently have. They are looking to replace existing solutions at a smaller cost or with more impact per dollar–without the immediate pressure to buy.

> **It may be wise to adopt "Land and Expand" sales tactics and younger startup strategies, such as free design partnerships, trials and case study initiatives."**

Aware that today's CISOs are prioritizing cost reduction, and that 18.2% are only meeting with vendors who meet their priorities, larger vendors may wish to consider how they can shape their products and value propositions to better position themselves in these economic conditions. It may be wise to adopt "Land and Expand" sales tactics and younger startup strategies, such as free design partnerships, trials and case study initiatives. Not only do such opportunities better appeal to the austere sensibilities of today's CISOs, when taken, they also provide important opportunities to build genuine trust and gain direct insight and understanding into their bespoke environments. Both are critical when building more meaningfully impactful products.

Though the need to optimize on cost and reduce headcount while reducing risk are clear, the means by which to accomplish these goals remain ambiguous beyond buzzwords like "automation". It is incumbent on vendors to demonstrate, through tangible means, how technology like automation can actually be of service. It is just as important that the factor of time-to-value is taken into account. The sheer volume of daily approaches CISOs contend with has made demonstrable time-to-value more critical than ever.

Have market conditions impacted the speed of solution adoption?



Numbers may not add up to 100% due to rounding

Current Top Cybersecurity Domains

Above all else, cybersecurity leaders are preoccupied with securing their existing environments as efficiently as possible.

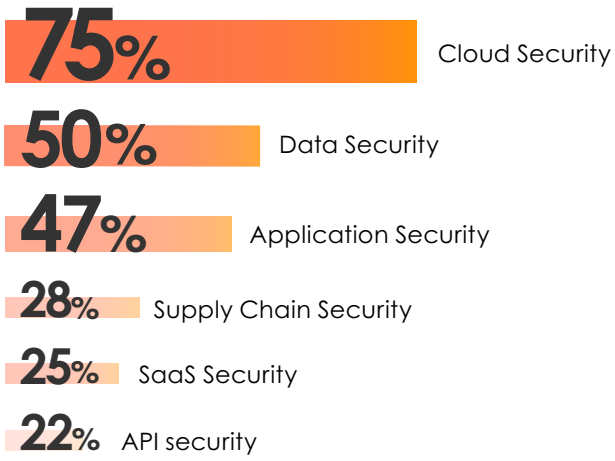
Though focused on the fundamentals for years, current market circumstances are forcing these leaders to even further concentrate their efforts on securing the basics, meaning their cloud environments, data, applications and supply chains. The basics have also expanded to include SaaS and APIs. Though current cybersecurity stacks remain bloated and full of redundancies, CISOs still lack the full coverage and assurances these areas require.

> **Though focused on the fundamentals for years, current market circumstances are forcing these leaders to even further concentrate their efforts on securing the basics."**

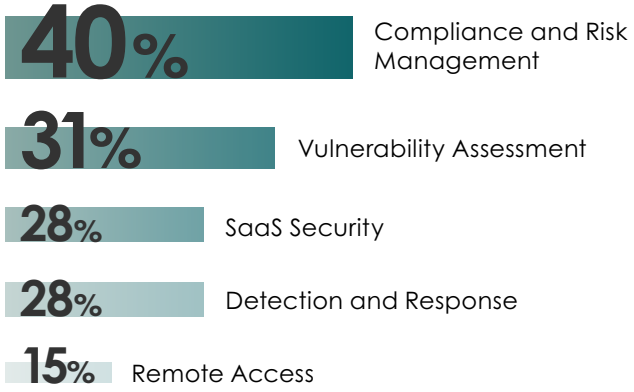
The disciplines by which our respondents are looking to resolve these gaps are telling. Many are looking towards GRC (Governance, Risk and Compliance) as the best approach to securing the basics. Vulnerability assessments, detection and response and securing remote access also make up the bulk of their current efforts. This is not to say, however, that our respondents are not keeping their eyes on the horizon. In qualitative responses, many have expressed a rapidly rising interest in improved solutions for Identity and Access Management (IAM), Orchestration, Remediation and User Behavior Analysis (UBA).

What are CISOs prioritizing most

ENVIRONMENTS



DISCIPLINES



***multiple responses permitted

Numbers may not add up to 100% due to rounding

This begs a very important question–how did Generative AI (GenAI) fail to make the list?

We have some theories. First, many CISOs are currently approaching GenAI risk with existing network and application tools for visibility and blocking where needed. We moreover expect highly regulated industries, such as finance and health, to keep GenAI services blocked for the foreseeable future and spend little on GenAI security solutions. Let us also consider that many CISOs are still in the process of learning about GenAI technology and large language models (LLM)–and will likely need more time to properly assess GenAI solutions that are permeating the market.

More nuanced GenAI security policies are only one half of the AI question still nascent in CISO agendas. Depending on the nature of their business, they might also find themselves charged with securing proprietary LLMs and integrating LLM functionality into business applications. Here too they must overcome a learning curve first as CISOs actively work towards understanding their needs.

We believe that entrepreneurs interested in this space must distinguish between what is generally understood about AI risk and where CISOs could genuinely use help with technological knowledge gaps. Vendors who can provide this valuable knowhow instead of providing well-worn warnings can, at the very least, get their foot in the door while the market matures.

Domains on the rise

- IAM
- Orchestration
- Remediation
- User Behavior Analysis
- AI

I wanted to investigate the relationships between the areas of cybersecurity priorities shared by my peers. I took a look at which answers came up in common between environments and disciplines to understand where they might converge.

Using the data from this survey, I detected three correlations among Cloud and Vulnerability Assessment, Cloud and Remote Access and Application and Remote Access. In other words, all respondents who selected Remote Access as a priority also selected both Cloud and Application as priority environments. In my view, Cloud and Application are environments that are mature enough for CISOs to look into additional ways to secure them beyond single-purpose solutions, while Data, Supply-Chain, SaaS and API are nascent environments still in need of effective solutions before they can be further optimized.

No other strong correlations appear aside from a small one between Application and Vulnerability Assessment as well as another small one between Detect and Response with both Cloud and Data. I was also interested in how Compliance/ Risk Assessments might correlate with specific kinds of environments, however it would appear to present as a priority for companies independent of the environments that they are focused on.

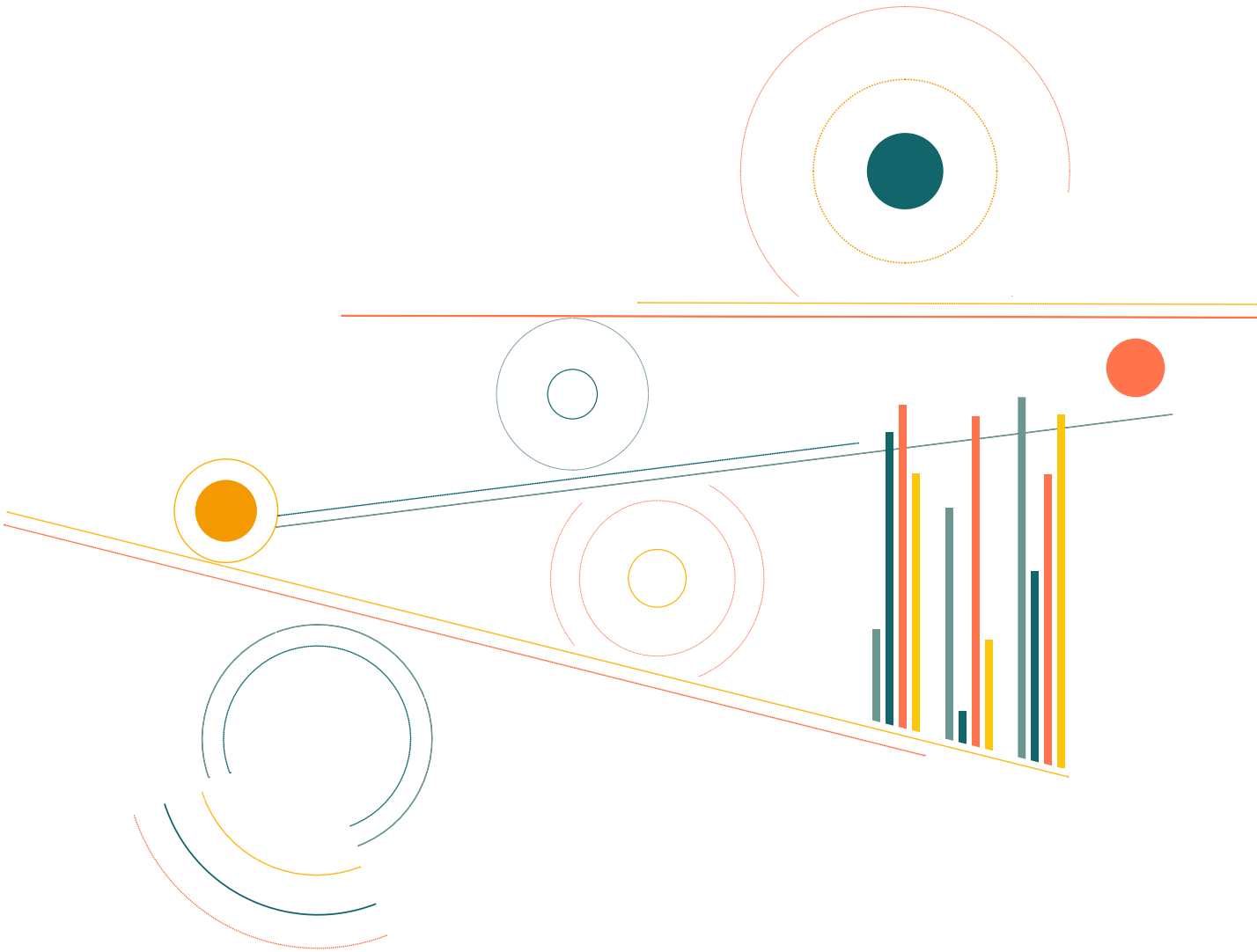
Andy Ellis, Operating Partner

Conclusions

Cybersecurity vendors would do well to remember that the market operates in cycles, and while certain limitations have been placed on CISO spending for now, they will not persist into perpetuity. Getting a foot in the door remains as important as ever, though it must be done with sensitivity to the current challenges that customers face. As one of our respondents explained, "it is very insensitive to approach us with costly contracts on the heels of layoffs".

Today's down market compels vendors to take a step back and truly listen. Though compelled to do so before, current circumstances require that it be done with more intention and care–at least for cybersecurity vendors who wish to create or maintain good relations with their customer base. However, listening does not have to be passive or limited to a single pitch session. Through strategic partnerships and trials, cybersecurity vendors can bypass budgetary restrictions and gain real insight into customer needs while also gaining critical opportunities to demonstrate real value.

Though it is clear that efficiency, cost saving and time-to-value preoccupy CISO decision making, how that translates may look different to each organization. Nonetheless, it is clear that solutions capable of demonstrating the ability to automate unskilled tasks, make better use of existing tools or eliminate the need for costlier tools altogether stand greater chances of success than ever before.



Outreach and Contact Information

This report was compiled with Israeli cybersecurity entrepreneurs in mind. If you are an Israeli-based startup looking for guidance for seed-stage funding, we invite you to contact our Senior Partner, **Ofer Schreiber**, at **ofer@ylventures.com**. We also invite you to direct any questions relating to this report to this address.

We would like to sincerely thank all of the CISOs who participated in this report. If you are an industry expert and would like to be interviewed for the next edition of the CISO Circuit, please contact Michael Cortez, YL Ventures Partner, at **michael@ylventures.com**.

Appendix

Survey Questions

1. **What is your industry?**

2. **What is your company size?**

3. **Has your budget been impacted?**
   a. By what factor has it changed

4. **What budgetary strategies are you employing in this economic climate?**

6. **Are you still open to meeting vendors?**
   a. If you responded in the affirmative, can you please elaborate on your goal for these meetings?

7. **To what extent has the economic situation impacted your criteria for evaluating vendors and products?**

8. **How has the current economic situation impacted the speed of your decision-making process for purchasing new cybersecurity products?**

9. **Has the current economic situation impacted your position on design partnerships with early-stage startups?**

10. **Should vendors change how they approach security decision-makers in this climate?**

11. **What kind of new solutions are you still considering purchasing?**

12. **In light of the current economic situation, which area of cybersecurity is your organization focusing its budgetary spend and roadmap for 2023?**