



7 Strategies for Cybersecurity Marketing and Sales Teams

to break through the
noise and reach security
decision makers

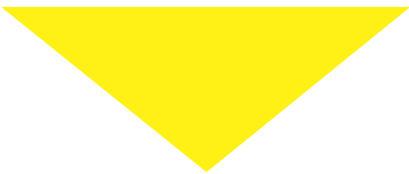




Table of Contents

Section 1

Executive Summary **3**

The Pitfalls of Current Outreach Methods and Root Causes **3**

Section 2 - Cybersecurity marketing solutions strategies

Strategy 1: **7**
Experiential Marketing

Strategy 2: **8**
Evaluating Cybersecurity Conferences

Strategy 3: **10**
Looking Beyond the CISO

Strategy 4: **11**
Offering Meaningful Content

Strategy 5: **12**
Position Your Organization as a Genuine Partner

Strategy 6: **12**
Aligning with Known and Trusted Organizations

Strategy 7: **13**
Increasing Digital and On Demand Options

Conclusion **15**

Executive Summary

One of the most pressing challenges for cybersecurity solution marketers and sales professionals in 2020 is that reaching cybersecurity decision makers and influencers is increasingly difficult.

This caught some by surprise.

After all, as the sophistication and volume of cyber threats increases, so should the appetite to evaluate security solutions that will help combat the threats.

From our research and interaction with security leaders across North America, we can report that there remains a robust appetite for dialogue around both evolving tools and new solutions in the space.

However, we've also gained fresh insight into why many traditional approaches to connecting with security leaders are no longer working.

This paper examines the challenges currently faced by cybersecurity marketers and sales teams, and for greater context, explores the root cause of these problems.

This overview will inform a discussion around 7 effective strategies that are working for cybersecurity marketers and sales teams. Strategies that can be implemented this quarter or the next.

Current Challenges and Root Causes

The 2020 marketing problem for cybersecurity solutions and service providers.

The modern marketing landscape makes traditional methods a source of constant inefficiency for sales teams. Team members reach out to prospective clients day after day, week after week. And most of the time, it is an exercise in frustration.

Efficiently connecting with cybersecurity decision makers and influencers is essential. How can this happen when many CISOs do not return unexpected emails or phone calls?



Current marketing methods are inefficient, and some are causing blowback

Carefully crafted emails go unanswered, or worse. Some enterprise organizations auto send them to a “vendor” mailbox, never to be seen again.

Call effectiveness is declining. Sales teams either proceed or follow up these emails with a call. However, CISOs do not pick up the phone when they know it is about a sales pitch or setting up a demo. And attempts to leave a voicemail are often in vain: voicemail boxes are often full and some are shut off altogether.

Social media prospecting is causing blowback. LinkedIn was a fruitful workaround a few years ago, but that avenue is drying up fast. It has been overused to the point of creating resentment among the very cybersecurity decision makers organizations need as key advocates in the sales process.

Anahi Santiago, Chief Information Security Officer at Christiana Care Health System, wrote an open letter to vendors using LinkedIn in 2020:

“If you are a vendor that I do not do business with, I am not actively assessing, nor have I met you, I will not accept your connection request. And if by mistake I do accept and you immediately ask me for 10-15 minutes of my time to sell me something, I will block you.”

The post garnered hundreds of likes and comments from fellow CISOs agreeing with her sentiment.

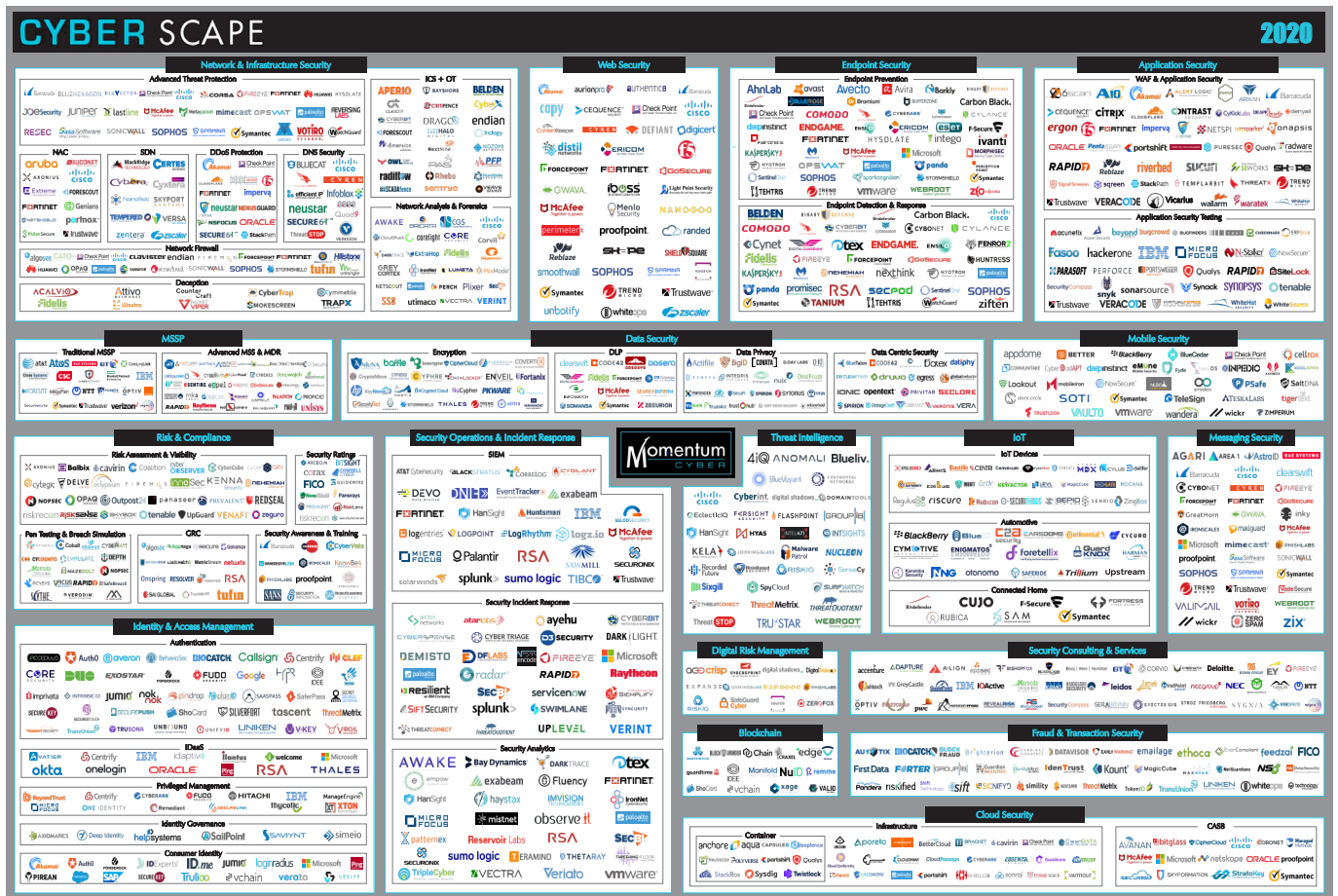
These challenges are a warning sign to marketers who notice them. To stay relevant, they must evolve the way they operate.

Cyber threats and cyber solutions are evolving, *so the marketing of cyber solutions and services must evolve as well.*

The root causes of this 2020 cybersecurity marketing challenge.

Most cybersecurity leaders we talk to are simply overwhelmed. And everyone feels that way at times, the problem is acute among cybersecurity leaders and their teams.

Noise in the market: One of the factors is that contact information for CISOs and other security leaders has lost its value. Any startup (or established company, for that matter) can purchase a list of roles or titles at virtually any organization.



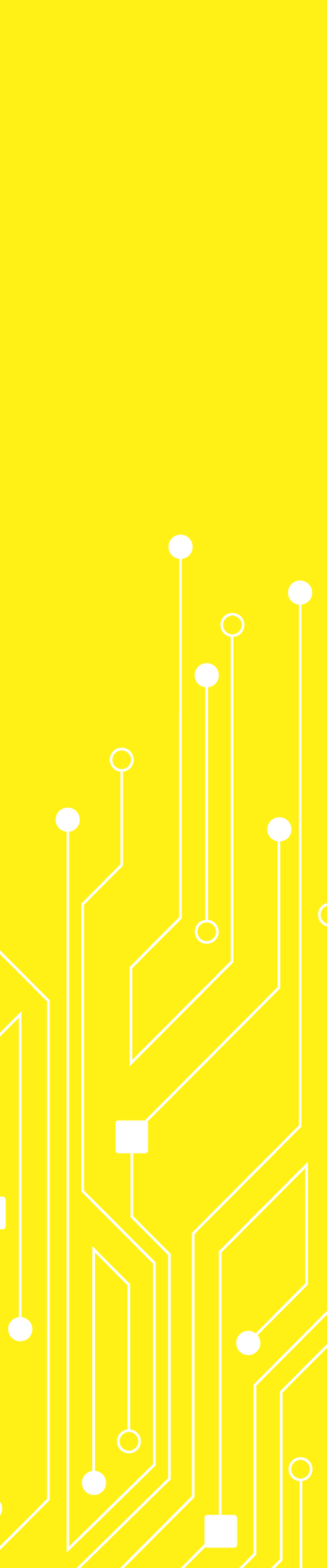
This makes it possible for any company on Momentum Cyber’s map of the vendor landscape (below) to email and call the cybersecurity leaders at an organization.

Looking at this map is overwhelming enough. Now imagine being a security leader slammed with emails and calls by dozens of vendors all asking for “just a few minutes of your time.”

If you were the one receiving all these random emails, would you respond? Could you respond? The noise from competitors in the vendor space is deafening.

Here are 3 more complicating factors security leaders face:

- **Talent Gap:** IT security teams are understaffed. It is well documented that there are several hundred thousand unfilled cybersecurity roles in North America because of a cyber talent gap. Security Magazine recently called this “An Industry Crisis.”
- **Regulation:** Regulatory and compliance demands are increasing because of a rapidly evolving privacy and security legal landscape.



“The biggest challenge we hear is, ‘I have a moving target and multiple different targets at the same time.’ And that’s a challenge for any company to hit,” says Cyberlaw Attorney Jordan Fischer, Managing Partner of XPAN Law Group.

- *Internal Pressure:* Cybersecurity leaders face growing internal pressure. Executive leadership and boards of directors are increasingly treating cyber risk as business risk, something security leaders have been asking for. But this leaves leaders and understaffed teams with even less time for anything considered less than mission critical.

Bruno Haring, Cybersecurity Advisor at Accenture, told us what this is like for security leaders. “The good news is the board gets it and wants to do something about cybersecurity. The bad news is the board gets it and wants to do something about cybersecurity.”

In the long run, however, this growing focus on security means tremendous upsides for securing corporate data and for cybersecurity vendors who approach security leaders *in the way they like to be approached*.

The Solution to the Problem

SecureWorld surveys the leaders of its regional cybersecurity conferences each year and the vast majority report steadily or significantly growing cybersecurity budgets.

Record spending in the market appears to be ahead. Cyber Ventures is forecasting more than \$1 billion dollars in cybersecurity spending during a 5-year time frame ending in 2023.

To take advantage of this opportunity, cybersecurity marketers and sales professionals must meet security leaders in the mind-space and the physical and virtual environments where leaders are open to considering solutions.

Here are some strategies to break through the noise and connect with security leaders when and where they would most like to connect with you.

7 Strategies To Connect With Cybersecurity Leaders

SecureWorld surveys the leaders of its regional cybersecurity conferences each year and the vast majority report steadily or significantly growing cybersecurity budgets.

Record spending in the market appears to be ahead. Cyber Ventures is forecasting more than \$1 billion dollars in cybersecurity spending during a 5-year time frame ending in 2023.

To take advantage of this opportunity, cybersecurity marketers and sales professionals must meet security leaders in the mind-space and the physical and virtual environments where leaders are open to considering solutions.

Here are some strategies to break through the noise and connect with security leaders when and where they would most like to connect with you.

Strategy 1. Experiential Marketing

Conferences are the king of experiential marketing. This is where overwhelmed security leaders come up for air. They are in learning mode and actually looking for solutions that might be a good fit.

Gary Patterson, Director of Security Architecture at Home Partners of America sums up how this is an 'experience' for security leaders:

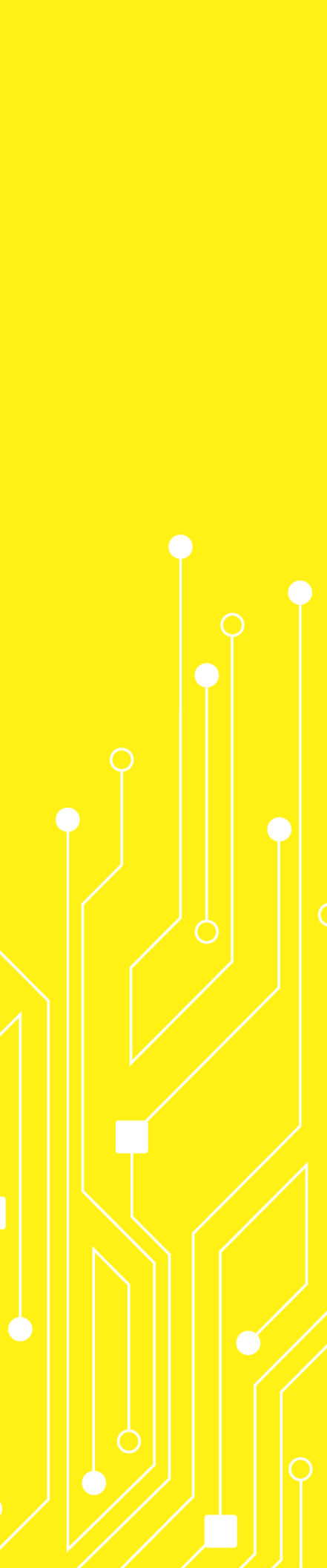
"When a vendor calls you don't usually have time for it. Having some time out where you can walk by and kind of see, smell, touch, feel a solution, and talk to somebody in real life in a nonaggressive manner, it's phenomenal."

And James Beeson, longtime VP & CISO at Cigna Insurance, says the conference experience helps him evaluate who his team should consider for a partnership.

"There are a lot people spending a lot of time, energy and money to try and develop new products and services that help us in the space. This is an opportunity, without having to have an hour meeting with each one of them, to use a concentrated space get to know some of the new technologies that are out there."

7 Strategies To Connect With Cybersecurity Leaders





This is not only valuable for CISOs, but also for solutions providers. Sales teams can quickly evaluate a possible fit, start developing advocates, and uncover where an organization needs help.

This short circuits the time and expense of hoping a sales presentation will align with an organization's needs only to find out it was sending the wrong message.

There are certainly other avenues of experiential marketing. Taking leaders to race cars on a test track or to sporting events are some can draw CISOs. These types of outings lead to an important question worth considering: are they coming to this outing because they are interested in exploring your solution? Or are they coming to this because it sounds fun and your budget is covering the cost?

When a security leader connects with your team at a conference and asks questions about your solution that's when you know this is a sincere effort to uncover the problems your solution may solve for that leader's organization.

Strategy 2. Evaluating Cybersecurity Conferences

A key best practice in evaluating conference sponsorship is determining conference series credibility. Ask about the longevity and track record of the organization behind the conferences.

Also, specifically ask about the true number of cybersecurity practitioner attendees. Some conference creators will give "attendee numbers" which look good but they fail to mention most of those "attendees" are actually other vendors.

Another key consideration is discovering a conference series that aligns with your budget. Some conferences charge \$50,000 (or more) for the privilege of speaking. Can your organization spend that amount on a single speaking engagement? What will the consequences be if only a few attendees are in the room?

What if you chose a mid-priced conference and did two speaking engagements for the same price? Mathematically this doubles your opportunity of success and avoids a single point of failure situation.

On the other hand, some small events may allow you to speak for only a few hundred to a few thousand dollars. If the sponsorship expense is that low, do some digging on why. It is likely that the decision makers and influencers you are hoping to reach are not in that audience, or the cost would be greater.

Here is an additional consideration: should you sponsor a national conference or a regional cybersecurity conference?

Alex Wood, CISO at Pulte Financial Services, mentioned hit on some key differences during a discussion at regional SecureWorld conference.

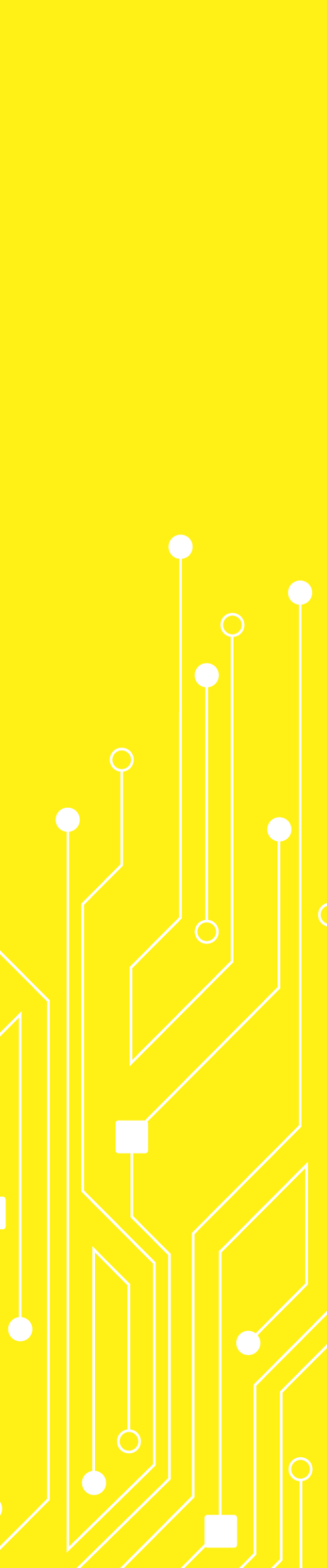
"Sometimes you get to a major national conference and you've got twenty to thirty-thousand people. It's hard to track what's going on. However, this is still nice and intimate but a good enough size that you get a lot out of it."

Regional conferences are usually just 1 or 2 days in duration and minimal travel is required to attend. These factors make it more likely for security leaders and teams to attend at a time where many are understaffed thanks to unfilled roles caused by the cybersecurity talent gap. Two days out of the office is more realistic than an entire week.

Also, many CISOs and leaders surveyed indicate they attend the same regional security conference each year to build a robust network of peers in their area whom they can contact for help.

Lastly, regional conferences are typically more affordable for both CISOs and cybersecurity vendors. And if you are an exhibitor at a regional conference you may be one of 30 or so vendors onsite. And at a national conference, you might be one out of 300.





All the numbers are bigger at national conferences, along with the cost to sponsor. However, organizations perceive value from branding themselves in front of as many eyeballs as possible. National conferences certainly outpace regional conferences if they are looking for venture capital or need exposure to investment funds. That is because many of the attendees at these conferences are looking for investments rather than cybersecurity solutions.

A final consideration beyond the cost of transporting a sales team across the country or around the world for a national conference is the time away from the office for these team members.

Sales teams with regional territories obtain leads which are typically handed off to someone else and they may lose up to a week of time closing sales or connecting with prospects in their territory.

Strategy 3. Look Beyond the CISO

A decade ago, as CISOs were rising to prominence, it made sense for cybersecurity marketing and sales teams to focus almost exclusively on these leaders. Since that time, significant shifts reveal the need for multiple advocates within an organization to avoid have the sales process derailed.

a. The sales process is more complex than ever
In their follow-up to the bestselling *“The Challenger Sale”* book, authors Brent Adamson and Matthew Dixon wrote *“The Challenger Customer.”* They revealed their research on what the modern buying process looks like:

“In a survey of more than 3,000 stakeholders involved in a typical B2B purchase, we found that customers themselves report an average of 5.4 different people formally involved in a typical purchase decision. That’s 5.4 opportunities for someone to say “No.”

b. An increasing number of CISOs come from business backgrounds

Dr. Larry Ponemon, one of the most respected IT and IT Security researchers in the world, recently told our organization that CISOs are, by necessity, becoming business leaders instead of technologists:

“A growing number of CISOs have business backgrounds, an MBA and the skills needed to communicate with other C-level executives and the board.”

In many cases, the CISO is focused on business risk rather than evaluating a specific solution or technology.

c. Solution purchasing decisions increasingly come from technologists

Technology consultant Natalie Nathanson, Founder & President, Magnetude Consulting, wrote about the shift she is seeing in the security space:

“While the executives may love your pitch and think your products have value, they will often pass the purchase decision down to middle management or the technical and engineering teams. Security is complicated and must take into account adherence to standards bodies, compliance, current existing infrastructure, and vendor compatibility.”

Modern marketers should make sure they are marketing to both CISOs and technologists and should look for opportunities to reach both audiences at the same time. This is the sweet spot of creating advocates who can help start the sales process, keep it on track, and see it through to completion.

Strategy 4. Offer Meaningful Content

Have you developed a content marketing strategy that can help keep a sales process on track?

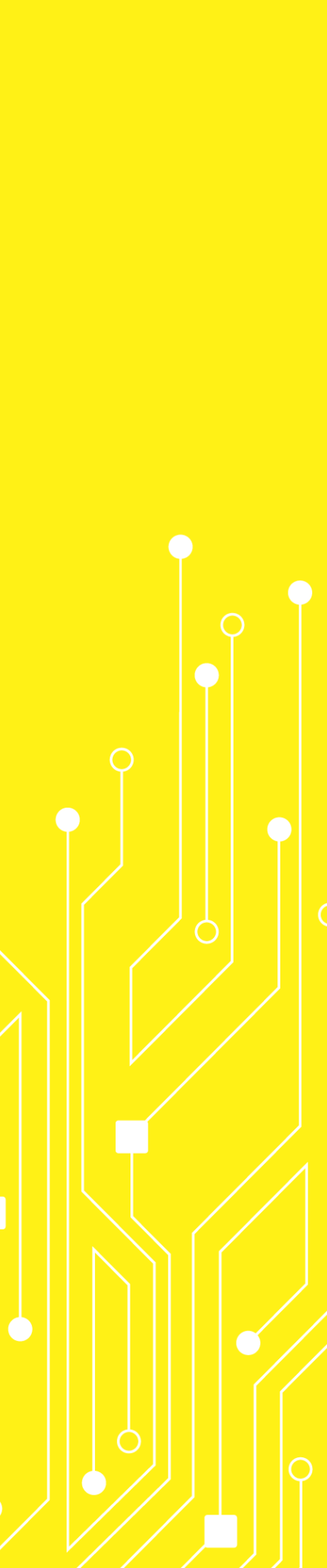
Point 3(a) emphasizes the complicated nature of today's solutions purchasing decisions. Arm any advocates you have within an organization with digestible and fact-based content they can share with others who are part of the buying process.

B2B writing expert Gordon Graham explains why white papers are called “The King of Content” and can greatly help your sales and marketing efforts:

“No other B2B marketing piece can do more to generate leads, nurture prospects, and build mindshare.”

These thought leadership pieces can be used at the top, middle or bottom of the funnel.





Also, case studies are another valuable content marketing piece. These take an emotionless technology solution and put a human face on it. It proves to security leaders that your solution has already been proven to help their peers.

Lastly, consider advertorials, blogging on cybersecurity industry news sites and media interviews on your latest research as tools you can share with security leaders. This can help your organization demonstrate the worth of a solution.

Strategy 5. Position your company as a genuine partner

Cause marketing is a powerful trend in the consumer marketplace, and increasingly, in the B2B cybersecurity marketplace as well.

Many security leaders and decision makers are not just looking for a cybersecurity vendor, they are looking for a solution partner. In a recent panel on working with startups at SecureWorld Bay Area, this message came across loud and clear.

Maarten Van Horenbeeck, CISO of Zendesk summed up this view:

“I look for alignment with the purpose of what a startup company is trying to accomplish. Ethics matter significantly to me. Their behavior needs to treat the issue of cybersecurity like it’s something we can solve together.”

How is your organization positioning itself to be seen in a positive light, as a partner in the fight against cyber adversaries?

Strategy 6. Align yourself with trusted partners

Security decision makers and influencers care about credibility. This includes the credibility of their sources for industry news, the credibility of the podcasts they appear on and the credibility of the conferences they are willing to help lead.

Jimmy Sanders, Vice President of Information Security at Netflix DVD, explains how he chooses which organizations to be involved with, given limited time:

“I’m a part of SecueWorld because I love organizations that are working with the community and trying to improve cybersecurity, as a whole.”

Are those you are partnering with to share the news of your organization seen in a positive light by security leaders? This can greatly benefit your marketing efforts.

Strategy 7. Increase Digital and On-Demand Footprint

The pace of life has never been faster. Security leaders have busy lives outside of the office and increasing your digital footprint is a crucial opportunity to reach them.

Build or sponsor online web conferences: the most effective web conference format tends to be a mix of practitioners and a sponsoring vendor, built around a specific topic. Doing this in-house, unfortunately, will limit the reach and requires you to ask your customers to participate. An easier option is to consider an external partner. However, be careful to explore the following: make sure the partner can demonstrate several months worth of highly attended web conferences. This proves the webinars are of value to the security audience. And work with a partner that has a vast network of practitioners with the necessary expertise to participate. This makes the process much easier for any marketing organization.

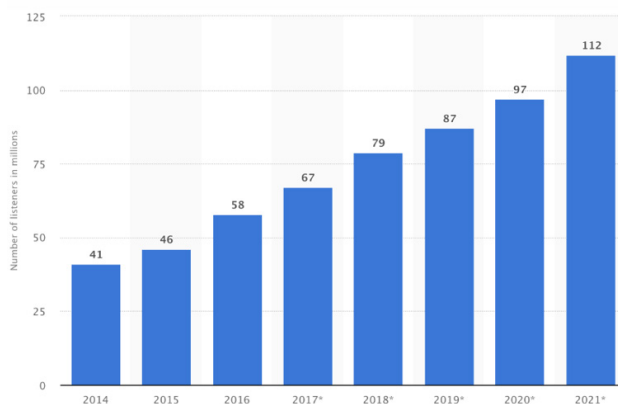
Also, does the marketing partner have a news portal which will cover the podcast and let readers know about it?

And make sure the company you are partnering with will allow you to distribute the web conference to your network, as well.

After doing this research to find a reliable partner, it should become obvious that in the case of webinar creation, production and audience reach, you generally get what you pay for.

Podcast boom: are you part of the worldwide podcast boom?

Is your organization part of the explosion in podcast listenership?

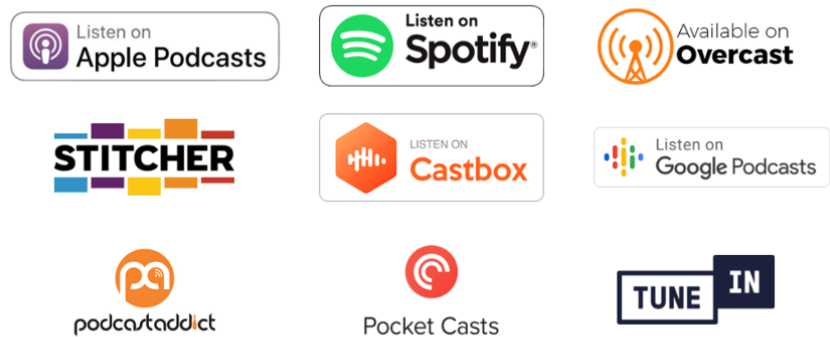


As podcasting listenership grows, previously published episodes keep getting “discovered” by security professionals. Sponsor these should be viewed as a drip campaign.

Considerations: linking your organization with a credible podcast is one consideration.

How is the podcasting organization viewed in the cybersecurity space? Is the podcast optimized for Apple Podcasts, which is far and away the dominant platform?

Also, ask if the podcast is distributed through all platforms with a greater than 1% market share, platforms like these:



Ask about the different types of sponsorship offered by the cybersecurity podcast.

Almost all will read a 30-second spot or insert one into the episode. However, some thought leadership podcasts will allow your executive to join a specific episode around a topic of their expertise. And some offer opportunities to highlight new research or solutions from your organization.

Lastly, ask the podcast you’re considering for sponsorship how the podcast is marketed.

This is a growing way to reach busy cybersecurity professionals as they commute or multi-task. And listenership is growing for established and regularly published podcasts.

Conclusions

To reach busy and understaffed security leaders in 2020 takes a multi-faceted approach which requires implementation of the ways modern security leaders want to be reached.

These methods increase efficiency, lead to legitimate exploration of solutions and services, and help keep an increasingly complex sales process on track.

SecureWorld can help your organization strategize and explore which methods are the best fit for your organization and the audience you are attempting to reach.

About SecureWorld

SecureWorld is a cybersecurity focused media company which brings together security leaders and vendor partners through 17 annual security conferences in the United States and Canada; and through key types of digital content creation and multiple digital platforms. To find out more about how SecureWorld can help your organization stand out in a crowded cybersecurity marketplace, contact Vice President Brad Graver at 503-344-4526 or media@secureworldexpo.com

Marketing tools
from SecureWorld
can help you reach
the right audience

