

Security products and services

How to engage and market to security buyers

The stress on CISOs everywhere is mounting.

Increased scrutiny is coming in the form of regulation and compliance requirements as well as greater board-level oversight. IT infrastructure complexity is only growing, making rising cybersecurity threats even more of a business risk. Not to mention, talent shortages and gaps threaten the security posture of organizations everywhere.

But it's not all doom and gloom as witnessed by the investment in security. Worldwide spending on security solutions and services was projected at \$219 billion last year, an increase of 12.1% compared to the year prior. And according to IDC, "Investments in hardware, software, and services related to cybersecurity are expected to reach nearly \$300 billion in 2026, driven by the ongoing threat of cyberattacks, the demands of providing a secure hybrid work environment, and the need to meet data privacy and governance requirements."

"Spend on security products and services will continue to outperform growth in overall IT spending," said Serena Da Rold, associate research director, IDC Data & Analytics.

That's likely due to CISOs pushing for businesses to recognize the risk rather than shouldering it alone while arguing for better-resourced teams and tools. Their role is certainly getting the attention it deserves with a greater C-suite and boardroom presence. With that comes ample opportunities for tech marketers to help

Worldwide spending on security solutions was projected at \$219 billion last year, with investments expected to reach nearly \$300 billion by 2026.

85% of IT security execs engage with the board of directors.

security teams improve their security posture and alleviate those pain points.

To better understand how the purchase process for security products

and services is distinct from those of other technologies, Foundry analyzed research from two recent buyer's journey studies—Customer Engagement and Role & Influence of the Technology Decision-Maker. This white paper aims to help guide tech marketers around the latest buyer's journey trends. Here, we'll explore who is involved in security purchase decisions, the content types and sources buyers turn to, and how they want to be engaged in digital, in-person, and sales settings.

The current security landscape

Overall, businesses are investing in their security by appointing a top security executive (65%), but especially so at enterprise (1,000+ employees) organizations (83%) where the most likely title is CISO (60%). While that remains fairly consistent, security executives' reporting structure has changed. They still report primarily to the CEO (44%); however, more now report to the Board of Directors than ever before (25%). And whether they do or not, 85% report regular or frequent engagement with their board of directors. Nearly half (48%) meet with the board one

or more times a month. That may be due to increased regulatory compliance.

As CSOonline notes, "It's clear that there may be a shift underway toward recognizing the key business value of cybersecurity leaders — the US Securities and Exchange Commission (SEC) has ramped up its support for cybersecurity as a top business concern and expressed its opinion that the CISO should be seen as an integral part of the enterprise's decision-making team."

The good news is that roughly six out of 10 security leaders say their engagement with the Board of Directors helps improve cybersecurity/security initiatives. However, there's a little more to be desired when it comes to security-related experience, as only 46% say their Board has experience with it.

Investment also comes in the form of dollars. The vast majority say their organization's overall security budget will either increase (43%) or remain the same (55%), with enterprise organizations much

"It's clear that there may be a shift underway toward recognizing the key business value of cybersecurity leaders."

CSOonline.com

more likely to increase (50%) than small-to-medium (SMB) businesses (36%).

When it comes to determining the priority of security spending, the top three factors influencing it are addressing risks that come because of a business' evolving technology use, compliance and regulatory mandates, and simply industry best practices. Of course, like a lot of technology, investment is complex. In fact, nearly 70% of security leaders agree that understanding which security tools and solutions fit best

within their company is becoming more complex.

That might be why security spending is not increasing in finite areas but spread across many areas. For tech marketers, that's a positive signal of opportunity across the

security landscape. The catch here is that it's imperative to help security buyers make the product fit connection.

Understanding a complex purchase process

Investment may be increasing, but given rising IT infrastructure complexity and talent shortages, it's no surprise that the security purchase process has become increasingly complex. The average length of the security

69% agree that understanding which security tools and solutions fit best within their company is becoming more complex.

28

people are involved in influencing security purchases on average.

IT: 15

LOB: 13



purchase process has crossed the half-year mark (6.2 months) with 28 influencers involved. The makeup of the purchasing team is split between IT (15) and line of business (13). This is up from a total of 23 influencers last year (12 IT and 11 LOB).

Each year Foundry's research measures leadership throughout the purchase process, assessing the involvement of 19 different job titles across seven decision stages. While top security executives have a leadership role in four out of the seven stages, it's not surprising to see CIOs have the most influential voice in five of the seven stages, considering 34% of security leaders say they report to the CIO.

Another prominent group is IT/networking management, who lead in determining technical requirements and then supports product evaluation, vendor selection, and selling internally. And with such a

Leadership throughout the security purchase process

Key **1** **2** **3**

	Determine the business need	Determine technical requirements	Evaluate products or services	Recommend and select vendors	Sell internally	Authorize and approve	Post-sales engagement
CIO or top IT executive	41%	36%	34%	32%	29%	39%	23%
CEO	34%	13%	15%	12%	11%	38%	8%
CISO or top security executive	27%	28%	28%	27%	19%	21%	16%
IT/networking management	23%	37%	38%	27%	18%	15%	15%
Security management	22%	27%	27%	20%	12%	13%	12%
CSO or top security executive	20%	25%	24%	19%	14%	16%	11%
CTO	20%	25%	22%	18%	15%	16%	10%
Security staff	20%	29%	35%	22%	11%	8%	16%
Line of business management	19%	14%	14%	10%	10%	10%	8%
COO	19%	10%	12%	10%	10%	18%	7%
IT/networking staff	18%	34%	39%	21%	10%	8%	21%
Architect	18%	33%	29%	22%	10%	6%	11%
Chief Data Officer or equivalent	17%	21%	19%	14%	11%	11%	10%
CFO	17%	8%	11%	9%	9%	36%	6%
Engineer	17%	35%	35%	23%	11%	7%	16%
Business relationship manager	16%	11%	12%	9%	9%	6%	7%
Chief Digital Officer or equivalent	16%	14%	15%	12%	8%	8%	5%
Software engineer/developer	15%	24%	25%	15%	6%	7%	11%

large purchasing team, it's predictable that other roles play important parts throughout, even if only for one stage. For example, IT/networking staff dominates in product evaluation, with security staff also playing a supporting role. Engineers

also step in when determining technical requirements and evaluating products.

At the same time, certain roles dominate in typical stages. For example, CEOs are most influential when determining

Tech marketer takeaway

It's not a one size fits all. Be sure to understand the key stakeholders at each stage of the purchase process and tailor engagement to those individuals.

For vendors to make an impact, they must be willing to help security leaders build the business case.

66% of security buyers are looking to vendors to help them develop the business case around investment in their technology.

the business need and authorizing the purchase, where CFOs also dominate. However, when it comes to post-sales engagement, there are multiple groups involved—CIO, CISO, security staff, IT/networking staff, and engineers.

As top security executives gain more prominence in the C-suite and reporting structures shift, it will be important to watch

for shifts in leadership throughout the purchase process. Tech marketers would do well to understand the current layout of key stakeholders at each stage of the purchase process and tailor engagement to those individuals while also targeting top security executives who stand to take on an even more dominant role in the future.

What influences vendor selection

The complexity around security investment means that targeted engagement is just the start. For vendors to make an impact, they also must be willing to help security leaders build the business case. In fact, 66% of security leaders are looking to vendors to help them develop the business case around investment in their technology. Showing business value

is especially important throughout the stages where the purchase process is most likely to stall. We see an increased likelihood when determining the business need, during product evaluation, and determining technical requirements.

To help combat this, consider offering additional support, guidance, and resources. Relevant and consistent education is essential, especially when the buying group extends to areas within line of business. In fact, 58% of security buyers say that it's essential to educate non-technical functions with more educational resources from vendors.

And those who make the investment to show value will win, regardless of whether they're an existing security vendor. In fact, when asked what type of vendor a business would seek to purchase from, 52% said they'd seek to purchase from an existing vendor and 48% from a new vendor. The main reason being because the new vendor or product is more innovative or feature-rich (41%), followed

73%

of security buyers say that technology vendor reputation is one of the top factors they consider when making purchase decisions

by the current product/service no longer met their business needs (34%).

While security buyers are open to the vendor who will provide the most value, there are certain aspects that influence vendor selection—brand awareness and reputation being some of them. These influence everything from content engagement to making the shortlist. Seventy three percent of security buyers said they are more likely to consume content from trusted brands and another 73% say that technology vendor reputation is one of the top factors they consider when making purchase decisions. Additionally, 69% agree that the internal sell-through process becomes easier when all stakeholders are aware of a brand.

Of course, effective sales follow-up also influences who gets the business. A significant 70% percent of security-focused IT decision-makers say that the vendor who responds to their questions in a quick and thoughtful manner usually

Marketers have some work to do

- **87%** of security-focused buyers say it's challenging to find high quality content.
- **Only 46%** say that the work-related content they downloaded over the past 6-12 months provided them with value.

How should security vendors communicate with their buyers?

- Share valuable content or information
- Be knowledgeable about their business or specific challenges
- Reach out at the right time
- Show respect for their time

gets the business. Though what does that mean exactly? Security-focused buyers expect a response to their inquiry within an average of 17 hours.

When asked what most prompts security-focused buyers to respond to vendor outreach, four primary reasons came to the fore:

1. The vendor shared valuable content or information with them.
2. The vendor was knowledgeable about their business or specific challenges.
3. The vendor reached out at the right time.
4. The vendor showed respect for their time.

The right content delivered at the right time will go a long way to winning the business so long as there's a heavy dose of showing value through knowledge of a customer's challenges and authenticity.

Delivering value through content engagement

Security-focused buyers are more than willing to share their information to access content. In fact, 91% said they're willing to register for content from a technology vendor. And they're willing to register for a variety of it. The top content type is product testing/reviews/opinions and vendor presentations, followed closely by technology news, analyst research, and case studies.

The problem lies within the value that content provides to security buyers.

- 87% of security-focused buyers say it is challenging to find high-quality content.
- Less than half (46%) of the work-related content they downloaded provided security buyers value over the past 6-12 months.

To overcome the disconnect, tech marketers will want to take note of specific preferences, starting with the experience. Security buyers are more likely to engage with a variety of content if it is presented in an organized experience—nearly three-quarters (72%) agree as such. We also know that security buyers are likely to view a vendor negatively if they can't easily find educational content throughout the

69%

of security buyers are more likely to consider an IT vendor who educates them through each stage of the decision process.

purchase process (71%). So, note that if you want security buyers to engage with more content, present it clearly and in an organized way. If you do so, security buyers will likely tell their peers. Forty-eight percent agree that they'll tell their friends if you provide a great customer experience.

Experience is one aspect, but another that is crucial is engagement from every aspect of the customer journey, beginning with an initial touchpoint for a tech marketer's brand, like advertisements. The majority (92%) of security buyers want ads tailored to their needs, primarily by their technologies in use (43%) and industry (42%). But there are also other factors that influence engagement. Security buyers are used to being served ads for tech solutions and will take additional actions after seeing one, including contacting a vendor or channel partner (57%), conducting further research online (50%), consuming content on a vendor's website (48%), or even downloading a demo or trial (34%). The caveat is that influencing security buyers to take that action

requires the ad to address their current challenges or business objectives (44%).

Marketers should also note the information that security buyers find most interesting during each stage of the purchase process, especially since 69% are more likely to consider an IT vendor who educates them through each stage of the decision process.

Without a doubt, security buyers want to know the skills or roles needed to deploy and support the technology, as noted in five of the purchase process stages. That makes sense considering the talent shortage facing security teams today. Otherwise, the topics vary by stage, giving tech marketers more to chew on when it comes to tailoring. A few key areas to note are that customer success stories are of high value during the beginning stages of the purchase process. When it comes to selling internally and authorization, security buyers are interested in the topic of the technology's business value. During the approval stage, security buyers are also

most interested in the estimated ROI and pain points the technology addresses.

Content consumption trends

Security turn to a variety of information sources throughout the purchase process, whether they be technology content sites, technology vendor websites, white papers, webcasts, or analyst firms. Not surprisingly, different sources assume more or less importance at different stages of the purchase process. However, tech marketers may be interested to note that technology vendors, in varying capacities (i.e., website, in-person, phone, email, or video conference), are among the top five influencing sources at every stage of the purchase process. Their strongest influence comes during product evaluation, taking two of the top three spots, and during post-sales engagement, taking the top three spots.

Technology content sites are also a clear source of information used

Tech marketer takeaway

The stage at which security decision-makers are in the purchase process impacts the topic of content they consume. Be sure to understand where they are on their journey and supply them with the information that is needed.

throughout the purchase process, taking a top five spot in all of the stages.

Peers both inside their company and outside their company, whether in-person, by phone, email, or social/business networking sites, are also extremely valuable and relied upon sources for security buyers. During the recommendation and selection stage we see peers taking the top spots right below technology vendor websites. This speaks to the importance of customer service and brand awareness, as IT decision-makers will tell their colleagues and peers about a positive experience. Peers inside their company are also considered the most valuable source when determining the business need, followed close by technology content sites. Technology content sites is also the number two source when determining the technical requirements, right after technology vendor websites. As buyers move into the later stages of the decision process, they turn again to peers inside and outside their

95%

of security buyers watch technology related video content for business purposes.

company as information sources for the internal selling and authorization stages.

Preferred content types also differ depending on the buyer's stage in the journey, where security buyers download an overall average of six pieces of content. Product tests are near the top of the list for security purchases for nearly every stage. Vendor presentations also make the top five list for six of the seven stages, ranking number one during vendor recommendation and internal selling. Technology news and case studies show their importance during the first half of the decision-making process, with case studies rising to the top again during post-sales engagement. Analyst research comes to

Tech marketer takeaway

Security buyers rely on technology news and case studies in the initial stage of the purchase process. Make sure your content is up to date and appropriately tailored to the individuals involved in these stages.

the fore primarily during the middle stages of the purchase process. ROI tools show up throughout the purchase process at varying stages, as do product demos.

Keeping tech buyers' attention amongst the noise

Tech buyers have abundant content available to them, making meaningful engagement difficult for tech marketers. It takes the right content at the right time across multiple mediums to truly grab tech buyers' attention, with audio, video, and events being among them.

Video is a mainstay for security-focused buyers, with 95 percent noting they watch tech-related videos. In-depth product reviews and industry research or tech analyst reports are the top two video types they are likely to watch for business purposes. The top five list is rounded out by interview with technology experts, technology news reports/live coverage news events, and how-to videos.

Podcasts are a dominant way people consume information, security-focused buyers included. Sixty-seven percent say they have listened to a business-related podcast in the past 12 months, with the top two reasons being to find out

94%

of security-focused IT decision-makers have attended an in-person or virtual event in the past 6-12 months.

Primary types attended

Training/workshop	75%
One day conference	74%
One day tradeshow	61%
Multi-day conference	61%

about emerging and new technologies and to keep up with business trends.

Events have long played a role in connecting with IT decision-makers. Yet, there continues to be a willingness to lean into different formats, whether in-person or virtual. Sixty-five percent of security buyers said they'd be more likely to attend in-person industry events in the next year. At the same time, 75% said that given the ease of attending, virtual events will continue to be an important source of information. And 94% have attended an event in both formats within the last six to 12 months. When asked what types of events they've attended, trainings or workshops were at the top of the list, followed by one-day conferences.

Key takeaways

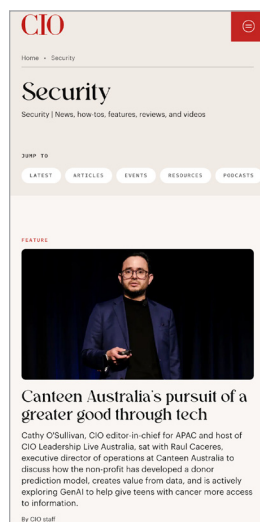
- Security teams face a tougher balancing act than ever before with risk, IT infrastructure complexity, talent shortages, and increasing cybersecurity attacks. They must help their organizations evolve their security posture. Tech vendors and marketers that can help security buyers meet these challenges will win, securing a piece of the investment these teams are making in the year ahead.
- New compliance requirements are positioning security as a strategic part of the business with a direct line to CEOs and Boards of Directors. However, tech vendors and marketers should still be aware of who has the most influence throughout the purchase process and tailor engagement to those individuals.
- Security buyers have clear preferences when it comes to the content experience and engagement, whether they're being served an advertisement or downloading a case study. Tech marketers who note security buyers' preferences around the experience, how they want their content tailored, and the topics that interest them most will have a better chance of grabbing their attention and ultimately winning their business.

Connect with security buyers

Foundry's editorial brands are at the forefront of security related coverage, arming IT leaders and professionals with the tools needed to execute efficient and protective security strategies

CIO

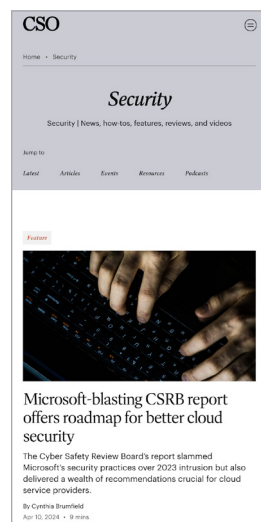
Business technology leadership
CIOs,
Business execs



2.7M
views per month

CSO

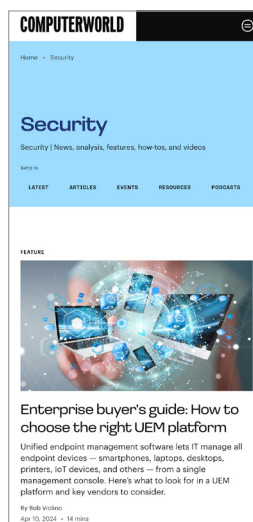
Business risk leadership
CSOs, CISOs,
Enterprise security
decision-makers



908K
views per month

COMPUTERWORLD

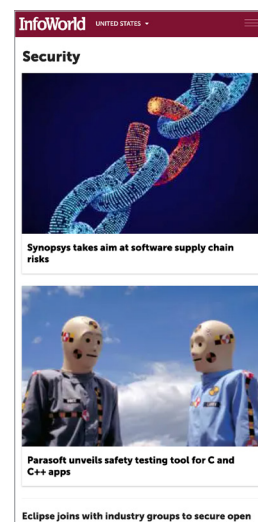
Making technology work for business
Enterprise IT,
management,
LOB, SMB



6.9M
views per month

InfoWorld

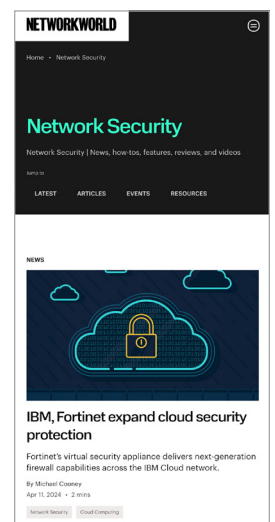
Building the next-gen enterprise
Developers,
IT architects



1.4M
views per month

NETWORKWORLD

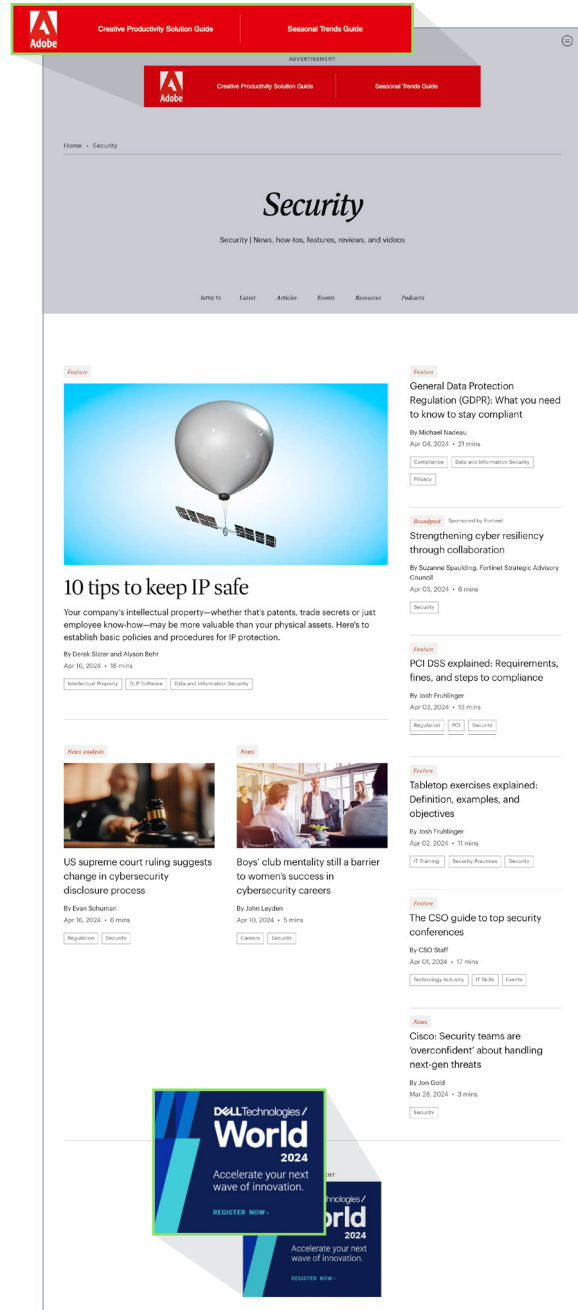
From the data center to the edge
Network
management, data
center managers



888K
views per month

Security topic sponsorship

Increase brand awareness through a sponsorship of the 'Security' topic pages across Foundry's award winning B2B brand sites. These month-long sponsorships include guaranteed impressions and an editorial newsletter sponsorship to maximize engagement within marketers' target audience.



Engage with security decision-makers where they are

Events are powerful experiences that forge intentional connections between ITDMs and solution providers. Ranging from multi-day educational symposiums and prestigious awards programs to intimate roundtable discussions, Foundry and IDC tailor the event type to deliver on audience objectives and needs, ultimately offering meaningful guarantees to sponsors, plus customized packages to meet your branding and lead generation needs.

Event formats



Leadership events and awards

Thought leadership events give you access to engage with over 200+ executive IT and security leaders



Roundtables and dinners

Virtual or in-person discussions with 7+ executives



Virtual summits

Virtually connect with 400+ powerful IT buyers



Custom events

Bespoke events to fit your marketing strategy

Topics covered

- AI and Machine learning
- CIO
- Cloud
- CSO
- Digital innovation
- Data and analytics
- Data center and storage
- Leadership
- Future of work
- Security

Stay in touch with us

Email: Sign up for Foundry's newsletters and receive media and marketing trends as well as our proprietary research, product and event information direct to your inbox. Go to foundryco.com/newsletter.

Twitter: To get results from Foundry research when it's released, or any other news, follow us on Twitter: [@FoundryIDG](https://twitter.com/FoundryIDG)

LinkedIn: For research, services and events announcements, visit us on LinkedIn: <https://www.linkedin.com/company/foundryidg/>

Find it all on foundryco.com

About Foundry

Foundry's vision is to make the world a better place by enabling the right use of technology, because we believe that the right use of technology can be a powerful force for good.

Foundry (an IDG, Inc. company) is a trusted and dependable editorial voice, creating quality content to generate knowledge, engagement and deep relationships with our community of the most influential technology and security decision-makers. Our premium media brands, including CIO®, Computerworld®, CSO®, InfoWorld®, Macworld®, Network World®, PCWorld® and Tech Hive®, engage a quality audience of the most powerful technology buyers with essential guidance on the evolving technology landscape.

Our trusted brands inform our global data intelligence platform to identify and activate purchasing intent, powering our clients' success. Our marketing services create custom content with marketing impact across video, mobile, social and digital. We simplify complex campaigns that fulfill marketers' global ambitions seamlessly, with consistency that delivers quality results and wins awards. Additional information about Foundry is available at foundryco.com.