

How Cybersecurity Buyers Decide Which Vendors to Trust

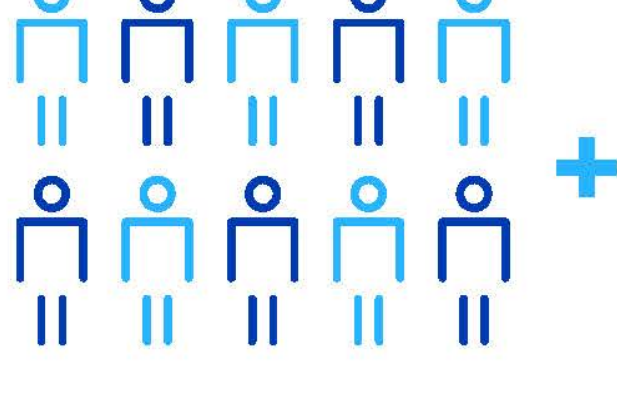
Where evaluation happens and how demand is generated



Cybersecurity Buying Is Complex

Cybersecurity purchasing is rarely driven by a single decision-maker. Multiple stakeholders, including practitioners, IT leaders, business stakeholders, and executive leadership, evaluate vendors from different perspectives, making credibility and alignment critical throughout the buying process.

With so many stakeholders involved, buying teams filter vendors carefully before formal evaluation begins.



10+ stakeholders commonly influence cybersecurity purchases.



72% of IT managers, directors and architects participate in early cybersecurity research.

Trust Determines Who Gets Evaluated

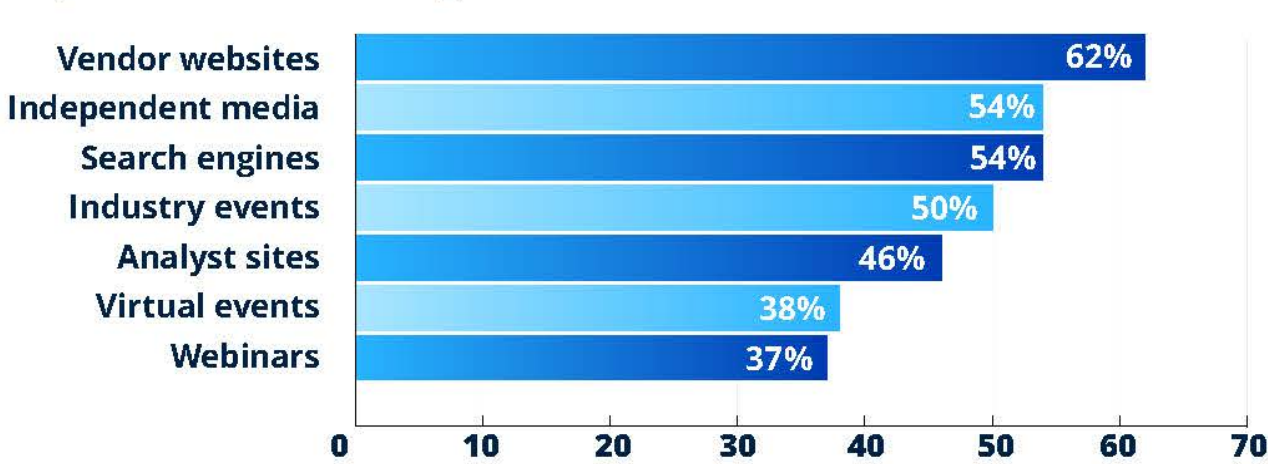
Trust acts as a credibility filter in cybersecurity buying decisions. Before vendors are compared on features or pricing, buying teams determine which providers appear credible enough to investigate further.

Many vendors are eliminated before formal evaluation begins.

Where Cyber Buyers Validate Vendors

Cybersecurity buyers rely on extensive research and multiple sources to compare claims and reduce risk.

Top sources used during evaluation



Evaluation rarely happens in a single place. Buyers move across these environments as they validate vendors and narrow down their options.

Demand Forms During Evaluation

Cybersecurity demand rarely begins with a cold lead.

Buying teams generate demand while researching, comparing vendors and validating claims across trusted environments.

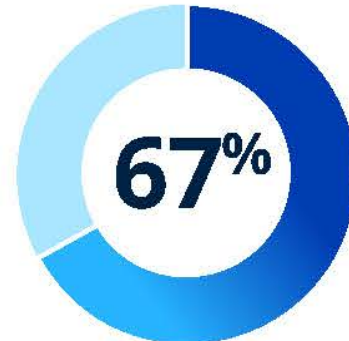
The interactions that move deals forward tend to happen when buyers can ask questions, hear expert perspectives and involve multiple stakeholders.



Sales Engagement Follows Buyer Validation

Cybersecurity buyers rarely engage vendors at the start of their research. Most conversations with sales happen after buyers have already compared solutions, consulted trusted sources and narrowed their options.

By the time a vendor meeting occurs, buying teams are typically validating shortlists and evaluating specific capabilities.



67% of cybersecurity buyers are more likely to meet with a vendor after engaging with educational research or expert content.



46% of cybersecurity buyers engage through industry events during evaluation.

High-Trust Engagements Accelerate Cybersecurity Evaluation

Not every interaction reflects real buying intent. The strongest demand signals appear when buyers are actively researching solutions, discussing options internally and involving multiple stakeholders.

Programs that intersect with these moments are more likely to influence evaluation and advance opportunities. Whether it's engaging with established and credible sources or meeting face-to-face at events, high-trust engagements can accelerate evaluation.

Strong Intent Signals Appear During Technical Evaluation

In cybersecurity, meaningful engagement usually reflects active solution evaluation.

Security teams validate vendor claims through technical research, expert perspectives and structured discussions with peers and specialists. As buying groups compare approaches and assess risk, engagement becomes more intentional and more predictive of opportunity creation.

Programs that intersect with these evaluation moments tend to surface stronger buying signals than passive content consumption.

As cybersecurity buyers become more selective, the environments where they research and validate vendors become increasingly important.

Trusted Environments Drive Cybersecurity Demand

Cybersecurity buyers evaluate vendors through a network of research sources, expert perspectives and industry conversations. Demand programs are most effective when they appear consistently in the environments where buyers are already validating solutions and involving stakeholders.

Informa TechTarget's media, analyst insights and event platforms bring cybersecurity buyers and vendors together during these high-intent evaluation moments. By combining trusted editorial, expert perspectives and industry events, marketers can engage buying groups where meaningful vendor consideration and evaluation actually occurs.

For cybersecurity demand teams, success increasingly depends on aligning programs with how buyers research, validate and advance decisions.



Ready to build trust with your most sought-after cybersecurity buyers? Talk to an Expert.