The ART & SCIENCE of PROSPECTING

Security Marketing Disconnect

simplyDIRECT

Contents

Does your marketing team truly understand what drives the buyers in their market?

In late 2015 account-based marketing firm, SimplyDIRECT, wanted to explore if marketing professionals within companies selling security solutions were "on the same page" as those IT executives who routinely buy security solutions. Seems simple enough, yes? The results were eye-opening; occasionally there was alignment, but often there was a disconnect.

As we will see, many marketers seemed to be making decisions based on wrong, incomplete or just "made up" information. It's easy to do. We make decisions all day, every day, based on incomplete information. The brain is always making assumptions, because it never has 100% of the information it needs to process the data.

In 2013 professional services titan McKinsey & Company published a report entitled, *"How B2B companies talk past their customers"* which showed a near-total disconnect between how the two audiences thought. Buyers felt that 80% of the content that marketers presented to them was not relevant.

That's why we went through this exercise. To challenge assumptions, and make decisions based more on fact than on "gut feelings." We went out and captured the voice of the buyer. It's not that hard. Our audience—indeed, most adults—will answer just about any question if you are polite, if you are clear, and if you tell them your motives.

This is the elegance behind many of the surveys that SimplyDIRECT deploys. All we're doing is capturing the voice of the buyer. We're not making up the results; we're simply reporting what we've heard. But it can make the difference between basing an entire messaging exercise on false information. Or pitching a solution without a foundation of fact.

Program Overview

SimplyDIRECT wrote two surveys; one for those who market security solutions for large software companies, and one for the technical buyers of those products: IT security executives within large firms. The two surveys were mirror images of each other. For instance, the IT security executives were asked, "What triggers the review of new security solutions?" We then asked those doing marketing for companies selling security solutions, "What do you feel triggers companies to review new security solutions?" The goal was to see how closely these two audiences were aligned. Did the marketers understand what made the buyers tick?

Who Participated?

The security executives worked for mid- to large-sized firms; a representative sampling were Bank of America, Best Buy, Empire Life of Canada. Respondents' job titles included "VP IT Security", "Exec. Director-Threat Management", "Manager IT Security." The marketing executives worked for security software firms, including NowSecurity, Fortinet, Blue Coat and ForeScout. Respondents' titles included VP Global Marketing, Manager of Demand Generation and VP Sales and Marketing. The surveys were deployed both via email and phone; participants were offered a jacket in exchange for completed surveys.

Analysis

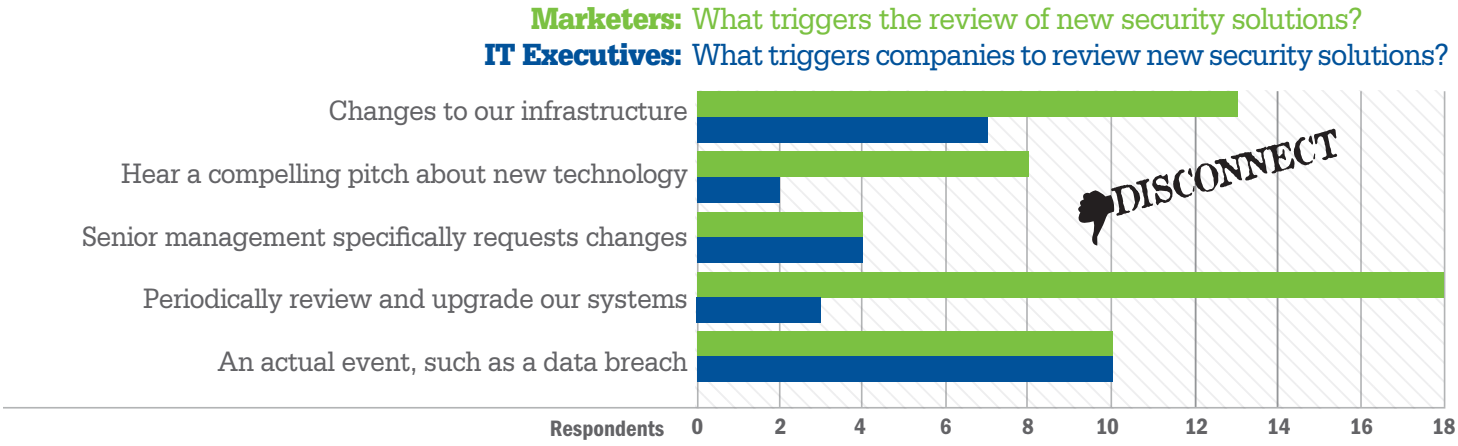
We will present here, on a question-by-question basis, how the two audiences answered the parallel questions, and the variations in each audiences' answers.

Why They Buy

The first question was, for the marketers, "What do you feel triggers companies to review new security solutions?" The IT security executives were asked, "What triggers the review of new security solutions?" Right off the bat, we saw a fascinating and significant variation in the way the two audiences responded.

The IT security executives' most common response was a rather nondramatic revelation: they simply did this kind of "review and upgrade" of their systems periodically. This was followed by an equally routine trigger: security solutions were reviewed while there were other changes to the infrastructure going on. Other factors cited that would trigger a review were an actual data breach, or the introduction of a compelling new technology.

The marketers saw things differently. By far they felt an actual event or data breach would have the CISOs scurrying for new weapons. Maybe this appeals to the Hollywood crowd—"Get me the CIA!" screams the President—but its not how things really happen. Fortunately, the marketers largely got it right on guessing the *second* most popular trigger: changes to the underlying infrastructure often is the catalyst for a review of other parts of the IT "ecosystem".



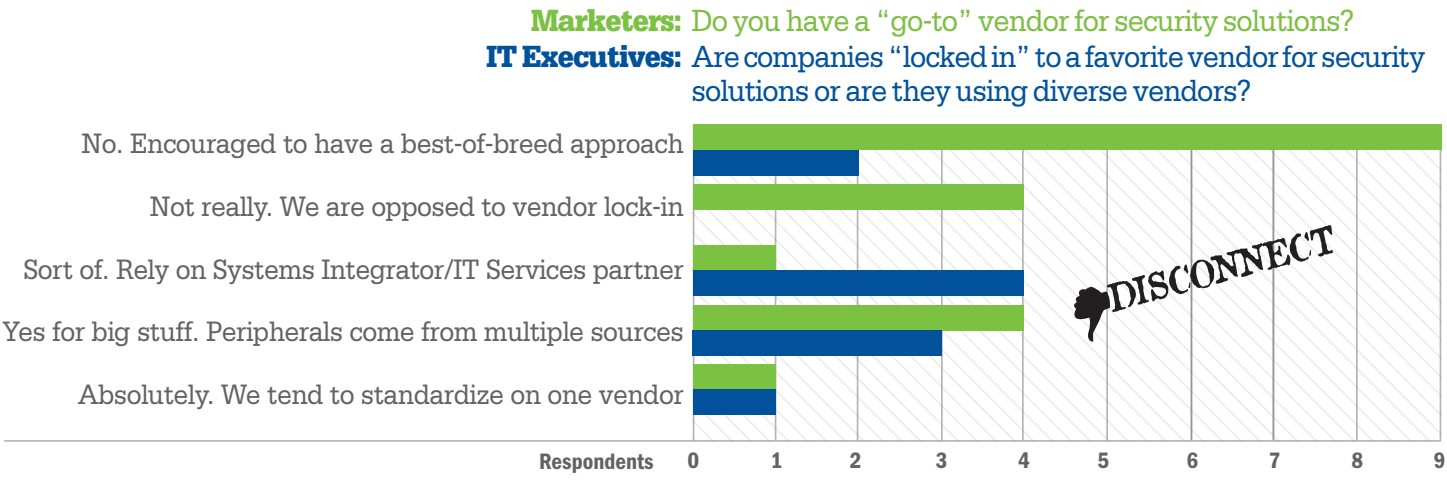
What can we learn here? Plenty! When a sales staff qualifies an account, they do so by asking questions. What's installed, what's going on, what are your plans, etc. Trouble is, that's really valuable intelligence, and not information with which many inside the fortress are willing to part with. But, just as we extracted information from IT executives about their buying behavior, properly asked its entirely realistic to expect to get an occasional executive to talk about relatively innocuous subject like when they plan to review internal systems and infrastructure. It's not a terribly sensitive question.

Conversely, the sales team that seeks to qualify an account—or a CISO—on whether or not they've suffered a recent security breach, is facing a tough challenge. That might be treated as a state secret. And, as we're learning, it's not the most important qualifier if you're selling a new security solution. That's not to say there isn't value to knowing if a breach has occurred. The company likely wants to keep such a mistake private, particularly if it is a public company. And particularly if it they are holding millions of customers' credit cards, and don't want their customers to fear their information has been compromised.

If you're an executive recruiter, determining that a breach has occurred might trigger a new executive search is about to take place. But if you're selling a solution to help lock down the company's data assets, simply learning that that IT department is going to be upgrading systems, that they're going to be "under the hood" might be a fantastically important, yet innocuous, bit of qualifying information.

Who They Buy

The next series of questions sought to explore if the buyers had preferences, and the extent to which they were willing to consider new options. It is unfair to be critical of an organization that appears at first glance to have an overwhelming favorite vendor. Many good reasons may be behind such a vendor-centric "shop." They might have a sweet deal with that vendor and favorable pricing keeps them from straying. They might have a plethora of legacy systems from that source and the possible advantages of using other brands could be outweighed by compatibility issues. There may be a key member of the Board who is behind this preference. You may never know.



You would be well served in advance if you knew of such preferences. You could avoid wasting a lot of time, or you might have a clever pitch that weaves your product into this environment, and come ready to discuss issues around not just compatibility but even synergy.

To this end, we wanted to explore if the IT executives we probed were themselves within companies that were "locked in" to a favorite vendor for security solutions or if they were open to using diverse vendors. Thus, we asked, "Do you have a "go-to" vendor for security solutions?" Questions asked like this have a high compliance rate because they are not explicitly asking what that preference is, an approach that is often met with resistance because the buyer often fears that their answer will trigger a well-rehearsed list of counter arguments. Who wants to hear that? So we simply took the high ground, and asked about, essentially, the culture of the IT organization.

By far, most IT security executives admitted to being open to a mixed-vendor environment. Such a "best of breed" approach is often music to the ears of IT sales professionals, since they all have ready-made pitches about how their solutions are, indeed, the best in their category. Now, the cynical among us might suggest that any product can be claimed as the best of breed... within a very narrowly defined category. The Yugo of the 1980s was a horrible car, but among cars that began with the letter "Y" it led the category.

The next question explored how locked down the fortress was if a new security solution was going to be offered. Approximately 70% of the answers to this question suggested environments that were not impenetrable and that new solutions were open to being considered.

Interestingly, when we asked those doing the marketing of security solutions, nearly the same amount—about 65%—felt these environments were, indeed, locked down and not particularly open to security solutions not currently on the list of favorites. What kind of defeatists are there among security marketers? Of course, there is some nuance to these preconceived notions. Many of the marketers felt that buying decisions were strongly influenced by systems integrators who, indeed, have their favorites. And several regarded the vendor lock-in was more likely to be found among the "big iron", the enterprise solutions and the large-scale systems that made up the IT backbone. But, again, it seems to be there was a misreading of the openness of companies to consider new, off-brand security solutions. Buck up, you timid marketers! David can slay Goliath in many markets!

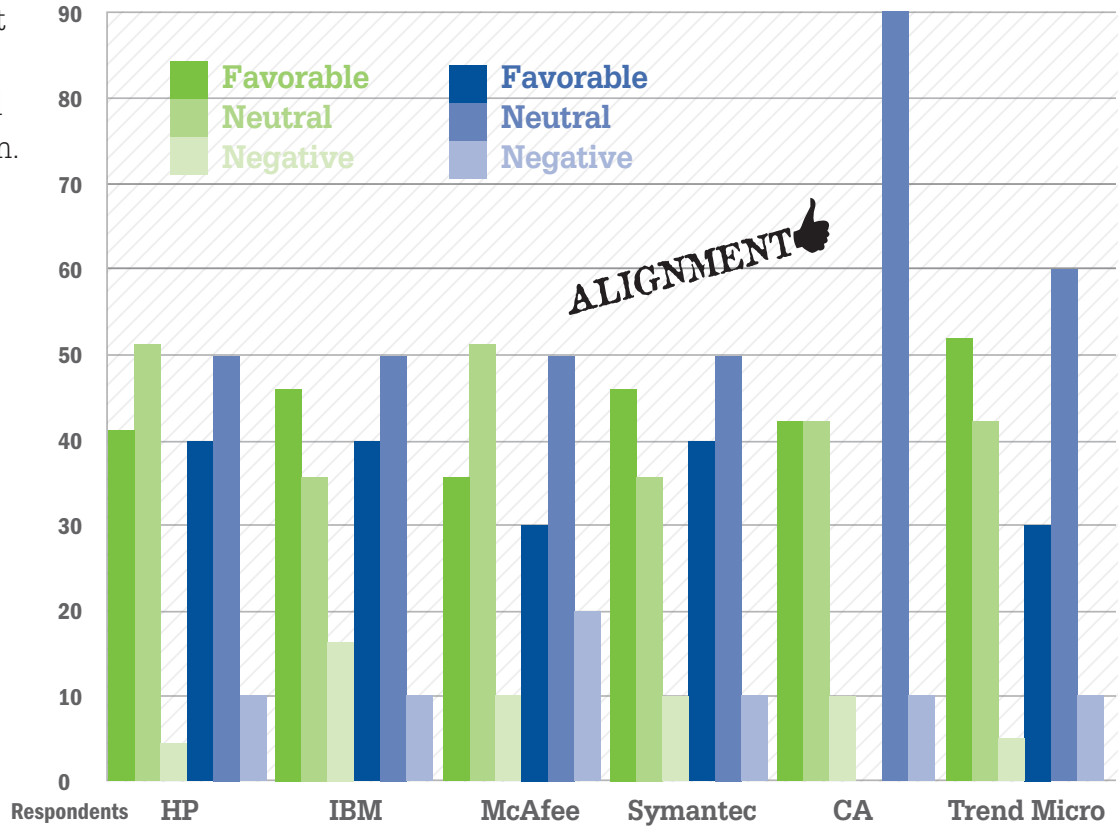
The second part of this question was, admittedly deployed to explore the possible disconnect about favorite brands, and was less about paving a path for the lesser know brand of security solution. But it certainly had the utility of helping the marketer understand what brands might be favored, and if such preferences could be leveraged in a pitch or promotion message. If we were to have discovered that the overwhelming favorite security brand was Symantec, compatibility with, or similarity to, that well-known name would be used to maximum advantage.

What we learned wasn't as dramatic a disconnect as we might have expected. Further, we believe that brand preference questions are part beauty pageant, part freak show. People like the big brands, even if they haven't had experience with them. And IF there was some negative experience with that brand, here was a rare opportunity to vent frustration, and possibly exaggerate the perceived grievances. But let's dig in.

There are some notables, but no great outliers. Most, among both the IT team and the marketers, defaulted to the "neutral" as the grade for most of the big name security vendors.

IBM has a slightly high negative from the IT crowd, but given the breadth of products IBM has—in addition to its security offerings—it is unclear how meaningful this might be. By that same measure TrendMicro faired well among the IT group, but their offerings are more narrow—and mostly in the security space—so that might hold significance. To that end, CA (now CA Technologies) did fairly well among the techies but less so among the marketers. Again, this may have less to do with CA's security offerings and more to do with their [ancient] legacy as a somewhat troubled company. Interestingly, many of CA's products are highly regarded among its tech users, so this may be a case of the beauty pageant effort, where judgments are made at face value. So it may not be that fair a question.

Marketers: How do IT executives regard the following security solution providers?
IT Executives: Do you have a go-to vendor for security solutions?



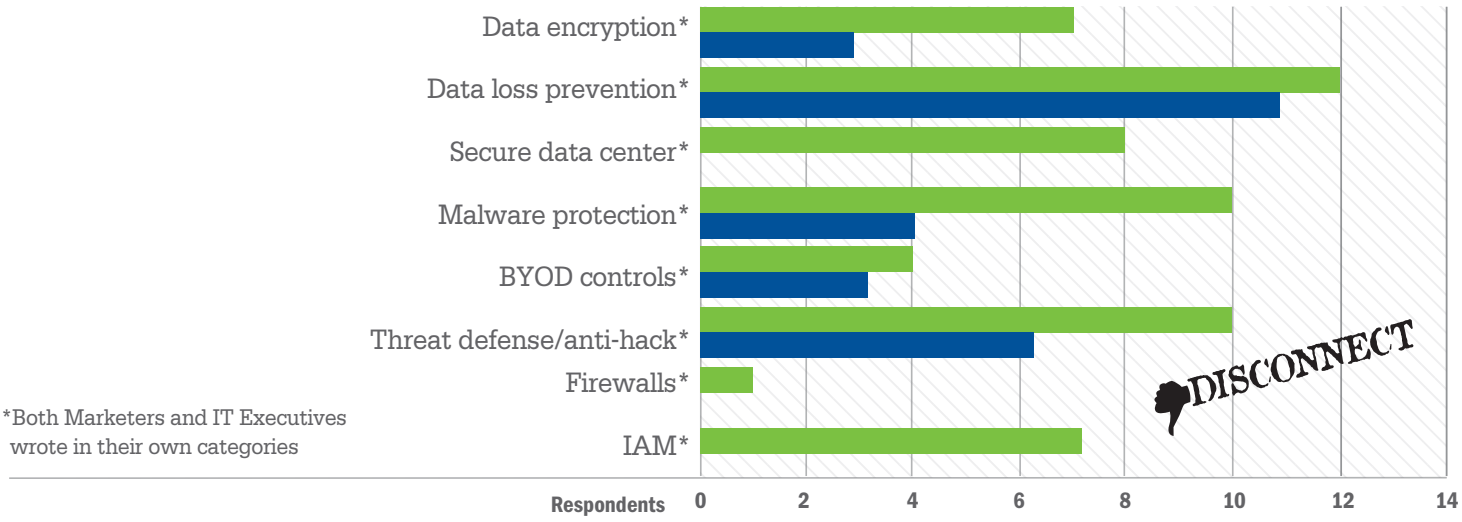
So what is to be learned here? Is there a disconnect? Do marketers truly know what are the favorite brands among their buyers, the IT crowd? It seems there isn't a significant parallax between the two. But we can posit a completely different interpretation: it seems that both groups have either positive or neutral regard for these "big names." That's refreshing. We may be looking at commonality; marketers and IT folks alike will either admit neutrality or trend positive. This is a good lesson for life, but certainly for marketing and sales professionals. In fact, this will come up later in the survey. There's not a lot to be gained by going negative. It may offer short-term effectiveness in political campaigning, but in the long term the environment is made bitter, toxic. Taking the high ground seems to work for both of these audiences.

In this next section we explored where each party felt investments were headed. We gave a list of possible solution areas to each audience, but also offered the responders the ability to identify their own choices. We did discover some dissonance, but nothing extreme.

We asked the IT security folks where they were actively planning to invest. The overall picture presents a sanguine investment picture that should excite anyone marketing or selling IT security solution; many items were on the shopping lists of the IT security buyers. Leading these, by far, were data loss prevention solutions and "threat defense/anti-hacking" tools. Also receiving multiple votes was "data encryption", "malware protection" and "IAM" (identity and access management) tools.

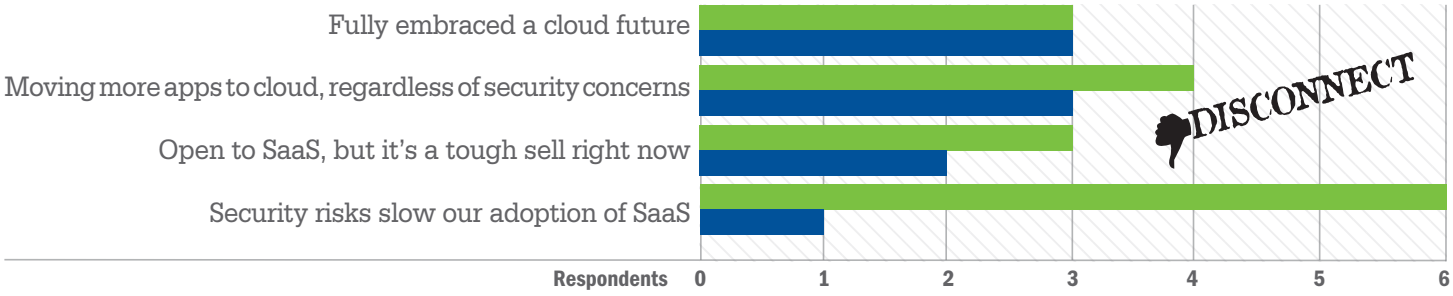
The marketers were asked a slightly different question: "Which of the following is currently the hottest security solution planned?" The marketers correctly saw the "threat defense/anti-hacking" tools emerging, and perhaps the data loss prevention solutions, but did not identify the areas IT buyers cited as critical. They also seemed to miss the market's interest in the solutions that had to be "written in" such as the IAM and malware solutions. Interestingly, none wrote in their own choices, and seemed satisfied with the answers provided to them.

Marketers: In which of the following solution areas are you actively planning to invest?
IT Executives: Which of the following is currently the hottest security solution planned?



*Both Marketers and IT Executives wrote in their own categories

Marketers: What is your opinion regarding security and cloud-based solutions?
IT Executives: How do IT executives regard security and cloud-based solutions?



The next question acts almost as a bit of a "control" as it—or a variation of it—is asked on many, many technology surveys deployed by SimplyDIRECT. So perhaps we were doing less probing into the mind of the test subjects, and we were more interested in their differences. And, yes, those differences were revealed.

Given the absolutely irreversible presence of SaaS-based or cloud-based solutions, we asked the participants' opinion of these new IT vehicle. We asked the IT executives their opinion regarding security and cloud-based solutions.

We knew the trends: security concerns slow the adoption of SaaS and this was, indeed, the overwhelming selection. Interestingly, about 70% of the IT executives seemed open to using, or at least trying this technology. Indeed, almost 50% said they were fully embracing "the cloud" or were moving there despite the known security risks. Only about 25% admitted that security concerns really held their organization back from using more cloud-based solutions.

The marketers had a much more rosy outlook on the cloud. When we asked the marketers, "How do IT executives regard security and cloud-based solutions?" to them it looked all rainbows and unicorns. They expected the IT security professionals to go whole hog into a SaaS world, and a real minority—about 20%—expressed security concerns as serious inhibitors to cloud adoption. Could this reflect the optimism of an audience that is dazzled by the advantages, and does have to clean up the mess when security vulnerabilities are introduced? Marty McFly prefers to jump into the DeLorean and hope that Doc Brown fixes those little time travel issues.

The final question was designed to speak directly to those selling security solutions, those further down the food chain from the marketers, closer to the buyer, where the rubber meets the road. We asked the question in such a way that it wasn't at all ambiguous or hypothetical. We asked the marketers, "What do IT security professionals avoid most?" and we asked the IT security professionals, "What advice would you give security salespeople?" The answers offered to both audiences illuminated what we were getting at (though, admittedly, there were some liberties used to try to square the two questions to each other).

Interestingly, there was a strong synchronic agreement between the two teams. Both were in agreement that "overstating or exaggerating capabilities, ROI and payback periods" was the biggest turnoff. Here we see something that was alluded to earlier. Stay positive. Take the high ground. Talk about your strengths, not the other guy's weaknesses. Other common elements resonated with this and received significant selection. Avoid trashing the competition. Know your product. Research the situation.

On this last point, the IT folks gave it their second highest rating. "Take the time to fully understand my situation." Hmmm. Where have we heard this before?

Remember at the beginning of the survey we asked what triggered an IT security team to review its security solutions? We learned that if a company was reviewing or updating its overall infrastructure, it was likely that they would be open to hearing about new and better security tools. You find out by asking. You become an informed seller. This is lost on so many in sales and marketing.

These are not impulse items. These are serious IT security solutions that play a critical role in not only a company's IT infrastructure but often in its business, its reputation. Blasting out a message that it will whiten your teeth or give you better gas mileage is consumer marketing, playing on impulse. B-to-B marketing is a sober, serious endeavor and you better know your audience if you're going to compete and close deals. What we're hearing multiple times in this exercise is that woe to the marketer who makes assumptions about his or her market or buyer. Even overworked, overstressed, techie security executives will take the time to listen to a good pitch, but it has to be calibrated to their needs, their very specific needs. Shaping a pitch—or basing targeting decisions—on assumptions will leave the marketer vulnerable to a better competitor, just as the IT security executive can't leave the door open to a hacker or scam attack. Your best defense is going with intelligence, not hope or assumptions.