January, 2012

The Quarterly

Issue Number 1

Analysis, snark, and updates for the vendor community

In this Issue:

MARKETING FUD SURVEY

What a small sample set of users told us they like, and don't like, in press releases.

RSA DOS AND DON'TS

How best to prep and work with analysts at the biggest show of the year.

GOOD/BAD SECURITY MARKETING

The top marketing collateral we see.

USER TRENDS

The latest questions from our user community.

Hello World

Welcome to our inaugural vendor newsletter. This is where we talk about all the things we see during the course of our daily research. Trends, analysis, data, and whatever we think will help you -- at least the stuff we can share! As industry analysts we see the good, bad, and ugly of everything from pitches, collateral, and messaging, to how products are used and abused in the field. Our goal for these pages is to highlight what works, what doesn't, and give you insight into what we're seeing out there, including the latest trends and data. Sometimes we will use this space to call out folks, but all in good fun — and always with the goal of educating everyone about what we think works. We'll also highlight good stuff when we see it — don't worry... this won't be all snark.

Speaking of what works... we put together a little survey to try to isolate what kind of marketing materials work to educate your prospects about the problem your company solves and why your product is better. Some of the answers are predictable; others aren't. So check out our analysis, which might impact your marketing plans. Right before the RSA conference. Yeah, you're welcome.

After that we added a short checklist of Dos and Don'ts for your RSA analyst interactions. We thought it might help to get an idea of what happens on our side of the event, what tends to work, and what doesn't work at all during the madness that is RSAC.

Finally, we poke fun at some of the worst examples of security marketing we have seen recently. To be balanced (because that's how we roll), we also give kudos to a campaign or two we thought resonated well.

Our goal is to produce a newsletter for our vendor retainer clients on a quarterly basis. Let us know what you think of this one — good, bad, and ugly. If this doesn't offer any value we don't want to waste your time, and we have plenty to keep us occupied.

The (Almost) Definitive Security Marketing FUD Survey

FUD

A key security marketing tactic remains educating the market and using value-added information to stay in front of potential buyers. But there are many ways to do that, and it seems that most of the materials pushed out to security buyers tend to stoke the furnace of Fear, Uncertainty, and Doubt (FUD). Since Mike has spent years in the trenches — trying to position products and services, bring them to market, and ultimately persuade customers to write checks, he decided to categorize the different types of FUD we see.

Image by Mark Strozier - http://flic.kr/p/urBo

After defining FUD, it made sense to ask real buyers what works for them and what doesn't. So that's what we did with our FUD survey. In terms of full disclosure, a few folks pointed out bias inherent to some questions, and we accept that characterization. All the same, we think the results of the survey are both telling and predictable. We also had a limited data set (36 respondents), so you draw conclusions from this data at your own risk. We won't pretend it's even close to scientific.

Digging into the Data

Any specific marketing content is focused on helping to accelerate the sales cycle and increase the chance of closing the deal. But different kinds of content are more appropriate for different stages in the sales cycle. Let's look at three possible outcomes of these marketing tactics:

Educate Management — This is typically an early step in the sales cycle: educating prospects on what the risks are, how the attacks work, and why it's important.

Sell Project Internally — Here we talk about giving prospects the ammunition they need to convince internal folks that the category of technology you are selling is important. This is a critical sales step, because without that understanding and buy-in there is no project and no sale.

Affect Vendor Selection — At some point in the sales cycle the customer transitions from internal education/evangelizing to figuring out which vendor to choose. Now you need some kind of information to swing the deal your way.

Now let's look at the survey results for each of these areas.

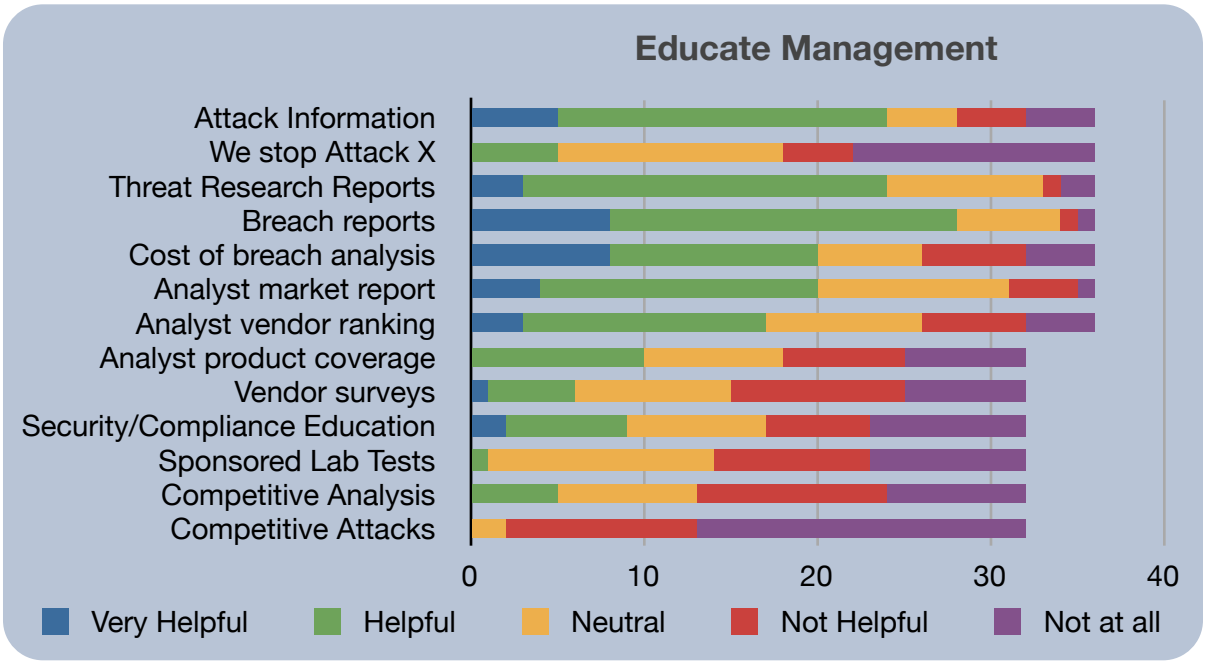
Educate Management

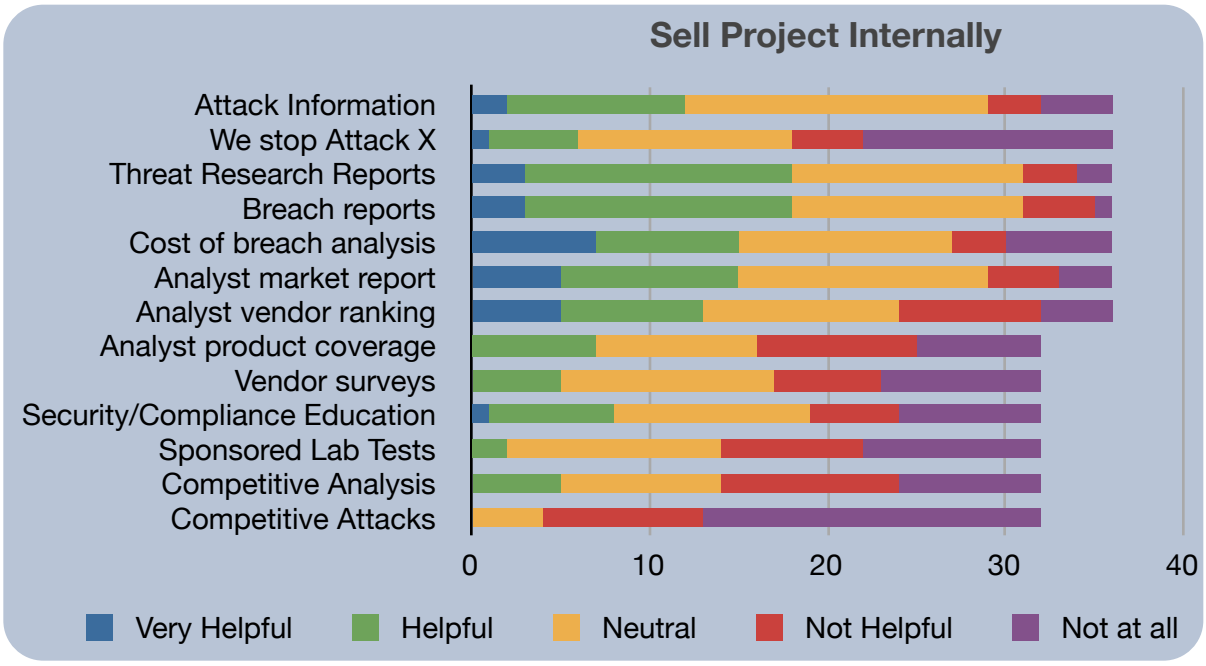
To understand the kinds of marketing tactics we refer to, be sure to read our Categorizing FUD post.

Educating management is less about demand creation and more about making sure champions in the prospect's organization understand the issue and the extent of their problem. For this requirement, we see threat research and breach reports, along with attack information, rise to the top of the interest pile. This is predictable — you need specific data to teach management about the specific issue, and then to position a potential solution. As they say, "an educated customer is the best customer" and this is how to educate them.

Given how important customers think threat research reports are, don't be surprised if your research team starts waving around this newsletter and asking for raises.

Specific information about how your product stops the attack is not useful in this context. These folks need information, not puffery. As easy as it is to just throw in a little about how your product addresses the issue, at this point that is **not** what's called for.





Sell Project Internally

You can see below that Threat Research Reports and Breach Reports have the most impact on creating demand for a specific technology. Cost of Breach Analysis reports and market reports from analysts (like Securosis) also have a favorable impact.

This isn't brain surgery. Folks need objective educational material to convince coworkers to do something. Pointing to an actual breach report, or specific details of an attack, brings the issues to the forefront. It's hard to argue with data that a high percentage of breaches resulted from [attack X]. At that point you need to make sure that [attack X] doesn't happen. And so the bull market for security researchers, who assemble this data and produce these reports.

Interestingly enough vendor surveys have very little impact on ability to sell the project. Given the number of these tools we see every week, it sure looks like a significant amount of money is being wasted. Though folks like Larry Ponemon may not be agree.

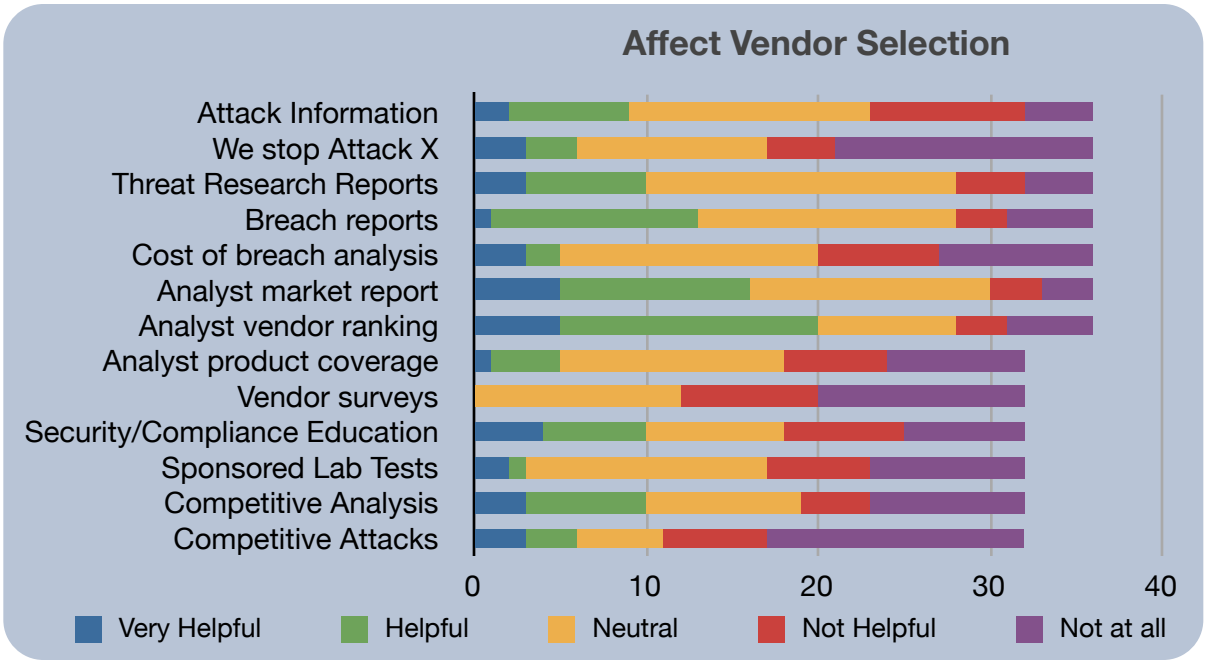
Affect Vendor Selection

Once the project is moving forward, how can you ensure you make the short list and ultimately win? Much of your success has to do with sales execution but that's another story for another day. If we are talking only about marketing content, we can see that the analyst ranking charts are most effective. Also not surprising.

But we will take this opportunity to discuss the two types of prospects that use magic charts to select vendors. There are the smart ones, who know what they want to buy and use the chart to justify their choice. And also the lazy ones, who use the it to define their short list. Both can be major factors, but it means most vendors will continue to focus on showing up well on the chart, sometimes instead of on solving the customer's emerging problems.

Surprisingly, analyst market reports are also regarded as helpful here, but they are generally vendor-neutral — at least the way we write ours. So that question was probably worded poorly. And note that sponsored lab tests and competitive attack documents tend not to go over well. Clearly 2nd (or 3rd) tier vendors need to figure out a way to get into the discussion, but savvy users can't stand these tactics.

Again, we think this survey does a decent job of telling you what you already know. Customers want solid information they can use to push projects forward. Not vendor puffery about how great you are or how bad the competitors are, or surveys trying to make you feel guilty if you don't seem to be worried about the same issues everyone else is.



RSA Analyst Dos

RSA is one of the best times of year to get face time with customers, prospects, press, and those pesky industry analysts. It's also a batsh crazy time for everyone involved, and having spent countless hours at RSA and other conferences, we have found major differences in what works and what doesn't. Here's a list of what works and what doesn't.**

- Wait until the RSA schedule is released before trying to confirm meetings. Many analysts can't confirm anything until they know when they are speaking at the conference.
- Schedule meetings a minimum of a month out. This seems obvious but every year we get requests the week before. Our calendars are usually pretty much locked down a month out. So even if we *want* to meet with you (and yes, we say that to all the vendors), the odds are we won't have a slot.
- Know your analyst. Cold calls to someone you have never talked to aren't a good idea, especially when time is so constrained. We won't take those meetings so let's not waste each other's time.
- Either have a conversation or present info we can't get over the phone. Demos are usually good. Arrange product briefings over the phone ahead of time, and **DO NOT** repeat information from the briefing in the meeting proper. RSA is about maximizing the value of face time — not wasting time rehashing phone briefings.
- Be flexible — everyone is 5.8 minutes late for everything because we schedule back to back meetings just like you do, except we have to run from booth to booth (Moscone seriously needs underground GPS).
- Have coffee meetings by the show floor unless you have a private room in your booth. Or schedule a press room.
- Set a very obvious meeting place that's easy to find among 10,000 friends, especially if we've never met in person. Google images of any of us, and you can see how pretty we are. Most analysts have a photo posted somewhere. FYI, we are the guys who wear the cool Securosis bowling shirts.
- If you have an offsite meeting area (hotel), **tell the analyst when you set up the meeting**, and be extra flexible with scheduling so the analyst can get there. We have worked up serious sweats trying to find those meetings when we didn't notice the off-site location during the scheduling process.
- Ask the analyst ahead of time if there's anything specific they want or need to see. Make sure you can answer those questions. Nothing is more frustrating than having the wrong folks at a meeting, forcing us all to chat about the weather for 45 minutes.
- Use the time to meet face to face, especially if we have spoken on the phone before. The real value of these meetings is in getting to meet, continuing discussions, and having a good back-and-forth. We see industry analysis as a relationship business, and RSA is a great opportunity to make and solidify those relationships.
- If you are a client of the firm/analyst, use the time to get feedback about what you are doing well, and perhaps not so well. There is nothing like taking a beating in person, but they are usually useful and better than doing it in public.
- Include an on-site contact number and email address for scheduling issues.
- **Attend the Securosis Disaster Recovery Breakfast**, Thursday morning at Jillian's. Then taunt us for marketing. our own event.

RSA Analyst Don'ts

Photo by Tomi Tapio - http://flic.kr/p/8F8azb

- Brief us on product details. If you use an RSA slot for an analyst briefing you waste everyone's time. We may nod our heads, but inside we're going, "WTF? We could have done this over the phone." Or we might blast you into outer space, which is unpleasant for everyone.
- Whip out the same slides you use all day for every prospect, customer, reporter, and analyst. We'd much rather just talk, even if you slides are really really pretty.
- Make the analyst watch your marketing video. (Special note — this one is for our own Mike Rothman, who starred in a ... video... a few years ago when he was a CMO. And yes, he had his pants on.)
- Ask the analyst what they've seen that's new, interesting, or cool. Nothing is new, interesting, or cool after even 5 minutes of the cacophony of that show floor.

The goal is to get the most value out of that face time. Wasting your slot on a regular briefing doesn't help anyone. The best meetings we have tend to be casual discussions, demos of new stuff that's hard to show over a call, detailed conversations about product roadmaps, or meeting people — execs, product managers, and other people we might only know as voices from group calls.

Security Marketing Good & Bad Practices

Photo by Profound Whatever - http://flic.kr/p/8UgrLv

Here we will share some of what we think are good practices, with examples. We will also poke things we think are not-so-good. Mostly puffery, pontification, and other activities that don't help customers solve problems.

The Good: Breach Reports

As we discussed regarding the FUD Survey data, customers get great value from breach reports. Details about what security controls didn't work, and resulted in a breach, is gold for many customers. A great example of this is Verizon Business's Data Breach Investigations Report. It's more of an event now, and it's great. Customers refer to it all the time to make internal cases for initiatives and projects. The press loves it because the report provides sound bites and detail that aren't available anywhere else.

Vendors who do this well get back a multiple of their investment in terms of awareness, visibility, and value — delivered to prospects and the industry at large. From where we sit that's a good practice.

The Bad: Success Releases

One of the end-of-quarter rituals at most start-ups is the "success release." That's where a private company lists their accomplishments for the quarter in an attempt to show momentum and to feel good about themselves. This is a great example of marketing to your competition rather than to your customers. I guarantee your customers don't care whether your company showed 60% growth. Have they deployed the product, or is it sitting on a shelf?

Marketers are paid to manipulate facts into favorable stories. **Just because you can doesn't mean you should.** A success release will not swing deals your way, and it's not going to grab the interest of potential sales reps or channel partners who want to associate with a winner. If anything, it will just turn off folks who recognize the puffery. If you are going to write one (which you shouldn't — in case we weren't clear), at least provide some detail. Like AlertLogic is specific about their billing run rate and they are private. Kudos to them. Saying you grew 120% without the context of the revenue base is useless. You could have gone from $200K in revenue to $240K. That's huge growth, eh? To sum up: if you have to talk about how fast you are growing you aren't growing that fast.

More Bad: Year-End Predictions

We get your need to show thought leadership in whatever space you play in. CTOs around the globe evidently have nothing better to do than go through the idiotic ritual of telling everyone what's going to happen over the next 12 months. The only thing we can be sure of is that they are all wrong. If we could actually predict anything like that we wouldn't be doing security, that's for sure. We would be doing stock market arbitrage.

These predictions always break down into a few categories:

- Our product category will break out. No kidding. What CTO will say, "it's still another 3-4 years before my stuff becomes important?" I'm sure their investors would love that. So every company says their product is poised to become mainstream. It's not.
- Compliance is important or attacks will increase. Really? These trivial statements don't show anything beyond an ability to state the obvious.

If you want to showing thought leadership, actually **do** something innovative and talk about customer success. Talking about a potential problem doesn't compel the market to solve it. We get self-fulfilling prophesy, but the world doesn't work like that.

Just 3

1. **The best marketing shows someone how you help them get their job done better and solve their problems.**
2. **Never predict breaches or risks — you are always wrong until you're right, and it's the worst kind of FUD.**
3. **Focus on what you do well, not FUD or what others do poorly. Stay classy.**

User Trends

As we build out our Nexus platform (nexus.securosis.com) this section of our newsletter will include anonymized analytics on what people are researching and asking questions about. We will never provide anything that could possibly identify a user, but we will include generic stats and anonymized questions.

The Securosis Nexus is currently in beta testing so we only have limited data at this time, but we want to highlight some of the questions we have gotten from the community.

Questions and Answers

Question

Hi, I want to pick one indicator to give me an idea how well our patch management practices are. I thought something like "Percentage of machines that have all required patches that have a release date older then X implemented". (The X is just because we give a certain window for patch implementation). To me that looked reasonable, but I'm now questioning myself since I found a similar report in a leading Vulnerability Management tool that we are using. Actually I didn't find any useful report that would give me an indication of how we are performing. Any suggestions? Should I consider something else? Am I on the right track and should I stick with the idea and work on developing a custom report?

Response

Rich wrote:

I suggest two metrics: one to measure efficiency, the other to measure effectiveness. For efficiency measure the time to patch after an advisory/patch is released. This shows you how well you can get a patch out. For effectiveness, measure the percentage of systems patched within x time period. This shows you how well you patch, and you can sometimes pull this from your vulnerability scanning software vs. your patch software since it is a more accurate representation.

Question

What is the definition of a Disaster in the context to BCP, DR? Looked at the relevant ISO standard but couldn't find a definition for "Disaster".

Response

Mike wrote:

The definition I use is "anything that disrupts normal operations and requires a dedicated response". I realize that isn't necessarily what "standards" use, but I've found it to be far more pragmatic. Another way of wording it might be "any disruption to service that cannot be recovered with normal operations". In other words — anything that causes an availability or integrity issue that can't be fixed without using your DR/BCP plan. I know it's circular, but that's simpler than some of the more complex stuff I've seen.

Question

How can I classify dynamic content? For example, unified communication sessions, web-site page creation, and more.

Response

Adrian wrote:

It depends on where the content is located, but usually you will need to use some sort of Data Loss Prevention tool (DLP). I'm actually writing out the DLP module right now, although it probably won't be ready until next week.

For communications, you can't "classify" them as they are streaming back and forth. Are you referring to tagging the logs, or identifying sensitive content within something like a chat/IM session? If so, some DLP tools support analysis of in-progress chat sessions and can generate alerts based on something like a credit card number appearing inside.

For web pages, you could point a DLP content discovery tool at any stored static pages. Again, if you give me more detail I can probably get you a more specific answer.

Rich escaping from China (photo courtesy Chris Hoff)

Mining Nexus Data

We won't release anything that could ever compromise the privacy of a Nexus user, but we do plan on aggregating data to identify trends and areas where we need to focus our research.

Our plan is to make this available to our clients both in and out of the Nexus to help you better understand what your peers or audience are most interested in. The data will include what research people are using, what questions they are asking (again, totally anonymized), and other feedback, even including the quality of our research.

We think this will be a tad more useful than paper download counts and web page hits.

Upcoming Research

This is a list of some of the work we have coming up this quarter. Some of these are open for external involvement/sponsorship, but others are already sold or not open. We just want to keep you all informed on what we are up to.

Visit the new Research page.

It only took 5 years, but we have finally built a page with every paper we've written.

You can find it at https://securosis.com/research/research-reports

We will keep this up to date so there's never any question of where to find a paper.

And someday maybe we'll even finish posting all our presentations and other content. We promise.

- **The Securosis Nexus soft launch in Q1.**
- **Deploying and Implementing a Data Loss Prevention Solution.** This paper continues where Understanding and Selecting a DLP Solution finishes. Launch at RSA.
- **Log Management is Not Dead!** We are seeing a bifurcation where fully functional security management platforms evolve to address advanced security use cases, and many organizations without the need for advanced security analysis will retrench on log management, not only to solve security and compliance needs, but also to address a number of other use cases leveraging log data.
- **Data Security for Cloud Computing.** This will be an in-depth co-branded paper with the Cloud Security Alliance. We are writing a master paper, which we will also break out into smaller pieces for better distribution.
- **Vulnerability Management Evolution.** Amazingly enough, we have never really documented our thoughts on how vulnerability management evolves and how it fits into the security ecosystem. What used to be scanners are now more fully functional assessment platforms, and it's time to help our readers understand how this will affect them.

- **Data Security Survey v2:** We are considering running another version of our Data Security Survey. This is a ton of work so we will only do it if we see enough interest. You can see the 2010 version at https://securosis.com/research/publication/the-securosis-2010-data-security-survey. Aside from fixing a couple survey errors, the questions will remain the same so we can do some really nice comparisons.
- **Certification of Cloud Security Knowledge (CCSK):** We are in the process of updating the Cloud Security Alliance CCSK training class to align with version 3.0 of the CSA Guidance. Our timeline is to update the class over the summer. We will also launch a CCSK Remote class, for those who cannot attend a live training session. Look for that to launch in February.

About Us

Securosis, LLC is an independent research and analysis firm dedicated to thought leadership, objectivity, and transparency. Our analysts have all held executive level positions and are dedicated to providing high-value, pragmatic advisory services.

- Primary research publishing: We currently release the vast majority of our research for free through our blog, and archive it in our Research Library. Most of these research documents can be sponsored for distribution on an annual basis. All published materials and presentations meet our strict objectivity requirements and follow our Totally Transparent Research policy.
- Research products and strategic advisory services for end users: Securosis will introduce a line of research products and inquiry-based subscription services designed to assist end user organizations in accelerating project and program success. Additional advisory projects are also available, including product selection assistance, technology and architecture strategy, education, security management evaluation, and risk assessment.
- Retainer services for vendors: Although we will accept briefings from anyone, some vendors opt for a tighter, ongoing relationship. We offer a number of flexible retainer packages. Example services available as part of a retainer package include market and product analysis and strategy, technology guidance, product evaluations, and merger and acquisition assessments. Even with paid clients we maintain our strict objectivity and confidentiality requirements. More information on our retainer services (PDF) is available.
- External speaking and editorial: Securosis analysts frequently speak at industry events, give online presentations, and write and speak for a variety of publications and media.
- Other expert services: Securosis analysts are available for other services as well, including Strategic Advisory Days, Strategy Consulting engagements, and Investor Services. These services tend to be customized to meet a client's specific requirements.

Securosis Quarterly
Issue 1.0

Securosis LLC

515 E. Carefree Highway
Suite 766
Phoenix, AZ 85085

Securosis

Awesomesauce

We know we're damn lucky to have our jobs and opportunities. We aren't a billion-dollar company with thousands of employees — we're just three partners with a few of our friends helping out when they can, all trying to bring a little value to the world. We get to write the research we want, give most of it away for free, and participate in the security community without worrying about corporate overlords watching over our shoulders. For that we thank you.

Adrian, Mike, and Rich