Securosis

Welcome to the RSA Conference Guide 2016

It's a bit hard to believe, but our little Securosis Guide to the RSA Conference turns 7 this year. And the RSA Conference folks are throwing our guide a party, with tens of thousands of their closest friends. Oh, how quickly our children grow! It seems only yesterday we were talking about cloud, APT, and compliance as the hot new trends you'd see at the show.

Huh. Maybe the security industry changes... not all that fast.

For those of you new to this guide (The RSAC-G for short, because as security weenies we have to use acronyms, and we're non-conformists so they can't be three letters), it's when the Securosis analyst team steps back and... oh heck, let's just flash back from last year to catch everyone up.

"The RSA Conference is the single biggest event in our industry. Love it or hate it, there is no better place to put your thumb on the security industry and get a sense of where things have been and where they are headed. But navigating such a large event and filtering out all the BS only gets harder as the event continues to grow. The goal of this RSAC-G is to help you better plan for, and take advantage of, the event.

Over the years we've learned that RSAC, not December 31, is the best time to take stock of the security year. It's the delineating event that many vendors plan their entire marketing cycles around. So this guide has evolved from a simple overview of a conference to an in-depth annual review of our industry. At least that's what our enormous egos tell us."

In previous years the RSAC-G followed a consistent format. An overview of top-level trends and themes you would see at the show, a deep dive into our coverage areas, and a breakout of what's on the show floor. We decided to change things up this year.

KEY THEMES
See what the Securosis folks think will (and won't) be the talk of the show this year.

SECUROSIS PROJECT ACCELERATORS
Learn about our new cloud security workshop offerings.

COVERAGE AREA DEEP DIVES
A deeper dive into each of our subject areas.

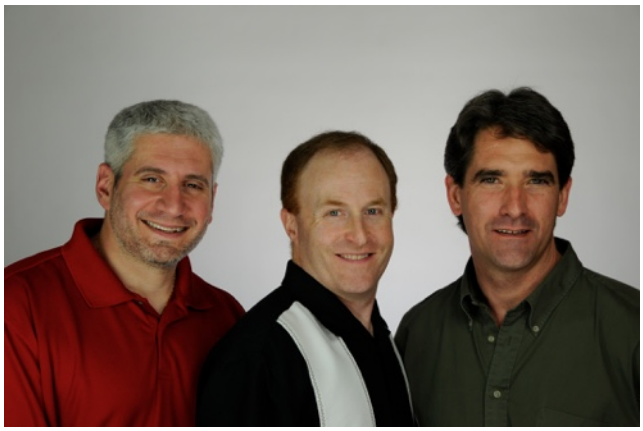
DISASTER RECOVERY BREAKFAST
Of course we are hosting breakfast again. Duh!

WHERE TO SEE US
Where you can see us speak, hang, and/or drink at the show.

NO BULL Research

The conference has grown enough that our old format doesn't make as much sense. And we are in the middle of shaking up the company, so we might as well update the RSAC-G while we're at it.

This year we'll still highlight main themes, which often set the tone for the rest of the security presentations and marketing you see throughout the year. But instead of deep dives into our coverage areas, we are focusing on projects and problems we see many clients tackling. When you go to a conference like RSA, it isn't really to learn about technology for technology's sake—you are there to learn how to solve (or at least manage) particular problems and projects.



This picture is ancient. Since before we started writing the RSA Guide. We look older now. Pretty much because we are older now. And security...

This year our deep dives are structured around the security problems and projects we see topping priority lists at most organizations. Some are old favorites, and others are just hitting the radar for some of you. We hope the new structure is a bit more practical. We want you able to pop open the Guide, find something at the top of your list, jump into that section, and know where to focus your time.

Because let's be honest—FUD and misdirection in the security industry are hitting epic new levels, exactly when we really need clarity and honesty. It is, frankly, embarrassing. But it isn't also about to change—just look at all the advertisements for 'traditional' home security involving ski masks and broken windows.

Don't buy the hype, and don't let some lazy marketing tempt you over to the Dark Side of budget black holes and new tools with conveniently located exhaust ports (right below the main ports). Know the issues you need to fix, find tools to help, and don't expect any magic hydrospanners to solve them for you.

Okay, it is possible we watched the new Star Wars a few too many times.

As always, we'd like to thank all our Contributing Analysts who pitch in on this massive project every year: David Mortman, James Arlen, Dave Lewis, and Jennifer Minella—and our ever-vigilant editor, Chris Pepper. And this year we'd like to thank the RSA Conference team for, once again, taking such a big risk in letting a bunch of snarky analysts post whatever we want on their official site.

Rich, Mike, and Adrian

Key Themes

How many times have you shown up at the RSA Conference to see the hype machine fully engaged on a topic or two? Can you remember before the APT was a thing? Yeah, we can't either. And now everything is rushing to the cloud. Or is it? So what will be the news of the show this year? Here is a quick list of some key topics that will likely be top of mind at RSAC, along with why you should care.

Every year we like to start the RSAC Guide with a review of major themes you will most likely see woven through presentations and marketing materials on the show floor. These themes are a bit like channel-surfing late-night TV — the words and images themselves illustrate our collective psychology more than particular needs. It is easy to get excited about the latest sequel to your favorite movie series, and all too easy to be pulled along by the constant media frenzy, but in the end what matters **to you**? What is the reality behind the hype? Is it all nonsense designed to extract your limited financial resources and even more limited attention? How can you glean useful nuggets from the constant noise?

Given that Rich is all Star Wars, all the time; we figured it would be cool to see if we could add a Star Wars angle to all of the key themes. It works pretty well, unless you don't like Star Wars. Then you'll hate it. Which is OK. Actually it's not OK. What kind of person reading an RSA Conference Guide doesn't like Star Wars?

Threat Intelligence and Bothan Spies

One of the overarching themes we have driven ourselves into a frenzy over is the need for threat intelligence. On the analyst side, we are constantly taking briefings from new threat intel vendors claiming to be the next big thing, but we really cannot tell the difference between them. We even have a nifty acronym, "YATIV" (Yet Another Threat Intel Vendor). On the upside, they're still outnumbered by all the security analytics clones, which we'll get to later.

In keeping with our geeky Star Wars theme, the essential questions when looking at these providers are: do you know how many Bothan spies actually died to bring you this information? What are you actually paying for in the end? Is your vendor force-choking you for a paycheck? In other words, does this data actually help you make security decisions which will stop some farm boy from wrecking your (small) moon-sized investments?

When the escape pod jettisoned with the droids on board they weren't blasted by the Imperial troops. As a result the plans for the Death Star ultimately fell into rebel hands. That was really the type of information the Empire could have have used to make better decisions. You almost have to wonder if Family Guy was onto something with the lines, "'Hold your fire'? What, are we paying by the laser now?" "You don't do the budget, Terry, I do!" Are you receiving valuable information from your threat intelligence vendor? Does it even come close to the level of what the Bothans managed to

deliver? Or are you paying for intelligence about the possible threat posed by the bounty hunter Boba Fett, while he is already lodged in the gullet of the Sarlacc? You need to peel back the layers of fear, uncertainty, and doubt to reach the meat.

H/T to Rick Holland

Ask tough questions, and don't believe the answers.

Take into account the cautionary tale of the threat intelligence vendor, Norse, who recently imploded in such spectacular fashion that even Industrial Light and Magic was jealous. Norse was known for an animated threat intelligence map that, well, let's be honest... really had zero value. The "pew pew" map would show animated attacks blasting all around the tubes of the Internet. But did it ever provide you anything remotely actionable? No, I didn't think so. It was a photogenic gimmick.

You need to understand that threat intelligence is not as simple as plugging it in and flipping a switch. These products are new and evolving. The data is only really useful if an analyst can make use of the data as provided. More isn't always better—just ask Jabba.

When the rebels got their hands on the plans for the Death Star they found a weakness. Not simply because they had the data, but because they were able to properly analyze it. Are you able to find the thermal exhaust port with your threat intelligence?

You have to wonder: is that information that you paid top dollar for really the work of Bothans?

May The Norse (Not) Be With You.

(Dave Lewis)

R2DevOps

If cloud is a new operational model (spoiler, it totally is), DevOps is the operational framework to fit it. Automation and standardization is awesome, but do you want an R2 working for you or a Battle Droid that's as likely to blast your Separatist envoy as the clone troopers in front of it?

DevOps has been around for five years now and in the last year or so has really started to gain traction in the security space. On the show floor this year, you'll hear terms like as DevOpsSec, DevSecOps, SecDevOps, and even Rugged DevOps (for the socially divergent). But before buying yet more software and yet more blinky boxes, you have to ask yourself: "Are these the droids I'm looking for?" Be wary, a lot of what you'll see won't actually be anything new, but rather just clones of an older generation from the old guard of the traditional security empire (I mean enterprise) players.

As regular readers of the blog know, we're big fans of both DevOps and security here at Securosis and strongly believe that DevOps is the new republic for technology. But the technology around DevOps is still in its infancy and suffers from all of the same security problems that any other set of technology does, especially those in the early stages. So when talking, take what you hear with a grain of salt, especially when it comes to API security and as always, IAM and like any technology that allows

you to centralize control, be extra careful with understanding your attack surface. Don't let your new technology become the exhaust port for your organization.

DevOps isn't even a single set of technologies. It's as much a philosophy and operating framework as anything else (which means we probably should have gone with a Force reference instead for this bit, but anyway). It's a combination of culture, philosophy, techniques, and tools that has some standard tenants, but definitely no single way of doing things. R2D2, Chopper, and BB-8 all have unique strengths, weaknesses, and personalities, and they all get the job done in their own way.

It's good to be skeptical, but these techniques are far from science fiction. Many of your peer organizations, be it large or small, are using DevOps today to good effect. Heck, the odds are high you already have projects leveraging DevOps, even if you don't know about it. And DevOps is a massive boon for security, bringing a level of standardization and audit trails we've only dreamed about. Plus, we can leverage the same philosophy, tools, and techniques to improve our own security operations.

Once you are on the RSA show floor, the FUD will be strong! Vendors trying to link all the wonderful things DevOps can deliver with their (not necessarily) so wonderful products. Some tools and products fit really well, while others will disrupt the DevOps process, slow down those deployment pipelines, and just drive your teams to find yet another friggin' exhaust port. Look for products that support automation through REST APIs, Jenkins plugins, and SDKs. Look for sessions with technical meat on integrating with DevOps initiatives, not ones that hype up the risk.

(David Mortman, Adrian Lane and Rich Mogull)

Escape from Cloud City

Cloud computing has been a pretty steady theme in both this RSAC Guide and the conference itself. Heck, it was our very first theme in our very first Guide back in 2010, and has shown up as a theme every year since. As much as we'd love to move past it to something "new" we strongly suspect you will see more cloud, not less, this year. Besides, while we eagerly anticipate the impending emergence of portable Fitbit firewalls, we really aren't looking forward to the competitive analysis charts as they battle automobile combination firewalls and breathalyzer interlocks for budget.

Oh please, you know they're coming.

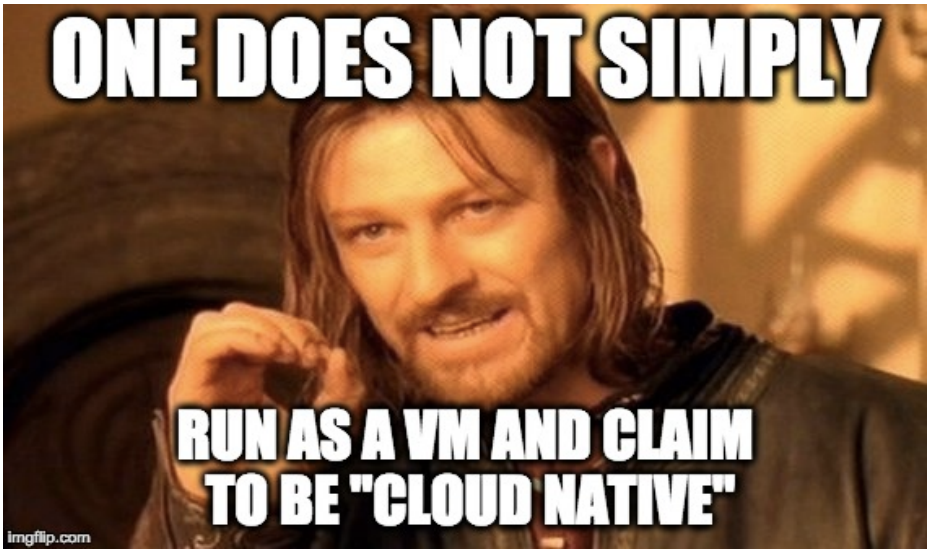
Cloud security is right about at that point on Bespin where C3PO disappears, Lando is smiling too much, and that dinner invitation showed up on suspiciously black stationary with the Imperial logo covered up with a marker. It looks great on the surface, but underneath something just doesn't feel right.

In past years, the conference sessions haven't always been overly strong; with too many people shouting "WARNING! CLOUD! DANGER!" without telling you what to do about it. Vendors wrote "cloud ready" on their marketing banners with a sharpie and kind of left it at that. In the meantime, cloud capabilities, including security capabilities, evolve so quickly that this year alone on three occasions major security features appeared overnight in the middle of one of our two-day training classes or client engagements.

The problem isn't the ridiculous rate of change in cloud computing, but that we still see that security professionals are behind the curve on working natively with cloud computing platforms. This isn't a criticism, it simply takes time. It requires a new skills set while retaining and converting the knowledge and experience many of you have spent decades building. That doesn't happen overnight. It also isn't limited to security, we see traditional ops and even dev experiencing the same struggles.

But just as Luke had to make the judgment call and abandon his training with Yoda to go try and save his friends (and hopefully not make out with his sister again), vendors are desperately throwing their products into the mix as security teams jump into projects and learn on the fly.

Like Lando's slick smile and hug, everything looks good on the surface, but underneath all is not right in Cloud City. Few products are both cloud native and ready for native cloud architectures. There is a massive difference between running a virtual machine on a cloud provider and improving the security of a micro-services architecture deployed in Docker containers and using various PaaS products. Sign a multi-year contract and you might find the deal changes, and you're told to pray they don't alter it any further. There are some good cloud-native tools out there, you just need to find a needle in a pile of Bantha fodder.



The good news? The Cloud and Virtualization track this year is chock-full of (potentially) strong sessions. It's the strongest looking agenda since the track was created, and we aren't just saying that because we are speaking. Easily half or more of the sessions are technical, practical, and being delivered by people we know have real, on-the-ground experience.

It's a great time to trust your instincts, feel the cloud flowing around and through you, and start seeing how the cloud can improve security. Cloud providers offer more for security than you might think, and in some cases can wipe out

traditional security problems or the need for third party products. This is probably the best year at the RSA Conference to improve your cloud skills, save your organization, and not lose a hand in the process.

(Rich Mogull)

The Beginning of the End(point) for the Empire

For as long as we can remember, computer devices have been "protected" by the Evil Empire of Endpoint Protection. This Empire is made up of many companies that all rely on the same technology, deploying their agents on every device to stop attacks by keeping a very large list of bad stuff and looking for that bad stuff every time the device takes an action.

This approach is pretty resource intensive, forcing the Empire to build an army of clones to keep pace with the exploding number of attacks. This plays right into their hands because one of the biggest members of the Empire makes most of their money by selling faster chips to the other planets every 18 months.

Given how dissatisfied everyone is with the draconian way of the Empire, Resistance has emerged through the years. First it came in the form of the free people, offering up protection without cost. Of course, this seemed too good to be true and it was. It turns out these free people turned to the Dark Side and started charging to manage all of their "free" agents.

Taking no chances, the Empire stood up a phony compliance organization called the PCI Standards Council, which mandated the use of old, ineffective technology provided by the Empire. Yet, the status quo remains ineffective. Devices continue to be compromised and citizens feel slighted. Their Governments become very irritated when they have to write a check for "protection" to the Empire.

Now there is a New Hope on the horizon. It comes in the form of advanced threat agents, which promise to protect these devices against advanced attacks. This resistance positioned as a complimentary solution to the Empire. They didn't want to displace the Empire, rather make it work a little better.

The Empire didn't take the threat seriously, since they haven't innovated in close to a decade. Rather choosing to milk each planet of its natural resources without providing additional value.

But at this year's RSA Conference we expect it'll be very apparent that the days of the Empire are numbered. You see, the Resistance is a lot closer to being ready for prime time. They have built tools to provide better protection for the same price. They have tools to migrate the planets away from the Empire and to the Resistance. They have the ability to forensically investigate attacks on the devices, and they can leverage the built-in capabilities of the operating systems to provide disk encryption.

And everyone hates the Empire, so the entire Galaxy wants the Resistance to prevail. And they will, but it may

take a few more years to truly render the Empire lifeless since it wasn't built in a day—and it won't be dismantled in a day either.

Yet, there are factions within the Resistance that worry we are just replacing one Empire with another. That a handful of the Resistance factions will rise in power and provide protection of the First Order. They will build yet another capability to lock in the planets and those that don't renew their contracts will have their stars killed. Will that be better for the citizens of the galaxy?

In the end, there is always an Empire and there is always innovative Resistance. The names change, but the cycles remain the same. Yet given the issues with the existing Empire, getting First Order protection will be a lot better. Until it's not, and then the cycle will start over again.

Which, of course, means more sequels.

(Mike Rothman)

Training Security Jedi

The lack of security Jedi is disturbing. With the evil forces of the Empire running rampant through all of the members of the Republic, there just aren't enough skilled practitioners trained in using the Security Force to keep the attackers at bay.

To be clear, it's not a resources issue. Leaders are willing to invest in training up the next generation of Security Jedi. Forget about finding and bringing on experienced Security Jedi. You need to build out your own Jedi Academy, finding a sufficient number of Padawan to grow into Jedi over the next few years with proper training.

And it's not like the job is getting easier. Adversaries are improving. Technology stacks are getting more complicated. So if anything, the level of skill required is increasing at a dramatic pace.

But here's the thing: Security Jedi are not built in a day. There is no academy where you can send them and they'll emerge a fully-functioning security person. Sure, lots of organizations will portray their programs as focusing on getting security n00bs up and running quickly. But that's crap. Security Jedi are built through experience. Not classrooms.

It takes time for practitioners to have sufficient experience and learn to harness the Force. To learn enough from experience to know how to handle situations under enemy fire. To have screwed enough things up to be able to know what not to do and live to tell the stories. When to act and when to let things play out. You don't learn that in some class or in even at the Jedi Temple in Coruscant.

So what do you do? You have the need for Jedi to protect

your sensitive assets. First, accept that training Padawan to become Security Jedi is your most important responsibility. More important than filling out reports for the CFO. More important than placating assessors. Even more important than cleaning up the mess from John from Finance that keeps clicking on nasty links promising to show pictures of Leia from Jabba's private stash.

Always be recruiting new Padawan. When you go to an event like the RSA Conference, network your behind off. Meet other practitioners. See if they are happy in their job. See if they are open to looking at other opportunities. Sure, you could hire one of the handful of headhunters specializing in security to do that, but guess what every other CISO is doing?

Go to other conferences, especially local security shows. Get involved in organizations like the Cloud Security Alliance that has local meetings. Go meet the interns your company has brought into other technology areas. Find out who are the highest potential IT operations people. See if they think security is cool. Those strong with the Security Force can be found anywhere. But only if you are looking.

Once you have identified a promising Padawan, team them with one of your existing Security Jedi. That's right, one is the Master and the other the Apprentice. To be clear, the Apprentice may have better security skills than the Master. But the Apprentice doesn't know how to get things done in your organization and that's what they need to learn. Remember that being an effective Security Jedi isn't all about technical skills.

Optimally you don't want to overwhelm the Master by having them handle more than one (two max) Apprentice(s). Focus is critical to success. If the Master cannot devote enough of their Force to the Apprentice, the Padawan will struggle and get fed up and leave.

And to be clear, regardless of what you do, a portion of your Security Jedi will leave and go to another galaxy to bring the Force to new places. Be proud of how you've taught them, what they will accomplish and let them go. Others will head to the Dark Side of Consulting. They believe spending years on a TiE-fighter and doing battle with the Sith across the galaxy is cool. Let them go as well.

And keep the cycle going by continuing to find new Security Padawan and training them to be functional Security Jedi. It's not like the forces of the Dark Side are going away.

(Mike Rothman)

Attack of the (Analytics) Clones

Opening Crawl...

"There is unrest in IT security. Thousand of malicious events pass undetected each day, and have overwhelmed the limited capabilities of SIEM to protect the enterprise. These attackers and rogue insiders, motivated by profit and revenge, continue to steal data without fear of detection. In an effort to stem the tide, dozens of companies have created an ARMY OF ANALYTICS TOOLS to assist the overwhelmed SIEM ... they are The Analytics Clones.

End Crawl.

As you wander the halls of Moscone center, you'll be wondering how and where all these little firms offering 'advanced' threat analytics and security insights came from. As if overnight, we got dozens of options to assess threats 'at scale'. To be honest, it really doesn't take that long to strap a visualization plug-in atop a Hadoop cluster and runs basic queries against it. It's a grass-roots solution to a very real security problem.

A lot of security folks are pissed off that their SIEMs don't detect many types of malware or can't discern common attack patterns. There is plenty of event data to be mined, but a lack of storage volume, data types and processing capabilities to take advantage is missing. Or it was until Hadoop and Cassandra and the few dozen analytics modules popped up in the open source community, and was easily transferable to security.

Clearly the sheer number of analytics companies comprise a Clone Army of sorts. From the outside they really all do look alike. A 'big data' cluster for ingestion and analytics. Maybe some cloud-based services to analyze data from multiple sources. Topped off with a shiny animated visualization engine to impress people with big checkbooks and 'Voila!'—a whole new security sub-market appeared.

As a potential buyer how do you differentiate one from the other? We're not sure. Clone troopers get tattoos and call themselves familial names like 'Hevy' and 'Fives' so they can tell themselves apart, but we don't even think Commander Codey could find the real thing. The analytics firms try to differentiate by saying stuff like 'Malware and cyberthreat detection via our patent-pending intelli-smart active-passive dynamic big data analytics and class-leading expert knowledge combined with deep meta-semantic behavioral science—in the cloud—stopping disgruntled rogue hack-fraudsters in their tracks. Especially when they wear black ski masks.' Actually, I made that last bit up. The rest of it is real. **All of it.**

The aggressive attempts at differentiation fail; because when it comes down to it, they still all look and act alike. And they are not getting the job done. In fact, a very real 'rebel alliance' formed by many large enterprises, who were compelled to build their own analytics tools from scratch. The clone army simply didn't deliver what enterprises need, and they still lack much of the customization and integration capabilities to be useful. That's right, the [pew pew pew] laser maps user interfaces only get you so far; sooner or later you need to conjure up the stolen data plans.

And who is funding all these firms? It must be some deep-pocketed inter-galactic banking clan who were Jedi mind-tricked during their diligence process. For example, if you're investing in a startup, surely you checked out the competition and stumbled across 25 or so of them in the field (yes, at least that many—I've set up a dedicated Hadoop cluster to track them)? Just a handful will ever make money before early financing runs out; even a Muun-ian will be heading for the exits if they realized their investment will not pay out, and force-choking your investors into a mezzanine round is not an option.

(Adrian Lane)

Securosis Project Accelerators

Cloud computing is the most disruptive technology innovation to impact Information Technology since we first crawled out of a sea of mainframes. It brings new opportunities for your organization to reap incredible agility, resiliency, economic, and yes, security benefits, but only if you go truly cloud native. Securosis has the field-tested techniques, frameworks, and programs to be **more** secure in the cloud than in your datacenters, without sacrificing agility.

Securosis Project Accelerators (SPA) are packaged consulting offerings to bring our applied research and battle-tested field experiences to your cloud deployments. These in-depth programs combine assessment, tailored workshops, and ongoing support to ensure you can secure your cloud projects better and faster. Based on a combination of the pragmatic, hands-on research and experience of Securosis, combined with the industry leadership of the Cloud Security Alliance, these field tested techniques and frameworks, already in use by organizations from F500 enterprises to early startups, improve security and save costs without sacrificing agility that makes cloud so compelling for organizations of all sizes. We take the lessons of the leading edge and make them accessible to everyone.

Each Securosis Project Accelerator includes four components:

1. **Pre-workshop assessment**
2. **Custom 1-day on-site workshop**
3. **Post-workshop findings and toolkits**
4. **2 follow-up calls**

Each workshop is custom-built using Securosis research modules tailored to your objectives, constraints, and needs. To be clear, project accelerators aren't training classes. These are highly-focused consulting engagements that cut the cruft and focus on practical recommendations to accelerate your success. Our methodologies help ensure your cloud deployments are secure, agile, and effective.

Workshops are provider-specific and available for Amazon Web Services and Microsoft Azure, with further platforms in development.

Program	Description
Security Fundamentals for Cloud Providers	This SPA is designed for organizations still building their foundation for cloud security.
Cloud Project Assessment for Cloud Providers	This SPA provides practical recommendations to rapidly secure a new or existing project.
Cloud Security Program Assessment	Once you understand the fundamentals, use this SPA to build an ongoing, sustainable, and effective cloud security program.

For more information, contact us at info@securosis.com

Welcome to Our Coverage Area Deep Dives

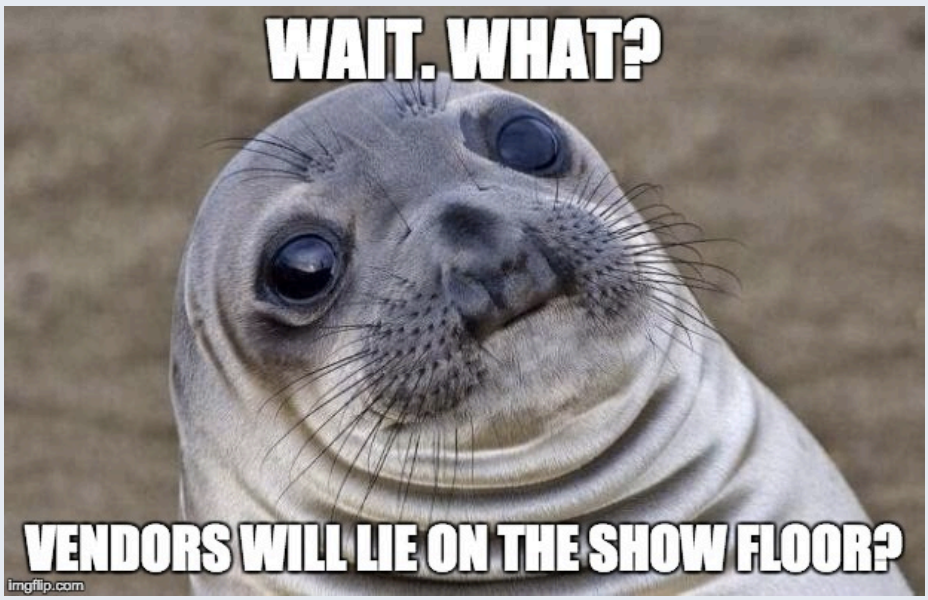
Everyone likes to talk about the "security market" or the "security industry" but security in practice is more a collection of markets, tools, and practices all competing for our time, attention, and dollars. Here at Securosis we have a massive coverage map (just for fun, which doesn't say much now that you've experienced some of our sense of humor), but everything nowadays seems to break down to the same three mega-issues: Cloud Security, Threat Protection, and Data Security.

Our next sections dig into these major coverage areas and detail what you can expect to see, based largely on what users and vendors have been talking about for the past year. You will notice considerable overlap. Cloud and DevOps, for example, affect multiple coverage areas in different ways, and the cloud is a coverage area all its own.

When you walk into the conference you are there for a reason. You already have some burning issues you want to figure out, or specific project needs. These sections will let you know what to expect and what to look for.

The information is based, in many cases, on dozens of vendor briefings and discussions with security practitioners. We try to illuminate what questions to ask, where to watch for snake oil, and what key criteria to focus on, based on successes and failures from peers who tried it first.

The earlier general themes are fun and interesting, but for those of you facing real projects these deep dives will be much more practical.



Cloud Security

To be honest, we are a bit biased on this particular topic. Our day to day work has been shifting to cloud projects for a number of years now, but the jump in terms of pure numbers the past year was pretty astounding. So much so that we are changing our logo to have a pretty little cloud in it, because even Securosis could use a little cloudwashing.

As analysts we've been strong proponents of cloud computing and cloud security, but the projects we've been involved with over the past 12-18 months put the entire industry about 2-3 years ahead of the adoption rates we expected, perhaps more. Every single organization we talk with, even casually, is working on one or more cloud projects. This even includes the kinds of enterprises that typically lag on new technology adoption.

Let's take a look at the different kinds of projects we see, and how you can use the RSA Conference to speed them up.

CASB becomes a Checkbox

We still hate the term "CASB" (Cloud Access and Security Brokers). The truth is it's a mashup due to some infighting over coverage areas among analysts inside Gartner. We prefer the term *Cloud Security Gateways*, but we lost that battle faster than an ant in Pamplona.

If you want greater control over the use of Software as a Service (mostly) in your environment, with a smattering of intelligence on PaaS and IaaS, then CASB is the way to go. Last year we thought the market was over-saturated, and we finally saw the first wave of acquisitions clean things up a bit. The CASB tools on the market are all very competitive, making decisions a bit tough at times.

We suggest you walk in with a list of what tools you already have in house, SaaS platforms you support plus

Big 3

1. Salesperson: "Of course we run in AWS." (whispers to SE: "We run in AWS, right?")
2. Good luck explaining to kids in 10 years that companies used to run their own data centers.
3. Of course we can protect your cloud infrastructure. Just run everything through our box…

your network security toolkit, and use that as a first pass filter to find compatible products. The needs in this particular market are so consistent and glaringly obvious that it can be tough to really differentiate between the products. They all hit the basics, so take the time to see which one just looks more usable to you. The two areas they seem to be most trying to differentiate on are threat detection/prevention (including workflow), and data security (e.g. better DLP).

There does seem to be a pretty big maturity line. You'll see very quickly which products are above and which are below. Since the market is starting to settle, be really careful going with anyone that looks like they have a ways to catch up. Holding a great pace at mile 12 isn't all that exciting when the winners are already at the beer tent and they are taking down the finish line.

Building New Applications on the Cloud

Most of our hands-on work lately has been helping organizations architect and implement security for "new" cloud applications. Typically these are either completely new applications being designed for, and deployed on, Infrastructure and Platform as a Service, or existing applications that are redesigned from the ground up.

That's our first tip — you can't drop ship an existing application to the cloud without it blowing up in your face. You need to pick a cloud provider, then design a new architecture to leverage the agility, resiliency, and economics of that particular provider. You can design for portability to a point, but fully portable apps cost more, are harder to maintain, and tend to be more fragile.

And the security? it's okay to keep your list of general requirements (e.g. "assess all the vulnerabilities"), but toss out any of the specifics. By far we see more success on both the non-security and security sides if you treat these deployments as total redesigns. The more expectations you allow to limit your choices, the harder it is to get the best results.

This is a situation where the vendor floor won't be much help. Many of them are still clinging to existing deployment and business models, and they can only sell to you if you also stick to the old ways. One quick litmus test is to fund out if their product can deploy in an auto scale group. That doesn't mean you might still not need these tools, but it is certainly a warning sign that you should look at other options first.

There will be a very small group of cloud-first products at the conference. Even if you end up with something more-traditional, we highly suggest you give these folks a listen. They are rarely names you already know, are purpose-built for cloud, and love APIs, workloads, and auto scaling.

The upside is that the cloud and virtualization track is pretty strong this year. Real examples from real organizations managing new cloud projects at enterprise scale.

Keep in mind, this section is focused on discrete projects, not building out an entire program. Most clients we work with start with one or more projects like this to get their feet wet and adjust their existing controls and processes.

It's really a great way to get started, and tends to give you more flexibility since decisions are limited to just that project. This is the chance to play around and get a better sense of what you need as you scale, which takes us to the next section...

Building a Cloud Security Program

There's a big difference between your first few isolated cloud projects and having to support dozens, or hundreds, of deployments and assets. A simplified project-based approach won't hold up, and you need to look to extend your existing security program in ways that don't break the reasons people use the cloud in the first place.

Yeah, you have to move faster.

The RSAC can, again, be pretty useful. One of the biggest challenges when moving into cloud is harmonizing operations. you can build a few one-offs for projects as you get your feet wet, but once you need to support something at scale you hit an entirely different set of requirements. This is especially true when you need to maintain some consistency between everything you do now, and everything you need to do "up there".

For example, one of the biggest challenges we commonly encounter is cloud auditing and logging, and then ensuring they are compatible with existing logging/auditing and incident response capabilities. Everything from basic tool compatibility to redesigning processes comes into play. RSAC is a good time to both survey your existing product vendors, learn some of the new best practices in sessions, and talk to your peers.

The areas we tend to see consistently come up are logging/auditing, identity management (one of the easier problems) endpoint security agents (your existing ones probably won't work at cloud scale), network security, and vulnerability assessment. Plus overall config/systems management, which has security implications but isn't always managed by security.

Unless you're a brand new startup extending your security program to the cloud is the very definition of building an aircraft in flight. That's why we really suggest testing things out in the isolated projects, but deeply engaging with those teams so you can build the centralization you need to scale. It isn't easy, but we do see a lot of organizations succeeding. It's your culture, not your tools or vendors, that's the best indicator of how smooth a transition you can expect.

Threat Protection

As we've focused more on topical issues facing security practitioners this year in the Guide, we're able to get away from the artificial category distinctions of things like Endpoint Protection, Network Security, Threat Intelligence, Analytics, SIEM, GRC, and about another two or three dozen categories that in some way, shape or form deal with one thing: threats.

Of course, there are about a hundred ways to define "threat protection." And it's not even clear what word should we use to discuss threats? Is it threat prevention? Absolutely, since we want to prevent threats from causing damage. What about threat detection? We probably need to do that too, since you can't prevent everything. Threat remediation? Threat investigation? Threat Intelligence? Yes, yes, and yes.

So we'll just use the umbrella term "threat protection," since that seems the broadest and candidly, I've already spent too much time writing about nonsensical categorizations of the same damn thing. Threat protection has evolved quickly, but not as quickly as the adversary. Thus, it seems like we lost ground since the last RSAC. But then again, why would this year be different than every other year I can remember?

But it's not all bad. The security funding fiesta isn't over yet (but it's pretty tired) and that means there is a lot of new technology being deployed that works (marginally) better. Note, I'm not going to say it totally works, but it's

certainly better than the crap you've been dealing with for years (yes, endpoint protection and ports/protocols firewalls, I'm looking at you).

At this years RSAC, you'll see a lot of activity around similar themes as we've seen in the recent past. Your endpoint protection sucks and needs to be replaced. Your network security sucks and needs to be replaced. Your security monitoring sucks, and you get the picture. Understand the machinery of the security industry thrives on this rip and replace, so there will always be a new shiny thing forcing you to figure out if the thing you bought 18 months ago is still shiny enough to keep.

All Roads Lead to the Endpoint

We expect 2016 to be the year upstarts land on the endpoint protection beach and storm the barricades of the incumbent AV vendors. They've been assembling their armaments for years. They've been stockpiling an army of

SEs and channel partners and raising boatloads of cash to fund the full frontal assault.

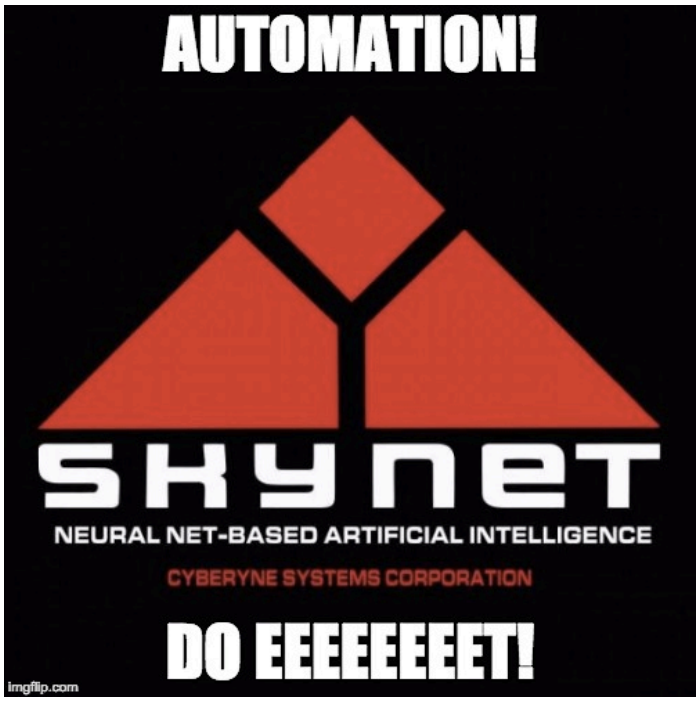
RSAC 2016 is the shot across the bow. The incumbents will be talking about their enhanced protection using behavioral technologies and global threat intelligence. Per usual, solving yesterday's problems tomorrow. The upstarts will be talking about endpoint forensics and isolation and a lot of other technical nuances that they can't prove and most of us can't understand.

Here's what you need to know: 1) Will your assessor be cool if you rip out your existing AV? 2) Will the new shiny thing actually stop more attacks? 3) Can you migrate to the new thing without visiting devices? 4) Will it save you 40% off the top of the money you've been flushing down the toilet for years?

Of course, the answer to all of those questions is yes. So it's time to consider moving away from AV incumbents, and that means you need to go shopping for some cool endpoint kit at RSAC.

The Race to Automate

There isn't a lot new that you'll see at RSAC from a network security standpoint. It's no longer about application policies and NGFW will be a lot less shiny, mostly because people are using it now. Sandboxes are passé and everyone can detect C&C traffic. Or at least lie and tell you they can.



What's going to be shiny on the network this year is automation. There will be a handful of new companies (and a handful of survivors formally known as NAC and firewall management) focusing on helping your manage your network security stuff in a policy-based, automated fashion.

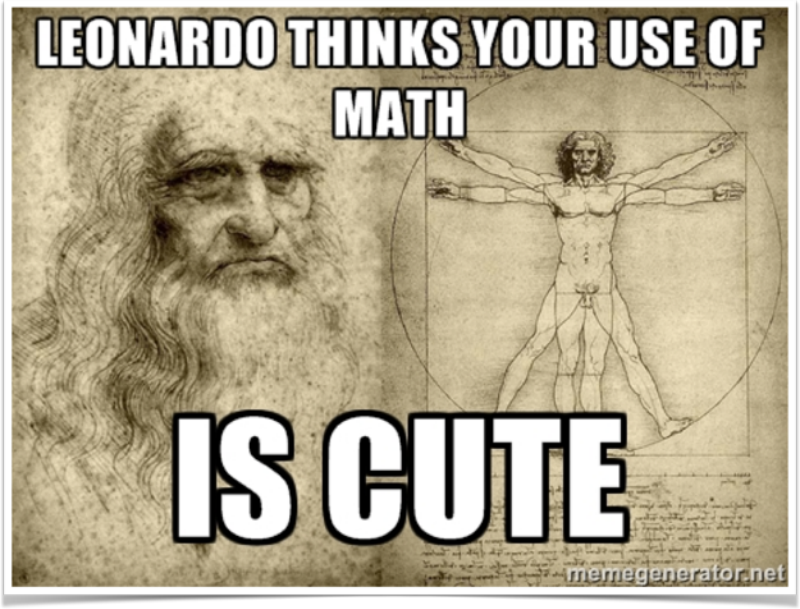
Before you soil your pants, this is actually a good thing. We're not sure that any of these folks are long-term survivors because this is really a feature of your network security fabric, but given the fact that you can't find people to do anything nowadays, having machines do machine-like work is great.

It's early for these folks, so a lot of their stuff will show better on the show floor than in your network, but automation and orchestration go beyond the cloud.

Pythagoras' Revenge

At this year's RSAC, you'll hear a lot about analytics. You know, math. It's this new thing that will change everything in security. It seems security is a few centuries behind other disciplines in leveraging math for better results.

But all the same, whether it's your SIEM, network forensics gear, insider threat detection devices, user behavioral analysis tools, or other handful of use cases masquerading as companies (which keep RSAC afloat, so we shouldn't bitch too much), you'll hear about data scientists in the proverbial coal mines figuring out how to find adversary activity in your network.



To be clear, none of this is novel. It's true that the new technologies do provide a more efficient way to do heavy analytics. And we have more security data than ever before, so the kinds of analyses possible now were not possible 5 years ago. But all the same, what they don't tell you (and you should ask about) is that someone will need to go through all of those fancy alerts and see if they are valid.

Regardless of the puffery you'll see on the show floor, you'll still need carbon-based models to wade through the morass of alerts generated by these new-fangled math toys. But Pythagoras is happy anyway, because there are new applications for math in security.

Intelligence to Action

For what seems like the 20th year in a row (though it's probably the third), you'll hear a lot about threat intelligence. There will be data battles and other marketing shenanigans about why one company's threat intel is better than another's. Ho hum.

What's important is not what data is better, but how easy is it for you to use? If you can't use the data, having it produce smoking gun after smoking gun doesn't matter. So focus on integration with the tools you use to manage your security program. Probe and ask questions about scale because doing heavy analytics on the terabytes of data you gather and comparing it to know indicators of compromise requires some computing horsepower. A lot of horsepower, in fact.

Don't believe the hype. Threat intel doesn't help you do your job. It's about how you can leverage threat intel to make your other tools and processes more effective. Period.

Teams of Artemis

I actually think it's fitting that the deity in charge of hunting is female. It will be great to see many more females roaming the halls looking at tools, as opposed to trying to get middle aged men to sit down for a presentation they don't want to see, so they can bring a t-shirt home. This year, there will be a lot of noise about this new concept called "hunting." You know, tasking

certain folks with finding adversary activity on your network. Right, haven't you been doing that already? If not, what the hell are you doing all day?

Once again, nothing is new under the security sun. Though calling these folks "hunters" definitely helps with their self-esteem and that's always appreciated. At RSAC, you'll see a lot of tools built specifically for hunters. Kind of in the same way a lot of tools were built for cloud security. I guess we should call this "IDS washing" now.

Yet, if you do have dedicated folks tasked with pinpointing adversary activity, a lot of these tools will be very shiny and you'll want them. The real question is where on the priority list do hunting tools land. I suspect somewhere below stronger coffee for the Tier 2 folks wading through all of the alerts from the new analytics platforms.

Though in 2-3 years, these tools will be a lot more commonplace and better integrated with the rest of the security program. Even hunters have to play nice with the other folks on the team.

Bottom Line

Will you leave RSAC with a better idea of how to protect your environment from threats? Probably not, but make sure to get some grapes at the Caesar Pavilion because it's not clear these halcyon days of being able to throw money after every new widget to find advanced attackers has much runway left.

Don't Miss the DR Breakfast

Once again Securosis and friends are hosting our RSA Conference Disaster Recovery Breakfast at Jillian's Thursday, March 3, from 8 to 11 am.

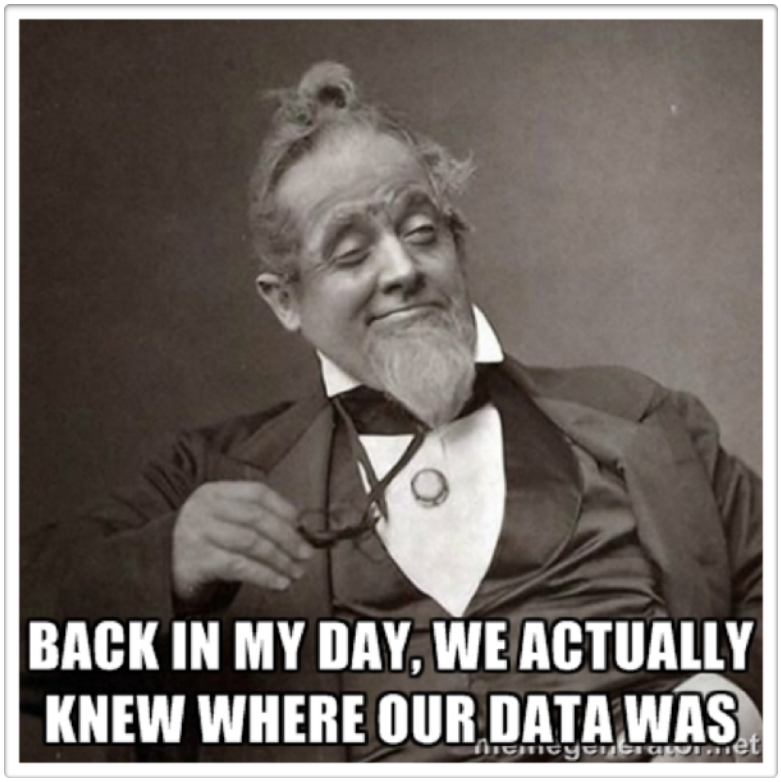
This is the EIGHTH year for this event, and all we see are clouds ahead. Not just because it's San Francisco in February. Or because we've been drinking for a week and everything is a fog. But also because we expect everything will be "cloud-ready."

Kidding aside, we are grateful that so many of our friends, clients, and colleagues enjoy a couple hours away from the glitzy show floor and club scene that is now the RSAC. By Thursday if you're anything like us you will be a disaster, and need to kick back, have some conversations at a normal decibel level, and grab a nice breakfast. Did we mention there will be bacon?

With the continued support of Kulesa Faul, and our new partners CHEN PR and LaunchTech, we are happy to provide an oasis in a morass of hyperbole, booth babes, and tchotchke hunters. RSVP and enjoy a nice quiet breakfast with plenty of food, coffee, recovery items (aspirin & Tums), and even the hair of the dog for those of you not quite ready to sober up.

Data Security

Ransomware. Pwning the IoT. Backdoors. Botnets. Skimmers. APT. Malicious apps. The NSA. Lots and lots of noise from the press about these scary threats, but what grabs the headline is not what drives the security budgets. Hacking devices and networks is all very clever, but when we get in front of enterprises, data security remains -- as it has for many years -- at the top their priority list. As we do each year, we offer the following guide to help you steer you clear of the hype and anti-trends and towards real data security solutions.



Behind the FUD

"How do you stop the insider threat?" and "What do we do about malicious insiders?" You'll see dozens of ads during RSA week throwing this problem into your face, daring you to come up with a response. From our analyst perch these questions use to appear as the very essence of FUD, preying on mental insecurities of IT folks. We don't know if it's a learned response from listening to vendors and media hype all these years, or maybe they've watched too many episodes of Mr. Robot, but enterprise clients are legitimately worried about employees and contractors, and now ask us these very questions. When it comes down to it, the entire conversation is B.S. Ignore it.

In reality attackers access your systems from their apartments, sitting in their underwear and drinking coffee, just like your 'work at home' employees and contractors. How do you tell the difference? If you said 'ski masks', stop reading now, and go update your resume. For the rest, understand that any attacker, once they gain a foothold on an endpoint or web server or admin account will begin to leverage your resources just like an employee. They will search for what they want, and then steal/alter data. It's

Big 3

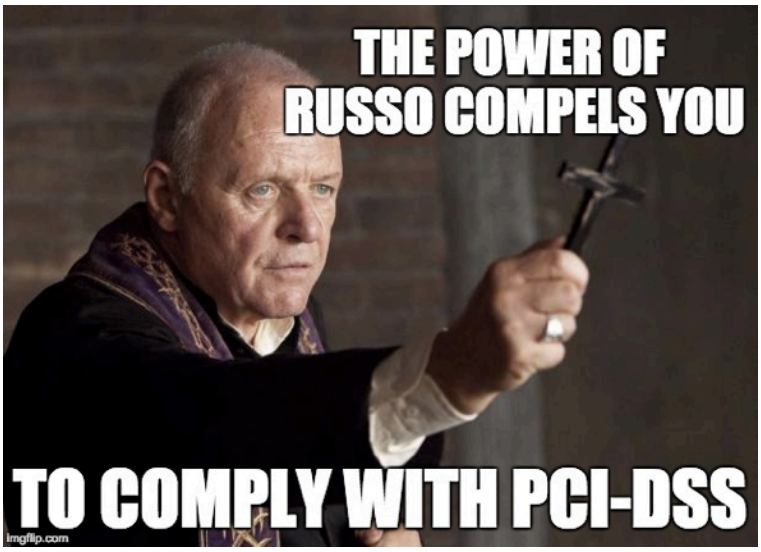
1. What is the cloud thing? And why is all of my data there?
2. What if this encryption stuff really works? And the NSA can't snoop our stuff?
3. Your fridge just called and said "All of your veggies belong to me."

less important at looking for 'insiders' than it is for misuse in general. Once you move past the basic protections provided by encryption and identity management, protecting data from misuse means actively detecting misuse. Activity monitoring and event analysis do this, and these tools will detect both classes of attacker.

We don't want the debate between insider and outsider — which is essentially vendors attempting to differentiate their products — to cloud the issue of protecting data beyond preventative security controls. Instead, approach it from the type of repository you want to protect, and the type of activity most likely to be misused. At that point there are only a couple options to detect data misuse, so you choices become clearer, and you can side-step the meaningless insider debate.

Where Have You Gone, Abe Vigoda

Most people were surprised Abe Vigoda passed away this year. In fact, so many people thought he passed away a long time ago that — in the late 90s — the Abe Vigoda clock was created to reflect Abe's status of being alive and well. Alas, the legendary actor has passed in January 2016 and the clock has stopped. But it got us thinking that from a data security standpoint, we need to create a PCI-DSS



status clock so people know "PCI-DSS is still alive". I know, I know, you're surprised by this news too. Considering the lack of updates to the standard and the continued stream of card breaches, it's easy to see why you might make this mistake. Serious discussions about the specification, the audit process, or any other facet seem to be on hold. When you consider how PCI-DSS was the major driver for data security for almost a decade, the silence is deafening. You may be thinking that the council has crawled into a hole somewhere waiting to die.

Being the person in change of PCI certification process is a like being the designated driver at a bachelor party, where you're buddies insist on pushing you onto a stage to perform Karaoke sober. Nobody looks good performing this charade to begin with, and it's definitely not fun without alcohol. The good news is this is the first year in a long time we're not trying to solve new PCI audit finding. And a relative status quo on the compliance front is OK with IT folks, who remain apathetic towards the standard, just going through the motions without embracing it as a serious exercise in security. And who can blame them when it seemed many breached firms had recently undergone the certification process. Even when the council does pop up, it appears they've lost their drive and vigor. Recent case in point, Christmas 2015 deadline to retire SSL and TLS 1.0 protocols pushed out till June 2018. Two and one half years is a lifetime in security.

We think the posture of the council reflects the truth. The writing is on the wall and sometime in the near future, the standard's relevance will cease. Payment systems will finally dispense with credit card numbers altogether. ApplePay, AndroidPay and SamsungPay are all based on tokenization systems, and the credit card need never be passed to the new contactless terminals. Credit card numbers will not be stored because it won't be shared with merchants; only a token will. For the same reasons it's going to take 2.5 years to fully adopt TLS 1.0, it will take time to fully realize tokenized payment systems. For now you still need to go through the process, as the 'Abe Vigoda clock' for PCI-DSS is still ticking.

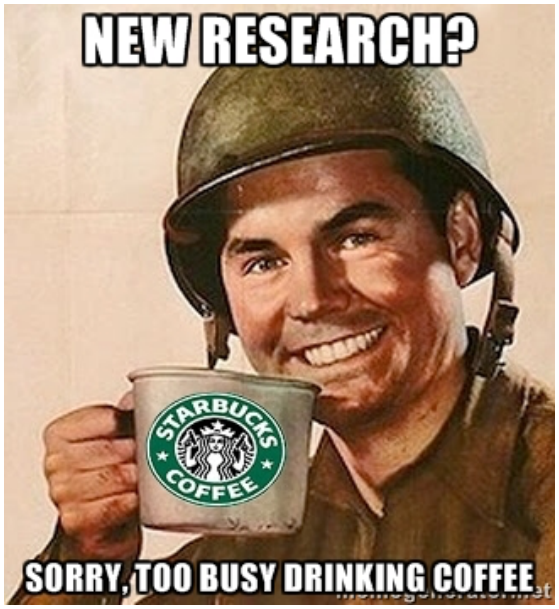
Love-Hate Relationship with Big Data

Big Data will have a huge presence on the RSA Conference floor this year. It's the secret sauce for all those new miracle products; you know, the ones that find profound value from all types of data. The ones that promise to find the APTs, reduce your risk, detect threats before they occur, do forensic analysis, help SIEMs scale, juggles chainsaws, has 'force visions' of the future and make your insides all tickle-y. But the security market has a curious bi-polar relationship with Big Data. It's a disruptive technology to be sure. At least that's the sales pitch for new security products. Ask IT practitioners and they are not so sure. "What's in the cluster? Is customer data stored there? Is it secure? Who has access? Do we need to worry about SQL Injection? Why does that elephant look so damned happy and carefree?" When it comes down to it, stories of the wonderful things NoSQL databases can do for you need to be balanced with the realities of owning and operating a big giant multi-tenant data warehouse. What you will be seeing is hype about the value Hadoop provides and very little about how to secure your copy of it! The hype is around battling the bad guys, but the real work to be done is protecting data. You're going to have to dig a bit at the show to find NoSQL security solutions, but there are vendors in attendance that offer data and database security for Hadoop and the common NoSQL platforms. And in many cases, there is no vendor at RSAC because the solutions are open source! A pre-conference Google-search will help identify the handful of commercial and open source identity, encryption, data discovery and management solutions that help tackle big data security.

SLAs - Keeping Data Insecure Since 1995

Of course you remember the Target breach. And like us you probably laughed about lunacy of a successful attack through and external network connection for HVAC management. That is until you realized that between your external SoC, third-party mainframe management, cloud gateways and contractors you have about 100 other remote connection points that provide the management conduit for most prized systems. They use generic admin accounts and your directory services lists these third parties under the same roles as employees; after-all, these contractors are performing a role an employee used to. Why go through the pain to set up new roles for contractors? Now they come in through VPN connections on unregistered devices, often without passwords, performing the admin duties you contracted them to do. You invited them to the party so good luck reigning them in. Most 3rd party firms simply reject new security constraints as outside the service level agreement. Those providers that volunteer only do so after you sign a 'change order', which means you pay lots of money not currently in your budget.

2FA — or two-factor authentication — is buzzing this year as a means to get better user authentication. By requiring users to not only possess a VPN certificate and general network credentials, it forced users to verify that they are who they say they are by requiring they validate from a registered mobile device as well. The same VPN and identity infrastructure is in play, but 2FA solves several problems related to system and data access. You validate the user by leveraging the mobile device authentication, it ties activity to a specific user/device combination, and it stops attackers with stolen laptops — the ones that have VPN certificates embedded — from automatically gaining access to the network.



Check Out Our Research

Have you visited our Research page? You should – we write a crap load of stuff. You can find it at https://securosis.com/research/research-reports. The rest of the research library is pretty busted (and being overhauled), but in the meantime this list is current. And awesome.

Recently Published Papers

- Threat Detection Evolution
- Building Security into DevOps
- Pragmatic Security for Cloud and Hybrid Networks
- Applied Threat Intelligence
- EMV Migration and the Changing Payments Landscape
- Endpoint Defense: Essential Practices
- Monitoring the Hybrid Cloud
- Best Practices for AWS Security
- Secure Agile Development
- Trends in Data Centric Security
- The Future of Security

Firestarter Video Blog

- Dec 8 — 2015 Wrap Up and 2016 Non-Predictions
- Nov 16 — The Blame Game
- Nov 3 — Get Your Marshmallows
- Oct 19 — re:Invent Yourself (or else)
- Aug 12 — Karma
- July 13 — Living with the OPM Hack
- May 26 — We Don't Know Sh-. You Don't Either.
- May 4 — RSAC wrap-up. Same as it ever was.
- December 8 — Using RSA
- March 16 — Cyber Cash Cow
- March 2 — Cyber vs. Terror (yeah, we went there)
- February 16 — Cyber!!!
- February 9 — It's Not My Fault!

See Securosis Speak

We keep busy at RSAC each year. But we do a number of speaking sessions and make other appearances throughout the week. Here is where you can find us:

Disaster Recovery Breakfast

- **Everyone!** It's pretty hard to get on our schedules at the conference, so the best place to see us will be the DRB. (Thursday 8-11am, Jillian's at the Metreon). With our partners Kulesa Faul, CHEN PR and LaunchTech https://securosis.com/blog/2016-recoverybreakfast.

Speaking Sessions

- **Mort (with Wendy Nather, David Hoffman, and Leigh Honeywell):** PDIL-T09 — Learning from Unicorns While Living with Legacy (Tuesday 1:10 - 2:00 PM, West Room 2009)
- **Rich (with Bill Shinn from AWS):** CSV-T10 — Aspirin as a Service: Using the Cloud to Cure Security Headaches (Tuesday 2:20-3:10 PM, West Room 3022)
- **Mort**: CSV-W03F — Docker: Containing the Security Excitement (Wednesday 9:10 - 10:00 PM, West Room 3002)
- **Rich and Mike:** CSV-R05 — Cloud Security Accountability Tour (Thursday 11:30 - 12:20 PM, West Room 3022)
- **Mort (with Chad Skipper):** PDAC-R05 — Leveraging Analytics for Data Protection Decisions (Thursday 11:30 - 12:20 PM, West Room 2005)

Other Events

- **AGC:** Monday Mike will participate in the AGC West Coast Investor Conference
  - Mike will be moderating "Cloud Security: Opportunity or Obstacle to Cloud Adoption" at 8:15 with folks from AlertLogic, Bracket Computing, Microsoft, Trend Micro, and VMWare.
  - Mike is also moderating "Directions in Enterprise Security: Analytics, Automation and Protection" at 9:30 with panelists from Blue Coat, Cisco, IBM Security Systems, Palo Alto Networks, and RSA.
- **Rugged DevOps:** Also Monday, Rich will give a talk at the DevOps Connect: Rugged DevOps event on "Architectures, Design Patterns, and Coding for Rugged DevOps at Scale" at 4 PM.

Dining and Beverage Guide

Over the years we have received many requests for favorite places to grab a bite or a drink. After all these years we hate to admit how much time we've spent grubbing for food around the Moscone Center, especially because this isn't the only event we attend there. Here are our recommendations with tips from friends on Twitter.

Photo by Road Fun — http://flic.kr/p/4DX684

Click Here. Really.

We even put together some nice maps. Click on the names of these establishments to pull up a map, description, and ratings in your web browser.

It's even mobile friendly!

(Not that the rest of this document is).

Best breakfast that's a little out of the way: Mo'z Cafe

Best convenient breakfast everyone knows about but might be slow: Mel's Cafe

Best coffee/breakfast/lunch place for quick meetings: The Grove

Best place to have a drunk marketing/PR person buy you a free drink: Lobby bar at W hotel

Close food courts with decent food for lunch:

Westfield Center, Metreon

Best Drinks: Bourbon and Branch

The place to get the scoop on all the RSAC Parties: @RSA Parties on Twitter

The best place to see people you probably don't want to see: W Hotel Bar (after midnight)

Best place to get a good beer even if there's a party upstairs: Thirsty Bear

Best Indian: Amber

Best spicy noodle place: Henry's Hunan

Mike's personal recommendation: Mitchell Brothers O'Farrell Theater (shhh! You didn't hear it from Mike.)

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:** 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 licensed for distribution on an annual basis. All published materials and presentations meet our strict objectivity requirements and follow our Totally Transparent Research policy.
- **Strategic advisory services for end users:** Securosis provides advisory for end user organizations, 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. Example services include market and product analysis and strategy, technology guidance, product evaluations, and merger and acquisition assessment. Even with retainer 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. More information on our expert services (PDF) is available.

RSA Conference Guide 2016

Securosis LLC

515 E. Carefree Highway
Suite 766
Phoenix, AZ 85085

It's All Good

We know we're damn lucky to do what we do. We aren't a billion-dollar company with thousands of employees; we're just three partners with a few friends helping out when they can, all trying to bring a little value to the security 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