Securosis

Welcome to RSAG 2013

The annual RSA Conference represents a great opportunity to learn what's new in security, see some old friends, and have a great time. That assumes you have a plan to take advantage of the time, as the 3 official days (up to 6 if you hit all the pre-event opportunities) tend to go by quickly. Your friends at Securosis want to kickstart your planning efforts with our fourth annual "Securosis Guide to the RSA Conference."

Over the 15+ years we've been going to the show, it has gotten bigger and harder to navigate as the security industry has grown bigger and harder to navigate. This guide should give you a good idea of what to expect at the show — laying out what we expect to be key themes of the show, diving into the major technology areas we cover, and letting you know where to find us.

Like last year, we have done our best to break out vendors by tech areas, and added a more comprehensive vendor list including web addresses, so you track down your favorite vendors after the show, since they probably won't be hammering your phone 10 minutes after you get back to the office. We'd also like to thank all our Contributing Analysts — David Mortman, Gunnar Peterson, Dave Lewis, and James Arlen — for helping keep us honest and contributing and reviewing content. And we definitely need to acknowledge Chris Pepper, our stalwart editor and Defender of Grammar.

Enjoy the show. We look forward to seeing you in San Francisco.

Rich, Mike and Adrian

KEY THEMES
See what the Securosis folks think will be the talk of the show this year.

UPCOMING RESEARCH
What we'll be writing over the next few months.

COVERAGE AREA BREAKDOWNS
A deeper dive into each of the subject areas in security.

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

VENDOR LIST
Figure out which vendors will be at the show, and where they'll be.

NO BULL Research

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? Remember how 1999 was going to be the Year of PKI? And 2000. And 2001. And 2002. So what's going to be news of the show this year? Here is a quick list of some key topics that will likely be top of mind at RSA, and why you should care.

Anti-Malware Everywhere

Security folks have been dealing with malicious software since the days when your networking gear came with a swoosh on it. Yes, you young whippersnappers – back when sneakernet was the distribution vector for viruses. But what's old is new again, and driven by advanced attackers who figured out that employees like to click on things, we expect almost every vendor at the show to be highlighting their ability to not block advanced attacks. Oh, was that a Freudian slip? Yes, you'll hear a lot about newfangled approaches to stop advanced malware. The reality remains that sophisticated attackers can and will penetrate your defenses, regardless of how many shiny objects you buy to stop them. That doesn't mean you should use 5-year-old technology to check the compliance box, but that's another story for another day.

Of course, kidding aside, there will be some innovative technologies in play to deal with this malware stuff. The ability to leverage cloud-based sandboxes that block malware on the network, advanced endpoint agents that look an awful lot like HIPS that works better, and threat intelligence services to learn who else got pwned and by what, are poised to improve detection. Of course these new tools aren't a panacea, but they aren't the flaming pile of uselessness that traditional AV has become.

Many of the emerging products and services are quite young, so there won't be much substantiation beyond outrageous claims about blocking this attack or that attack. So leave your checkbook at home but spend some time learning about the different approaches to stopping advanced malware. This will be an area of great interest to everyone through 2013.

BYOD Is No BS

We may not all be Anonymous, but we are certainly all consumers. It seems a little fruit company in Cupertino sparked the imaginations of technology users everywhere, so now the rest of us have to put out the fire. Technology used to be something you used at work, but now it is embedded into the fabric of our daily lives. So we shouldn't be surprised as the workforce continually demands work tools that keep up with the things the kids are playing with in the back seat.

While consumerization of IT is the trend of people bringing consumer-class devices and services into the workplace, BYOD encompasses the policies, processes, and technologies to safely enable this usage. In the past year we have moved beyond the hype stage, and we see more and more companies either developing or implementing their BYOD and general consumerization strategies. This trend won't go away, you can't stop it, and if you think you can block it you will get to find a new job. Even the government and financial services companies are starting to crack and take hard looks at supporting consumer devices and services.

On the device side we see the core as Mobile Device Management, but MDM is merely the hook to enable all the other interesting technologies and controls. The constantly changing nature of BYOD and varied enterprise cultures will likely keep the market from ever maturing around a small set of options. We will see a huge range of options, from the mostly-mature MDM, to network access gateways (the rebirth of NAC), to containerized apps and security wrappers, to new approaches to encryption and DRM. And each of them is right… for someone. There is no silver bullet, but wandering the show floor is a great opportunity to see all the different approaches in one place and think about where they fit into your strategy and culture. Are you lockdown artists? Free-loving tech hippies? Odds are you can find the pieces to meet your requirements, but it definitely isn't all completely there yet, regardless of what the sales droids say.

The main thing to focus on is whether the approach is really designed for BYOD, or whether it's just marketed as BYOD. There is a huge difference, and a fair number of vendors haven't yet adjusted their products to this new reality beyond cosmetic changes. Think hard about which controls and deployment models will fit your corporate culture and, especially, workflows. Don't look at approaches that take these wonderful consumer experiences and suck the life out of them, reverting to the crappy corporate tech you know you hate yourself. Yes, there will be a lot of hype, but this is a situation where we see more demand than supply at this point.

Viva la revolucíon!

Security Big Data

In the past two years at RSA we have heard a lot about risk management and risk reduction, which basically mean efficiently deploying security to focus on threats you face – rather than hypothetical threat scenarios or buying more protection than you need. This year's risk management will be security analytics. Analytics is about risk identification, but the idea is that big data clusters mine the sea of security event data and for actionable intelligence. We will have real data so we will understand our risks, make better security decisions, and make them faster than ever. Great idea, right? Yes and no.

The idea is sound. We collect a massive amount of security-relevant data every day – from servers, network devices, mobile devices, applications, and so on. And we have been behind on the analysis curve as the amount of data has grown faster than our ability to do useful stuff with it. Clearly there is useful information within the data we collect, and so far we have done a poor job of mining it. So wringing out information from the sea of data is both possible and useful. The question is how.

Big data technologies can be utilized to find security event data and then analyze it. But today it's a pretty messy proposition; neither the integration layer nor data analysis capabilities are fleshed out. The queries – think MapReduce data analysis – are hypothetical and still require you to know what you're looking for. If you want this capability it's something you need to write. Since you probably don't have someone on your team who is fluent with both security and

writing big data queries, you will look to vendors and service providers to do this for you. Which is a problem because they don't have any more answers on this than you do. Moreover, it's not likely an off-the-shelf product could fully meet your needs, regardless. As if that weren't enough, most companies don't have the big data engine hooked into their event streams. The integration of SIEM/Log Management and Big Data is just now being deployed, but each vendor does so in a slightly different way. It works with a bunch of duct tape, bailing wire, and consultants. But it's hardly mature.

But that doesn't mean we won't hear a lot about how Security Big Data will change everything at RSA. We will. We'll hear all about how these new shiny objects will address issues of event data volume/velocity, scale, multi-type data and alternative query techniques to provide better analysis. Security big data analytics has the capability to address the problems with SIEM and real promise for the future, but for at this year's show, keep your expectations in check.

Watchlist: In Soviet Russia, Things Internet You!

Most of the time we talk about what you will see on the show floor, but this entry is all about what you won't see… unless you really look. Hard. As you meander the floor check out the wrists and belts of your colleagues. Odds are more than a few will be wearing fitness tracking gizmos or other toys. Check out the display areas – how many have smart TVs? Embedded devices? Cars with Internet connectivity? (Yes, some idiot vendors give away cars). How many security cameras with embedded web servers? Everywhere you look you will see small devices connected to the Internet that move in and out of home, work, public, and private with nary a thought given to them.

We are only at the earliest edge of the Internet of Things, a term applied to all the myriad of devices that infuse our lives with oft-unnoticed Internet connectivity. This won't be a big deal this year, nor for a few years, but from a security standpoint we are talking about a collection of wireless, Internet-enabled devices that employees won't even think about bringing everywhere. Most of these won't have any material security concerns for enterprise IT. Seriously, who cares if someone can sniff out how many steps your employees take in a day (maybe your insurance underwriter). But some of these things, especially the ones with web servers or access to data, are likely to become a much bigger problem.

We are keeping an eye on this space, on the potential risks, benefits, and security controls. It isn't something to pay too much attention to yet, but one of these years we fully expect it to move to the forefront. Just think of the Internet of Things as SCADA security, except you don't actually realize precisely when you became a hybrid waste treatment plant/solar-electric provider.

The Anti-Theme: Security Programs

As most of our faithful readers know, process centricity drives most everything we do. Most of the time it feels like we are talking to ourselves. But clearly the lack of structured and sustainable security programs continues to adversely impact the ability of organizations to protect themselves. We fear far too many folks will walk the RSA floor continuing to search for the silver bullet, without having the process foundation to actually do anything.

Even though you should, you won't see many companies at the show evangelizing the need to have a process in place before you buy technology. That's not good for business when a company sells widgets. But the best favor you can do yourself is to look at all the shiny objects and clearly understand how any new technologies or controls fit into your program.

Upcoming Research

Have you visited the new Research page? 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.

Soon to Come

- Endpoint Protection Evolution
- Firewall Operations Management
- The CISOs Guide to Advanced Attacks
- Implementing and Managing Application White Listing
- Perimeter Security Evolution
- Defending Data in Cloud Infrastructures- IaaS Encryption and Data Security
- Defending Cloud Data- Encrypting for Dropbox, Box.net, and Friends
- BYOD Security Fundamentals
- Building a Web Application Security Program (2.0 update)

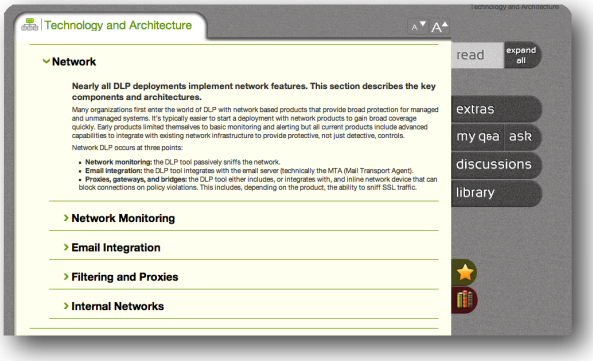
Securosis

Security in knowledge
Mastering data. Securing the world.
RSA CONFERENCE 2013

Get your job done better, faster.

The Securosis Nexus provides pragmatic research on security topics that tells you exactly what you need to know, backed with industry-leading expert advice to answer your questions. The Nexus was designed to be fast and easy to use, and to get you the information you need as quickly as possible.

the Securosis Nexus

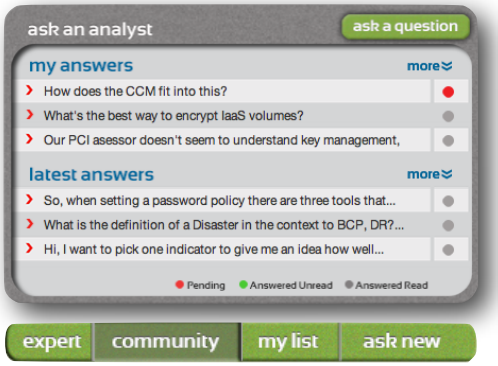


Work Smarter with Pragmatic, Applicable Research

Research in the Nexus has one (and only one) purpose: Help you successfully execute on your project responsibilities. The documents are clearly focused on what you need to know, whether it's selecting a new firewall or getting ready for a PCI assessment. There are templates, action lists, and videos and other dynamic content, all focused on your success.

Direct Answers from Experienced Professionals or Your Peers

Our exclusive Ask an Analyst system allows you to submit questions to our staff and receive instant alerts when your answer is ready. Or, send an answer to the entire community. All your answers are stored in the system in case you need them again someday. There's no limit on the number of questions you can ask, and the best answers are anonymized and fed back into the system to help others.



Killer Design

Time you spend lost a labyrinth of content is time you are not working on your projects. The Nexus is organized in a clean, easy to navigate hierarchy, with a sleek UI and a dynamic help system instead of archaic documents. The user experience ensures you get to *exactly* what you are looking for as quickly as possible.

After over two years of development, the Securosis Nexus is officially launching with our first partner, the Cloud Security Alliance, this week at RSA.

The full Securosis-branded offering will follow in a few months.

Securosis, L.L.C. 515 E. Carefree Highway, Suite 766 Phoenix, AZ 85085 **T** 602-412-3051 info@securosis.com www.securosis.com

Data Security

Between WikiLeaks imploding, the LulzSec crew going to jail, and APT becoming business as usual, you might think data security was just so 2011, but the war isn't over yet.

Throughout 2012 we saw data security slowly moving deeper into the market, driven largely by mobile and cloud adoption. And slow is the name of the game – with two of our trends continuing from last year, and fewer major shifts than we have seen in some other years. You might mistake this for maturity, but it is more a factor of the longer buying cycles (9 to 18 months on average) we see for data security tools. Not counting the post-breach panic buys, of course.

Cloud. Again. 'Nuff Said?

Yes, rumor is strong that enterprises are only using private cloud – but it's wrong. And yes, cloud will be splattered on every booth like a henchman in the new Aaarnoold movies (he's back). And yes, we wrote about this in last year's guide. But some trends are here to stay, and we suspect securing cloud data will appear in this guide for at least another couple years.

The big push this year will be in three main areas – encrypting storage volumes for Infrastructure as a Service; a bit of encryption for Dropbox, Box.net, and similar cloud storage; and proxy encryption for Software as a Service. You will also see a few security vendors pop off their own versions of Dropbox/Box.net, touting their encryption features.

The products for IaaS (public and private) data protection are somewhat mature – many are extensions of existing encryption tools. The main thing to keep in mind is that, in a public cloud, you can't really encrypt boot volumes yet so you need to dig in and understand your application architecture and where data is exposed before you can decide between options. And don't get hung up on FIPS certification if you don't need FIPS, or will you limit your options excessively.

Big 3

1. I can store my keys in the cloud, right? What could possibly go wrong?
2. Your solution is subpoena proof, right?
3. Do you have an app on Cydia? I need to protect the jailbroken phones...

As for file sharing, mobile is the name of the game. If you don't have an iOS app, your Dropbox/Box/whatever solution/replacement is deader than Ishtar II: The Musical. We will get back to this one in a moment.

There are three key things to look for when evaluating cloud encryption. First, is it manageable? The cloud is a much more dynamic environment than old-school infrastructure, and even if you aren't exercising these elastic on-demand capabilities today, your developers will tomorrow. Can it enable you keep track of thousands of keys (or more), changing constantly? Is everything logged for those pesky auditors? Second, will it keep up as you change? If you adopt a SaaS encryption proxy, will your encryption hamper upgrades from your SaaS provider? Will your Dropbox encryption enable or hamper employee workflows?

Finally, can it keep up with the elasticity of the cloud? If, for example, you have hundreds of instances connecting to a key manager, does it support enough network sockets to handle a distributed deployment?

If encryption gets in the way, you know what will happen.

Is that my data in your pocket?

BYOD is here to stay, as we discussed in the Key Themes post, which means all those mobile devices you hate to admit are totally awesome will be around for a while. The vendors are actually lagging a bit here – our research shows that no-one has really nailed what customers want from mobile data protection.

This has never stopped a marketing team in the history of the Universe. And we don't expect it to start now.

Data security for BYOD will be all over the show floor. From network filters, to Enterprise DRM, with everything in between. Heck, we see some MDM tools marketed under the banner of data security. Since most organizations we talk to have some sort of mobile/BYOD/consumerization support project in play, this won't all be hype. Just mostly. There are two things to look for. First, as we mentioned in Key Themes, it helps to know how people plan to use mobile and personal devices in your workplace. Ideally you can offer them a secure path to do what they need to solve their business problems, because if you merely block they they will find ways around you.

Second, pay close attention to how the technology works. Do you need a captive network? What platforms does it support? How does it hook into the mobile OS? For example, we very often see features that work differently on different platforms, which has a major impact on enterprise effectiveness. When it comes to data security, the main components that seem to be working well are container/sandboxed apps using corporate data, cloud-enhanced DRM for inter-enterprise document sharing, and containerized messaging (email/calendar) apps. Encryption for Dropbox/Box.net/whatever is getting better, but you really need to understand whether and how it will fit your workflows (e.g., does it allow personal and corporate use of Dropbox?).

And vendors? Enough of supporting iOS and Windows only. You do realize that if someone is supporting iOS, odds are they have to deal with Macs, don't you?

Shhh. Size does matter

Last year we warned you not to get Ha-duped, and good advice never dies. There will be no shortage of Big Data hype this year, and we will warn you about it continually throughout the guide. Some of it will be powering security with Big Data (which is actually pretty nifty), some of it will be about securing Big Data itself, and the rest will confuse Big Data with a good deal on 4tb hard drives.

Powering security with Big Data falls into other sections of this Guide, and isn't necessarily about data security, so we'll skip it for now. But securing Big Data itself is a tougher problem. Big Data platforms aren't architected for security, and some even lacking effective access controls. Additionally, Big Data is inherently about collecting massive sets of heterogenous data for advanced analytics – it's not like you could just encrypt a single column.

Our very own Adrian Lane wrote a great paper on big data security, which can help you get started if you haven't dug into the platforms and options yet. We highly suggest you know what kind of Big Data your organization is working with before talking to vendors, as many of them use different definitions and vernacular. Large data repositories can generally be handled with existing strategies and technologies, but real Big Data requires different approaches for security, and some companies on the floor will not understand the difference – as savvy users will detect from their product offerings.

Access control and entitlement management aren't boring anymore

They aren't high on the hype scale but managing users, access rights, and entitlements around data (especially files) is growing again. So much so that we are adding an identity management section to the RSA Guide this year, but one area falls squarely under data security: file access controls.

Knowing who has access to what is a big problem in most organizations. Products that help discover and manage this are growing like gangbusters, as unfettered access to files appears on more and more audit deficiency lists. Executives are also still a little gunshy from some of the bigger data disclosures of the past couple years.

We don't expect to see too much hype, but if you are interested in data security we strongly suggest you keep an eye out for tools that help manage and control file access on a combined enterprise/cloud scale. Rich wrote a white paper on one of these categories (FAM), and general feedback from real folks in the field is that entitlement management tools in particular can really help clean up various internal messes.

Stuff we wish you cared about

Here's what you won't see much of on the show floor: DLP and database security. They are still extremely important, but the show floor is a weird representation of what vendors think you will spend on, and their efforts to establish thought leadership for future opportunities. DLP and database security are moving into the productivity phase and out of the hype phase, which means this is the stuff enterprises are actually spending money on. Yes, now you see the idiocy of tracking market trends based on trade-show hype.

These markets still aren't as nearly as large as many other areas of security, but the sales cycles are slow enough to affect innovation. Products are updating more incrementally, with fewer big bang features designed to get your attention. Largely because few customers are using the old big bang features, so there is little drive for major innovation. We don't regards this as bad – some of these products got ahead of the market needs in the feature/function wars common to earlier less mature markets. In some ways it's nice to see the feature bidding wars stabilize out as the markets mature.

Of course folks will be talking about DLP and DB Security at the show. But these technologies tend to be part of a larger stack offered by large security vendors. And we all know the barkers outside the booths will be enticing you with dreams of cloud and mobile more than DLP and DB Security, until deployments start pushing the edges again. If they ever do.

Data Security Vendors at RSA 2013:

DLP	Database Security	Encryption/DRM
CA Technologies (1447)	Application Security (732)	Cryptomathic (2358)
Device Lock (745)	BeyondTrust (1045)	Entrust (2325)
McAfee (1117)	DB Networks (322)	Fasoo (2241)
RSA (1727)	Fortinet (2025)	Netronome Systems (2333)
Symantec (1417)	GreenSQL (3107)	Symantec/PGP (1417)
TITUS (1017)	IBM (241)	RSA (1727)
TrustWave (1324)	Imperva (417)	SafeNet (1825)
Verdasys (2738)	McAfee (1117)	Sophos (1817)
Websense (1332)	Oracle (1941)	SPYRUS (2333)
		Thales E-Security (517)
		Venafi (1655)
		Voltage Security (2627)
		Vormetric (445)

Application Security

So what hot trends in application security will you see at the RSA Conference? Mostly the same as last year's trends, as lots of things are changing in security, but not much on the appsec front. Application security is a bit like security seasoning: Companies add a sprinkle of threat modeling here, a dash of static analysis there, marinate for a bit with some dynamic app testing (DAST), and serve it all up on a bed of WAF. The good news is that we see some growth in security adoption in every phase of application development (design, implementation, testing, deployment, developer education), with the biggest gains in WAF and DAST. Additionally, according to many studies – including the SANS application security practices survey – better than 2/3 of software development teams have an application security program in place.

The Big Money Game

With WhiteHat Security closing a $31M funding round, and Veracode racking up $30M themselves in 2012, there won't be any shortage of RSA Conference party dollars for application security. Neither of these companies are early stage, and the amount of capital raised indicates they need fuel to accelerate expansion. In all seriousness, the investment sharks smell the chum and are making their kills. When markets start to get hot you typically see companies in adjacent markets reposition and extend into the hot areas. That means you should expect to see new players, expanded offerings from old players, and (as in all these RSA Guide sections) no lack of marketing to fan the hype flames (or at least smoke). But before you jump in,

Big 3

1. How does throwing a great party help you secure my apps?
2. All I need is a WAF right?
3. Will your products cause the developers to hate me less?

understand the differences and what you really need from these services. The structure of your development and security teams, the kinds of applications you work with, your development workflow, and even your reliance on external developers will all impact what direction you head in. Then, when you start talking to company reps on the show floor, dig into their methodology, technology, and the actual people they use behind any automated tools to reduce false positives. See if you can get a complete sample assessment report, from a real scan; preferably provided by a real user, because that gives you a much better sense of what you can expect. And don't forget to get your invite to the party.

Risk(ish) Quantification(y)

One of the new developments in the field of application security is trying out new metrics to better resonate with the keymasters of the moneybags. Application security vendors pump out a report saying your new code still has security bugs and you're sitting on a mountain of "technical debt", which basically quantifies how much crappy old code you don't have time or resources to fix. Vendors know that Deming's principles, the threat of a data breach, compliance requirements, and rampant fraud have not been enough whip companies into action. The conversation has shifted to Technical Debt, Cyber Insurance, Factor Analysis of Information Risk(FAIR), the Zombie Apocalypse and navel gazing at how well we report breach statistics.

The common thread through all these is the providing a basis to quantify and evaluate risk/reward tradeoffs in application security. Of course it's not just vendors – security and development teams also use this approach to get management buy-in and better resource allocation for security. The application security industry as a whole is trying to get smarter and more effective in how it communicates (and basically sells) the application security problem. Companies are not just buying application security technologies ad hoc – they are looking to more effectively apply limited resources to the problem. Sure, you will continue to hear the same statistics and all about the urgency of fixing the same OWASP Top 10 threats, but the conversation has changed from "The End is Nigh" to "Risk Adjusted Application Security". That's a positive development.

(Please Don't Ask Us About) API Security

Just like last year, people are starting to talk about "Big Data Security," which really means securing a NoSQL cluster against attack. What they are not talking about is securing the applications sitting in front of the big data cluster. That could be Ruby, Java, JSON, Node.js, or any one of the other languages used to front big data. Perhaps you have heard that Java had a couple security holes. Don't think for a minute these other platforms are going to be more secure than Java. And as application development steams merrily on, each project leveraging new tools to make coding faster and easier, little (okay – no) regard is being paid to the security of these platforms. Adoption of RESTful APIs makes integration faster and easier, but unless carefully implemented they pose serious security risks. Re-architecture and re-design efforts to make applications more secure are an anomaly, not a trend. This is a serious problem that won't have big hype behind it at RSA because there is no product to solve this issue. We all know how hard it is to burn booth real estate on things that don't end up on a PO. So you'll hear how insecure Platform X is, and be pushed to buy an anti-malware/anti-virus solution to detect the attack once your application has been hacked. So much for "building security in".

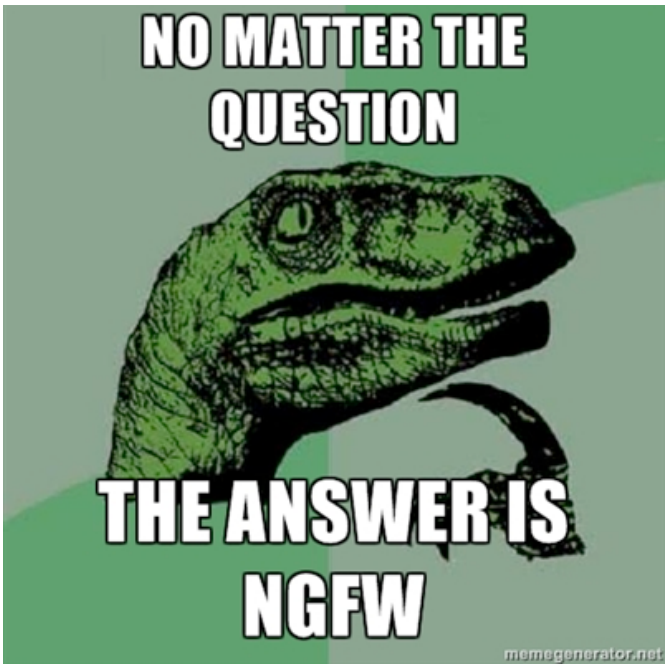
Application Security Vendors at RSA 2013:

Web App Firewalls	Application Testing	Secure Development
Akamai (1630)	Armorize (628)	Arxan (324)
Alert Logic (2417)	Checkmarx (657)	Cigital (132)
Barracuda Networks (1147)	Cigital (132)	Coverity (1759)
HP (1717)	Core Security (457)	IBM (241)
Fortinet (2023)	HP (1717)	HP (1717)
Imperva (417)	IBM (241)	
Juniper/Mykonos (2645)	nCircle (1023)	
Qualys (1431)	Qualys (1431)	
TrustWave (1324)	Rapid7 (2247)	
	Tenable (856)	
	Veracode (1342)	

Network Security

After many years in the wilderness of non-innovation, there has been a lot of activity in the network security space over the past few years. Your grand-pappy's firewall is dead and a lot of organizations are in the process of totally rebuilding their perimeter defenses. At the same time, the perimeter gradually becomes even more a mythical beast of yesteryear, forcing folks to ponder how to enforce network isolation and segmentation while the underlying cloud and virtualized technology architectures are built specifically to break isolation and segmentation.

The good news is that there will be lots of good stuff to see and talk about at the RSA Conference. But, as always, it's necessary to keep everything in context to balance hype against requirements, with a little reality sprinkled on top.



Whatever the question, the answer is NGFW…

For the 4th consecutive year we will hear all about how NGFW solves the problem. Whatever the problem may be. Of course that's a joke, but not really. All the vendors will talk about visibility and control. They will talk about how many applications they can decode, and how easy it is to migrate from your existing firewall vendor and instantaneously control the scourge that is Facebook chat.

As usual they will be stretching the truth a bit. Yes, NGXX network security technology is maturing rapidly. But unfortunately it's maturing much faster than most organizations' ability to migrate their rules to the new application-aware reality. So the catchword this year

Big 3

1. Your NGFW with the NGIPS feature set isn't really a UTM, is it?
2. I should put your network-based malware detection box inline? Really?
3. I want to turn on all the NGFW features. Good thing my pipe is only 10MB…

should be operationalization. Once you have the technology, how can you make best use of it? That means talking about scaling architectures, policy migration, and ultimately consolidation of a lot of separate gear you already have installed in your network.

The other thing to look out for this year is firewall management. This niche market is starting to show rapid growth, driven by the continued failure of the network security vendors to manage their boxes, and accelerated by the movement towards NGFW – which is triggering migrations between vendors, and driving a need to support heterogenous network security devices, at least for a little while. If you have more than handful of devices you should probably look at this technology to improve operational efficiency.

Malware, malware, everywhere.

The only thing hotter than NGFW in the network security space are network-based malware detection devices. You know, the boxes that sit out on the edge of your network and explode malware to determine whether each file is bad or not. Some alternative approaches have emerged that don't actually execute the malware on the device – instead sending files to a cloud-based sandbox, which we think is a better approach for the long haul, because exploding malware takes a bunch of computational resources that would better be utilized to enforce security policy. Unless you have infinite rack space – then by all means continue to buy additional boxes for every niche security problem you have.

Reasonable expectations about how much malware these network-resident boxes can actually catch are critical, but there is no question that network-based malware detection provides another layer of defense against advanced malware. At this year's show we will see the first indication of a rapidly maturing market: the debate between best of breed and integrated solution. That's right, the folks with standalone gateways will espouse the need for a focused, dedicated solution to deal with advanced malware. And Big Network Security will argue that malware detection is just a feature of the perimeter security gateway, even though it may run on a separate box. Details, details.

But don't fall hook, line, and sinker for this technology to the exclusion of other advanced malware defenses. You may go from catching 15% of the bad stuff to more than 15%. But you aren't going to get near 90% anytime soon. So layered security is still important regardless of what you hear.

RIP, Web Filtering

For those network security historians this may be the last year we will be able to see a real live web filter. The NGFW meteor hit a few years ago, and it's causing a proverbial ice age for niche products including web filters and on-premise email security/anti-spam devices. The folks who built their businesses on web filtering haven't been standing still, of course. Some moved up the stack to focus more on DLP and other content security functions. Others have moved whole hog to the cloud, realizing that yet another box in the perimeter isn't going to make sense for anyone much longer.

So consolidation is in, and over the next few years we will see a lot of functions subsumed by the NGFW. But in that case it's not really a NGFW, is it? Hopefully someone will emerge from Stamford, CT with a new set of stone tablets calling the integrated perimeter security device something more relevant, like the Perimeter Security Gateway. That one gets my vote, anyway, which means it will never happen.

Of course the egress filtering function for web traffic, and enforcement of policies to protect users from themselves, are more important than ever. They just won't be deployed as a separate perimeter box much longer.

Protecting the Virtually Cloudy Network

We will all hear a lot about 'virtual' firewalls at this year's show. For obvious reasons – the private cloud is everywhere, and cloud computing inherently impacts visibility at the network layer. Most of the network security vendors will be talking about running their gear in virtual

appliances, so you can monitor and enforce policies on intra-datacenter traffic, and even traffic within a single physical chassis. Given the need to segment protected data sets and how things like vMotion screw with our ability to know where anything really is, the ability to insert yourself into the virtual network layer to enforce security policy is a good thing. At some point, that is.

But that's the counterbalance you need to apply at the conference. A lot of this technology is still glorified science experiments, with much better logos. It is still very very early for private cloud deployments, and we all know that security lags every new technology innovation by years. So we will see some cool stuff on the show floor, and you should check it out – if only to understand how vendors are trying to solve the problem of enforcing security policy within the new virtualized datacenter. Just keep in mind that they are competing for 2015 mindshare.

Your application is DENIED

The other big trend in network security is trying to figure out how to deal with increasingly common denial of service (DoS) attacks. We recently wrote a paper describing the technologies and solution architectures, so check it out as a primer before you hit the show. As with network-based malware detection, you'll hear some best of breed vs. integrated solution hyperbole, but it's more complicated than that.

With DoS attacks, you also need to deal with the network services side of the equation. Which means you need to talk to anti-DoS service providers and CDNs, who can absorb the brunt of attacks while trying to keep your applications up and running. There is some technology to check out, including common signaling protocols between DoS equipment and anti-DoS service providers. Keep in mind that you need to redirect traffic very quickly, which means the network ops processes to trigger and implement redirection must be nailed down in advance. Also be sure to dig deep into the anti-DoS capabilities of your existing network security gear. Odds are you don't yet have good anti-DoS defenses available. So challenge your vendor on how you can keep things up and running while their boxes are falling down.

Network Security Vendors at RSA 2013:

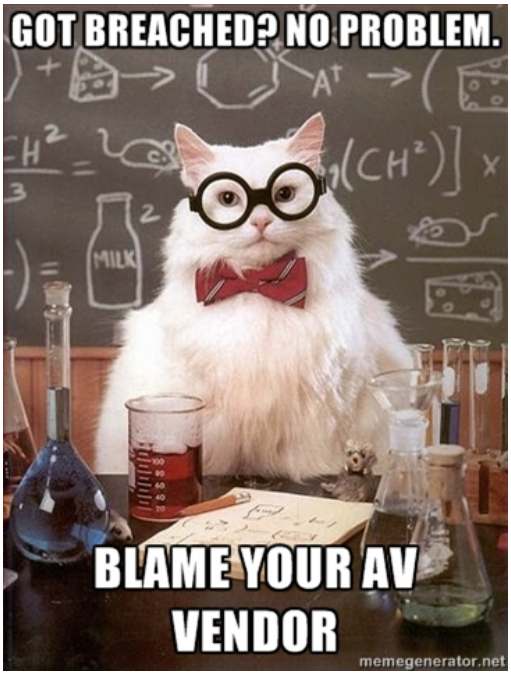
Network Security		Network Analysis/ Forensics	Email/Web Security
AUCONET (1332)	NetScout (2735)	Accolade Technology (126)	Akamai (1630)
Barracuda Networks (1147)	Net Optics (1051)	APCON (2451)	AlertLogic (2417)
Bradford Networks (119)	Palo Alto Networks (931)	Arbor Networks (555)	Authernative (651)
Celestix Networks (2551)	Prolexic (2539)	Broadweb (2125)	Axway (728)
Check Point (1925)	Radware (453)	Click Security (655)	AppRiver (1459)
Cisco (1316)	Sophos/Astaro (1817)	Gigamon LLC (1753)	Barracuda Networks (1147)
Cyberoam (2433)	SonicWALL (1348)	Ixia (2217)	Blue Coat (2017)
Damballa (2233)	SourceFire (2552)	Lancope (1653)	ClearSwift (120)
FireEye (1646)	StoneSoft (1953)	Narus (1841)	Cisco (1316)
ForeScout (831)	TrustWave (1324)	Qosmos (1059)	CommTouch (553)
Fortinet (2025)	Vineyard Networks (2739)	RSA/NetWitness (1727)	McAfee (1117)
F5 Networks (1354)	VMWare (2253)	Solera Networks (2345)	Microsoft (1616)
GFI Software (2141)	WatchGuard (1153)	VSS Monitoring (2147)	ProofPoint (739)
HOB (851)			RIM (632)
HP/TippingPoint (1717)			SilverSky Security (149)
HS USA (2651)			SonicWALL (1153)
Infoblox (122)			Sophos (1817)
InfoExpress (2623)			Symantec (1417)
IBM (241)			Trend Micro (1833)
Juniper (1031)			Websense (1129)
McAfee (1117)			Webroot (832)
Motorola (114)			Zix Corp (550)
Netgear (428)			Zscaler (639)

Endpoint Security

The more things change, the more they stay the same. Endpoint security remains predominately focused on dealing with malware and the bundling continues unabated. Now we increasingly see endpoint systems management capabilities integrated with endpoint protection, since it finally became clear that an unpatched or poorly configured device may be more of a problem than fighting off a malware attack. And as we discuss below, mobile device management (MDM) is next on the bundling parade. But first things first: advanced malware remains the topic of every day.

AV Adjunctivitus

Last year we talked about the Biggest AV Loser and there is some truth to that. But it seems most companies have reconciled themselves to the fact that they still need an endpoint protection suite to get the compliance checkbox. Endpoint protection vendors, of course, haven't given up, and continue to add incremental capabilities to deal with advanced attacks.



But the innovation is outside endpoint protection. IP reputation is yesterday's news. As we discussed in our Evolving Endpoint Malware Detection research last year, it's no longer about what the malware file looks like, but now all about what it does. We call this behavioral context, and we will see a few technologies addressing it at the RSA Conference. Some integrate at the kernel level to detect bad behavior, some replace key applications (such as the browser) to isolate activity, and others actually use very cool virtualization technology to keep everything separate. Regardless of how the primary technology works, the secondary bits provide a glimmer of hope that someday we might able to stop advanced malware. Not that you can really stop it, but we need something better than trying to get a file signature for a polymorphic attack.

Big 3

1. Your cloud is bigger than their cloud, right? RIGHT?
2. How many times has your app been downloaded?
3. How did you manage to use BYOD in your signage 200 times?

Also pay attention to proliferation analysis to deal with the increasing amount of VM-aware malware. Attackers know that all these network-based sandboxes (network-based malware detection) use virtual machines to explode the malware and determine whether it's bad. So they do a quick check and when the malware is executed in a VM it does nothing. Quite spiffy. That a file that won't trigger in the sandbox is likely wreak havoc once it makes its way onto a real device. At that point you can flag the file as bad, but it might already be running rampant through your environment. It would be great to know where that file came from and where it's been, with a list of devices that might be compromised. Yup, that's what proliferation analysis does, and it's another adjunct we expect to become more popular over the next few years.

Mobile. Still management, not security

BYOD will be hot hot hot again at this year's RSA Conference, as we discussed in Key Themes. But we don't yet see much malware on these devices. Sure, if someone jailbreaks their device all bets are off. And Google still has a lot of work to provide a more structured app environment. But with mobile devices the real security problem is still management. It's about making sure the configurations are solid, only authorized applications are loaded, and the device can be wiped if necessary.

So you will see a lot of MDM (mobile device management) at the show. In fact, there are a handful of independent companies growing like weeds because any company with more than a dozen or so folks has a mobile management problem. But you will also see all the big endpoint security vendors talking about their MDM solutions. Eventually you won't need to buy a separate MDM solution – it will just be built in.

But 'eventually' means years, not months. Current bundled endpoint/MDM solutions are less robust than standalone solutions. But as consolidation continues the gap will shrink, until MDM is eventually just a negotiating point in endpoint protection renewal discussions.

We will also see increasing containerization of corporate data. Pretty much all organizations have given up on trying to stop important data making its way onto mobile devices, so they are putting the data in walled gardens instead. These containers can be wiped quickly and easily, and allow only approved applications to run within the container with access to the important data. Yes, it effectively dumbs down mobile devices, but most IT shops are willing to make that compromise rather than give up control over all the data.

The Increasingly Serious "AV Sucks" Perception Battle

We would be the last guys to say endpoint security suites provide adequate protection against modern threats. But statements that they provide no value aren't true either. It all depends on the adversary, the attack vector, monitoring infrastructure to react faster and better, and most importantly on complimentary controls. Recently SYMC took a head shot when the NYT threw them under the bus for an NYT breach. A few days later Bit9 realized that Karma is a Bit9h, when they apparently forgot to run their own software on internal devices and got were breached. I guess what they say about the shoemaker's children is correct.

It will be interesting to see how much the endpoint protection behemoths continue their idiotic APT defense positioning. As we have said over and over, that kind of FUD may sell some product but it is a short-sighted way to manage customer expectations. They will get hit, and then be pissed when they realize their endpoint protection vendor sold them a bill of goods.

To be fair, endpoint protection folks have added a number of new capabilities to more effectively leverage the cloud, the breadth of their customer bases, their research capabilities, and to improve detection – as discussed above. But that doesn't really matter if a customer isn't using the latest and greatest versions of the software, or if they don't have sufficient additional controls in place.

Endpoint Security Vendors at RSA 2013:

Endpoint Anti-Malware	Disk Encryption	Mobile Security
Antiy Labs (2125)	BeCrypt (442)	AirWatch (2153)
AhnLab (951)	Check Point (1925)	AppRiver (1459)
Bit9 (545)	Entrust (1139)	Appthority (245)
BeyondTrust (1045)	McAfee (1117)	Cisco (1925)
BitDefender (756)	Microsoft (1616)	Device Lock (745)
CA Technologies (1447)	RSA (1727)	Good Technology (226)
Check Point (1925)	IronKey (2425)	IronKey (2425)
Comodo Group (2734)	Imation (2525)	Juniper (2031)
Commtouch (553)	SafeNet (1825)	Kaspersky (2117)
CounterTack (2533)	Sophos (1817)	McAfee (1117)
ESET (1638)	Symantec (1417)	MobileIron (354)
GFI Software (2141)	Thales e-Security (517)	RIM (632)
IBM (241)	Trend Micro (1833)	Sophos (1817)
Kaspersky (2117)	Wave Systems (1847)	Symantec (1417)
Kingsoft (2125)		Trend Micro (1833)
Lumension (1959)		Wave Systems (1847)
McAfee (1117)		Webroot (832)
Microsoft (1616)		Zenprise (3022)
Norman (2047)		
Sophos (1817)		
Symantec (1417)		
Trend Micro (1833)		
Webroot (832)		

Identity and Access Management

Usually at security events there isn't much buzz about Identity and Access Management. Actually, identity is rarely thought of as a security technology; instead it is largely lumped in with IT operational stuff. But 2013 feels different. Over the past year our not-so-friendly hacktivists (Anonymous) embarrassed dozens of companies by exposing private data, including account details and passwords. And the drive towards mobility and cloud computing/SaaS at best disrupts, and at worst totally breaks, traditional identity management concepts. These larger trends have forced companies to re-examine their IAM strategies. At the same time we see new technologies emerge, promising to turn IAM on its ear.

We will see several new (start-up) IAM vendors at this year's show, offering solutions to these issues. We consider this is a very positive development – the big lumbering companies largely dominating IAM over the past 5 years haven't kept pace with these technical innovations.

IDaaS = IAM 2.0

The most interesting of the shiny new objects you will see at RSAC is identity-as-a-service (IDaaS), which extend traditional in-house identity services to external cloud providers and mobile devices. These platforms propagate and/or federate identity outside your company, providing the glue to seamlessly link your internal authoritative source with different cloud providers – the latter of which generally offer a proprietary way to manage identity within their environment. Several vendors offer provisioning capabilities as well, linking internal authorization sources such as HR systems with cloud applications, helping map permissions across multiple external applications. It may look like we are bolting a new set of capabilities onto our old directory services, but it is actually the other way around. IDaaS really is IAM 2.0. It's what IAM should have looked like if it had originally been architected for open

Big 3

1. So IDaaS means I don't have to deal with password resets anymore?
2. Do I need a UN Resolution to get my Federation approved?
3. What do I do with these password diary books we bought last year?

networks, rather than the client-server model hidden behind a network firewall.

But be warned: the name-brand directory services and authorization management vendors you are familiar with will be telling the same story as the new upstart IDaaS players. You know how this works. If you can't innovate at the same pace, write a data sheet saying you do. It's another kind of "cloud washing" – we could call it Identity Washing. They both talk about top threats to identity, directory integration, SSO, strong authentication, and the mobile identity problem. But these two camps offer very different visions and technologies to solve the problem. Each actually solves distinctly different problems.

When they overlap it is because the traditional vendor is reselling or repackaging someone else's IDaaS under the covers. Don't be fooled by the posturing. Despite sales droid protestations about simple and easy integrations between the old world and this new stuff, there is a great deal of complexity hiding behind the scenes. You need a strong understanding of how federation, single sign-on, provisioning, and application integration are implemented to understand whether these products can work for you. The real story is how IDaaS vendors leverage standards such as SAML, OAuth, XACML, and SCIM to extend capabilities outside the enterprise, so that is what you should focus on.

Unfortunately managing your internal LDAP servers will continue to suck, but IDaaS is likely the easier of the two to integrate and manage with this new generation of cloud and mobile infrastructure. Extending what you have to the cloud is likely easier than managing what you have in house today.

Death to Passwords

Another new theme as RSAC will be how passwords have failed us and what we should do about it. Mat Honan said we shouldKill The Password. Our own Gunnar Peterson says Infosec Slowly Puts Down Its Password Crystal Meth Pipe. And I'm sure Sony and Gawker are thinking the same thing. But what does this mean, exactly?

Over time it means we will pass cryptographic tokens around to assert identity. In practice you will still have a password to (at least partially) authenticate yourself to a PC or other device you use. But once you have authenticated to your device, behind the scenes an identity service that will generate tokens on your behalf when you want access to something. Passwords will not be passed, shared, or stored, except within a local system. Cryptographic tokens will supplant passwords, and will transparently be sent on your behalf to applications you use. Instead of trusting a password entered by you (or, perhaps, not by you) applications will establish trust with identity providers which generate your tokens, and then verify the token's authenticity as needed. These tokens, based on some type of standard technology (SAML, Kerberos, or OAuth, perhaps), will include enough information to validate the user's identity and assert the user's right to access specific resources. Better still, tokens will only be valid for a limited time. This way even if a hacker steals and cracks a password file from an application or service provider, all its data will be stale and useless before it can be deciphered.

The "Death to Passwords" movement represents a seismic shift in the way we handle identity, and seriously impacts organizations extending identity services to customers. There will be competing solutions offered at the RSA show to deal with password breaches – most notably RSA's own password splitting capability, which is a better way to store passwords rather than a radical replacement for the existing system. Regardless, the clock is ticking. Passwords' deficiencies and limitations have been thoroughly exposed, and there will be many discussions on the show floor as attendees try to figure out the best way to handle authentication moving forward.

Identity and Access Management Vendors at RSA 2013:

Identity and Provisioning	IDaaS	Authentication
Attachmate (2626)	Okta (352)	Authentify (629)
Aveksa (347)	Ping Identity (2158)	Behaviosec (2455)
BeyondTrust (1045)	SecureAuth (123)	Collective Software (351)
CA Technologies (1447)	Symplified (255)	Entrust (1139)
Centrify (233)	Symantec (1417)	Equifax/Anakam (1659)
Cyber-Ark (1947)		HID Global (2517)
Dell Quest (2053)		Okta (352)
IBM (241)		OneLogin (2359)
Intel (1439)		PhoneFactor (717)
Lieberman Software (633)		RSA (1727)
Microsoft (1616)		SecureAuth (123)
Oracle (1941)		StrongAuth (330)
Ping Identity (2158)		Symantec (1417)
RSA (1727)		Symplified (255)
		SafeNet (1825)
		Thales e-Security (517)
		Vasco Data Security (332)

Security Management and Compliance

Given RSA's investment in security management technology (cough, NetWitness, cough) and the investments of the other big RSAC spenders (IBM, McAfee, HP), you will see a lot about the evolution of security management this year. We alluded to this a bit when talking about Security Big Data Analytics in our Key Themes, but let's dig in a bit more…

SIEM 3.0? We can't even get SIEM 1.0 working.

The integration of logs and packet capture is now called Security Analytics; we will hear a lot about how SIEM is old news and needs to evolve into Security Analytics to process, index, search, and report on scads of data. Make that two scads of data. So the buzz at the show will be all about NoSQL data structures, MapReduce functions, Pigs, and all sorts of other things that are basically irrelevant to getting your job done.

Instead of getting caught up in the tsunami of hype, at the show focus on a pretty simple concept. How are these new tools going to help you do your job better? Today or maybe tomorrow. Don't worry about the 5-year roadmap of technology barely out of the lab. Can the magic box tell you things you don't know? Can it look for stuff you don't know to look for? You need to understand enough to make sure you don't trading one boat anchor, which you could never get to work, for another shinier anchor. So focus heavily on your use cases for that tool.

You know, boring and unsexy things like alerting, forensics, and reporting, as we discussed in Selecting SIEM and Security Management 2.0 in days gone by. We do expect these new data models, analysis capabilities, and the ability to digest packet traffic and other data sources will make a huge difference in the effectiveness of security management platforms. But it's still early, so keep a skeptical eye on show-floor marketing claims.

Big 3

1. Who are you? And what happened to all of the start-up guys here last year?
2. I bet you can't say Security Analytics 10 times fast…
3. Can you save me .50 on my PCI assessment?

Deeper Integration (Big IT's Security Revenge)

Big IT got religion over the past two years about how important security is to things like, well, everything. So they wrote big checks, bought lots of companies, and mostly let them erode and hemorrhage market share. The good news is that at least some of the Big IT players learned the errors of their ways, reorganized for success, and have done significant integration; all aimed at positioning their security management platforms in the middle of a bunch of complimentary product lines providing application, network, endpoint, and data security.

Of course they all play lip service to heterogeneity and coopetition, but really they hate them. They want to sell you everything, with lock-in, and they are finally starting to provide arguments for doing it their way.

Back in the real world you cannot just forklift the entire installed base of security technologies you have implemented over years. But that doesn't mean you have to tell either your incumbent or competitors about that. Use better product integration as leverage when renewing or expanding controls. And especially for more mature technologies, looking at an integrated solution from a Big IT/Security player may be a pretty good idea.

Compliance

Every security practitioner's 'favorite' way to get budget, compliance remains a central theme at RSA. But compliance is moving underground a bit, as there are just too many other sexy things to push on the show floor. How can PCI measure up to the sheer star power of Hadoop at this point? Compliance won't be the ever-present force it was last year, but it will still be all over the marketing collateral at just about every booth.

PCI is still alive and causing headaches for companies; despite arguments that vendors will embrace smart-card technologies to get a PCI audit waiver, the reality is that companies pay less to audit than they would to swap out all their mag-stripe readers and point of sale systems. For now, EMV remains a non-starter here. The PCI "Security Special Interest Group" for e-commerce, starting a brand new game of "Liability, Liability, who's got the Liability?" just released an "Information Supplement" for good security practices. It addressed the burning question on all our minds, "Is SQL Injection still a problem"? Which in turn caused many IT staff members to ask the philosophical question "If an information supplement falls in the woods, and nobody notices, does – wait, what were we talking about?"

HIPAA, with updated Omnibus Rules on Security and Privacy remains a newsworthy, although un-motivating, topic. The limited number of cases where fines have been levied (e.g., Cignet, UCLA Health, and a Prescott AZ firm you have never heard of), and the incredibly diverse way these breaches occurred (losing boxes of files, insiders leaking celebrity medical data, posting surgical appointments in a public place) are simply not enough to alter they way the medical industry handles information. Again, lots of wind for very little movement.

So what does all this mean? It means we are keeping the status quo. It means companies will continue to invest the absolute bare minimum into compliance. But compliance will still fund some security product purchases, companies will continue to complain bitterly about it, and the press will continue to yell from the treetops about how this breach will spur companies to take security seriously. God, I love re-runs! At least this is new stuff for the n00bs.

Security Management & Compliance Vendors at RSA 2013:

SIEM/Log Management	Configuration/ Patch	VM/Pen Testing	GRC	Forensics
AccelOps (136)	GFI Software (2141)	AppSec (732)	Agiliance (317)	GFI Software (2141)
Alert Logic (2417)	IBM (241)	Core Security (457)	Aveksa (347)	Guidance (222)
AlienVault (2317)	HP (1717)	Critical Watch (633)	Archer/RSA (1727)	HBGary (2650)
Dell Secureworks (2033)	Lumension (1959)	GFI Software (650)	Brinqa (221)	Mandiant (2439)
HP (1717)	McAfee (1117)	IBM (241)	CA (1447)	Microsoft (1616)
IBM/Q1Labs (241)	Microsoft (1616)	Imperva (417)	Fox Technologies (850)	
LogRhythm (823)	NetIQ (828)	McAfee (1117)	HP (1717)	
McAfee (1117)	Qualys (1431)	nCircle (1023)	IBM (241)	
NetIQ (828)	RSA (1727)	Pwnie Express (2747)	MetricStream (3003)	
RSA (1727)	Symantec (1417)	Qualys (1431)	Modulo (523)	
SenSage (939)	TripWire (923)	Rapid7 (2247)	Oracle (1941)	
Splunk (1917)	VMWare (2041)	Secunia (817)		
Symantec (1417)	**Operations Management**	Tenable (856)		
Tenable (856)	AlgoSec (433)			
TripWire (923)	FireMon (645)			
TrustWave (1324)	RedSeal Networks (1157)			
	Skybox Security (323)			
	Tufin (439)			

Cloud Security

2012 was a tremendous year for cloud computing and cloud security, and we don't expect any slowdown in 2013. The best part is watching the discussion slowly march past the hype and into the operational realities of securing the cloud. It is still early days, but things are moving along steadily as adoption rates continue to chug along.

On the downside, this steady movement is a total buzzkill when it comes to our tendency toward pithy deconstruction. Much of what you see on the show floor (and in all marketing materials for the next couple quarters) represent mere incremental advancements of the trends we identified last year. Cloudwashing is alive and well, the New Kids on the Cloud Security Block are still chugging along patiently waiting for the market to pop (though their investors may not be so patient), data security is still a problem for cloud computing, and ops is handling more security than you realize. What is old is new again. Again.

SECaaS: Good for More Than Cheap Laughs

We realize we sometimes push the edge of acceptable language during our presentations and blog posts, but nothing seems to garner a laugh better this year than saying 'SECaaS'. The thing is, Security as a Service is maturing faster than security for cloud services, with some very interesting offerings hitting the market. Some security operations, including inbound email security, web filtering, and WAF, demonstrate clear advantages when

implemented outside your perimeter and managed by someone else. You can provide better protection for mobile users and applications, reduce overhead, and keep the easily identified crud from ever hitting your network by embracing SECaaS.

One of the most interesting aspects of SECaaS (we know, so juvenile!) is the far-reaching collection of security data across different organizations, and the ability to feed it into Big Data Analytics. Now that we've attained our goal of writing Big Data Analytics at least a few times each day, this isn't all smoke and mirrors – especially for threat intelligence. Pretty much every anti-malware tool worth a darn today relies on cloud-based information sharing and analysis of some sort, along with most of the monitoring and blocking tools with cloud components. We will also touch on this tomorrow for endpoint security. We all know the limitations of sitting around and only getting to see what's on your own network, but cloud providers can pull data from their entire customer base, so they get a chance to recognize the important bits and react faster. Admittedly, a few neighbors need to get shot before you can figure out who pulled the trigger and what the bullet looked like, but as long as it's not you, the herd benefits, right?

Other areas, such as network monitoring (including forensics), configuration management, and key management, all demonstrate creative uses for the cloud. The trick when looking at SECaaS providers is to focus on a few key characteristics to see if they are really cloud-based, and if they provide benefits over more traditional options. The first acid test is whether they are truly architected for multi-tenancy and security. Throwing some virtual appliances into a few colocation data centers and billing the service monthly isn't quite good enough to make our personal SECaaS list. Also make sure you understand how they leverage the cloud to benefit you, the customer. Some things don't make sense to move to the cloud – for example certain aspects of DLP work in the cloud but many others don't. Will moving a particular function to the cloud make your life easier without reducing security? Skip the marketing folks and sales droids (wearing suits) and find the most anti-social-looking guy or girl you can in a scruffy logo shirt. That's usually a developer or engineer – ask them what the service does and how it works.

SecDevOps or SecByeBye

DevOps refers to the operational model of increasing the communications and agility between operations and development to increase overall responsiveness and technology velocity. It relies heavily on cloud computing, agile/iterative development processes, automation, and team structures to reduce the friction normally associated with creating, managing, and updating software applications (internal or external). DevOps is growing quickly, especially in organizations leveraging cloud computing. It is the reason, for example, that many self-service private clouds start as tools for developers.

DevOps is more than just another overhyped management trend. Cloud computing, especially IaaS and PaaS, with APIs to manage infrastructure, draw DevOps like a moth to flame. One benefit is that developers don't need to ask IT ops to provision a server for a new project, and it is irresistible to many developers. If it reduces developer and operations overhead, what's not to love?

Oh, right. Security.

Security has a reputation for slowing things down, and while at times that is the right approach, it is often the wrong one. For example, it just doesn't work well if security has to manually update the firewall for every cloud instance a dev spins up for external testing. Fortunately DevOps also brings some security advantages, such as extensive use of automated configuration scripts and pre-set platforms and applications that can start from a secure state. But what does this all have to do with the RSA Conference?

Keep an eye out for security options that tie into agile DevOps approaches if you are evaluating cloud security. These products will typically consume, and even deliver, APIs for automation and scripting. They rely on security policies more than manual operations. Frequently they tie directly into the leading cloud platforms, such as your private cloud or something up on Amazon, Rackspace, Microsoft Azure, or HP.

When looking at security tools for cloud computing, definitely talk DevOps with reps on the show floor to see if the tool is as agile as what it's protecting. Otherwise it's deader than a red shirt on Walking Dead. (We like to mix analogies).

Cloud Security Vendors at RSA 2013:

Note- Many vendors cross into cloud/virtualization security, so this is our best faith effort

Cloud Security	SECaaS	Virtualization Security
Afore (135)	Accuvant (353)	Bitdefender (756)
AccelOps (136)	Akamai (1630)	CA Technologies (1447)
CipherCloud (132)	Alert Logic (2417)	Cisco (1316)
Cloud Security Alliance (3020)	AppRiver (1459)	Check Point (1925)
CloudLock (2635)	AT&T (723)	HP (1717)
Core Security Technologies (457)	Barracuda Networks (1147)	HyTrust (1853)
PerspecSys (251)	Cybera (338)	IBM (241)
Ping Identity (2158)	Dell SecureWorks (2033)	Juniper Networks (1031)
SkyHigh Networks (147)	Digital Defense (2637)	Kaspersky Lab (2117)
Symantec (1417)	FireHost (959)	McAfee (1117)
Symplified (255)	HP (1717)	Palo Alto Networks (931)
Thales e-Security (517)	IBM (241)	RSA (1727)
Trend Micro (1833)	Imperva (417)	SafeNet (1825)
VMWare (2253)	Mandiant (2439)	SourceFire (2552)
Voltage Security (2627)	McAfee (1117)	Tenable (856)
Vormetric (445)	Okta (352)	Thales e-Security (517)
	Perimeter E-Security (SilverSky) (149)	Trend Micro (1833)
	ProofPoint (739)	VMWare (2253)
	Qualys (1431)	Voltage Security (2627)
	SAIC (2041)	Vormetric (445)
	Solutionary (344)	
	Sophos (1817)	
	Symantec (1417)	
	Trend Micro (1833)	
	Trustwave (1324)	
	Verizon Business (917)	
	Websense (1129)	

Dining and Beverage Guide

Through the years we had a request for some of our 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 since this isn't the only event we attend there. Here's a combination of our recommendations and some tips from our friends on Twitter.

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

Click Me. Really.

We even put together some nice maps. Click on the names of the 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 drink 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: Burbon and Branch

Easy places to find a party you might not get into: Thirsty Bear, Ruby Skye, and (All the hotels directly surrounding Moscone)

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

Pretend Mexican place to avoid unless you're desperate: Chevy's Fresh Mex

Best Indian: Amber

Best spicy noodle place: Henry's Hunan

Mike's personal recommendation: Mitchell Brothers O'Farrell Theater (shhh! Don't tell the Boss)

Don't Miss the DR Breakfast

Once again this year Securosis will be hosting our FIFTH annual Disaster Recovery Breakfast on Thursday, February 28 between 8 and 11 with help from our friends at SchwartzMSL and Kulesa Faul. 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.

See Securosis Speak

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

Speaking Sessions

- With our session hog (Rich) out on paternity leave this year we are a little lighter on sessions than usual, but you can catch David Mortman at the following sessions:
  - ASEC-T19 - Making Rugged DevOps and Infosec Work (Tuesday 3:50 - 4:50, Room 132)
  - CISO-W22 - Psychographics of the CISO (Wednesday 9:20 - 10:20, Room 130)
  - GRC-W23 - Managing Enterprise Risk: Y U NO HAZ METRICS? (Wednesday 10:40-11:40, Room 133)

Other Events

- **e10+:** Mike, Adrian, and our Contributors are the hosts and facilitators for the RSA Conference's e10+ program targeting CISO types. That's Monday morning (Feb. 27) from 8:30 to noon.

RSA Conference 2013 Vendor List

Company Name	Booth Number	Level	Website
3M	532	Exhibitor	www.3mprivacyfilter.com
6WIND	854	Exhibitor	www.6wind.com
Accellion, Inc.	340	Exhibitor	www.accellion.com
AccelOps	136	Exhibitor	www.accelops.com
Accolade Technology	126	Exhibitor	www.accoladetechnology.com
Accuvant	353	Exhibitor	www.accuvant.com
Advantech	751	Exhibitor	www.advantech.com
Afore	135	Partner Pavilion	www.aforesolutions.com
Agency for Science, Technology and Research (A*STAR)	3024	Exhibitor	www.a-star.edu.sg
Agiliance	317	Exhibitor	www.agiliance.com
AhnLab	951	Exhibitor	www.ahnlab.com
AirWatch	2153	Exhibitor	www.air-watch.com
Akamai Technologies, Inc.	1630	Global Platinum Sponsor	www.akamai.com
Alert Logic	2417	Exhibitor	www.alertlogic.com
AlgoSec	433	Exhibitor	www.algosec.com
AlienVault	2317	Exhibitor	www.alienvault.com
Allegro Software Development Corporation	239	Exhibitor	www.allegrosoft.com
Alta Associates Inc.	551	Exhibitor	www.altaassociates.com
AMAX Information Technologies	2351	Exhibitor	www.amax.com
American National Standards Institute (ANSI)	127	Exhibitor	www.ansi.org
American Portwell Technology, Inc.	438	Exhibitor	www.portwell.com
Anonymizer, Inc.	153	Exhibitor	www.anonymizer.com
Antiy Labs	2125	Partner Pavilion	www.antiy.net
APCON, Inc.	2451	Exhibitor	www.apcon.com
Application Security, Inc.	732	Exhibitor	www.appsecinc.com
AppRiver	1459	Exhibitor	www.appriver.com
Appthority	245	Exhibitor	www.appthority.com
Arbor Networks	555	Exhibitor	www.arbornetworks.com
Armorize Technologies Inc.	628	Exhibitor	www.armorize.com
Arxan Technologies	324	Exhibitor	www.arxan.com
AT&T	723	Exhibitor	www.att.com
Attachmate	2626	Exhibitor	www.attachmate.com
AUCONET, Inc.	1332	Partner Pavilion	www.auconet.com
AuthentiDate International AG	1332	Partner Pavilion	www.authentidate.de/en.html
Authentify, Inc.	629	Exhibitor	www.authentify.com
Authernative, Inc.	651	Exhibitor	www.authernative.com

Company Name	Booth Number	Level	Website
Aveksa	347	Exhibitor	www.aveksa.com
Axiomtek	2723	Exhibitor	us.axiomtek.com
Axway	728	Exhibitor	www.axway.com
Barracuda Networks	1147	Exhibitor	www.barracudanetworks.com
Bear Data Solutions	234	Exhibitor	www.beardatasolutions.com
BeCrypt	442	Exhibitor	www.becrypt.com
Behaviosec	2455	Exhibitor	www.behaviosec.com
BeyondTrust Software	1045	Exhibitor	www.beyondtrust.com
Bit9, Inc.	545	Exhibitor	www.bit9.com
Bitdefender	756	Exhibitor	www.bitdefender.com
Blue Coat Systems	2017	Silver Sponsor	www.bluecoat.com
Bradford Networks	119	Exhibitor	www.bradfordnetworks.com
Brinqa	221	Exhibitor	www.brinqa.com
Broadweb	2125	Partner Pavilion	www.broadweb.com
C4ISR Journal	2720	Exhibitor	www.defensenews.com
CA Technologies	1447	Gold Sponsor	www.ca.com
Celestix Networks	2551	Exhibitor	www.celestix.com
CenterTools Software GmbH	1332	Partner Pavilion	www.drivelock.com
Centrify Corporation	233	Exhibitor	www.centrify.com
Check Point Software Technologies	1925	Silver Sponsor	www.checkpoint.com
Checkmarx	657	Exhibitor	www.checkmarx.com
CHERRY	2633	Exhibitor	www.cherrycorp.com
Cigital	132	Exhibitor	www.cigital.com
Cisco	1316	Platinum Sponsor	www.cisco.com
Clearswift Corporation	120	Exhibitor	www.clearswift.com
Click Security	655	Exhibitor	www.clicksecurity.com
Cloud Security Alliance	3020	Exhibitor	www.cloudsecurityalliance.com
CloudLock	2635	Exhibitor	www.cloudlock.com
Collective Software, LLC	351	Exhibitor	www.collectivesoftware.com
Commtouch	553	Exhibitor	www.commtouch.com
Comodo Group Inc.	2734	Exhibitor	www.comodo.com
Core Security Technologies	457	Exhibitor	www.coresecurity.com
CORISECIO GmbH	1332	Partner Pavilion	www.corisecio.com
COSEINC	3009	Exhibitor	www.coseinc.com/en
CounterTack	2533	Exhibitor	www.countertack.com
Coverity, Inc.	1759	Exhibitor	www.coverity.com
Covisint, a Compuware Company	654	Exhibitor	www.covisint.com
Critical Watch	650	Exhibitor	www.criticalwatch.com
Cryptography Research, Inc.	2225	Exhibitor	www.cryptography.com
Cryptomathic, Inc.	2358	Exhibitor	www.cryptomathic.com
cv cryptovision gmbH	1332	Partner Pavilion	www.cryptovision.com
Cybera	338	Exhibitor	www.cybera.net

Company Name	Booth Number	Level	Website
Cyber-Ark Software, Inc.	1947	Exhibitor	www.cyber-ark.com
CyberMaryland	216	Exhibitor	www.cybermaryland.org
CYBEROAM	2433	Exhibitor	www.cyberoam.com
Cybertap LLC	112	Exhibitor	www.cybertapllc.com
Cypherbridge Systems LLC	3001	Exhibitor	www.cypherbridge.com
Damballa	2233	Exhibitor	www.damballa.com
DB Networks	3220	Exhibitor	www.dbnetworks.com
DBAPP Security Ltd.	253	Exhibitor	www.dbappsecurity.com
Dell Quest Software	2053	Exhibitor	www.quest.com/identity-management
DELL SecureWorks	1933	Silver Sponsor	www.secureworks.com
Device Lock	745	Exhibitor	www.devicelock.com
DHS/National Cyber Security Division	945	Exhibitor	www.dhs.com/cyber
Diebold, Inc.	2628	Exhibitor	www.diebold.com
Digital Defense, Inc.	2637	Exhibitor	www.ddifrontline.com
DriveSavers Data Recovery	451	Exhibitor	www.drivesavers.com
Easy Solutions, Inc	2258	Exhibitor	www.easysol.net
eleven GmbH	1332	Partner Pavilion	www.eleven.de
Elliptic	135	Partner Pavilion	www.elliptictech.com
Endgame	144	Exhibitor	endgamesystems.com
Enforcive	217	Exhibitor	www.enforcive.com
Enterprise Ireland	3206	Exhibitor	www.enterprise-ireland.com/en
ENTERSEKT (Pty) Ltd.	2753	Exhibitor	www.entersekt.com
Entrust	1139	Silver Sponsor	www.entrust.com
Equifax	1659	Exhibitor	www.anakam.equifax.com
Esentire	135	Partner Pavilion	www.esentire.com
ESET, LLC	1638	Silver Sponsor	www.eset.com
F5 Networks	1354	Exhibitor	www.f5.com
Faronics Technologies, Inc.	225	Exhibitor	www.faronics.com
Fasoo.com	2241	Exhibitor	www.fasoo.com
Federal Bureau of Investigation	3216	Exhibitor	www.fbi.gov
Federal Reserve Bank of San Francisco	3005	Exhibitor	www.frbsf.org
FEITIAN Technologies Co., Ltd.	2125	Partner Pavilion	www.ftsafe.com
FireEye, Inc.	1646	Global Gold Sponsor	www.fireeye.com
FireHost Inc.	959	Exhibitor	www.firehost.com
FireMon	645	Exhibitor	www.firemon.com
Fixmo	135	Partner Pavilion	fixmo.com
ForeScout Technologies, Inc.	831	Exhibitor	www.forescout.com
Fortinet	2025	Exhibitor	www.fortinet.com
Fox Technologies, Inc.	850	Exhibitor	www.foxt.com
Freescale Semiconductor Inc.	3002	Exhibitor	www.freescale.com

Company Name	Booth Number	Level	Website
Futurex	357	Exhibitor	www.futurex.com
Garner Products	432	Exhibitor	www.garner-products.com
GFI Software	2141	Exhibitor	www.gfi.com
Gigamon LLC	1753	Exhibitor	www.gigamon.com
Glimmerglass Optical Cyber Solutions	2058	Exhibitor	www.glimmerglass.com
Global Knowledge Training	2722	Exhibitor	www.globalknowledge.com
GlobalSCAPE	2259	Exhibitor	www.globalscape.com
GlobalSign	329	Exhibitor	www.globalsign.com
Good Technology	226	Exhibitor	www.good.com
GreenSQL Ltd.	3107	Exhibitor	www.greensql.com
Guardian Analytics	733	Exhibitor	www.guardiananalytics.com
Guidance Software, Inc.	222	Exhibitor	www.guidancesoftware.com
Gurucul Solutions	229	Exhibitor	www.guruculsolutions.com
GWAVA Technologies	3100	Exhibitor	www.gwava.com
HBGary, Inc.	2650	Exhibitor	www.hbgary.com
HID Global	2517	Exhibitor	www.hidglobal.com
Hitachi ID Systems, Inc	450	Exhibitor	http://hitachi-id.com
HOB GmbH Co	851	Exhibitor	www.hobsoft.com
HP	1717	Platinum Sponsor	www.hpenterprisesecurity.com
Huawei Technologies Co.,Ltd.	2651	Exhibitor	www.huawei.com/enterprise
HyTrust	1853	Exhibitor	www.hytrust.com
I Think Security	141	Partner Pavilion	qiportal.ithinksecurity.com
IBM Corporation	241	Exhibitor	www.ibm.com
iBoss Security	3200	Exhibitor	www.iboss.com
Identity Finder, LLC	350	Exhibitor	www.identityfinder.com
IEEE Computer Society	2529	Exhibitor	computer.org
Imperva Inc.	417	Exhibitor	www.imperva.com
Infineon Technologies AG	1332	Partner Pavilion	www.infineon.com
Infoblox	122	Exhibitor	www.infoblox.com
InfoExpress, Inc.	2623	Exhibitor	www.infoexpress.com
InfoGard	554	Exhibitor	www.infogard.com
Information Networking Institute - Carnegie Mellon	240	Exhibitor	www.ini.cmu.edu
Information Systems Security Association (ISSA)	152	Exhibitor	www.issa.org
Infosecurity Magazine	223	Exhibitor	www.infosecurity-magazine.com
Intel	1439	Exhibitor	www.intel.com
Interface Masters Technologies	117	Exhibitor	www.interfacemasters.com
International Association of Privacy Professionals (IAPP)	154	Exhibitor	www.privacyassociation.org
Ipswitch File Transfer	752	Exhibitor	www.ipswitchFT.com
IronKey by Imation	2425	Exhibitor	www.imationmobilesecurity.com

Company Name	Booth Number	Level	Website
Ironkey, Inc.	2525	Exhibitor	www.ironkey.com
ISACA	150	Exhibitor	www.isaca.org
ISC²	146	Exhibitor	www.isc2.org
ITAC	2459	Exhibitor	itac.ca
it-sa – The IT-Security Expo	1332	Partner Pavilion	www.it-sa.de/en
itWatch GmbH	1332	Partner Pavilion	www.itwatch.info
IXIA	2217	Exhibitor	www.ixiacom.com
Jiransoft Inc.	1859	Exhibitor	www.jiransoft.com
Juniper Networks	1031	Silver Sponsor	www.juniper.net
Kaspersky Lab	2117	Exhibitor	www.kaspersky.com
Key Source International	2355	Exhibitor	ksikeyboards.com
Keypasco AB	452	Exhibitor	www.keypasco.com
Kingsoft	2125	Partner Pavilion	www.kingsoftresearch.com
Klocwork	2732	Exhibitor	www.klocwork.com
Lancope	1653	Exhibitor	www.lancope.com
Lanner Electronics Inc	316	Exhibitor	www.lannerinc.com
Lieberman Software Corporation	633	Exhibitor	www.liebsoft.com
Linoma Software	242	Exhibitor	www.linomasoftware.com
Lionic Inc.	257	Exhibitor	www.lionic.com
LJ Kushner & Associates, LLC	446	Exhibitor	www.ljkushner.com
Lockheed Martin	341	Exhibitor	www.lockheed.com
LogRhythm	823	Exhibitor	www.logrhythm.com
Lumension	1959	Exhibitor	www.lumension.com
Lynux Works	2450	Exhibitor	www.lynuxworks.com
MANDIANT	2439	Exhibitor	www.mandiant.com
MBX Systems	528	Exhibitor	www.mbx.com
McAfee an Intel Company	1117	Platinum Sponsor	www.mcafee.com
Messageware, Inc.	2550	Exhibitor	www.messageware.com
Metaforic	3026	Exhibitor	www.metaforic.com
MetricStream	3003	Exhibitor	www.metricstream.com
Microsoft Corporation	1616	Global Diamond Sponsor	www.microsoft.com
MirageWorks Inc.	2619	Exhibitor	www.mirageworks.us
MITRE	2617	Exhibitor	http://msm.mitre.org
MobileIron, Inc.	354	Exhibitor	www.mobileiron.com
Mocana Corporation	2454	Exhibitor	www.mocana.com
Modulo	523	Exhibitor	www.modulo.com
Motorola Solutions	114	Exhibitor	www.motorolasolutions.com
Mykonos Software	2645	Exhibitor	www.mykonossoftware.com
Myricom, Inc.	3207	Exhibitor	www.myricom.com
NagraID Security	1039	Exhibitor	www.NIDsecurity.com
Napatech	2545	Exhibitor	www.napatech.com
Narus, Inc.	1841	Silver Sponsor	www.narus.com

Company Name	Booth Number	Level	Website
National Institute of Standards and Technology	250	Exhibitor	www.nist.gov
nCircle	1023	Gold Sponsor	www.ncircle.com
NEI	617	Exhibitor	www.nei.com
Net IQ	828	Exhibitor	www.netiq.com
Net Optics, Inc.	1051	Exhibitor	www.netoptics.com
NETGEAR, Inc.	428	Exhibitor	www.netgear.com
Netronome	2339	Exhibitor	www.netronome.com
NetScout	2735	Exhibitor	www.netscout.com
Neusoft Corporation	2033	Partner Pavilion	http://neteye.neusoft.com
New Horizons Computer Learning Centers	320	Exhibitor	www.nethorizons.com
Nexcom	859	Exhibitor	www.nexcom.com
Niometrics	3000	Exhibitor	www.niometrics.com
NopSec, Inc.	3105	Exhibitor	www.nopsec.com
Norman ASA	2047	Exhibitor	www.norman.com
NSA	845	Exhibitor	www.nsa.gov
NSFOCUS	529	Exhibitor	www.nsfocus.com
NSS Labs, Inc.	729	Exhibitor	www.nsslabs.com
NuCaptcha	2749	Exhibitor	www.nucaptcha.com
NXP Semiconductors	1657	Exhibitor	www.nxp.com
OASIS Interoperability Standards Showcase	3012	Exhibitor	www.oasis-open.org
OATH	839	Exhibitor	www.openauthentication.org
Oberthur Technologies	423	Exhibitor	www.oberthur.com
Okta, Inc.	352	Exhibitor	www.okta.com
Onapsis Inc.	456	Exhibitor	www.onapsis.com
OneLogin, Inc.	2359	Exhibitor	www.onelogin.com
OPSWAT, Inc.	429	Exhibitor	www.opswat.com
Oracle	1941	Exhibitor	www.oracle.com
Palo Alto Networks	931	Exhibitor	www.paloaltonetworks.com
Patriot Technologies	656	Exhibitor	www.patriot-tech.com
Perimeter E-Security	149	Exhibitor	www.silversky.com
PerspecSys Inc.	251	Exhibitor	www.perspecsys.com
PhishMe, Inc.	2727	Exhibitor	www.phishme.com
Phishnix	3106	Exhibitor	www.phishnix.com
PhoneFactor, a Microsoft Company	717	Exhibitor	www.phonefactor.com
Pindrop Security	259	Exhibitor	pindropsecurity.com
Ping Identity Corporation	2158	Exhibitor	www.pingidentity.com
PistolStar, Inc.	248	Exhibitor	www.pistolstar.com
PointSharp AB	2755	Exhibitor	www.pointsharp.com
Portcullis Inc.	3007	Exhibitor	www.portcullis-security.com
Premio, Inc.	140	Exhibitor	www.premioinc.com

Company Name	Booth Number	Level	Website
PrivateCore Inc	3102	Exhibitor	www.privatecore.com
Prolexic Technologies	2539	Exhibitor	www.prolexic.com
ProofPoint, Inc.	739	Exhibitor	www.proofpoint.com
Protected-Networks.com GmbH	2658	Exhibitor	www.protected-networks.com
Pwnie Express	2747	Exhibitor	http://pwnieexpress.com
Qosmos	1059	Exhibitor	www.qosmos.com
Qualys, Inc.	1431	Global Platinum Sponsor	www.qualys.com
QuintessenceLabs	128	Exhibitor	qlabsusa.com
Radiant Logic, Inc.	129	Exhibitor	www.radiantlogic.com
Radware, Inc.	453	Exhibitor	www.radware.com
Rapid7	2247	Exhibitor	www.rapid7.com
RedSeal Networks, Inc	1157	Silver Sponsor	www.redsealnetworks.com
Research in Motion	632	Exhibitor	www.rim.com
Rohde & Schwarz SIT GmbH	1332	Partner Pavilion	www.sit.rohde-schwarz.com
RSA, The Security Division of EMC	1727	Global Diamond Sponsor	www.rsa.com
RSAM	623	Exhibitor	www.rsam.com
SafeNet, Inc.	1825	Global Gold Sponsor	www.safenet-inc.com
SAIC	2041	Exhibitor	www.saic.com
SANS/GIAC/STI	2716	Exhibitor	www.sans.org
SECnology, Inc.	236	Exhibitor	www.secnology.com
secunet Security Networks AG	1332	Partner Pavilion	www.secunet.com/en/
Secunia	817	Silver Sponsor	www.secunia.com
Secure Commerce Systems, Inc	3104	Exhibitor	www.securecommercesystems.com
SecureAuth Corporation	123	Exhibitor	www.goSecureAuth.com
Security Mentor	750	Exhibitor	www.securitymentor.com
Securonix LLC	3103	Exhibitor	www.securonix.com
SecuTech Solutions PTY LTD	3109	Exhibitor	www.esecutech.com
SenSage Inc.	939	Exhibitor	www.sensage.com
Sentry	141	Partner Pavilion	www.sentrymetrics.com
Shenzhen NORCO Intelligent Technology Co., Ltd.	118	Exhibitor	www.norco-group.com
Sims Recycling Solutions	246	Exhibitor	www.us.simsrecycling.com
Sirrix AG security technologies	1332	Partner Pavilion	www.sirrix.com
Skybox Security, Inc.	323	Exhibitor	www.skyboxsecurity.com
Skyhigh Networks, Inc.	147	Exhibitor	www.skyhighnetworks.com
SmartDisplayer Technology	2624	Exhibitor	www.smartdisplayer.com.tw
Software Engineering Institute	2059	Exhibitor	www.sei.cmu.edu
Solarflare	3214	Exhibitor	www.solarflare.com
Solera Networks	2345	Exhibitor	www.soleranetworks.com
Solutionary, Inc.	344	Exhibitor	www.solutionary.com

Company Name	Booth Number	Level	Website
SonicWALL, Inc.	1348	Exhibitor	www.sonicwall.com
Sophos	1817	Gold Sponsor	www.sophos.com
Sourcefire, Inc.	2552	Exhibitor	www.sourcefire.com
SparkWeave, LLC.	138	Exhibitor	www.sparkweave.com
Splunk Inc.	1917	Global Gold Sponsor	www.splunk.com
SPYRUS, Inc	2333	Exhibitor	www.spyrus.com
SSH Communications Security	333	Exhibitor	www.ssh.com
Stealthbits Technologies, Inc.	2555	Exhibitor	www.stealthbits.com
Stonesoft Inc.	1953	Exhibitor	www.stonesoft.com
StrikeForce Technologies, Inc.	539	Exhibitor	www.strikeforce.com
StrongAuth, Inc.	330	Exhibitor	www.strongauth.com
Symantec Corporation	1417	Global Diamond Sponsor	www.symantec.com
Symplified	255	Exhibitor	www.symplified.com
SynerComm Inc	3108	Exhibitor	www.synercomm.com
SYPRIS Europe Aps	2726	Exhibitor	www.sypriselectronics.com
SYSMATE	757	Exhibitor	www.sysmate.com
TechGuard Security	2717	Exhibitor	www.techguard.com
TeleSign Corporation	533	Exhibitor	www.telesign.com
TeleTrusT - IT Security Association Germany	1332	Gold Sponsor	www.teletrust.de
Tenable Network Security, Inc.	856	Exhibitor	www.tenable.com
Thales e-Security	517	Exhibitor	www.thales-esecurity.com
ThreatMetrix, Inc.	3203	Exhibitor	threatmetrix.com
Thycotic Software Ltd.	2644	Exhibitor	www.thycotic.com
TIBCO Software	2325	Exhibitor	www.tibco.com
Tilera Corporation	2751	Exhibitor	www.tilera.com
TITUS	1017	Silver Sponsor	www.titus.com
TraceSecurity, Inc.	3101	Exhibitor	www.tracesecurity.com
Trend Micro Incorporated	1833	Silver Sponsor	www.trendmicro.com
Tripwire, Inc.	923	Silver Sponsor	www.tripwire.com
Trustwave	1324	Platinum Sponsor	www.trustwave.com
Tufin Technologies	439	Exhibitor	www.tufin.com
TÜV Informationstechnik GmbH	1332	Partner Pavilion	www.tuvit.de/en/
Unisys	3028	Exhibitor	www.unisys.com
University of Denver	328	Exhibitor	www.du.edu
University of Maryland University College	3204	Exhibitor	www.umuc.edu
VASCO Data Security	332	Exhibitor	www.vasco.com
Venafi, Inc.	1655	Silver Sponsor	www.venafi.com
Veracode, Inc.	1342	Silver Sponsor	www.veracode.com
Verdasys, Inc.	2738	Exhibitor	www.verdasys.com

Company Name	Booth Number	Level	Website
Verizon	917	Silver Sponsor	www.verizonbusiness.com
Viewfinity	3212	Exhibitor	www.viewfinity.com
Vineyard Networks	2739	Exhibitor	www.vineyardnetworks.com
Visible Statement	339	Exhibitor	www.greenidea.com
V-Key Pte Ltd	3006	Exhibitor	www.v-key.com
VMware	2253	Exhibitor	www.vmware.com
VoIP Shield	141	Partner Pavilion	www.voipshield.com
Voltage Security	2627	Exhibitor	www.voltage.com
Vormetric, Inc.	445	Exhibitor	www.vormetric.com
VSS Monitoring, Inc.	2147	Exhibitor	www.vssmonitoring.com
WatchGuard Technologies, Inc.	1153	Exhibitor	www.watchguard.com
Watsec	141	Partner Pavilion	www.watsec.com
Wave Systems Corp.	1847	Exhibitor	www.wave.com
Webroot, Inc.	832	Exhibitor	www.webroot.com
Websense Inc.	1129	Gold Sponsor	www.websense.com
Wombat Security Technologies, Inc.	3201	Exhibitor	www.wombatsecurity.com
WWPass Corporation	3209	Exhibitor	www.wwpass.com
yaSSL.com	755	Exhibitor	www.yassl.com
Zenprise, Inc.	3022	Exhibitor	www.zenprise.com
Zix Corporation	550	Exhibitor	www.zixcorp.com
Zscaler, Inc.	639	Exhibitor	www.zscaler.com

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.

- **The Securosis Nexus:** The Securosis Nexus is an online environment to help you get your job done better and faster. It provides pragmatic research on security topics to tell you exactly what you need to know, backed with industry-leading expert advice to answer your questions. Access it at https://nexus.securosis.com/.
- **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 2013

Securosis LLC

515 E. Carefree Highway
Suite 766
Phoenix, AZ 85085

Awesomesauce

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