Securosis

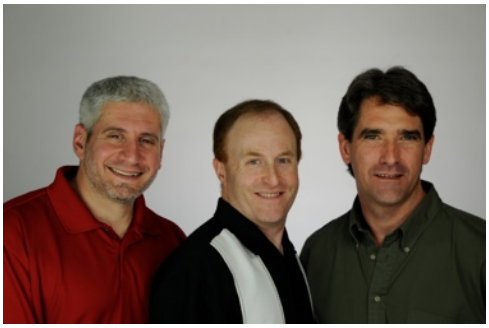
Welcome to the RSA Conference Guide 2014

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 — 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 fifth annual "Securosis Guide to the RSA Conference".

Over the 15+ years we have been going to this show, it has gotten bigger and harder to navigate along with the security industry. 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.

We have once again broken out the vendors by tech areas, although note that this year the vendors are split between the North and South Halls. Our vendor grids specify in which hall your favorite vendors will be at the show. But be careful who you let scan your badge, since every scan equals at least 10 calls from the vendor once you get back to the office.

We would also like to thank all our Contributing Analysts — David Mortman, Gunnar Peterson, Dave Lewis, James Arlen, and Gal Shpantzer — 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 (and won't) be the talk of the show this year.

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

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

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 will be the news of the show this year? Here is a quick list of some key topics that will likely be top of mind at RSA, along with why you should care.

APT-ZERO

Last year the big news at the RSA Conference was Mandiant's research report outing APT1 and providing a new level of depth on advanced attacks. It seemed like every vendor at the show had something to say about APT1, but the entire conference was flowing in Mandiant's wake. They should have called the report "How to increase your value by a couple hundred million in 12 short months", but that's another story for another day.

In 2014 Edward Snowden put on his Kevin Mandia costume and identified the clear predecessor to the APT1 group. That's right, the NSA is APT0. Evidently the NSA was monitoring and hacking things back when the APT1 hackers were in grade school. We expect most vendors will be selling spotlights and promises to cut through the fog of the NSA disclosures. But getting caught up in FUD misses the point: Snowden just proved what we have always known. It is much harder to build and secure things than to break them.

Our position on APT0 isn't much different than on APT1. You cannot win against a nation-state. Not in the long term, anyway. Rather than trying to figure out how much public trust in security tools has eroded, we recommend you focus on what matters: how to protect information in your shop. Are you sure an admin like Snowden cannot access everything and exfiltrate gigabytes of critical data undetected? If not, you have some work to do.

Keep everything in context. Never forget that the security marketing machine is driven by high-profile breaches as a catalyst, for folks who don't know what they are doing, to install the latest widget selling the false hope of protection. And the RSA Conference is the biggest security marketing event of the year. So Snowden impersonators will be the booth babes of 2014.

Cloud Everything. Again. We're Bored Now.

The cloud first appeared in this illustrious guide a mere three or four years ago. The first year it was all hype: with no products, few vendors realized that cloud computing had nothing at all to do with NOAA, and plenty of security pros thought they could just block the cloud at the firewall. The following year was full of cloudwashing, as booths branded themselves with more than sticky notes saying "We Heart Cloud" — but again almost nobody did more than port a custom-hardware-accelerated platform onto a commodity hypervisor. But over the last year or so we saw glimmers of hope, with not only a few real (okay, **virtual**) products, cloud curious security pros starting to gain a little experience, and more honest-to-goodness native cloud products. (Apologies to the half-dozen cloud native vendors who have been around for more than a few years — and don't worry, we know who you are.)

We honestly hoped to drop the cloud from our key themes, but this is one trend with legs. More accurately, cloud computing is progressing nicely through the adoption cycle, deep into the early mainstream. The problem is that many vendors recognize the cloud will affect their business, but don't yet understand exactly how, so they find themselves in tactical response mode. They have products, but they are mostly adaptations of existing tools rather than the ground-up rebuilds that will be required. There are more cloud-native tools on the market now, but the number is still relatively small, and we will see massive cloudwashing on the show floor again. While we're at it, we may was well lump in Software Defined Networking, though 'SDN-washing' doesn't really roll off the tongue.

Two areas you will see hyped on the show floor, which provide real benefits, are Security as a Service (SECaaS — say it loud and love it), and threat intelligence. Vendors may be slow to rearchitect their products to protect native cloud infrastructure and workloads, but they are doing a good job of pushing their own products into the cloud, both from a management standpoint and to share information amongst customers. This collective intelligence breaks some of the information sharing walls that have held security back for decades.

But here is all you need to know about what you will see across the show: big financial institutions are all kicking around various cloud projects. The sharks smell the money, unlike in previous years when it was about looking good for the press and early adopters. In the immortal words of the great sage Jimmy Buffett, "Can you feel them circling honey, can you feel them schooling around? You got fins to right, fins to the left, and you're the only game in town."

After-School Special: It's Time We Talked – about Big Data Security

The RSA Conference floor will be packed full of vendors talking about the need to secure big data clusters, and how the vast stores of sensitive information in these databases are at risk. The only thing that can challenge "data velocity" into a Hadoop cluster is the velocity at which FUD comes out the mouth of a sales droid. Sure, potential customers will listen intently to this hot new trend because it's shiny and totally new. But the customers won't actually be doing anything about it.

To recycle an overused analogy, big data security is a little like teen sex: lots of people are talking about it, but not many are actually doing it. Don't get us wrong — companies really are using big data in all sorts of

really cool use cases including analyzing supply chains, looking for signs of life in space, fraud analytics, monitoring global oil production facilities, and even monitoring the metadata of the entire US population. Big data works! And it provides advanced analysis capabilities at incredibly low cost. But rather than wait for your IT department to navigate their compliance mandates and budgetary approval cycles, your business users slipped out the back door because they have a hot date with big data in the cloud.

Regardless of whether users understand the risks, they are pressing forward. This is where your internal compliance teams start to sound like parents telling you to be careful and not to go out without your raincoat on. What users hear is that the audit/compliance teams don't want them to have any fun because it's dangerous. The security industry is no better, and the big data security FUD is sure to come across like those grainy old public service films you were forced to watch in high school about something-something-danger-something... and that's when you fell asleep. We are still very early in our romance with big data, and your customers (yes, those pesky business users) don't want to hear about breaches or discuss information governance as they explore this new area of information management.

It PoSitively Sucks to Be in Retail

Just when you were getting numb to all the angst around the NSA, Target got thoroughly owned via a busted web server accessed via third-party credentials, which gave attackers access to all their POS systems and lots of other goodies on their internal networks. So clearly this year we will hear lots of rumblings about retailers and their inability to secure anything. At least brick and mortar retailers have great margins, no online competition, and limited attack surface, right?

At first we thought this kind of attack was the return of Gonzales and his band of merry wireless hackers. But actually that was an outside-in attack, where the attackers gained presence through stores and then moved into the data center. This is the opposite. They gained presence through the corporate network and then moved out to stores. But the end result was the same: 70+ million credit cards exposed, along with other personal information.

Even better, these attackers waited until the holidays, when the card brands relax their fraud protections a bit, to start monetizing cards. So they maximized their ability to steal stuff. Now that's innovation, folks. I guess PCI 4.0 will specify that all ROCs go into hiatus from Black Friday to New Year's Day.

But the points you hear this year will be typical FUD-laden nonsense. "Buy this box and everything will be all right." That focuses on the wrong issue. It's not the compromise that's disturbing — it's the fact that they penetrated so deeply and exfiltrated so much information without being noticed.

And if your new shiny business plan involves building 10,000 stores and aggregating 100 million credit cards, maybe you should start working on a different idea, or hire some security rock stars onto your founding team.

CryptoZoology

The biggest noisemaker at RSA this year — besides Rothman — will be everyone talking about the NSA revelations. Everyone with a bully pulpit (basically everyone) will be yelling about how the NSA is all up in our stuff. Self-aggrandizing security pundits will be preaching about how RSA took a bribe, celebrating their disgust by speaking in the hallways and at opportunistic splinter conferences, rather than at the RSA podia. DLP, eDiscovery, and masking vendors will be touting their solutions to the "insider threat" with Snowden impersonators (discussed above). Old-school security people will be mumbling quietly in the corners of the Tonga Room, clutching drinks with umbrellas in them, saying, "I told you so!"

One group will be very, very quiet during the show: encryption vendors. They will not be talking about this! Why? Because they cannot prove their stuff is not compromised, and in the absence of proof, they have already been convicted in the security star chamber. Neither Bruce Schneier nor Ron Rivest will be pulling proofs of non-tampering out of magic math hats. And even if they could, the security industry machine isn't interested. There is too much FUD to throw. What's worse is that encryption vendors almost universally look to NIST to validate the efficacy of their solutions — now that NIST is widely regarded as a pawn of the NSA, who can provide assurance? I feel sorry for the encryption guys — it will be a witch hunt!

The real takeaway here is that IT is — for the first time — questioning the foundational technologies data security has been built upon. And it has been a long time coming! Once we get past Snowden and NSA hype, the industry won't throw the baby out with the bathwater, but will continue to use encryption — now with contingency plans, just in case. Smart vendors should be telling customers how to adjust or swap algorithms if and when parts of the crypto ecosystem becomes suspect. These organizations should also be applying disaster recovery techniques to encryption solutions, just in case.

Watch List: DevOps, Cloud, and the Death of Traditional IT

Recently in one of my cloud security classes I had a developer from one of those brand-name consumer properties all of you, and your families, probably use. When he writes a code update he checks it in and marks it for production; then a string of automated tools and handoffs runs it through test suites and security checks, and eventually deploys it onto their infrastructure/platform automatically. The infrastructure itself adjusts to client demands (scaling up and down), and an admin accessing a production server directly would be an anachronism.

At the latest Amazon Web Services conference, Adobe (I believe the speaker was on their Creative Cloud team) talked about how they deploy their entire application stack using a series of AWS templates. They don't patch or upgrade servers, but use templates to provision an entirely new stack, slowly migrate traffic over, and then shut down the old one once they know everything works okay. The developers use these templates to define the infrastructure they run on, then deploy applications on top of it.

Microsoft Office? In the cloud. Your CRM tool? In the cloud. HR? Cloud. File servers? Cloud. Collaboration? Cloud. Email? Cloud. Messaging? Get the picture? Organizations can move almost all (sometimes actually all) their IT operations onto cloud services.

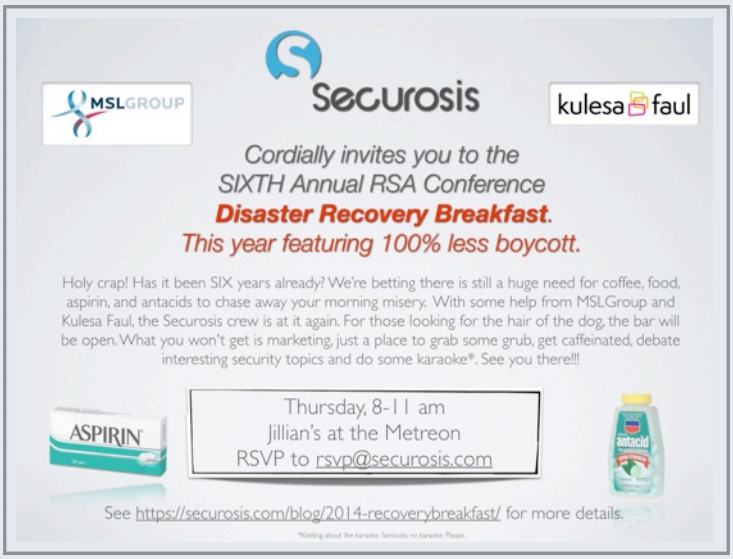
DevOps is fundamentally transforming IT operations. It has its flaws, but implemented well it offers clear advantages for agility, resiliency, and more efficient operations. At the same time cloud services are replacing many traditional IT functions. This powerful combination has significant security implications. Currently many security pros are completely excluded from these projects, as DevOps and cloud providers take over the most important security functions.

Only a handful of security vendors are operating in this new model, and you will see very few sessions address it. But make no mistake — DevOps and the Death of IT will show up as a key theme within the next couple years, following the same hype cycle as everything else. But like the cloud, these trends are real and here to stay, and have an opportunity to become the dominant IT model in the future.

Don't Miss the DR Breakfast

Once again this year Securosis will be hosting our SIXTH annual Disaster Recovery Breakfast at Jillian's on Thursday, February 27 between 8 and 11 am 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.



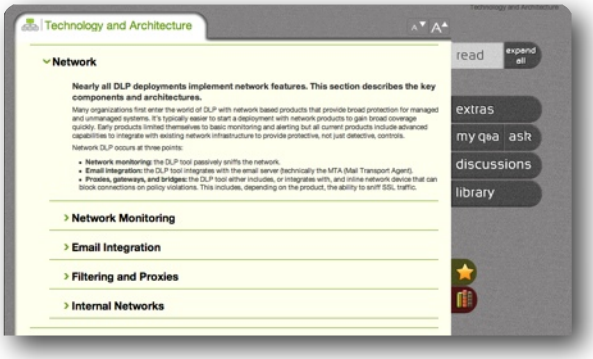
Upcoming Research

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

- Advanced Endpoint and Server Protection
- Inflection: The Future of Information Security
- Securing Big Data Clusters
- Reducing Attack Surface with Application Control
- Security Essentials for AWS (Amazon Web Services)
- Network DDoS: Preparing for the Flood
- Tokenization 2.0
- Rebel Federation — Building a Best of Breed IAM solution
- Securing Your SaaS
- Perimeter Security Gateways: Rebuilding the Perimeter
- Leveraging Threat Intelligence with Security Monitoring

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.

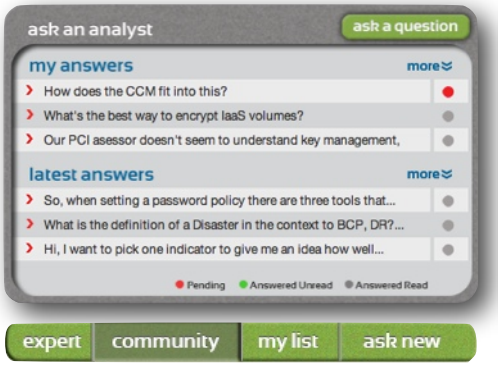


Work Smarter with Pragmatic, Applicable Research

Research in the Nexus has one (and only one) purpose: Help you successfully execute on your project responsibilities. Its 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 in a labyrinth of content is time you are not working on projects. The Nexus is organized in a clean, easy-to-navigate hierarchy, with a sleek UI and a dynamic help system rather than archaic documents. The user experience ensures you get to **exactly** what you are looking for as quickly as possible.

Data Security

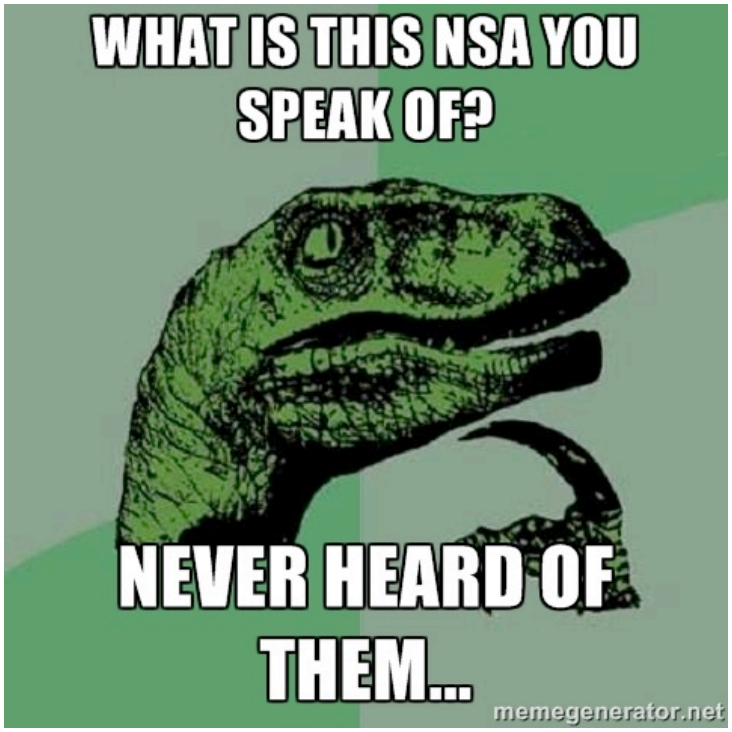
It is possible that 2014 will be the death of data security. Not only because we analysts can't go long without proclaiming a vibrant market dead, but also due to rapid evolution of the cloud and mobile devices. Okay — data security is actually far from dead, but it is increasingly difficult to talk about outside the context of cloud, mobile, or, uh, Snowden. Oh yeah, and the NSA — we cannot forget them.

Organizations have always been worried about protecting their data, kind of like the way everyone worries about flossing. You get motivated for a few days after the most recent root canal, but you somehow forget to buy new floss after you use up your free sample from the dentist. But if you get 80 cavities per year, and all your friends get cavities and complain of severe pain, it might be time for a change.

Buy us or the NSA will sniff all your Snowden

We covered this under key themes, but the biggest data security push on the marketing side is going after one headlines from two different angles:

- Protect your stuff from the NSA.
- Protect your stuff from the guy who leaked all that stuff from the NSA.



Before you get wrapped up in this spin cycle, ask yourself whether your threat model really includes defending yourself from a nation-state with an infinite budget, and whether you need to consider the kind of internal lockdown that the NSA and other intelligence agencies skew towards. Some of you seriously need to consider these scenarios, but those folks are definitely rare.

If you care about these things, start with defenses against advanced malware, encrypt everything on the network, and look heavily at File Activity Monitoring, Database Activity Monitoring, and other server-side tools to audit data usage. Endpoint tools can help but miss huge swaths of attacks.

Big 3

1. Hey, who is this "Snowden" guy in the HR database?
2. Where can we buy the black box to encrypt the cloud? Beige is also acceptable.
3. Can you protect big data on an iPad?

Really, most of what you will see on this topic at the show is hype. Especially DRM (with the exception of some of the mobile stuff) and "encrypt all your files" because, you know, your employees have access to them already.

Mobile is not all bad

We talked about BYOD last year, and it is still clearly a big trend this year. But a funny thing is happening: Apple now provides extensive (but definitely not perfect) data security. Fortunately for vendors Android is still a complete disaster. The key is to understand that iOS is more secure, even though you have less direct control. Android you can control more visibly, but its data security is years behind iOS, and Android device fragmentation makes it even worse. (For more on iOS, check out our deep dive into iOS 7 data security. I suppose some of you Canadians are still on BlackBerry, and those are pretty solid.

For data security on mobile, you'll need to split your thinking. MDM can get you started, but it's not the longer term answer. MDM allows you to get what you need on the device. What exactly that is depends on your needs, but for now container apps are popular — especially cross-platform ones. Focus on container systems as close to the native device experience as possible, and match your employee workflows. If you make it hard on employees, or force them into apps that look like they were programmed in Atari BASIC (yep, I used it), they will quickly find ways around you. And keep a close eye on iOS 7 — we expect Apple to close its last couple serious holes soon, and then you will be able to use nearly any app in the App Store securely.

Cloud cloud cloud cloud cloud… and a Coke!

Yes, we talk about the cloud a lot. And yes, data security concerns are one of the biggest obstacles to cloud deployments. On the upside, there are a lot of legitimate options now.

For Infrastructure as a Service look at volume encryption. For Platform as a Service either encrypt before you send it to the cloud (you will see products on the show floor for this) or go with a provider who supports management of your own keys (there are only a couple right now). For Software as a Service you can encrypt some of what you send these services, but you really need to keep it granular and ask hard questions about how they work. If they ask you to sign an NDA first, our usual warnings apply.

We have looked hard at some of these tools, and used correctly they can really help wipe out compliance issues. Because we all know compliance is the reason you need to encrypt in the cloud.

I'm sure this guy is selling Big Data. Kind of makes you want to leave a Hadoop on the windshield, no?

Photo credit: http://flic.kr/p/3jLYBk

Big data, big budget

Expect to see much more discussion of big data security. Big data is very useful when the technology fits, but the base platforms include almost no security. Look for encryption tools that work in distributed nodes, good access management and auditing tools for the application/analysis layer, and data masking. We have seen some tools that look like they can help, but they aren't necessarily cheap, and we are on the early edge of deployment. In other words the initial offerings look good on paper, but we don't yet have enough data points to know whether the technologies will ultimately solve the problems.

Data Security Vendors at RSA 2014:

DLP	Database Security	Encryption/DRM
CA Technologies (2709N)	BeyondTrust (3535N)	Cryptomathic (1739S)
Device Lock (732S)	DB Networks (901S)	Entrust (2615N)
McAfee (3203N)	Fortinet (1317S)	Fasoo (1721S)
RSA (3021N)	IBM (1109S)	Ionic Security (220S)
Symantec (2803N)	Imperva (701S)	Netronome Systems (1427S)
TITUS (801S)	McAfee (3203N)	Symantec/PGP (2803N)
TrustWave (3527N)	Oracle (1509S)	RSA (3021N)
Verdasys (2326S)		SafeNet (2729N)
Websense (3413N)		Sophos (2701N)
		Thales E-Security (909S)
		Venafi (2621N)
		Voltage Security (1921S)
		Vormetric (515S)
		Vaultive (Microsoft/3005)

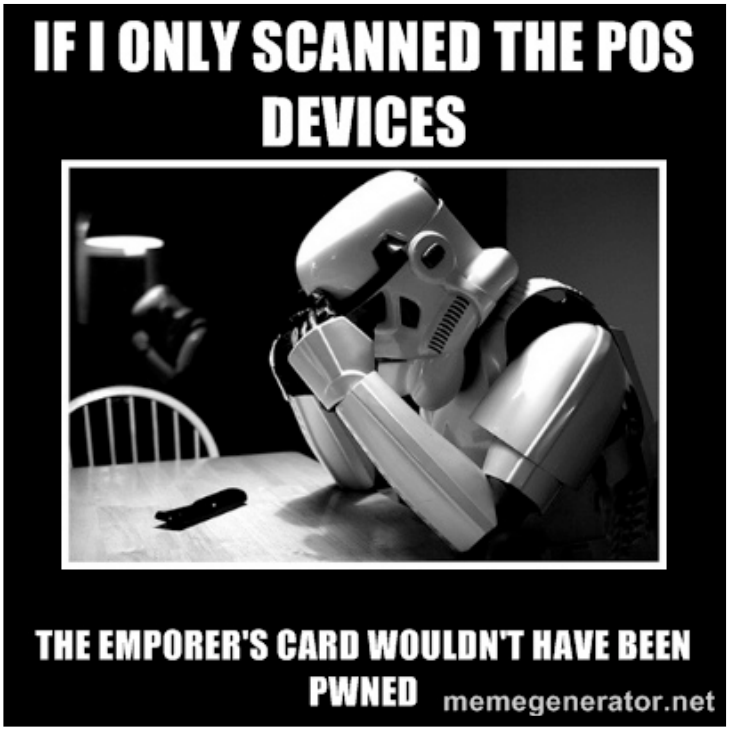
Application Security

With PoS malware, banking trojans, and persistent NSA threats the flavors of the month and getting all the headlines, application security seems to get overshadowed every year at the RSA Conference. Then again, who wants to talk about the hard, boring tasks of fixing the applications that run your business. We have to admit it's fun to read about who the real hackers are, including selfies of the dorks apparently selling credit card numbers on the black market.

Dealing with a code vulnerability backlog? Not as much fun. But very real and important trends are going on in application security, most of which involve "calling in the cavalry": outsourcing to people who know more about this stuff, to jumpstart application security programs.

The Application Security Specialists

Companies are increasingly calling in outside help to deal with application security, and not just for classic



dynamic web site and penetration testing. On the show floor you will see several companies offering cloud services for code scanning. You upload your code and associated libraries, and they do the analysis "up there" and report back on known vulnerabilities. Conceptually this sounds an awful lot like white-box scanning, just located in the cloud, but there is more to it — the cloud services can do some dynamic testing on the application code as well. Some firms leverage these services before they launch public web applications, while others are responding to customer demands to prove and document code security assurance. In some cases code scanning vendors can help validate third-party libraries — even when source code is not

Big 3

1. Application Security Gateways is just another way of saying NGFW, right?
2. Penetration testers? Never use them. It's not like they'll find anything…
3. Source code scanning in the cloud? Are you crazy? And let the NSA steal our code?

available — to provide confidence and substantiate platform providers' foundational security.

Several small professional services firms are popping up to evaluate code development practices — helping to find bad code and more importantly getting development teams pointed in the right direction. Finally, there is new a trend in application vulnerability management — no, not tools that scan for platform defects. The new approaches track vulnerabilities in much the same way we track general software defects, but with a focus on specific security issues. Severity, path to exploit, line of code responsible, and calling modules that rely on defective code, are all areas where tools can help development teams prioritize security fixes.

Exposing Yourself

At the beginning of 2013 several small application security gateway vendors were making names for themselves. Within a matter of months the three biggest were acquired (Mashery by Intel, Vordel by Axway, and Layer 7 by CA). Large firms snapping up little firms often signals the end of a market, but in this case it is just the beginning — to become truly successful these smaller technologies need to be integrated into a broader application infrastructure suite. Time waits for no one, and we will see a couple new vendors on the show floor with similar models.

You will also see a bunch of activity around API gateways because they serve as application development accelerators. The gateway provides base security controls, release management, and identity functions in a building block platform, on top of which companies publish internal systems to the world via RESTful APIs. This means an application developer can focus on delivery of a good user experience rather than worrying extensively about security. Even better, a gateway does not care whether the developer is an employee or a third party. That supports the trend of using third-party coders to develop mobile apps. Developers are compensated according to the number of users of their apps, and gateways track which app serves each customer. This simple technology allows crowdsourcing apps, so we expect the phenomenon to grow over the next few years.

Bounty Hunters – Bug Style

Several companies, most notably Google and Microsoft, have started very public "security bug bounty" programs and hackathons to incentivize professional third-party vulnerability researchers and hackers to find and report bugs for cash. These programs have worked far better than the companies originally hoped, with dozens of insidious and difficult-to-detect flaws disclosed quickly, before new code went live. Google alone has paid out more than $1 million in bounties — their programs has been so successful that they have announced they will quintuple rewards for bugs on core platforms. These programs tend to attract skilled people who understand the platforms and uncover things development teams were totally unaware of. Additionally, internal developers and security architects learn from attacker approaches. Clearly, as more software publishers engage the public to shake down their applications, we will see everyone jumping on this bandwagon — which will provide an opportunity for small services firms to help software companies set up these programs.

Not sure how well this will work against bugs in App Engine, but I might as well try, no?

Photo credit: http://flic.kr/p/d6FcD3

Application Security Vendors at RSA 2014:

Web App Firewalls	Application Testing	Secure Development
Akamai (3035N)	Armorize (now Proofpoint) (520S)	Arxan (326S)
Alert Logic (601S)	Checkmarx (3541N)	Cigital (132S)
Barracuda Networks (3237N)	Cigital (132S)	Coverity (2417S)
HP (3401N)	CORE Security (721S)	HP (3401N)
Fortinet (1317S)	HP (3401N)	IBM (1109S)
Imperva (701S)	IBM (1109S)	Klocwork (2229S)
Juniper (3105N)	Qualys (2821N)	Metaforic (435S)
Qualys (2821N)	Rapid7 (1727S)	
TrustWave (3527N)	Tenable (3631N)	
F5 (1801S)	Tripwire (3501N)	
	Veracode (3521N)	

Network Security

We have been tracking next-generation network security (NGNS) evolution for 5 years, during which time it has fundamentally changed the the perimeter, as we will explain below. Those who moved quickly to embrace NGNS have established leadership positions at the expense of those who didn't. Players who were leaders 5 short years ago are now non-existent, and we have a new generation of folks with innovative network security approaches to handle advanced attacks. After many years of stagnation, network security has come back with a vengeance.

Back to Big Swinging (St)icks

The battle for the perimeter is raging right now in network security land. In one corner we have incumbent firewall players, who believe that because the future of network security has been anointed 'NGFW' by those guys in Stamford, their manifest destiny is to subsume every other device in the perimeter. Of course the incumbent IPS folks

have something to say about that, and are happy to talk about how NGFW devices keel over when you turn on IPS rules and SSL decryption.

So we come back to the age-old battle, descending into the muck of the network. Whose thing is bigger? Differentiation on the network security front has gone from size of application libraries in 2012, to migrating from legacy port/protocol policies in 2013, to who has the biggest and fastest gear in 2014. As they work to substantiate their claims we see a bunch of new entrants in the security testing business. This is a good thing — we still don't understand how to read NSS Labs' value map.

Big 3

1. I know deploying 3 boxes on each ingress/egress port to catch malware is good for you, but what about me?
2. Just because the vendor calls it an NG device doesn't mean it's an NG device…
3. Help me understand how 150gbps becomes 500mbps when I turn on SSL decryption…

Besides the size of the equipment, there is another more impactful differentiation point for NGXX boxes: network-based malware detection (NBMD). All the network security leaders claim to detect malware on the box, and then they sling mud about where analysis occurs. Some run analysis on the box (more often a set of boxes) while others run in the cloud — and yes, they are religious about it. If you want to troll a network security vendor tell them their approach is wrong.

You will also hear the NGXX folks who continue to espouse consolidation, but not in a UTM-like way because UTM is so 2003. But in a much cooler and shinier NGXX way. No, there is no actual difference — but don't try telling a marketeer that. They make their money ensuring things are sufficiently shiny on the RSAC show floor.

More Bumps (in the Wire)

Speaking of network-based malware detection (NBMD), that market continues to be red hot. Almost every organization we speak to either has or is testing it. Or they are pumping some threat intelligence into network packet capture devices to look for callbacks. Either way, enterprises have gotten religion about looking for malware on the way in — **before** it wreaks havoc.

One area where they continue to dawdle, though, is putting devices inline. Hold up a file for a microsecond, and employees start squealing like stuck pigs. The players in this market who offer this capability as a standalone find most of their devices deployed out-of-band in monitor mode. With the integration of NBMD into broader NG network security platforms, the capability gets deployed inline because the box is inherently inline.

This puts standalone devices at a competitive disadvantage, and likely means there won't be any standalone players much longer. By offering capabilities that must be inline (such as IPS), vendors like FireEye will force the issue and get their boxes deployed inline. Problem solved, right? Of course going inline requires a bunch of pesky features like fail open, hot standby, load balancing, and redundant hardware. And don't forget the flack jacket when a device keels over and takes down a Fortune 10 company's call center.

ET Phone Home

Another big theme you will see at this year's RSA is the attack of Threat Intelligence (TI). You know, kind of like when ET showed up all those years ago, got lost, and figured out how to send a network ping zillions of light years with a Fisher Price toy. We are actually excited about how TI offerings are developing — with more data on things like callbacks, IP reputation, attack patterns, and all sorts of other cool indicators of badness. Even better, there is a drive to integrate this data more seamlessly into security monitoring, and eventually to update blocking rules on network security devices automatically.

If this guy leads your Threat Intelligence function, you may be in trouble…

Photo credit: http://flic.kr/p/7viawa

Of course automatic blocking tends to scare the crap out of security practitioners. Mostly because they saw Terminator too many times. But given the disruption of cloud computing and this whole virtualization thing, security folks will get much more comfortable having a machine

tune their rules, because it will hit fast. There is no alternative — carbon-based units just can't keep up.

Though we all know how that story featuring Skynet turned out, so there will be a strong focus on ensuring false positives are minimized, probably to the point of loosening up blocking rules just to make sure. And that's fine — the last thing you want is a T1000 showing up to tell you that sessions you knocked down caused a missed quarter.

Network and Endpoints: BFFs

When it comes to advanced malware, the network and endpoints are not mutually exclusive. In fact over the past year we have seen integration between endpoint folks like Bit9 and network-based malware detection players such as FireEye and Palo Alto Networks. This also underlies the malware defense stories from Sourcefire (now Cisco) and McAfee, and pushed the FireEye/Mandiant acquisition announced in January. You can bet the Mandiant folks were drinking some high-end champagne as they welcomed 2014.

Don't worry. Soon enough the network and endpoint folks will be fighting again…

Photo credit: http://flic.kr/p/umQVE

There is method to the madness, because network folks need visibility on endpoints. Those network detection devices will inevitably miss at some point, both due to new attack tactics (those notorious 0-days) and devices that escape the comfy confines of the corporate network and perimeter defenses. It's hard to keep track of those pesky laptops and mobile devices. If you can't catch everything on the way in, you had better be able to figure out what happened on the devices and determine if that thing you missed caused a mess — quickly.

So what does it all mean? You will likely see a bunch of kumbaya on the show floor — these enemies are now friends. Best friends, at that.

Clouds on the Horizon

As we wrote under key themes, cloud everything remains a big driver for security stuff. And yes, it's boring. But the network security folks have been largely left out of cloudwashing for the past few years, and this year they get to catch up. We will cover that in depth in our cloud security deep dive, but for now suffice it to say that all the network security vendors continue to roll their stuff into VMs and AMIs that can run in public and private clouds. So they are ready to solve the cloud computing security problem. Incumbents continue to solve yesterday's problems tomorrow.

This isn't all bad — but understand the performance impact of routing all your traffic through a virtual network security device choke point for policy enforcement. But all those issues go away as Software Defined Networks (SDNs) provide much more flexibility to route traffic as you need, and offer bigger faster networks. SDNs do promise to change a lot, but be wary of the double-edged sword: now your admins (or anyone who hacks them) can press a button and take your entire security layer out of the traffic flow.

Network Security Vendors at RSA 2014:

Network Security		Network Analysis/ Forensics	Email/Web Security
Arbor Networks (1323S)	Juniper (3105N)	Accolade Technology (2432S)	Akamai (3035N)
AUCONET (3421N)	McAfee (3203N)	APCON (632S)	AlertLogic (601S)
Barracuda Networks (3237N)	NetCitadel (341S)	Arbor Networks (1323S)	AppRiver (1533S)
Blue Cat (2504S)	Net Optics (1329S)	Blue Coat/Solera Networks (2721N)	Axway (726S)
Big Switch Networks (2512S)	OpenDNS (2522S)	Click Security (438S)	Barracuda Networks (3237N)
Bradford Networks (114S)	Palo Alto Networks (3433N)	Gigamon LLC (1753)	Blackberry (1827S)
Celestix Networks (1933S)	Procera Networks (2321S)	GD Fidelis (2028S)	Blue Coat (2721N)
Check Point (1101S)	Prolexic (1433S)	Ixia (3135N)	Cisco (3221N)
Corero (2407S)	Radware (1915S)	Lancope (3634N)	ClearSwift (539S)
Cisco (3221N)	Shape Security (2001S)	Light Cyber (118S)	CommTouch (1633S)
Cyberoam (615S)	Sophos (2701N)	Narus (2715N)	Malcovery (2140S)
Damballa (1129S)	SourceFire (2741N)	Netscout (2435S)	McAfee (3203N)
Dell SonicWALL (1301S)	SSH Communications (2608N)	nPulse (741S)	Microsoft (3005N)
F5 Networks (1801S)	StoneSoft (409S)	Qosmos (1639S)	ProofPoint (3615N)
FireEye (2813N)	TrustWave (3527N)	RSA (3021N)	SilverSky (1501S)
ForeScout (1027S)	VMWare (1615S)	VSS Monitoring (301S)	Sophos (2701N)
Fortinet (1317S)	WatchGuard (1335S)		Symantec (2803N)
HOB (3231N)			Trend Micro (2601N)
HP (3401N)			Websense (3413N)
Huawei Technologies (2101S)			Zix Corp (1832S)
Infoblox (226S)			Zscaler (1135S)
InfoExpress (2127S)			
IBM (1109S)			

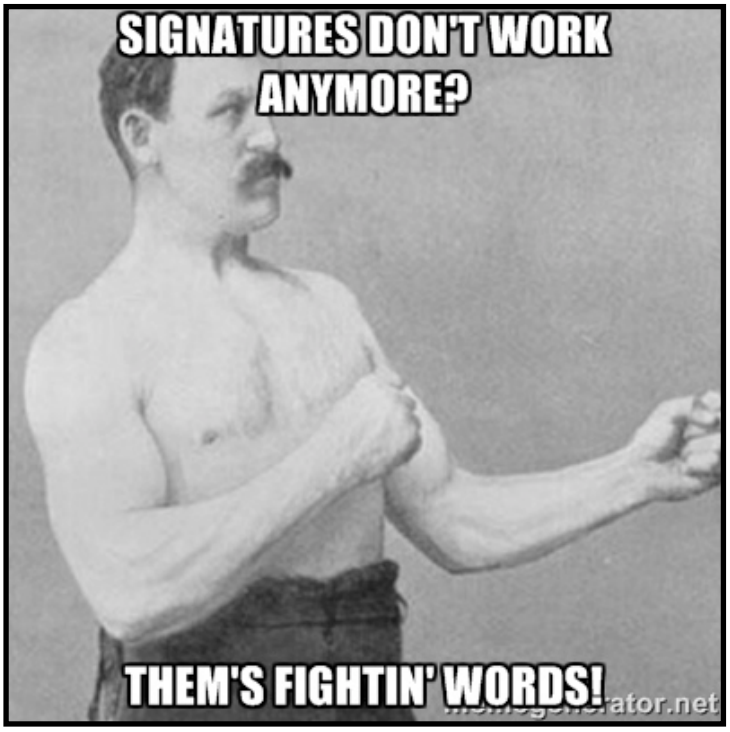
Endpoint Security

The Endpoint Security market clearly remains in transition. Existing EPP products are stuck in purgatory — unable to change without killing the golden goose, but not really doing the job either. And the emerging technologies that promise to detect and prevent malware better aren't yet ready for prime time. So what's an organization to do? Invest in endpoint forensics, of course...

EPP: Living on Borrowed Time?

Every year we take a step back and wonder if this is the year customers will finally revolt against endpoint protection suites and shift en masse to something free, or one of the new technologies focused on preventing advanced attacks. It is so easy to forget how important inertia is to security buying cycles. With the continued (ridiculous) PCI mandate for 'anti-malware' (whatever that means), AV vendors continue to print money.

Our friends at 451 Group illustrated this with a recent survey. A whopping 5% of respondents are reducing their antivirus budget, while 13% are actually increasing it. Uh, what?!?! Most are maintaining the status quo, so you will see the usual AV suspects with their big RSA Conference booths, paid for by inertia and the PCI Security Standards Council. Sometimes we wish for a neutron clue-bat to show the mass market the futility of old-school AV...



Don't Call It a Sandbox

The big AV vendors are all afraid to rock the boat, so don't expect innovation from them. The good news is that plenty of companies are trying different approaches to detection on endpoints and servers. Some look at file analysis, others have innovative heuristics, and you will also see isolation technologies on the floor. Don't forget old-school application control, which is making a comeback on the back of Windows XP's end of life, and the fact that servers and fixed-function devices **should** be totally locked down.

We expect isolation vendors to make the most noise at the Conference. Their approach is to isolate vulnerable programs (including Java, browsers, and/or Office suites) from the rest of the device, so malware cannot access the file system or other resources to further compromise devices. Whether via virtualization, VDI, old-school terminal services, or newfangled endpoint isolation (either at the app or kernel level), isolation is all about accepting that you cannot stop infection, so you need to make sure malware cannot reach anything interesting on the device.

These technologies are promising but not yet mature. We have heard of very few large-scale implementations but we need to do **something** different, so we are watching these technologies closely and you should too.

The Rise of the Endpoint Monitors

As we described in the introduction to our Advanced Endpoint and Server Protection series, we are seeing a shift in budget from predominately prevention to detection and investigation functions. This great because you cannot stop all attacks.

At the show we will see a lot of activity around endpoint forensics, driven by hype over the recent FireEye/Mandiant and Bit9/Carbon Black deals, bringing this technology into the spotlight. But there is a bigger theme: what we call "Endpoint Activity Monitoring". It involves storing very detailed historical endpoint (and server) telemetry, and then searching for indicators of compromise in hopes of identifying new attacks that evade preventative controls. This allows you to find compromised devices even when they are dormant.

Of course if isolation technology is 'immature', endpoint activity monitoring is embryonic. There are a bunch of different approaches to storing that data, so you will hear vendors poking each other about whether they store on-site or in the cloud. They also have different approaches to analyzing that massive amount of data. But all these technical details obscure the real issue: whether they can scale. But this is another technology to keep an eye on.

Endpoints and Network: BFFs

The other side of the coin discussed in our Network Security deep dive is that endpoint solutions to prevent and detect advanced malware need to work with network stuff. The sooner an attack can be blocked or detected, the better, so being able to do some prevention/detection on the network is key.

Interoperability is also important because running a full-on malware analysis environment on every endpoint is inefficient. Having an endpoint or server agent send a file, either to an on-premise network-based sandbox or a cloud-based analysis engine, is a better way to determine how malicious the file really is.

Of course this malware analysis doesn't happen in real time, and you usually cannot wait for a verdict from off-device analysis before allowing a file to execute. So devices will still get popped but technology like endpoint activity monitoring, described above, gives you the ability to search for devices that have been pwned using a malware profile from an analysis engine.

Mobile?

Most MDM vendors have been bought, so managing these devices is pretty much commodity technology now. Every endpoint protection vendor bundles a mobile offering into their suite. But nobody seems to care. It's not that these products aren't selling. They are flying off the virtual shelves, but they are simply not exciting. And if it's not exciting you won't hear much about it at the Conference.

Some new startups will be introducing technologies like mobile IPS, but that just seems like yesterday's approach to a problem that requires thinking differently. Maybe these folks should check out Rich's work on protecting iOS, which gets down to the real issue: the data. It seems like the year of mobile malware is coming — right behind the year of PKI. Not that mobile malware doesn't exist, but it's not having enough impact to fire the industry up. Which means it will be a no-show at the big event.

Endpoint Security Vendors at RSA 2014:

Endpoint Anti-Malware	Disk Encryption	Mobile Security
AhnLab (3515N)	Check Point (1101S)	AirWatch (1627S)
Antiy Labs (1117S)	Entrust (2615N)	AppRiver (1533S)
Bit9 (827S)	IronKey by Imation (1601S)	Appthority (2021S)
BeyondTrust (1415S or 3535N)	McAfee (3203N)	Blackberry (1827S)
BitDefender (638S)	Microsoft (3005N)	Cisco (3221N)
Bromium (2408S)	RSA (3021N)	Device Lock (732S)
Check Point (1101S)	SafeNet (2729N)	Good Technology (939S or 2630N)
Commtouch (1633S)	Sophos (2701N)	IronKey by Imation (1601S)
CounterTack (933S)	Symantec (2803N)	Juniper (3105N)
ESET (1926S)	Thales e-Security (909S)	Kaspersky (1401S)
IBM (1109S)	Trend Micro (2601N)	McAfee (3203N)
Kaspersky (1401S)		MobileIron (2439S)
Kingsoft (1117S)		Sophos (2701N)
Lumension (1009S)		Symantec (2803N)
McAfee (3203N)		Trend Micro (2601N)
Microsoft (3005N)		Webroot (832S)
Sophos (2701N)		
Symantec (2803N)		
ThreatTrack (1901S)		
Trend Micro (2601N)		
Trusteer/IBM (2239S)		
Webroot (832S)		

Identity and Access Management

One of the biggest trends in security never gets any respect at RSA. Maybe because identity folks still look at security folks cross-eyed. But this year things will be a bit different.

The Snowden Effect

Companies are (finally) dealing with the hazards of privilege — a.k.a. Privileged User Access. Yes, we hate the term "insider threat" — not least because we have good evidence that external risks are the real issue. That said, logic does not always win out — many companies are asking themselves right now, "How can I stop a 'Snowden Incident' from happening at my company?" This Snowden Effect is getting traction as a marketing angle, so you will see it on the RSA Conference floor — people are worried about their dirty laundry going public.

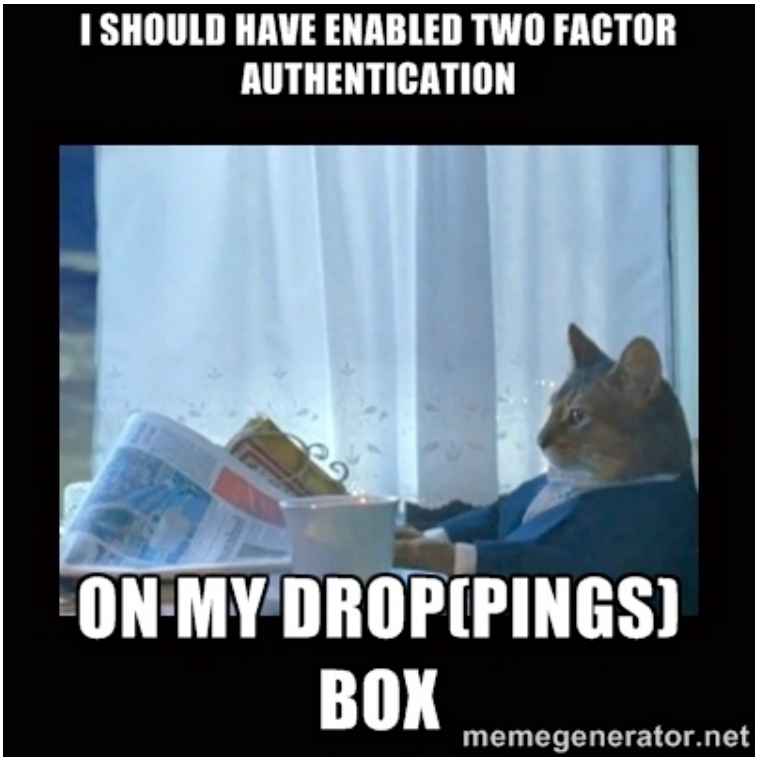
Aside from the marketing hype, we have been surprised by how zealously companies are now pursuing technology to enforce Privileged User Access policies. The privileged user problem is not new, but companies' willingness to incur cost, complexity, and risk to address it is. Part of this is driven by auditors assigning higher risk to privileged accounts (On a cynical note, we have to ask, "What's the matter, big-name audit firm? All out of easy findings?"). But sometimes headline news does really scare the bejesus out of companies in a vertical (that's right, we're looking at you, retailers). Whatever the reason, companies and external auditors are waking up to privileged users as perhaps the largest catalyst in downside risk scenarios. To be clear, that doesn't mean it's the biggest risk, but it provides the largest downside. Attackers go after databases because that's where the data is (duh). The same goes for privileged accounts — that's where the

Big 3

1. We need to up our bandwidth — 48,000 users just forgot their passwords.
2. Facebook ID, the Enterprise Edition. What could possibly go wrong?
3. When do I get Active Directory for my iPhone?

access is! An insider with access can do a lot more damage than your typical external attacker.

But while the risk is almost universally recognized, what to do about it isn't — aside from "continuous improvement", because hey, everyone needs to pass their audits. One reason the privileged user problem has persisted so long is that the controls often reduce productivity for some of the most valuable users, drive up cost, and generally increase availability risk. Career risk, anyone? But that's why security folks make the big bucks. High-probability events gets the lion's share of attention, but lower-probability gut-punch events like privileged user misuse have come to the fore. Buckle up!



Nobody cares what your name is!

Third-party identity services and cloud-based identity are gaining momentum. The need for federation (to manage customer, employee, and partner identities), and two-factor authentication (2FA) to reduce fraud, are both powerful motivators. We expected last year's hack of Mat Honan to start a movement away from passwords in favor of certificates and other better user authentication tools. Instead we got risk-based handling of requests on the back end. It is not yet the year of PKI, apparently.

Companies are less concerned with logins and more concerned with request context and metadata. Does the user normally log in at this time? From that location? With that app? Is this a request they normally make? Is it for a typical dollar amount? A lot more is being spent on analytics to determine 'normal' behavior than on replacing identity infrastructure, and fraud analytics on the backend are leading the way. In fact precious little attention is being paid to identity systems on the front end — even payment processors are discussing third-party identity from Facebook and Twitter for authentication. What could possibly go wrong? As usual cheap, easy, and universally available trump security — for authentication tools, this time. To compensate, effort needs to be focused on risk-based authorization on the backend.

Identity and Access Management Vendors at RSA 2014:

Identity and Provisioning	IDaaS	Authentication
Attachmate (2726N)	Okta (1938S)	Authentify (526S)
BeyondTrust (1415S or 3535N)	Ping Identity (1439S)	Behaviosec (2238S)
CA Technologies (2709N)	SecureAuth (315S)	Collective Software (534S)
Centrify (2015S)	Symantec (2803N)	Entrust (2615N)
Cyber-Ark (915S)	Symplified (433S)	GlobalSign (320S)
Dell Quest (1301S)		HID Global (3507N)
FoxT (733S)		NagraID (3611N)
IBM (1109S)		OATH (709S)
Identity Finder (3635N)		Okta (1938S)
Intel (3203N)		OneLogin (1141S)
Lieberman Software (1515S or 2604N)		Microsoft (PhoneFactor) (3005N)
Microsoft (3005N)		RSA (3021N)
Obethur Technologies (609S)		SafeNet (2729N)
Oracle (1509S)		SecureAuth (315S)
Ping Identity (1439S)		StrongAuth (2129N)
RSA (Aveksa) (3021N)		Symantec (2803N)
Thycotic Software (415S)		Symplified (433S)
Viewfinity (841S)		Thales e-Security (909S)
		Vasco Data Security (833S)

Security Management and Compliance

Say "BIG DATA" 10 times fast. Now you'll only be about 10,000 mentions short of what you'll hear at the RSA Conference this year. If it's about security management or monitoring, big data will be all the rage. Of course the vendors haven't yet figured out that you don't care how the technology works — just that it tells you what you need to know. You can tell them on March 3. Don't spoil the fun at the conference...

If You Don't Like It, SECaaS!

We have taken a bunch of calls this year from folks looking to have someone else manage their SIEM. Why? Because after two or three failed attempts, they figure if they are going to fail again, they might as well have a service provider to blame. Though that has put some wind in the sails of service providers who offer monitoring services, providing an opening for those who can co-source and outsource SIEM. Just make sure to poke and prod the providers about how you are supposed to respond to an incident when they have your data. And to be clear... they have your data.

Counter Intelligence

As we mentioned in our network security deep dive, threat intelligence (TI) is hot. But in terms of security management many early TI services were just about integrating IP blacklists and malware file signatures — not actually all that intelligent! Now you will see all sorts of intelligence services on malware, botnets, compromised devices, and fraud analytics — and the ability to match their indicators against your own security events. This is not just machine-generated data, but often includes user behaviors, social media analysis, and DoS tactics. Much of this comes from third-party services whose sole business model is to go out looking for malware and figure out how best to detect and deal with it. These third parties have

Big 3

1. You think the NSA will be getting into the threat intelligence business?
2. So you're telling me THIS is the year SIEM becomes useful?
3. Did Doctor Who consult the PCI council on time machine design?

been very focused on making it easier to integrate data into your SIEM, so keep an eye out for partnerships between SIEM players and TI folks trying to make SIEM useful.

Shadow of Malware

SIEMs have gotten a bit of a black eye over the last couple years — just as vendors were finally coming to terms with compliance requirements, they got backhanded by customer complaints about failures to adequately detect malware. As malware detection has become a principal use case for SIEM investment, vendors have struggled to keep pace — first with more types of analytics, then more types of data, and then third-party threat intelligence feeds. For a while it felt like watching an overweight mall cop chase teenage shoplifters — funny so long as the cop isn't working for you. But now some of the mall cops are getting their P90X on and chasing the mall rats down — yes, we see SIEMs becoming faster, stronger, and better at solving current problems. Vendors are quietly embracing "big data" technologies, a variety of built-in and third-party analytics, and honest-to-goodness visualization tools.

So you will hear a lot about big data analytics on the show floor. But as we said in our Security Management 2.5 research, don't fall into the trap of worrying about specific technologies. Big data technologies are key, but keep in mind it doesn't actually matter what the underlying technology is, so long as it meets your needs at the scale you require.

Third Time Is… the Same

There hasn't been much activity around compliance lately, since it got steamrolled by the malware juggernaut. Although your assessors show up right on time every quarter, and you haven't figured out how to get rid of them any quicker yet, have you? We didn't think so. PCI 3.0 is out but nobody really cares. It's the same old stuff, and you have a couple years to get it done. Which gives you plenty of time for cool malware detection stuff at the show. Unless you get breached, that is. Then every ROC you ever got is revoked instantaneously. It still amazes us how the PCI Security Standards Council can bend the space-time continuum again and again... The 'GRC' meme will be on the show floor, but that market continues to focus on automating the stuff you need to do, without adding real value to either your security program or your business. A good thing, yes, but not sexy enough to build a marketing program on. Aggregating data, reducing data, and pumping out reports — good times. If your organization is big enough and you have many moving technology parts (yeah, pretty much everyone), then these technologies make sense. Though odds are you already have something for compliance automation. The question is whether it sucks so badly you need to look for something else.

Vulnerability Management Plateaus

You know a market has reached the proverbial summit when the leading players talk about the new stuff they are doing. Clearly the vulnerability management market is there, with its close siblings configuration and patch management, although the latter two can be subsumed by the Ops group (to which security folks say, "Good riddance!"). The VM folks are talking about passive monitoring, continuous assessment, mobile devices, and pretty much everything except vulnerability management. Which makes sense because VM just isn't sexy. It is a zero-sum game, which will force all the major players in the space to broaden their offerings — did we mention they will all be talking about 'revolutionary' new features?

But the first step in a threat management process is 'Assessment'. A big part of that is discovering and understanding the security posture of devices and applications. That is vulnerability management, no? Of course it is — but the RSA Conference is about the shiny, not the useful...

Security Management & Compliance Vendors at RSA 2014:

SIEM/Log Management	Configuration/ Patch	VM/Pen Testing	GRC	Incident Response/ Forensics
AccelOps (122S)	IBM (1109S)	CORE Security (721S)	Agiliance (2600N)	Accuvant (2201S)
Alert Logic (601S)	HP (3104N)	IBM (1109S)	brinQa (115S)	Bit9 (827S)
AlienVault (1701S)	Lumension (1009S)	Imperva (701S)	CA (2709N)	Dell Secureworks (1309S)
Dell Secureworks (1309S)	McAfee (3203N)	McAfee (3203N)	Fox Technologies (733S)	GD Fidelis (2028S)
Hexis (815S)	Microsoft (3005N)	Qualys (2821N)	HP (3104N)	Guidance (1421S)
HP (3104N)	NetIQ (1409S)	Rapid7 (1727S)	IBM (1109S)	HBGary (309S)
IBM (1109S)	Qualys (2821N)	Secunia (2609N)	LockPath (238S)	IBM (1109S)
LogRhythm (1001S)	RSA (3021N)	Tenable (3631N)	MetricStream (101S)	Mandiant (501S)
McAfee (3203N)	Symantec (2803N)	TripWire (3501N)	Modulo (2440S)	Microsoft (3005S)
NetIQ (1409S)	TripWire (3501N)	TrustWave (3527N)	Oracle (1509S)	RSA (3021N)
RSA (3021N)			RSA (3021N)	Verizon Business (2735N)
Solarwinds (2507S)			TraceSecurity (2314S)	
Splunk (2835N)	**Operations Management**		**Training/ Education**	**Threat Intelligence**
SumoLogic (2519S)	AlgoSec (427S)		PhishMe (2121S)	Damballa (1129S)
Symantec (2803N)	FireMon (927S)		The Hacker Academy (2034S)	Malcovery (2140S)
Tenable (3631N)	RedSeal Networks (401S)		Wombat (2315S)	Norse Corporation (2334S)
TIBCO (1709S)	Skybox Security (715S)			Seculert (127S)
TripWire (3501N)	Tufin (1821S)			
TrustWave (3527N)				

Cloud Security

In our 2013 RSA Guide we wrote that 2012 was a tremendous year for cloud security. We probably should have kept our mouth shut and remembered all those hype cycles, adoption curves, and other wavy lines, because 2013 blew 2012 away. That said, cloud security is still nascent, and in many ways losing the race with the cloud market itself — widening the gap between what's happening in the cloud and what is being secured in the cloud. The next few years are critical for security professionals and vendors, as they risk being excluded from cloud transformation projects and finding themselves disengaged in enterprise markets as cloud vendors and DevOps take over security functions.

Lead, Follow, or Get the Hell out of the Way

2013 saw cloud computing begin to enter the fringes of the early mainstream. Already in 2014 we see a bloom of cloud projects, even among large enterprises. Multiple large financials are taking tentative steps into public cloud computing. When these traditionally risk-averse technological early adopters put their toes in the water, the canary sings (we know the metaphor should be that the canary dies, but we don't want to bring you down).

Simultaneously we see cloud providers positioning themselves as a kind of security providers. Amazon makes abundantly clear that they consider security one of their top two priorities, that their data centers are more secure than yours, and that they can wipe out classes of infrastructure vulnerabilities to let you focus on applications and workloads. Cloud storage providers are starting to provide data security well beyond what most

enterprises can even dream of implementing (such as tracking all file access, by user and device). In our experience security has a tiny role in many cloud projects, and rarely in the design of security controls. The same goes for traditional security vendors, who have generally failed to adapt their products to meet new cloud deployment patterns.

We can already see how this will play out at the show and in the market. There is a growing but still relatively small set of vendors taking advantage of this gap by providing security far better attuned to cloud deployments. These are the folks to look at first if you are involved in a cloud project. One key to check is their billing model: do they use elastic metered pricing? Can they help secure SaaS or PaaS, like a cloud database? Or is their answer, "Pay the same as always, run our virtual appliance, and route all your network traffic through it."? Sometimes that's the answer, but not nearly so often as it used to be.

And assess honestly when and where you need security tools, anyway. Cloud applications don't have the same attack surface as traditional infrastructure. Risks and controls shift — so should your investments. Understand what you get from your provider before you start thinking about spending anywhere else.

SECaaS Your SaaS

We are getting a ton of requests for help with cloud vendor risk assessment (and we are even launching a 1-day workshop), mostly driven by Software as a Service. Most organizations only use one to three Infrastructure as a Service providers, but SaaS usage is exploding. More often than not, individual business units sign up for these services — often without going through the procurement process.

A new set of vendors is emerging to detect usage of SaaS, help integrate it into your environment (predominantly through federated identity management), and add a layer of security. Some of these providers even provide risk ratings, although that is no excuse for not doing your own homework. And while you might think you have a handle on SaaS usage because you block Dropbox and a dozen other services, there are thousands of them in active use. In the words of one risk officer who went around performing assessments: at least one of them is a shared house on the beach with a pile of surfboards out front, an open door, and a few servers in a closet.

There are a dozen or more SaaS security tools now on the market, and most of them will be on the show floor. They offer a nice value proposition but implementation details vary greatly, so make sure whatever you pick meets your needs. Some of you care more about auditing, others about identity, and others about security — but none of the options really offers everything yet.

Workload Security Is Coming

"Cloud native" application architectures combine IaaS and SaaS in new highly dynamic models that take advantage of autoscaling, queue services, cloud databases, and automation. They might pass a workload (such as data analysis) to a queue service, which spins up a new compute instance in the currently cheapest zone, which completes the work, and then passes back results for storage in a cloud database.

Under these new models — which are in production today — many traditional security controls break. Vulnerability assessment on a server that only lives for an hour? Patching? Network IDS, without a network to sniff?

Talk to your developers and cloud architects before becoming too enamored of any cloud security tools you see on the show floor. What you buy today may not match your needs in six months. You need to be project driven rather than product driven, because you can no longer purchase one computing platform and use it for everything. That is another reason you should focus on elastic pricing that will fit your cloud deployments as they evolve and change. An elastic pricing model is often the best indicator that a vendor 'gets' the cloud.

Barely Legal SECaaS

We are already running long, so suffice it to say there are many other security offerings as cloud services, and a large percentage of them are mature enough to satisfy your needs. The combination of lower operational management costs, subscription pricing, pooled threat intelligence, and other analytics, is often better than what you can deploy and manage completely internally. You still need to ask hard questions and be very careful with technobabble pillow talk, because not all cloud services are created equal. Look for direct answers — especially

on how providers protect your data, segregate users, and allow you to get data back if necessary. Finally, walk away if they want you to sign an NDA first.

Here's to the Server Huggers

Many of you are considering private clouds, or have one already, to reduce the perceived risks of multitenancy. As we wrote in What CISOs Need to Know about Cloud Computing, we think private clouds are largely a transition technology to make server huggers feel they are still in control. Well, that and to hold us over until there is more competition in the real public cloud market — in contrast to outfits merely offering a different flavor of hosting.

Most of the private cloud security focus is, rightfully, on network security. The key questions to ask are how it affects your network topology and how well Software Defined Networking is supported, because this is the first place we see SDN establishing a beachhead. Also understand the costs and hardware requirements of supporting a private cloud. You definitely need something that supports distributed deployments, tightly integrated with your cloud platform.

You can certainly hold onto your workloads. But they are going to the cloud anyway…

Photo credit: http://flic.kr/p/f9vs5

The Cloudwashing Dead

Finally, we see no shortage of cloudwashing, and expect to see a lot more at the show. Nearly every product will feature a 'cloud' version. But by this point you should know what to look for to determine which are built for the cloud, and which are merely the same software wrapped in a virtual appliance or an endpoint/server agent that has barely been modified. Ask for reference clients who have deployed on Azure, Amazon, or Google — not just on one of the many semi-private hosted cloud providers.

Cloud Security Vendors at RSA 2014:

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

Cloud Security	SECaaS	Virtualization Security
Afore (2501S)	Accuvant (2201S)	CA Technologies (2709N)
AccelOps (122S)	Akamai (3035N)	Check Point (1101S)
CipherCloud (2115S)	Alert Logic (601S)	Cisco (3221N)
Cloud Security Alliance (2433S)	AppRiver (1533S)	Fortinet (1317S)
CloudLock (2135S)	AT&T (809S)	HP (3401N)
PerspecSys (538S)	Barracuda Networks (3237N)	HyTrust (1715S)
Ping Identity (1439S)	Cybera (2033S)	IBM (1109S)
SafeNet (2729N)	Dell SecureWorks (1309S)	Juniper Networks (3105N)
SkyHigh Networks (133S)	Digital Defense (2032S)	Kaspersky Lab (1401S)
Symantec (2803N)	FiberLink, now IBM (2405S)	McAfee (3203N)
Symplified (433S)	HP (3401N)	Palo Alto Networks (3433N)
Thales e-Security (909S)	IBM (1109S)	RSA (3021N)
Trend Micro (2601N)	Imperva (701S)	SafeNet (2729N)
VMWare (1615S)	Mandiant (501S)	SourceFire (2741N)
Voltage Security (1921S)	McAfee (3203N)	Tenable (3631N)
Vormetric (515S or 2614N)	Okta (1938S)	Thales e-Security (909S)
	ProofPoint (1527S or 3615N)	Trend Micro (2601N)
	Qualys (2821N)	VMWare (1615S)
	SilverSky (1501S)	Voltage Security (1921S)
	Solutionary (1621S)	Vormetric (515S or 2614N)
	Sophos (2701N)	
	Symantec (2803N)	
	Trend Micro (2601N)	
	Trustwave (3527N)	
	Verizon Business (2735N)	
	Websense (3413N)	

See Securosis Speak

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

Speaking Sessions

- **Rich:** STR-T09 — Inflection: Security's Next 10 Years
  (Tuesday 4:00-5:00, West Room 2020)
- **Mike:** MASH-W01 — Neuro-Hacking 101: Taming Your Inner Curmudgeon
  (Wednesday 8:00-9:00, West Room 3018) — with Jennifer Minella
- **Rich:** CSV-W02 — Dueling Banjos — Cloud v Enterprise Security: Using Automation & DevOps NOW
  (Wednesday 9:20-10:20, West Room 2002) — with Chris Hoff
- **Mort:** ASEC-W03 — DevOps/Security Myths Debunked
  (Wednesday 10:40-11:40, West Room 2014) — panel
- **Mort:** CSV-R01 — Oh the PaaSabilities, Security in a Platform as a Service World
  (Thursday 8:00-9:00, West Room 2002)
- **Mort:** GRC-F02 — Visualize This! Meaningful Metrics for Managing Risk
  (Friday 10:20-11:20, West Room 2011) — panel

Other Events

- **AGC:** On Monday Mike will be moderating a panel at the AGC West Coast Investor Conference on "Productizing Incident Response" with folks from FireEye, Guidance Software, Carbon Black, GD Fidelis, and iSIGHT Partners.

- **AccessData Lunch:** On Wednesday, Rich is participating on a panel on incident response sponsored by AccessData.

- **Flash Talks:** Rich was invited back to the RSA Flash Talks on Thursday at 5:30 (formerly known as PK Night). He will remain clothed. Probably.

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 because this isn't the only event we attend there. Here are our recommendations with some tips from 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 these establishments to pull up a map, description, and ratings in your web browser.

It's even mobile friendly!

(Not that the rest of this document is).

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

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

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

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

Close food courts with decent food for lunch:

Westfield Center, Metreon

Best Drinks: Bourbon and Branch

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 a 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)

RSA Conference 2014 Vendor List

Organization	Sponsor Level	Booth #	Location
10ZIG Technology Inc.		2516	South Expo
21CT, Inc.		2420	South Expo
3M		527	South Expo
6WIND		940	South Expo
Accellion, Inc.		214	South Expo
AccelOps		122	South Expo
AccessData		2338	South Expo
Accolade Technology, Inc.		2432	South Expo
Accuvant		2201	South Expo
Advantech		209	South Expo
Afore Solutions		2501	South Expo
Agiliance	Bronze	2600	North Expo
AhnLab	Silver	3515	North Expo
AirWatch		1627	South Expo
Akamai Technologies, Inc.	Global Gold	3035	North Expo
AlertEnterprise		339	South Expo
Alert Logic		601	South Expo
AlgoSec		427	South Expo
AlienVault		1701	South Expo
Allegro Software Development Corporation		233	South Expo
Alta Associates Inc.		938	South Expo
AMAX Information Technologies		426	South Expo
American Portwell Technology, Inc.		420	South Expo
Antiy Labs		1117	South Expo
APCON		632	South Expo
AppRiver		1533	South Expo
Appthority		2021	South Expo

Arbor Networks		1323	South Expo
Armorize now Proofpoint		520	South Expo
Arxan Technologies		326	South Expo
atsec information security GmbH		3421	North Expo
AT&T		809	South Expo
Attachmate	Bronze	2726	North Expo
AUCONET GmbH		3421	North Expo
Authentify, Inc.		526	South Expo
Axway, Inc.		726	South Expo
BAE Systems Detica		2226	South Expo
Barracuda Networks	Silver	3237	North Expo
Bay Dynamics, Inc.		2240	South Expo
Behaviosec		2238	South Expo
Beijing Zhongguancun Overseas Science Park		1117	South Expo
BeyondTrust Software		1415	South Expo
BeyondTrust Software		3535	North Expo
Big Switch Networks		2512	South Expo
Bit9, Inc.		827	South Expo
Bitdefender		638	South Expo
BlackBerry		1827	South Expo
Black Lotus		2506	South Expo
BlueCat		2504	South Expo
Blue Coat Systems		2721	North Expo
Bradford Networks		114	South Expo
Brainloop AG		3421	North Expo
brinQa		115	South Expo
Bromium		2408	South Expo
Bundesdruckerei GmbH		3421	North Expo
Catbird		2505	South Expo
CA Technologies	Silver	2709	North Expo
Celestix Networks		1933	South Expo
CenterTools Software GmbH		3421	North Expo

Centrify		2015	South Expo
Champlain College		340	South Expo
Checkmarx	Bronze	3541	North Expo
Check Point Software		1101	South Expo
CHERRY		2227	South Expo
Cigital		132	South Expo
CipherCloud		2115	South Expo
Cisco	Global Platinum	3221	North Expo
ClearBridge Technology Group		2500	South Expo
Clearswift Corporation		539	South Expo
Click Security		438	South Expo
CloudLock		2135	South Expo
Cloud Security Alliance (CSA)	Association Sponsor	2433	South Expo
Code 42 Software		2401	South Expo
Collective Software, LLC		534	South Expo
Commtouch		1633	South Expo
Corero Network Security		2407	South Expo
CORE Security		721	South Expo
CORISECIO GmbH		3421	North Expo
CounterTack		933	South Expo
Coverity, Inc.		2417	South Expo
Covertix Ltd.		136	South Expo
Covisint	Bronze	2635	North Expo
cPacket Networks		2511	South Expo
Cryptography Research, Inc.		1609	South Expo
Cryptomathic, Inc.		1739	South Expo
CSG Systems		2400	South Expo
cv cryptovision gmbH		3421	North Expo
Cybera		2033	South Expo
CyberArk		915	South Expo
CyberMaryland		200	South Expo
Cyberoam Inc.		615	South Expo

CyberPoint International		1037	South Expo
Cybertap LLC		100	South Expo
CyFIR		2504	South Expo
Cyphort		2329	South Expo
Cyvera Ltd.		2510	South Expo
Damballa		1129	South Expo
DaoliCloud Information Technology (Beijing) Co., LTD.		1117	South Expo
Daon		2523	South Expo
DBAPPSecurity Ltd.		239	South Expo
DB Networks		901	South Expo
Deja vu Security		332	South Expo
Dell Inc.		1301	South Expo
Dell SecureWorks		1309	South Expo
Denim Group		2332	South Expo
Device Lock		732	South Expo
DHS/Office of Cybersecurity & Communications		921	South Expo
DigiCert, Inc.		334	South Expo
Digital Defense, Inc.		2032	South Expo
DynamiCode Company Limited		1117	South Expo
Easy Solutions, Inc		1838	South Expo
eco e.V. Verband der deutschen Internetwirtschaft		3421	North Expo
Emerging Threats		2235	South Expo
Emulex		2333	South Expo
Enforcive		2027	South Expo
ENTERSEKT		3625	North Expo
Entrust	Silver	2615	North Expo
ESET North America		1926	South Expo
F5 Networks		1801	South Expo
Fasoo.com		1721	South Expo

Federal Bureau of Investigation		121	South Expo
Federal Reserve Bank of San Francisco		2416	South Expo
FEITIAN Technologies Co., Ltd.		1117	South Expo
Fiberlink		2405	South Expo
FileTrek		2414	South Expo
FireEye	Global Platinum	2813	North Expo
FireMon		927	South Expo
ForeScout Technologies, Inc.		1027	South Expo
ForgeRock		2438	South Expo
Fortinet		1317	South Expo
Fox Technologies, Inc.		733	South Expo
Freescale Semiconductor		1733	South Expo
Futurex		227	South Expo
Garner Products		1833	South Expo
General Dynamics Fidelis Cybersecurity Solutions		2028	South Expo
German Federal Ministry of Economics and Technology (BMWi)		3421	North Expo
Gigamon LLC		1021	South Expo
Glimmerglass Optical Cyber Solutions		2427	South Expo
Global Knowledge Training		2233	South Expo
GlobalSign		320	South Expo
Good Technology	Bronze	939	South Expo
Good Technology	Bronze	2630	North Expo
GreeNet Information Service Co., Ltd.		335	South Expo
Guardian Analytics		627	South Expo
Guidance Software, Inc.		1421	South Expo
Gurucul Solutions		215	South Expo
Halon Security AB		235	South Expo
HBGary		309	South Expo

Heshengda Information Security Technology Co., Ltd.		1117	South Expo
Hexis Cyber Solutions		815	South Expo
HID Global	Silver	3507	North Expo
Hillstone Networks, Inc.		201	South Expo
HitmanPro		2503	South Expo
HOB GmbH & Co. KG		3231	North Expo
HP	Platinum	3401	North Expo
Huawei Technologies Co., Ltd.		2101	South Expo
HyTrust		1715	South Expo
IBM		1109	South Expo
iBoss Security		221	South Expo
Identity Finder, LLC	Bronze	3635	North Expo
IEEE Computer Society		2126	South Expo
Imperva Inc.		701	South Expo
Infineon Technologies AG		3421	North Expo
Infoblox		226	South Expo
InfoExpress, Inc.		2127	South Expo
InfoGard		432	South Expo
Information Networking Institute - Carnegie Mellon		2132	South Expo
Information Security Media Group (ISMG)		700	South Expo
Information Systems Security Association (ISSA)	Association Sponsor	300	South Expo
InfoSecurity Magazine		739	South Expo
Intel Corporation		3203	North Expo
Intellicus		2426	South Expo
International Association of Privacy Professionals (IAPP)	Association Sponsor	302	South Expo
Ionic Security, Inc.		220	South Expo
Ipswitch File Transfer		1927	South Expo
IronKey by Imation		1601	South Expo
$(ISC)^2$	Global Education Sponsor	2100	South Expo

itWatch GmbH		3421	North Expo
IXIA	Global Gold	3135	North Expo
Jiransoft Inc.		2626	North Expo
Juniper Networks	Global Diamond	3105	North Expo
Kaspersky Lab		1401	South Expo
Keypasco AB		2409	South Expo
Key Source International		838	South Expo
Kingsoft Internet Security Software		1117	South Expo
Klocwork		2229	South Expo
Lancope	Bronze	3634	North Expo
LANDesk Software		2515	South Expo
Lanner Electronics Inc		109	South Expo
Leidos		1515	South Expo
Lieberman Software	Bronze	1515	South Expo
Lieberman Software	Bronze	2604	North Expo
Light Cyber		118	South Expo
Link11 GmbH		3421	North Expo
Linoma Software		333	South Expo
LJ Kushner & Associates, LLC		533	South Expo
LockPath, Inc.		238	South Expo
LOGbinder (a division of Monterey Technology Group, Inc.)		2422	South Expo
LogRhythm		1001	South Expo
Lumension Security, Inc.		1009	South Expo
Lynux Works	Bronze	2620	North Expo
Malcovery Security LLC		2140	South Expo
ManageEngine		2039	South Expo
Mandiant		501	South Expo
Marble Security		620	South Expo
MBX Systems		626	South Expo
McAfee an Intel Company		3203	North Expo
Messageware, Inc.		1935	South Expo
Metaforic		435	South Expo

MetricStream, Inc.		101	South Expo
Microsoft	Global Diamond	3005	North Expo
MITRE		2301	South Expo
MobileIron, Inc.		2439	South Expo
Mocana Corporation		338	South Expo
Modulo		2440	South Expo
NagraID Security	Bronze	3611	North Expo
Nallatech Inc.		2339	South Expo
Napatech Inc.		1932	South Expo
Narus	Silver	2715	North Expo
National Institute of Standards and Technology		108	South Expo
NetCitadel		341	South Expo
NetIQ Solutions		1409	South Expo
Net Optics, Inc.		1329	South Expo
Netronome		1427	South Expo
NetScout		2435	South Expo
Neustar		139	South Expo
New Horizons Computer Learning Centers		314	South Expo
Nexcom		738	South Expo
Norman Shark		2009	South Expo
Norse Corporation		2334	South Expo
Northrop Grumman		2509	South Expo
NPCore,Inc		2413	South Expo
nPulse Technologies		741	South Expo
NSA		1815	South Expo
NSFOCUS		521	South Expo
Ntrepid Corporation		327	South Expo
NuData		2138	South Expo
NXP Semiconductors		1341	South Expo
OASIS Interoperability Showcase		1909	South Expo
OATH		709	South Expo
Oberthur Technologies		609	South Expo

Okta, Inc.		1938	South Expo
Onapsis S.R.L		2109	South Expo
OneLogin, Inc.		1141	South Expo
OpenDNS		2522	South Expo
Oracle		1509	South Expo
Palo Alto Networks	Silver	3433	North Expo
Paraben Corporation		120	South Expo
PerspecSys Inc.		538	South Expo
PhishMe, Inc.		2121	South Expo
Pindrop Security		138	South Expo
Ping Identity Corporation		1439	South Expo
Portcullis Inc.		2134	South Expo
Portnox		2139	South Expo
PrimeKey Solutions AB		439	South Expo
PrivateCore		641	South Expo
Procera Networks		2321	South Expo
Prolexic Technologies		1433	South Expo
Proofpoint, Inc.	Bronze	1527	South Expo
Proofpoint, Inc.	Bronze	3615	North Expo
Protected-networks.com GmbH		2215	South Expo
QGroup GmbH		3421	North Expo
QIHU Technology Co., Ltd.		1117	South Expo
Qosmos		1639	South Expo
Qualys	Platinum	2821	North Expo
QuintessenceLabs	Bronze	2641	North Expo
Radiant Logic, Inc.		2232	South Expo
Radware, Inc.		1915	South Expo
Rapid7		1727	South Expo
Raytheon		1539	South Expo
RedSeal Networks		401	South Expo
Reservoir Labs		535	South Expo
Riscure North America		2415	South Expo
RiskIQ Inc.		2341	South Expo

Rohde & Schwarz SIT GmbH		3421	North Expo
RSA		3021	North Expo
RSAM		1015	South Expo
SafeNet	Silver	2729	North Expo
Safe-T		2514	South Expo
SANS		2303	South Expo
Seccuris USA Inc.		2520	South Expo
SECUDRIVE		112	South Expo
Seculert		127	South Expo
Secunia	Silver	2609	North Expo
Secure Access Technologies, Inc.		2434	South Expo
SecureAuth Corporation		315	South Expo
SecureNinja		840	South Expo
Security Mentor		532	South Expo
Securonix		2038	South Expo
SecuTech Solution PTY LTD		2404	South Expo
Shape Security		2001	South Expo
SilverSky		1501	South Expo
Sims Recycling Solutions		2421	South Expo
Sirrix AG security technologies		3421	North Expo
Skybox Security, Inc.		715	South Expo
Skyhigh Networks, Inc.		133	South Expo
SmartDisplayer Technology		2128	South Expo
Software Diversified Services		2508	South Expo
Software Engineering Institute		2026	South Expo
Solarflare		2220	South Expo
SolarWinds		2507	South Expo
Solutionary, Inc.		1621	South Expo
Sonatype, Inc.		2327	South Expo
Sophos	Gold	2701	North Expo

Sourcefire	Bronze	2741	North Expo
SpectorSoft Corporation		2428	South Expo
Spirent		621	South Expo
Splunk	Global Gold	2835	North Expo
SSH Communications Security	Bronze	2608	North Expo
STEALTHbits Technologies, Inc.		2340	South Expo
Stonesoft Inc.		409	South Expo
StrikeForce Technologies, Inc.		821	South Expo
StrongAuth		2129	South Expo
Sumo Logic		2519	South Expo
Swivel Secure Ltd		240	South Expo
Symantec Corporation		2803	North Expo
Symplified		433	South Expo
Syncplicity an EMC Company		2526	South Expo
SynerComm, Inc.	Bronze	2734	North Expo
SYPRIS Europe Aps		2634	South Expo
SYSMATE		1738	South Expo
Talariax Pte Ltd		241	South Expo
TeleSign Corporation		421	South Expo
TeleTrusT – IT Security Association Germany		3421	North Expo
Tenable Network Security	Bronze	3631	North Expo
Thales e-Security		909	South Expo
The Hacker Academy		2034	South Expo
ThreatMetrix		232	South Expo
ThreatTrack Security		1901	South Expo
Thycotic Software Ltd.		415	South Expo
TIBCO Software		1709	South Expo
Tilera Corporation		2320	South Expo
TITUS		801	South Expo
Topsec Science & Technology Co., Ltd.		1117	South Expo
TraceSecurity		2314	South Expo

Trend Micro Incorporated		2601	North Expo
Tripwire	Silver	3501	North Expo
Trusteer Ltd.		2239	South Expo
Trustwave	Silver	3527	North Expo
Tufin		1821	South Expo
TUV Informationstechnik GmbH		3421	North Expo
UNICOM Engineering		2841	North Expo
Unisys	Bronze	3621	North Expo
University of Denver		2133	South Expo
University of Maryland University College		141	South Expo
VASCO Data Security		833	South Expo
Venafi	Silver	2621	North Expo
Venustech Cybervision Co., Ltd		1117	South Expo
Veracode	Silver	3521	North Expo
Veraxes, Inc.		2526	South Expo
Verdasys, Inc.		2326	South Expo
Verizon	Silver	2735	North Expo
ViaForensics		2627	North Expo
Viewfinity		841	South Expo
Visible Statement		639	South Expo
V-Key Corp		727	South Expo
VMware		1615	South Expo
Voltage Security		1921	South Expo
Vormetric, Inc.	Bronze	515	South Expo
Vormetric, Inc.	Bronze	2614	North Expo
VSS Monitoring		301	South Expo
Watchdata Technologies		1117	South Expo
WatchGuard Technologies, Inc.		1335	South Expo
Webroot, Inc.		832	South Expo
Websense	Gold	3413	North Expo
WolfSSL.com		839	South Expo
Wombat Security Technologies, Inc.		2315	South Expo

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 2014

Securosis LLC

515 E. Carefree Highway
Suite 766
Phoenix, AZ 85085

Securosis

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