Securosis Guide to the RSA Conference 2011

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

Welcome to RSA 2011!

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 second 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. Plus our newest member and admin — Melissa (aka GeekGrrl); who spent many painful hours pulling together the vendor list.

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

Rich, Mike, and Adrian

from l to r: Mike Rothman, President; Rich Mogull, CEO; Adrian Lane, CTO

Table of Contents

Key Themes	**3**
Securosis Coverage Areas	**7**
Data Security	**8**
Application Security	**11**
Network Security	**13**
Endpoint Security	**15**
Email/Web (Content) Security	**17**
Security Management	**19**
Compliance	**20**
Virtualization and Cloud	**22**
See Securosis at RSA 2011	**23**
Evil Plans	**24**
Coming Soon: The Securosis Nexus	**25**
RSA Exhibitor List	**26**
About Securosis	**35**

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.

Cloud Security — From Pre-K to Kindergarten

Last year you could count *real* cloud security experts on one hand... with a few fingers left over. This year you'll see some real, practical solutions, but even more marketing abuse than last year. Cloud computing is clearly one of the major trends in enterprise technology, and woe unto the vendor that misses that boat. But we are only on the earliest edge of a change that will reshape our data centers, operations, and application design over the next 10 years. The number of people who truly understand cloud computing is small. And folks who really understand cloud computing *security* are almost as common as unicorns. Even fewer of them have actually implemented anything in production environments (something only one Securosis Contributors has done).

The big focus in cloud security these days is public Infrastructure as a Service offerings such as Amazon EC2 and Rackspace, due to increasing enterprise interest and the complexity of the models. But don't think everyone is deploying all their sensitive applications in the cloud. Most of the bigger enterprises we talk with are only at the earliest stages of public Infrastructure as a Service (IaaS) projects, while a lot more use of "private clouds". Medium-size and small organizations are actually more likely to jump into public cloud because they have less legacy infrastructure and complexity to deal with, and can realize the benefits more immediately (we're sure glad *we* don't need our own data center). It's important to separate a trend from its current position on the maturity curve — cloud computing is far from being all hype, but we're still early in the process.

Before hitting the show, we suggest you get a sense of what cloud projects your organization is looking at. We also recommend taking a look at the architectural section of the Cloud Security Alliance Security Guidance for Critical Areas of Focus in Cloud Computing and the *Editorial Note on Risk* on pages 9-11 (yes, Rich wrote this, and we still recommend you read it). On the security front, remember that design and architecture are your friends, and no tool can simply "make you secure" in the cloud, no matter what anyone claims.

For picking cloud sessions, we suggest you filter out the FUD from the meat. Skip over session descriptions that say things like, "will identify the risks of cloud computing" and look for those advertising reference architectures, case studies, and practical techniques (don't worry, despite the weird titles, Rich includes those in his cloud presentation with Chris Hoff). With the lack of standardization among cloud providers, and even conflicting definitions among organizations as to what constitutes "the cloud", it's all too easy to avoid specifics and stick to generalities on stage and in marketing materials.

Cloud security is one of our technology areas, so we'll cover specific things we think you'll see later in this guide. We are also running the inaugural Cloud Security Alliance training class the Sunday before RSA, and Rich is moderating a panel on government cloud and speaking with the always-entertaining Chris Hoff on cloud security Friday.

The Economy Sucks Less — What now?

The last few years have been challenging. For one, success has involved keeping yourself and your team employed. It's not like you had a lot of extra funds lying around, so many projects kept falling off the list. So you tried your best to do the minimum and sometimes didn't even reach that low bar. Nice-to-have became not-gonna-happen.

But now it looks like things are starting to recover a bit. Global stock markets, which tend to look 6 months ahead, are expecting strong growth, and many of our conversations with end users (both large and small) tend to indicate a general optimism we haven't seen in quite a while. To be clear, no one (certainly not us) expects the go-go days of the Internet bubble to return any time soon — unless you run a mobile games company. But we do think the economy will suck less in 2011, and that means you'll need to start thinking about projects that have fallen off the plate. Such as:

- **Perimeter renewal:** Many organizations let the perimeter go a bit. So it's overgrown, suboptimal, and not well positioned to do much against the next wave of application and targeted attacks. One project to consider might be an overhaul of your perimeter. Or at minimum, start moving to a different, more application-aware architecture to more effectively defend your networks. At RSAC, you'll hear a lot about next generation firewalls, which really involve building rules based on application behavior rather than just ports and protocols. At the show, your job will be to determine what is real and what is marketing hyperbole. So challenge the vendors on the floor to actually show you how their policy engines work in the age of application awareness. Also chat with other users during the hallway track, to discern how many folks are deploying these boxes and what their experiences have been.

- **Operationalization:** When times are tough, the last thing you look to do is write a big check to automate a process that works well enough. Sure, you can always make the point that investing in tools and automation will save money in the long run. How'd that work out for you? So now that things are loosening up a bit, it may be time to restructure some management and operational processes that can be resource intensive. That means looking at vulnerability and configuration management tools. Look for those which leverage your existing processes, and pay attention to those offering 'cloud' hooks — laying down yet another heavy, hierarchical set of tools is no longer interesting.

- **Secure applications:** Given time to market constraints and budget realities, messing around with your application development process and embracing more secure practices fell off the table. Now may be the time to start checking out the integration the big companies (such as HP, IBM, and Oracle) have been working on since acquiring many of the innovative start-ups. Again, this is where the hallway track is critical, as many folks have had lots of fits and starts with secure development and should be more than willing to share war stories. In terms of sessions, target the examples (especially within the Peer2Peer program) which focus on practical case studies. Theory isn't interesting — it's time to get things done.

Leakage and Seepage — Breaches, Leaks, and APT

Between WikiLeaks, the Advanced Persistent Threat (China), Gawker, and all the post-WikiLeaks Distributed Denial of Service attacks, we can expect to see all too much FUD around breaches and the ever-nebulous "insider threat". Some attacks *are* more sophisticated, but most of those were the result of plain old basic mistakes; and in the case of highly targeted situations like APT and WikiLeaks, all you can really do is try to contain and minimize, because you can't eliminate the problem.

At RSA 2011 there won't be any shortage of vendors claiming their tool would stop the latest fail-du-jour, or security pundits (yes, our somewhat-brethren) claiming you should have done it better (either the attack or the defense). And on

the off chance you find a product brochure that *doesn't* mention the insider threat, odds are you should buy whatever they are selling. We expect the Moscone cafes to be serving lots of hyperbole sandwiches.

Security failures are an unavoidable fact of life — especially in large organizations with complex infrastructures. Yes, blocking USB sticks and CD/DVD drives would have made it harder to swipe all those State Department cables. But that doesn't mean **you** have to go buy the latest tool, or that the leaker wouldn't have found some other way to leak sensitive information. Data Loss Prevention is a great security tool, but it can't stop **all** data leaks. No matter what the vendors claim on the floor.

As for APT, the term is now being used to advance so many different personal and corporate agendas that it's nearly impossible to understand the real threat. So count on the vendors to try to 'educate' you on the dangers of these attackers and their products' abilities to stop them. And try not to laugh too hard as they pitch. But let's keep it real here: many of you may be the targets of advanced attackers with the time and resources to slice through your security defenses. In some cases, these attackers track back to China, making them *real* APT. But anyone hawking a solution to yesterday's attacks, APT or otherwise, is missing the point of a persistent, resource-rich, patient, and innovative attacker.

But as important as it is to slice through the hype, we also need to recognize that there really are some very serious directed attacks — including APT, advanced financial attacks, and others — as well as run-of-the mill security breaches. You can't stop everything so you need the ability to detect and investigate attacks as quickly as possible — we call this "React Faster and Better". Spend some time at the show checking out the folks doing full packet capture and forensic data collection, which won't help stop the attack but will help understand what happened much faster.

Compliance — the World According to PCI

Compliance remains the cornerstone of vendor marketing and sales collateral. Why? Simply because most security products and services are funded with compliance dollars. Also enduring in 2011 is security professionals' love/hate relationship with compliance. They still generally view security as *the* most important task, but being secure for its own sake must take a back seat to compliance. We know being compliant is not the same as being secure, but fortunately compliance and security are on parallel missions, and security tool vendors provide enough flexibility in their products to accomplish multiple goals — *if* you choose to leverage them in that way.

What's different this year is the amount of hype surrounding compliance. There is no new shiny compliance object for all the vendors to tout this year. So you will not see 15 new regulations you are 'mandated' to address, nor hear about the billions of dollars you will save — as demonstrated in bogus use cases. Despite the rash of late 2010 data breaches, overall breaches are down, and the shrill hype is giving way to predictable business operations management. Most companies have been dealing with PCI, Sarbanes-Oxley and — for those selling into government — FISMA for a few years now. The maturity of the space has thankfully reduced the rhetoric, and now that customers have a handle on what they need to achieve compliance, they are looking for ways to do it **cheaper, faster, and easier**. So we expect many vendors to focus on how their tools and technologies integrate into compliance and operations management tools and streamline your daily work.

As far as trends in the compliance space, the Payment Card Industry Data Security Standard (PCI-DSS) remains the gorilla of mandates. Despite the glacially slow progression of this standard itself (codified in its new 3-year cycle), there is a steady increase in the number of merchants following the PCI Council's guidance. Go figure. Some because they are forced to by their payment providers (who service thousands of other merchants), some required thanks to the number of

transactions they process yearly, and others simply worried about associated risks. Sure, PCI isn't perfect, but it has helped — regardless of what the haters say.

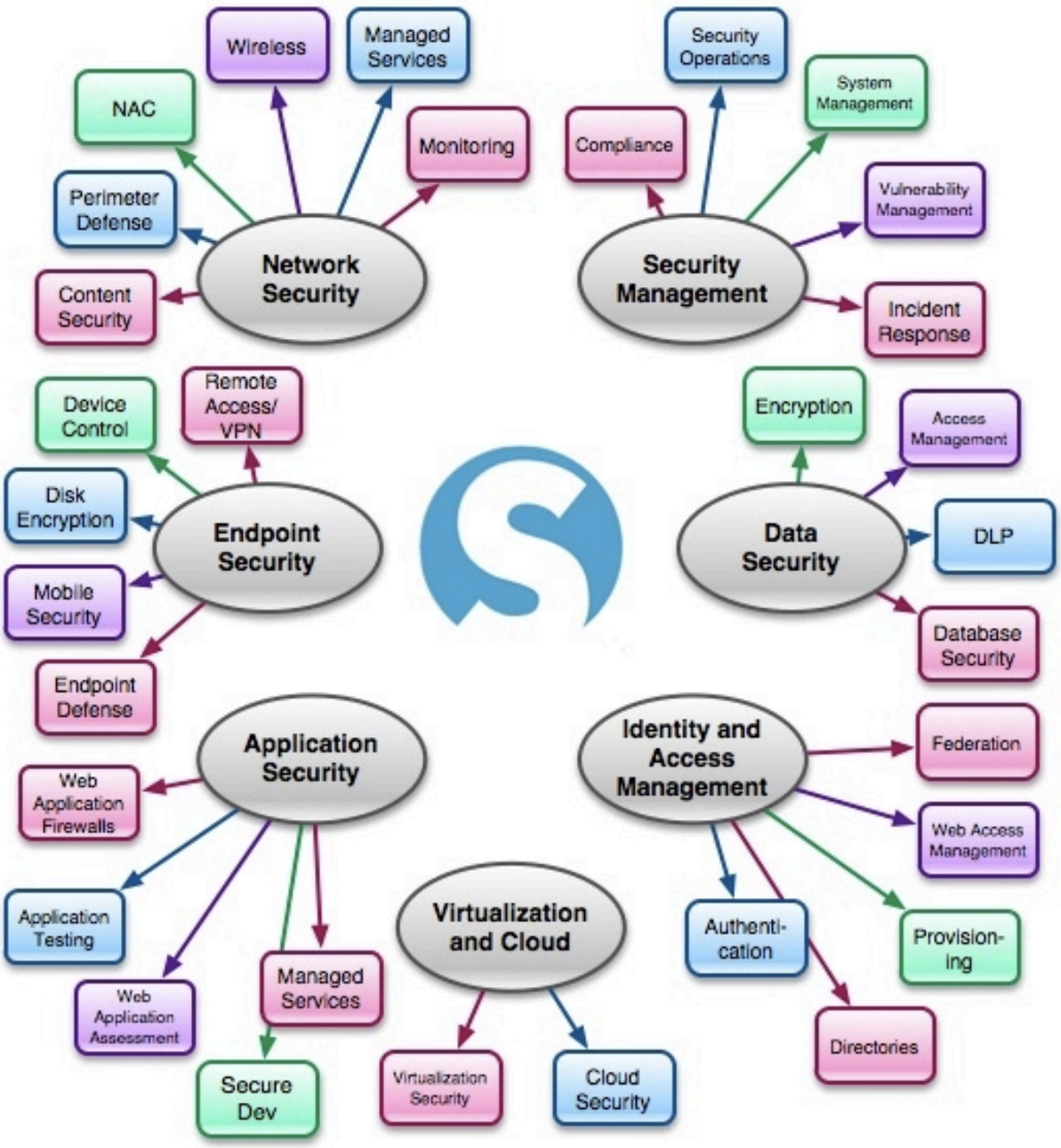
I Can Haz UR Mobile

There is no doubt you will hear a lot about mobile devices and your need to secure the iDevices at the show. There will be plenty of FUD and hyperbole bandied about because, well, as devices have become pervasive the risks have become real. Every vendor on the show floor will be happy to show you their cool iPad app, which allows you to manage their devices from a coffee shop. Like you'd do that. But the reality remains that there are precious few weaponized exploits you need to worry about — for now. And you won't see groundbreaking research on new mobile attacks at RSA — but do check out BlackHat/DEFCON this summer for plenty.

So there is nothing to see here, right? Well, not quite. Your real focus at the show needs to be on how to *manage* these devices, and gain some leverage with your existing processes. With thousands of these smart phones and tablets permeating your environment, you need to figure out if a new management infrastructure is required, or if you can use some of your existing tools. And focus on the data protection aspects of mobile devices, because a 64gb iPad or iPod provides enough space to exfiltrate a significant portion of your intellectual property. Don't forget to check into tactics for securing their network connections as well. See how your network security vendors are supporting smart phones with VPN clients and the like.

To be clear, you can't stop these devices from connecting to your critical data. And you can't control what your employees do with their own devices. But you can't afford to stick your head in the sand and hope the problem goes away. It won't. So spend some time at RSA figuring out who is doing what, and how those practices can be applied to your environment.

Securosis Coverage Areas



For our complete coverage map, please go to http://securosis.com/research

Data Security

As someone who has covered data security for nearly a decade, some days I wonder if I should send Bradley Manning, Julian Assange, whoever wrote the HITECH act, and the Chinese hacker community a personal note of gratitude. If the first wave of data security was driven by breach disclosure laws and a mixture of lost laptops and criminal exploits, this second wave is all about stopping leaks and keeping your pants on in public. This year I've seen more serious interest in large enterprises to protect more than merely credit card numbers than ever before. We also see PCI and the HITECH act (in healthcare) pushing greater investment in data security down to the mid-market. And while the technology is still far from perfect, it's definitely maturing along nicely.

What We Expect to See

There are five areas of interest at the show for data security:

- **DLP- Great taste, less filling:** There are two major trends in the Data Loss Prevention market- DLP Light comes of age, and full-suite DLP integration into major platforms. A large percentage of endpoint and network tools now offer basic DLP features. This is usually a regular expression engine or some other technique tuned to protect credit card numbers, and maybe a little personally identifiable information or healthcare data. Often this is included for free, or at least darn cheap. While DLP Light (as we call this) lacks mature workflow, content analysis capabilities, and so on, not every organization is ready for, or needs, a full DLP solution. If you just want to add some basic credit card protection, this is a good option. It's also a great way to figure out if you need a dedicated DLP tool without spending too much up-front.

  As for full-suite DLP solutions, most of them are now available from big vendors. Although the "full" DLP is usually a separate product, there's a lot of integration at various points of overlap like email security or web gateways. There's also a lot of feature parity between the vendors- unless you have some kind of particular need that only one fulfills, if you stick with the main ones you can probably flip a coin to choose.

  The key things to ask when looking at DLP Light are what's the content analysis engine, and how are incidents managed. Make sure the content analysis technique will work for what you want to protect, and that the workflow fits how you want to manage incidents. You might not want your AV guy finding out the CFO is emailing out customer data to a competitor. Also make sure you get to test it before paying for it. As for full-suite DLP, focus on how well it can integrate with your existing infrastructure (especially network gateways, directories, and endpoints). I also suggest playing with the UI since that's often a major deciding factor due to how much time security and non-security risk folks spend in it.

  Last of all we're starting to see more DLP vendors focus on the mid-market and easing deployment complexity.

- **Datum in a haystack:** Thanks to PCI 2.0 we can expect to see a heck of a lot of discussion around "content discovery". While I think we all know it's a good idea to figure out where all our sekret stuff is in order to protect it, in practice this is a serious pain in the rear. We've all screamed in frustration when we find that Access database or spreadsheet on some marketing server all chock full of Social Security numbers. PCI 2.0 now requires you demonstrate how you scoped your assessment, and how you keep that scope accurate. That means having some sort of tool or manual process to discover where all this stuff sits in storage. Trust me, no marketing professional will possibly let this one pass. Especially since they've been trying to convince you it was required for the past 5 years. All full-suite DLP tools include content discovery to find this data, as well as some DLP Light options. Focus on checking out the management side, since odds are there will be a heck of a lot of storage to scan, and results to filter through.

- **There's a new FAM in town:** I hate to admit this, but there's a new category of security tool popping up this year that I actually like. File Activity Monitoring watches all file access on protected systems and generates alerts on policy violations and unusual activity. In other words, you can build policies that alert you when a sales guy about to depart is downloading all the customer files, without blocking access to them. Or when a random system account starts downloading engineering plans to that new stealth fighter. I like the idea of being able to track what files users access and generate real-time alerts. I started talking about this years ago, but there weren't any products on the market. now I know of 3, and I suspect more are coming down the pipe.

- **Battle of the tokens:** Last year we predicted a lot of interest and push in encryption and tokenization, and for once we got it right. One thing we didn't expect was the huge battle that erupted over ownership of the term. Encryption vendors started pushing encrypted data as tokens (which I find hard to call a token), while tokenization advocates try to convince you encryption is no more secure than guarding Hades with a chihuahua. The amusing part is all these guys offer both options in their products.

- **Play the WIKILEAKS! WIKILEAKS! APT! WIKILEAKS! PCI! HITECH! WIKILEAKS!!! drinking game:** Since not enough of you are buying data security tools, the vendors will still do their best to scare your pants off and claim they can prevent the unpreventable. Amuse yourself by cruising the show floor with beer in hand and drinking anytime you see those words on marketing materials. It's one drink per mention in a brochure, 2 drinks for a postcard handout, and 3 if it's on the booth banner. Chug if it's on a t-shirt, and grab a shot if it's on a t-shirt on some random booth-babe hired from a modeling agency.

DLP	Database Security	Encryption
CA (1533)	Application Security (639)	CipherOptics (1923)
McAfee (1117)	dataguise (645)	Entrust (717)
RSA (1725)	IBM (756)	Netronome Systems (2333)
Symantec (1416)	Imperva (517)	nuBridges (733)
Websense (1129)	LogLogic (828)	Symantec/PGP (1416)
	Nitro Security (739)	RSA (1725)
	Oracle (1559)	SafeNet (1849)
	Quest Software (2232)	SPYRUS (2544)
		THALES (2023)
		Townsend Security (439)
		Venafi (1843)
		Vormetric (445)
		WinMagic (839)

Application Security

When we say application security, for we generally mean web application security. We probably could have cheated and simply reposted last year's guide to application security and still been close. Yes, application security is still a nascent market. Last year the focus was anti-exploitation to prevent code injection attacks, and the value provided by integrating assessment and web application firewall technologies. While the threats remain the same, there are some new twists which deserve attention.

What We Expect to See

- **Code Review Services:** Strapping security onto the network layer and hoping it catches your application vulnerabilities is a band-aid at best, and companies that produce applications know this. With HP's acquisition of Fortify a few months ago, Microsoft's announcement of Attack Surface Analyzer, and IBM's acquisition of Ounce Labs in 2009, it's clear that the world's major software providers know this as well. And they are looking to capitalize on the movement. Third party source code review services are on the rise, and most web development teams now use either white-box or black-box testing in their certification processes. "Building security in" is an increasingly common mantra for development teams, and there is tremendous opportunity to sell security products and services into this nascent market. Most development teams are just now learning about secure coding techniques, threat modeling, and how to build unit-based security tests to run alongside their functional tests. We expect to see many vendors offering tools, education, and services that foster secure code everywhere from design to post-deployment. Not just pre-and-post deployment checkers and firewalls, but security offerings for every single step in the development lifecycle.

- **Buyer Shift:** "What?" you say. I am not selling to the IT manager? Not here you are not. IT plays a part, but the buying center is shifting to the development team for web application security technologies. And that's a very different conversation, with a much different set of requirements and use cases the vendor needs to address.

- **OWASP As the Guiding Light:** Publicity concerning application security issues is growing. OWASP — the Open Web Application Security Project — provides a Top 10 list of the most common threats to applications. And it's a good rundown of sneaky, underhanded tricks attackers use to compromise web applications for fun and profit. Even better, it's backed by measurable statistics so it's not all conjecture and innuendo. This list is driving many companies' marketing campaigns, and the alignment of their service offerings as well. How well any given vendor protects applications from these threats is open for debate, but the fact that they are responding to the most common threat vectors we see today is very good news. Web application vulnerabilities represent a significant threat to organizations as web services are an integral part of business operations, and the push for more SaaS and cloud based services means attackers have an increasing number of potential targets.

Web App Firewalls	Application Testing	Secure Development
Akamai (2017)	Armorize (329)	Arxan (328)
art of defense (342)	Cenzic (332)	Coverity (333)
Barracuda Networks (1440)	Dasient (554)	IBM (756)
Fortify, an HP Company (1324)	Fortify, an HP Company (1324)	HP (1324)
Fortinet (923)	IBM (756)	Vineyard Networks (2454)
Imperva (517)	IOActive (532)	
Qualys (1432)	Mykonos (2151)	
TrustWave (817)	nCircle (1023)	
	Qualys (1432)	
	Rapid7 (429)	
	Tenable (729)	
	Veracode (629)	

Network Security

2010 was an interesting year for the network security space. There has been a resurgence in interest and budget projections for spending, largely for perimeter security. Part of this is a loosening of the budget purse strings, which is allowing frustrated network security folks to actually start dreaming about upgrading their perimeters. So there will be plenty of vendors positioning to benefit from the wave of 2011 spending.

What We Expect to See

There are four areas of interest at the show for network security:

- **Next Generation Firewall:** Last year we talked about application awareness as absolutely critical to the next wave of network security devices. That capability — to build policies based on applications and users, rather than just ports and protocols — has taken the name *next generation firewall*. Unless a vendor has no interest in the enterprise market, they will be touting their next generation wares. Some of these will be available exclusively on slide decks in the booth, while other vendors will be able to show varying levels of implementation. While you've got an SE at your disposal at the show, ask them some pointed questions about how their application categorization happens and what the effective throughput is for their content oriented functions. It should be pretty clear to what degree their gear is next-generation, or if it's really just an IPS bolt-on.

- **More marketecture:** As these new generation capabilities start to hit, they present the opportunity for a fairly severe disruption in the status quo of vendor leadership. So what do the incumbents do when under attack, without a technical response? Right, they try to freeze the market with some broad statement of direction that is light on detail and heavy on hyperbole. It wouldn't surprise us to see at least one of the RSA keynoters (yeah, those who pay EMC $250K for the right to pontificate for an hour) talk about a new initiative to address all ills of everything.

- **Virt suck:** The good news is that a bunch of the start-ups talking about virtualization security hit the wall and got acquired by big network security. So you probably won't see many folks talking about their new widget to protect inter-VM network traffic. What you will hear is every vendor on the floor playing up the advantages of their shiny new virtual appliances. It's just like the box you pay $50K for, but you get to use your own computing power in a horribly wasteful fashion. You know how attractive it is to slice out a chunk of your computers to run IPS signatures. It's like these folks want to bring us back to 1995 and because it runs on ESX, it's all good. Not so much.

- **Full packet capture maturing:** Yes, this is a carry-over from last year. The fact remains that we still have a lot of work to do in order to streamline our incident response processes and make them useful. So you'll see folks stacked up to learn about the latest and greatest packet capture and the associated analysis. These tools are now starting to bring some cool visualization and even malware analysis to the table. Check them out because as the market matures (and prices come down), this is a technology you should be looking at.

Network Security		Network Packet Capture	Authentication
Astaro (1855)	Huawei Symantec (553)	Endace (2151)	ActivIdentity (1128)
Black Box (2550)	InfoExpress (2417)	Narus (1917)	Anakam (226)
Cavium Networks (528)	IBM (1316)	NetWitness (1448)	Authentify (1029)
Celestix Networks (852)	Juniper (1745)	Solera Networks (2359)	Entrust (717)
Check Point (1929)	McAfee (1117)		Gemalto (1923)
Cisco (1717)	Net Optics (2339)		Imprivata (2520)
Crossbeam (525)	Nitro Security (2051)		PhoneFactor (1554)
Cyberoam (723)	Palo Alto Networks (539)		RSA (1725)
Damballa (433)	PacketMotion (450)		SecureAuth (2616)
Endace (2151)	Radware (2655)		StrongAuth (2629)
FireEye (332)	SonicWALL (423)		Symantec (1416)
ForeScout (845)	SourceFire (1831)		Symplified (2720)
Fortinet (2225)	StillSecure (2228)		
HBGary (556)	StoneSoft (2533)		
HOB (1338)	WatchGuard (617)		
HP/TippingPoint (1825)			

Endpoint Security

In 2010, there was broad acknowledgement that most of the endpoint protection deployed was more about passing PCI (yes, it's still a requirement) than actually stopping attacks. Unfortunately, at the show we'll continue to hear about all the advances happening in malware detection, and we'll laugh again. The traditional signature-based model is broken, no matter how many clouds we see inserted into the mix. But with the AV cash cow continuing to moo uncontrollably, the industry will continue trying to convince customers to maintain their investments. So the real question is: who will show some type of innovation in terms of endpoint malware detection. Anyone? Anyone? Bueller? Bueller?

What We Expect to See

There are some areas of interest at the show for endpoint security:

- **You get what you pay for (or do you?):** Given the clear issues around endpoint malware detection, we'll be hearing a lot from the Free AV crowd. They'll be talking about the hundreds of millions of folks who use the free engines, just before they try to upsell you to their paid offerings. The reality is that you need management, because these tools involve deploying software agents to many endpoints. But you should pay the least amount possible. So see who seems the hungriest on the show floor. If they aren't foaming at the mouth, they likely aren't hungry enough to win your business.

- **Cloudy with a chance of hyperbole:** You will also hear a lot about cloud signatures and crowd sourcing to address the limitations of the traditional AV signature model. To be clear, moving a lot of signatures to the cloud is a good thing. But it's not an answer. The model of matching bad stuff is still broken, and no amount of cloudy stuff will change that. The idea of crowd sourcing is interesting so check out the folks, like Sourcefire/Immunet and Webroot/PrevX, who are doing this in practice. Ask them how they shorten the window from the time an issue is discovered to distributing an update to the rest of the network. This is yet another option to keep the broken AV model running a bit longer.

- **AWL MIA:** What you probably won't see a lot of is application white listing (AWL). Why? Because the technology remains a niche. It is a core aspect of our Positivity security model, but both perception and reality are still slowing deployment of AWL. Not that the handful of vendors offering these solutions won't be trying to make some noise. But they have no chance to stand out against the status quo, which represents billions in revenue and spends like drunken sailors at RSA. But this remains an important technology, so you should search out the vendors who offer it and learn how they are working to address the deployment and scaling issues.

- **Signs of the iPocalypse:** You will see a lot of vendors giving away iPads and iPhones. Why not? If you don't have one, you want one. If you already have one, you want another one. Or ten. But the reality is these devices are big, and consumerization is taking root. That means you need to figure out how to control them. OK, maybe not control, but at least manage. So check out the configuration management folks and those with specific mobile technologies to reign in the chaos. OK, maybe not reign in, but at least ensure that when they get lost (and they will), you won't be in career jeopardy.

- **Man(ning) up:** One of the other major stories in 2010 was WikiLeaks, spearheading by Bradley Manning, your friendly neighborhood data leaker. So you'll hear a lot of vendors talking about the importance of controlling USB ports and doing content control/analysis on the endpoint. Try to figure out how they scale. Try to understand how they classify sensitive data and actually do anything without killing the performance of the endpoint. Yeah, it would be good to figure out whether and how they can play nice with any DLP/device control technologies you already have implemented.

Anti-Malware	Disk Encryption	Mobile Security
Bit9 (2621)	BeCrypt (2129)	Device Lock (2228)
BeyondTrust (945)	Check Point (2317)	IronKey (2339)
BitDefender (2737)	Entrust (717)	Kaspersky (1145)
Comodo Group (2439)	McAfee (1117)	Kingston Technology (223)
CoreTrace (1963)	Microsoft (1517)	McAfee (1117)
ESET (1151)	RSA (1725)	RIM (442)
GFI (538)	Safend (2624)	Safend (2624)
Kaspersky (2217)	Sophos (1817)	Symantec (1416)
McAfee (1117)	Symantec (1416)	
Microsoft (1517)	Trend Micro (1929)	
Norman Data Defense (2517)	Wave Systems (939)	
Sophos (1817)	WinMagic (839)	
Symantec (1416)		
Trend Micro (1929)		
Trusteer (233)		
Webroot (1045)		

Email/Web (Content) Security

Global Threats. APT. Botnets. Infected Web Pages. Grannies with shotguns. We expect to see anything and everything it takes for vendors to get your attention, including never before seen awards and security metrics. Some ask “Why the hype?” The value of content security — both inbound filtering to prevent unwanted garbage from coming into the network, as well as detection of unwanted activity like surfing for porn or sending company secrets to your cousin as investment advice — is proven. All the major players and most mid-tier providers have closed the major holes in their products, provide unified management for all functions, and offer some type of SaaS service. The technology works. The problem is that the segment is both mature and saturated. To earn a new customer, a vendor must steal one from a competitor. Growing revenue means convincing customers they need a new service. It is increasingly difficult to differentiate the top tier from the mid-tier players, so that noise you hear is vendors trying to find an edge. For the most part, the vendors offer quality services at a price point that continues to drop with reduced cost cloud and SaaS based offerings. But you can't blame the vendors from trying to “one up” the competition in a crowded market.

What We Expect to See

There are three areas of interest at the show for content security:

- **It’s Raining Devices**: One thing you are going to learn wandering around Moscone is how the cloud protects those endpoint devices. Yep! The Content Security Cloud protects the endpoint. Isn't that what cloud security is all about? Well, no, actually, but you are will hear about it. Those services that run on your iPhone/Droid/Blackberry are theoretically just as susceptible to attack as what’s on your desktop or laptop. Supposedly. That’s the vendor argument, but attacks against mobile devices are more likely to target lower layers of the infrastructure — but don’t worry, vendors won’t let facts ruin a good story. In most cases the vendor is offering exactly the same services they already provide for your laptop/workstation to protect from the same threats on new devices. But hey, it’s ‘the cloud’, so it must be good!

- **More (poor man’s) DLP**: Yes, content security providers offer Data Loss Prevention. In most cases, it's just the subset of DLP needed to detect data exfiltration. And regular expression checking for outbound documents and web requests is good enough to address the majority of content leakage problems, so this is a good addition for most customers. By and large we hear from satisfied customers who implement a dozen or so content policies for specific violations they are interested in detecting, and find the analysis techniques sufficient. Deployments of this type are far less daunting than a full featured soup-to-nuts DLP platform, so we hear far more success stories and less about shelf ware.

- **Users Are Employees Too**: Scams, fraud, and phishing attacks continue to hammer those uninterested in security, and the IT managers who support them. The content security vendors know that nothing else matters to some users besides getting to their Facebook pages on their lunch hour. It also means these users are unusually susceptible to phishing attacks, drive-by malware, and account compromises. In and of themselves these attacks are fairly low-yield

and low-damage. But a compromised computer on a corporate network acts as a launching pad for all sorts of network mayhem. Content security providers can no longer claim the “Insider Threat” is your biggest security concern, but they will let IT managers know they help mitigate damages from stupid human tricks.

Email Security	Web Security
AppRiver (1059)	Astaro (2251)
Astaro (2251)	Barracuda Networks (1440)
Barracuda Networks (1440)	Blue Coat (1139)
Cisco (1717)	Cisco (1717)
M86 Security (1825)	M86 Security (1825)
McAfee (1117)	McAfee (1117)
Microsoft (1517)	ProofPoint (728)
ProofPoint (728)	Sophos (1817)
RIM (442)	Symantec (1416)
SonicWALL (423)	Websense (1129)
Sophos (1817)	Webroot (1045)
Symantec (1416)	Zscaler (317)
Trend Micro (1929)	
Websense (1129)	
Webroot (1045)	
Zix Corp (954)	

Security Management

Compliance is still driving most of what happens from a management standpoint, which is why have a specific compliance section below. On the security management front, there was still plenty of activity in 2010. But most customers continued to feel the same way: underwhelmed. It's still very hard to keep control of much of anything, which is problematic as the number of devices and amount of sensitive data grow exponentially. Good times. Good times.

What We Expect to See

There are a couple areas of interest at the show for security management:

- **The (Not) Easy Button:** Given the absolutely correct perspective of customers that security management is too complex, difficult, ponderous, and lots of other negative descriptors, we expect vendors to focus on ease of use for many of these security management tools (especially SIEM/Log Management). Don't believe them. They continue to sell false hope. To be fair, the tools *are* much improved. Interfaces are better. User experience is tolerable. *But it's still not easy.*

  So spend some time in the booth checking out interfaces. How you set up rules, analyze data, and generate reports. Make the demo dude go into excruciating detail on how things really get done with the tool. Remember, anything you select, you will need to live with. So do your homework and choose wisely.

- **The next act for scanners:** Vulnerability management is so 2005. But tack on some kind of cloud stuff and it's, uh, 2007? The new new shiny object is configuration auditing/policy compliance. Which actually makes sense because you need to scrutinize the device to check for vulnerabilities, so why not just assess the configuration while you are at it. And just as with vulnerability scanning, the question will be whether you do it on-site or via a cloud service. Or both, because we expect most vendors to offer both.

- **MSS comes of age:** The good news is that folks finally realize it's not novel to monitor firewalls or IPS themselves, and combined with consolidation of pretty much all the big players, this means MSS isn't a big deal anymore. So the big vendors with big booths will be talking about their monitoring (and even management) services. If you still have 5 folks parsing firewall alerts, check out these offerings. At minimum it will be interesting to get a sense of how efficiently you do things internally. Just make sure you understand exactly what the service and support model is, because when alerts start firing you don't want to be dialing the main number of a $100 billion telco.

- **Start-up X, a Big IT company:** Big IT, with its big management stacks and big professional services teams, will be at RSAC in force. Maybe they'll even have a story for how all the crap they've bought over the past year makes Big IT finally relevant in the security space. You'll see HP and IBM (and EMC and Cisco and Juniper) in 5-6 different booths each, because companies they acquired had already committed to exhibit in this year's show. They should have one of those passport programs, just to make sure you visit all their booths to win an iPad or something like that.

Compliance

Compliance isn't merely a major theme for the show, it's also likely the biggest driver of your security spending. But that doesn't mean folks don't want to minimize the cost and hassle of compliance, so scope reduction will be a major theme that we hear throughout the show. While there's no such thing as a compliance solution, many security technologies play major roles in helping achieve and maintain compliance.

What We Expect to See

With compliance we will see a mix of regulation-focused messages and compliance-specific technologies:

- **PCI & Tokenization:** The Payment Card Industry Data Security Standard (PCI-DSS) is the single regulation that generates the most attention, and a lot of the growth for security and compliance spending. And frankly, especially within the retail and finance verticals, companies are looking to reduce costs and minimize PCI audits. It's viewed as little more than a tax on the business so they want to at least reduce — if not eliminate — the expense. At the show this year, we expect you'll hear and see a lot about tokenization. This approach substitutes credit card numbers stored at a merchant site with a harmless, well, *token*. It only represents the credit card transaction, so a stolen token cannot be used to commit fraud. At the show, focus on the sessions where savvy users talk about how they **reduce the scope** of PCI audits along with the associated costs of securing credit card data using this approach. While only a handful of tokenization vendors will be at the show, many of the payment processors have partnered with technology providers to offer tokenization as a managed service. Expect to see plenty of interest and discussion on this topic, and long lines at select vendor booths.

- **There's an App for That:** Expect to see vendors offer neat iPhone and iPad apps for their management and reporting products. Sure, reports and dashboards are popular with vendors because they bring the eye candy sales teams want to demonstrate product value. But what's cooler than a fancy dashboard? A fancy new iPhone. Put the two together and it's like two great eye-candies that go great together! It's going to be a big hit. Not just because anyone really wants to take that FISMA report with them in their pocket; it's because IT, sales, and marketing all secretly lust after the new toy. It's the thought of catching a spring training game while configuring SIEM policies. Does it make you more productive? Maybe. But having your IT products running on the toy justifies the purchase of both. Yeah, anywhere, anytime access is pretty cool too, but it's like getting two for one. Expect to see this *everywhere*!

- **GRC Oopsie:** Last year we expected to see a lot of collateral about GRC: Governance, Risk, and Compliance. And we did. It's a convenient term to encapsulate a lot of compliance, operations, and regulatory issues under one umbrella. The problem is that most customers don't see their challenges the same way. Only a handful of large enterprises actually buy GRC products, most have specific problems to address within specific regulations, and they need a tool that will fit within their operational model. So 2010 saw a lot of GRC tools and banners on the show floor, and after falling on their faces, this year GRC will be mostly absent. Look for vendors to position their products within an operations management framework, with enterprise workflow management and advanced trouble ticket integration. Policy compliance and operations management put the focus back on the issues most customers want to address.

SIEM/Log Management	Configuration/ Patch	Vulnerability Management	GRC	MSS
AlienVault (652)	EMC (1937)	AppSec (2539)	Agiliance (2351)	Akamai (2017)
ArcSight/HP (931)	IBM (756)	GFI (538)	CA (1533)	AlertLogic (2529)
CA (1533)	HP (1324)	Imperva (517)	Archer/RSA (1725)	Alert Enterprise (351)
LogLogic (828)	Microsoft (1517)	nCircle (1023)	Modulo (1951)	AT&T (831)
LogRhythm (617)	Novell (1033)	Qualys (1432)	Oracle (1559)	eDMZ Security (2639)
Nitro Security (739)	Symantec (1416)	Rapid7 (328)		IBM (756)
Novell (1033)	TripWire (1332)	Secunia (917)		SAIC (2239)
RSA (1725)		StillSecure (2228)		SecureWorks (1017)
SenSage (523)	**Operations Management**	Tenable (956)		Symantec (1416)
Splunk (2433)	AlgoSec (856)			Verizon Business (323)
Symantec (1416)	FireMon (545)			
Tenable (729)	RedSeal (745)			
TripWire (1332)	Skybox Security (632)			
TrustWave (817)	Tufin (2551)			

Virtualization and Cloud

2010 was a fascinating year for cloud computing and virtualization. VMWare locked down the VMSafe program, spurring acquisition of smaller vendors in the program with access to the special APIs. Cloud computing security moved from hype to hyper-hype at the same time some seriously interesting security tools hit the market. Despite all the confusion, there was a heck of a lot of progress and growing clarity. And not all of it was from the keyboard of Chris Hoff.

What We Expect to See

For virtualization and cloud security, there are four areas to focus on:

- **Innovation cloudination:** For the second time in this guide I find myself actually excited by new security tech (don't tell my mom). While you'll see a ton of garbage on the show floor, there are a few companies (big and small) with some innovative products designed to help secure cloud computing. Everything from managing your machine keys to encrypting IaaS or SaaS data. These aren't merely virtual appliance versions of existing hardware/software, but ground-up, cloud-specific security tools. The ones I'm most interested in are around data security, auditing, and identity management.

- **Looking SaaSy:** Technically speaking, not all Software as a Service counts as cloud computing, but don't tell the marketing departments. But this is another area that's more than mere hype- nearly every vendor I've talked with (and worked with) is looking at leveraging cloud computing in some way. Not merely because it's sexy, but since SaaS can help reduce management overhead for security in a bunch of ways. And since all of you already pay subscription and maintenance licenses anyway, pure greed isn't the motivator. These offerings work best for small and medium businesses, and reduce the amount of equipment you need to maintain on site. They also may help with distributed organizations. SaaS isn't always the answer, and you really need to dig into the architecture, but I've been pleasantly surprised at how well some of these services can work.

- **VMSafe cracking:** VMWare locked down its VMSafe program that allowed security vendors direct access to certain hypervisor functions via API. The program is dead, except the APIs are maintained for any existing members in the program. This was probably driven by VMWare wanting to control most of the security action, and they forced everyone to move to the less-effective VShield Zones system. What does this mean? Anyone with VMSafe access has a leg up on the competition, which spurred some acquisitions. Everyone else is a bit handcuffed in comparison, so when looking at your private cloud security (on VMware) focus on the fundamental architecture (especially around networking).

- **Virtual appliances everywhere:** You know all those security vendors that promoted their amazing performance due to purpose-built hardware? Yeah, now they all offer the same performance in virtual (software) appliances. Don't ask the booth reps too much about that though or they might pull a Russell Crowe on you. On the upside, many security tools do make sense as virtual appliances. Especially the ones with lower performance requirements (like management servers) or for the mid-market.

We guarantee your data center, application, and storage teams are looking hard at, or are already using, cloud and virtualization, so this is one area you'll want to pay attention to despite the hype.

See Securosis at RSA 2011

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

- **DAS-106:** Everything You Ever Wanted to Know About DLP — Rich (Tuesday, Feb 15 @ 1 PM)
- **CLD-108:** Private and Government Sectors: Why are Agencies Hesitant to Adopt Cloud? — Rich moderates (Tuesday, Feb 15 @ 3:40 PM)
- **DAS-203:** Cutting Through the Data Loss Prevention Confusion – DLP Myths Busted — Rich (Wednesday, Feb 16 @ 11:10 AM)
- **P2P-203A:** Evolving Perimeter(s): Protecting the Stuff That's Really Important — Mike (Wednesday, Feb 16 @ 11:10 AM)
- **BUS-303:** Putting the Fun in Dysfunctional — How the Security Industry Really Works — Rich and Mike (Thursday, Feb 17 @ 11:10 AM)
- **AND-304:** Agile Development, Security Fail — Adrian (Thursday, Feb 17 @ 1 PM)
- **EXP-402:** Cloudiquantanomidatumcon: The Infra/Info-Centric Debate in the Cloud — Rich (Friday, Feb 18 @ 10:10 AM)

Other Events

- **Disaster Recovery Breakfast:** Once again this year Securosis will be hosting the Disaster Recovery Breakfast on Thursday, Feb 17 between 8 and 11 with help from our friends at **Threatpost** and **Schwartz Communications**. 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.
- **e10+:** Rich and Mike are the hosts and facilitators for the RSA Conference's e10+ program targeting CISO types. That's Monday morning (Feb. 14) from 8:30 to noon.
- **America's Growth Capital Conference:** Mike will be moderating a panel at the AGC Conference on the future of network security with folks from Cisco, Juniper, Palo Alto, Packet Motion, and Fidelis. The session is Monday afternoon, Feb. 14 at 2:15 PM.
- **Security Blogger Meet up:** Securosis will be at the 4th annual Security Blogger Meet up at the classified location. You need to have a blog and be pre-registered to get in.
- **Fortinet Panels:** Mike will also be moderating the *Security Mythbusting: Blowing Up the Security Hype* panels at Fortinet's booth (#923) on Tuesday and Wednesday from 1:30 - 2 PM.
- **Holding court at the W:** If you are up for late night hijinx — and like to laugh at stumbling, bumbling security industry folks — show up at the W's lobby bar after the parties break up. It's always a good time and you are very likely to see one or all of us Securosis folks there getting into trouble. And accepting drink donations.

Evil Plans

We know that most of you think being an analyst involves pontificating, drinking lots of coffee, waving our hands a lot, and maybe even writing from time to time. And you're not wrong. But we Securosis folks do spend a lot of time thinking about how to advance the practice of security and provide actionable information that makes your job (and life) easier. Here are a couple links to our planned research agenda for 2011, as well as a screen shot of our super secret project that we plan to launch, um, soon.

We currently release the vast majority of our research for free through our blog, and archive it in our Research Library (http://securosis.com/research). All published materials and presentations meet our strict objectivity requirements, as well as our Totally Transparent Research policy.

2011 Research Agenda:

- 2011 Research Agenda: the Practical Bits
- 2011 Research Agenda: Quantum Cloudiness, Supervillan Shields, and No-BS Risk
- Research Agenda 2011: the Open Research Version
- Infrastructure Security Research Agenda 2011—Part 1: Positivity
- Infrastructure Security Research Agenda 2011—Part 2: Posturing and Reacting Faster/Better
- Infrastructure Security Research Agenda 2011—Part 3: Vaulting and Assurance
- Infrastructure Security Research Agenda 2011—Part 4: Egress and Endpoints

Most of these research documents can be sponsored for distribution on an annual basis. Regardless of sponsorship all papers will be released for free under a Creative Commons license on the Securosis site.

Coming Soon:
The Securosis Nexus

RSA Exhibitor List

Company Name	Booth Number	Website
3M Mobile Interactive Solutions Division	2740	http://solutions.3m.com/wps/portal/3M/
ActivIdentity	1128	http://www.actividentity.com/
Advanced Product Design	340	
Advantech	217	
AFC Industries	235	http://www.afcindustries.com/
Agiliance	2351	http://www.agiliance.com/
Akamai Technologies	2017	http://www.akamai.com
Alert Enterprise	351	http://www.alertenterprise.com/
Alert Logic	2529	http://www.alertlogic.com/
AlgoSec	856	http://www.algosec.com/en/index.php
AlienVault	652	http://www.alienvault.com/
Alta Associates Inc.	850	http://www.altaassociates.com/
AMAX Information Technologies	346	http://www.amaxit.com/
American Portwell Technology, Inc.	628	http://www.portwell.com/
Anakam, an Equifax Company	226	http://www.anakam.com/
Anne Arundel Community College	2728	http://www.aacc.edu/
Anonymizer, Inc.	2722	http://www.anonymizer.com/
Antiy Labs	1541	http://www.antiy.net/
Anue Systems Inc.	2445	http://www.anuesystems.com/
APCON	832	http://www.apcon.com/
Application Security, Inc.	639	http://www.appsecinc.com/
AppRiver	1059	http://www.appriver.com/
Approva	428	http://www.approva.net/
Araknos SRL Unipersonale	347	http://www.araknos.it/en/azienda/azien
ArcSight	931	http://www.arcsight.com/
Armorize Technologies Inc.	329	http://www.armorize.com/
Art of Defence GmbH	1350	http://www.artofdefence.com/
Art of Defence GmbH	342	http://www.artofdefence.com/
Arxan Technologies	328	http://www.arxan.com/
Astaro	2251	http://www.astaro.com/

Company Name	Booth Number	Website
AT&T	831	http://www.att.com/
atsec information security	1350	http://www.atsec.com/
Authentify, Inc.	1029	http://www.authentify.com/
Authernative, Inc.	550	http://www.authernative.com/
Avenda Systems	318	http://www.avendasys.com/
Axway	2225	http://www.axway.com/
BeCrypt Inc.	2129	http://www.becrypt.com/
Beijing LinkTrust Technologies Development Co.,Ltd.	1541	http://www.linktrust.com.cn/
Beijing Topsec Science and Technology Co.,Ltd	1541	
Beijing Venustech Inc.	1541	http://english.venustech.com.cn/
Beijing Zhongguancun Overseas Science Park	1541	http://www.zgc.gov.cn/english/
BeyondTrust Corp.	945	http://www.beyondtrust.com/
Bit9, Inc.	2621	http://www.bit9.com/
Bivio Networks	2133	http://www.bivio.net/
Black Box Network Services	2550	http://www.blackbox.com/
BlockMaster AB	2425	http://www.blockmastersecurity.com/
Blue Coat Systems, Inc.	1139	http://www.bluecoat.com/
BluePoint Security	2559	http://www.bluepointsecurity.com/
Brainloop Inc.	1350	http://www.brainloop.com/
BreakingPoint Systems, Inc.	951	http://www.breakingpointsystems.com/
BroadWeb Corporation	1541	http://www.broadweb.com/
Bsafe Information Systems Inc.	855	http://www.bsafesolutions.com/
BSI	1344	http://www.bsigroup.com/
C4ISR Journal	2650	http://www.c4isrjournal.com
CA Technologies	1533	http://ca.com/
Capella University	251	http://www.capella.edu/
Cavium Networks	528	http://www.caviumnetworks.com/
CCSO.com	2619	http://www.ccso.com/
Celestix Networks	852	http://www.celestix.com/
Cenzic, Inc.	332	http://www.cenzic.com/
Check Point Software Technologies	2317	http://www.checkpoint.com/
Cherry	755	http://www.cherrycorp.com/
China quality certification certificate authority	1541	http://www.cqc.com.cn/english/
CipherOptics	1923	http://www.cipheroptics.com/

Company Name	Booth Number	Website
Cisco	1717	http://www.cisco.com/
Cloud Security Alliance	2718	http://www.cloudsecurityalliance.org/
Comodo Group, Inc.	2439	http://www.comodo.com/
CoreTrace Corporation	1963	http://www.coretrace.com/
CORISECIO GmbH	1350	http://www.corisecio.com/
Coverity	333	http://www.coverity.com/
Critical Watch	950	http://www.criticalwatch.com/
Cryptography Research, Inc.	2233	http://www.cryptography.com/
cv cryptovision GmbH	1350	http://www.cryptovision.com/
Cyber-Ark Software, Inc.	2045	http://www.cyber-ark.com/
Cybera	752	http://www.cybera.com/
Cyberoam	723	http://www.cyberoam.com/
Damballa	433	http://www.damballa.com/
Dasient, Inc.	554	http://www.dasient.com/
Dataguise Inc.	645	http://www.dataguise.com/
Department of Homeland Security/ US-CERT	457	http://www.us-cert.gov/
DeviceLock	2228	http://www.devicelock.com/
DHS Control Systems Security Program	453	http://www.us-cert.gov/control_systems
Digital Defense, Inc.	2455	http://www.ddifrontline.com/
DriveSavers Data Recovery	446	http://drivesaversdatarecovery.com/
Echoworx Corporation	MS-02	http://www.echoworx.com/
eDMZ Security	2639	http://www.e-dmzsecurity.com/
Electronic Frontier Foundation	255	http://www.eff.org/
eleven GmbH	1350	http://www.eleven.de/index.html
EMC Corporation	1937	http://www.emc.com/
Emulex Corporation	2729	http://www.emulex.com/
Endace	1039	http://www.endace.com/
Endgame Systems	2754	http://www.endgames.us/
ENTERSECT Technologies	2726	http://www.entersect.co.za/
Entrust	717	http://www.entrust.com/
ESET, LLC	1151	http://www.eset.com/
Exar	2739	http://www.exar.com/
Fasoo.com, Inc.	533	http://www.fasoo.com/
Federal Bureau of Investigation	452	http://www.fbi.gov/
FEITIAN Technologies Co.,Ltd	1541	http://www.ftsafe.com/
FireEye, Inc.	2345	http://www.fireeye.com/

Company Name	Booth Number	Website
FireID	2516	http://www.fireid.com/
FireMon	545	http://www.securepassage.com/
First Data Corporation	557	http://www.firstdata.com/
ForeScout Technologies, Inc.	845	http://www.forescout.com/
Fortify Software, an HP company	1324	https://www.fortify.com/
Fortinet Inc.	2325	http://www.fortinet.com/
Freescale Semiconductor, Inc.	2450	http://www.freescale.com/
G Data Software	2727	http://www.gdata-software.com/
Garner Products	2259	http://www.garner-products.com/
Gemalto	1945	http://www.gemalto.com/
General Services Administration	350	http://www.gsa.gov/
Gentle Security Software S.A.	2738	http://www.gentlesecurity.com/
German Federal Ministry of Economy and Technology	1350	http://www.bmwi.de/English/Navigatior
GFI Software	538	http://www.gfi.com/
Giesecke & Devrient	1145	http://www.gi-de.com/
Gigamon LLC	539	http://www.gigamon.com/
GlobalSCAPE	2159	http://www.cuteftp.com/
GlobalSign	657	http://www.globalsign.com/
GoldKey Security Corporation	2051	http://goldkey.com/
GOTrust Technology Inc.	2058	http://www.go-trust.com/
Greenidea, Inc.	338	http://www.greenidea.com/
Guangzhou JN Union Technology Co., Ltd.	751	http://www.keyou.cn/
Guardian Analytics	339	http://www.guardiananalytics.com/
HBGary, Inc.	556	http://www.hbgary.com/
HID Global	823	http://www.hidglobal.com/
High Density Devices	2545	http://www.hiddn.no/
Hillstone Networks	2459	http://www.hillstonenet.com/
Hitachi ID Systems, Inc	236	http://www.hitachi-id.com/
HOB, Inc.	1338	http://www.hobsoft.com/
HP	1324	http://www.hp.com/
Huawei Symantec	553	http://www.huaweisymantec.com/en/
IBM Corporation	756	http://www.ibm.com/
Identity Finder, LLC	2637	http://www.identityfinder.com/
Identity Theft 911	229	http://www.identitytheft911.com/

Company Name	Booth Number	Website
IEEE Security & Privacy	2633	http://www.computer.org/security
Imperva Inc.	517	http://www.imperva.com/
Imprivata	2520	http://www.imprivata.com/
Infineon Technologien AG	1350	http://www.infineon.com/
Info Security Magazine	2723	http://searchsecurity.techtarget.com/
InfoExpress, Inc.	2417	http://www.infoexpress.com/
InfoGard	650	http://www.infogard.com/
Information Systems Security Association (ISSA)	253	http://www.issa.org/
Integralis, Inc.	357	http://www.integralis.us/
Intel	2029	http://www.intel.com/
Inteligensa USA Inc.	239	http://www.inteligensa.com/
IntraLinks	230	http://www.intralinks.com/
IOActive, Inc	532	http://www.ioactive.com/
Ipswitch, Inc.	633	http://www.ipswitch.com/
IQ 20/20	443	http://www.iq2020.com/
IronKey, Inc.	2339	http://www.ironkey.com/
ISC²	250	http://www.isc2.org/
Ixia	2627	http://www.ixiacom.com/
Juniper Networks	1745	http://www.juniper.net/
Kaspersky Lab	2217	http://www.kaspersky.com/
Key Source International	2620	http://www.ksikeyboards.com/
KikuSema GmbH	1350	http://www.kikusema.com/
KOBIL Systems GmbH	1356	http://www.kobil.com/
Lanner Electronics Inc.	2451	http://www.lannerinc.com/
Legendsec Technology Co.Ltd	1541	http://www.legendsec.com/english/inde
Lieberman Software Corporation	529	http://www.liebsoft.com/
Linoma Software	247	http://www.linomasoftware.com/
Lionic	2732	http://www.lionic.com/
LJ Kushner & Associates, LLC	542	http://www.ljkushner.com/
LogLogic	828	http://www.loglogic.com/
LogRhythm, Inc.	617	http://www.logrhythm.com/
Lumension	923	http://www.lumension.com/
M86 Security	1825	http://www.m86security.com/
Mandiant	456	http://www.mandiant.com/
MBX Systems	544	http://www.mbx.com/
McAfee, Inc.	1117	http://www.mcafee.com/us/

Company Name	Booth Number	Website
Messageware Incorporated	854	http://www.messageware.com/
Mi-Token	2652	http://www.mi-token.com/
Microsoft	1517	http://www.microsoft.com/
Microsoft Pavilion	1527	
MITRE - CVE/OVAL/CWE	2617	http://measurablesecurity.mitre.org/
Modulo	1951	http://www.modulo.com/
Motorola	1855	http://www.motorola.com/
MXI Security	1132	http://www.mxisecurity.com/
MXTools - Spamhaus	1159	http://www.mxtools.com/Home/tabid/39
Mykonos Software, Inc.	2151	http://www.mykonossoftware.com/
nagra ID Security	2037	http://www.nidsecurity.com/
Napatech Inc.	451	http://www.napatech.com/
Narus, Inc.	1917	http://www.narus.com/
nCircle	1023	http://www.ncircle.com/
NEI	2539	http://www.nei.com/
Net Optics, Inc.	2245	http://www.netoptics.com/
NETGEAR, Inc.	959	http://www.netgear.com/
Netronome Systems	2333	http://www.netronome.com/
NetWitness Corporation	1448	http://www.netwitness.com/
Network Critical	2653	http://www.networkcritical.com/
New Horizons Computer Learning Centers	222	http://www.newhorizons.com/
NitroSecurity	739	http://www.nitrosecurity.com/
NOGACOM	753	http://www.nogacom.com/
Norman Data Defense Systems Inc.	2517	http://www.norman.com/
Novell	1033	http://www.novell.com/
NSA	2139	http://www.nsa.gov/
NSFOCUS Information Technology Co, Ltd.	651	http://www.nsfocus.com/en/
NSS Labs, Inc.	2419	http://www.nsslabs.com/
nuBridges, Inc.	733	http://www.nubridges.com/
NXP Semiconductors	956	http://www.nxp.com/
OASIS Security Interoperability Demonstration	732	http://www.oasis-open.org/
OATH	2123	http://www.openauthentication.org/
Oberthur Technologies	1757	http://www.oberthur.com/
Open Systems Management, Inc.	316	http://www.osminc.com/

Company Name	Booth Number	Website
OPSWAT, Inc.	356	http://www.opswat.com/
Oracle	1559	http://www.oracle.com/
PacketMotion, Inc.	450	http://www.packetmotion.com/
Palantir Technologies	1751	http://www.palantirtech.com/
Palo Alto Networks	2145	http://www.paloaltonetworks.com/
Patriot Technologies	341	http://www.patriot-tech.com/
PFU Systems, Inc.	857	http://www.pfusystems.com/
PhoneFactor	1554	http://www.phonefactor.com/
PistolStar Inc.	218	http://www.pistolstar.com/
ProofPoint, Inc.	728	http://www.proofpoint.com/
Psylock GmbH	1350	http://www.psylock.com/en
Qgroup GmbH	1350	http://www.qgroup.de/index.php?setLa
Qualys, Inc.	1432	https://www.qualys.com/
Quest Software	2232	http://www.quest.com/
Radiant Logic, Inc.	757	http://www.radiantlogic.com/
Radware, Inc.	2655	http://www.radware.com/
Rapid7	429	http://www.rapid7.com/
RedSeal Systems, Inc.	745	http://www.redseal.net/
Research In Motion	442	http://www.rim.com/
Revere Security Corporation	225	http://www.reveresecurity.com/
Rohde & Schwarz	1350	http://www.rohde-schwarz.us/
RSA, The Security Division of EMC	1725	http://www.rsa.com/
RSAM	623	http://www.rsam.com/
Safelight	1831	http://www.securityadvisors.com/
Safend Inc.	2624	http://www.safend.com/
SafeNet, Inc.	1849	http://www.safenet-inc.com/
SAIC	2239	http://www.saic.com/
SANS Institute	2716	http://www.sans.org/
secunet Security Networks AG	1350	http://www.secunet.com/en/
secunet Security Networks AG	1344	
Secunia	917	http://secunia.com/
SecureAuth Corporation	2616	http://www.gosecureauth.com/
SecureWorks	1017	http://www.secureworks.com/
Security Mentor	551	http://www.securitymentor.com/
Secusmart	1350	https://www.secusmart.com/en/home-e
SenSage, Inc.	523	http://www.sensage.com/
Silicium Security	2750	http://www.siliciumsecurity.com/

Company Name	Booth Number	Website
Simena	2635	http://www.simena.net/
Sims Recycling Solutions	2555	http://simsrecycling.com/
SIRRIX AG security technologies	1350	http://www.sirrix.com/
Skybox Security, Inc.	632	http://www.skyboxsecurity.com/
Smart Displayer Technology	2059	http://www.smartdisplayer.com.tw/
Softex, Inc.	750	http://www.softexinc.com/
Software Engineering Institute	2158	http://www.sei.cmu.edu/
Solera Networks	2359	http://www.soleranetworks.com/
SonicWALL, Inc.	423	http://www.sonicwall.com/
Sophos, Inc.	1817	http://www.sophos.com/
Sourcefire	2552	http://www.sourcefire.com/
Splunk Inc.	2433	http://www.splunk.com/
SPYRUS	2544	http://www.spyrus.com/
SRA International	417	http://www.sra.com/
STMicroelectronics	216	http://www.st.com/
Stonesoft Inc.	2533	http://www.stonesoft.com/
StrongAuth, Inc.	2629	http://www.strongauth.com/
Switzerland Trade & Investment Promotion	2651	http://www.osec.ch/internet/osec/en/ho
Swivel Secure Ltd.	2751	http://www.swivelsecure.com/
Symantec Corporation	1316-1416	http://www.symantec.com/
Symantec Corporation Pavilion	1426	
Symplified	2720	http://www.symplified.com/
Sysmate, Inc.	656	http://www.sysmate.net/
Systematic Development Group, LLC	2719	http://www.lok-it.net/
TechGuard Security	2717	http://www.techguardsecurity.com/
TeleSign Corporation	432	http://www.telesign.com/
TeleTrusT Deutschland e.V.	1344	http://www.teletrust.de/en/startseite/
TeleTrust/German Pavilion	1350	
Tenable Network Security, Inc.	729	http://www.tenable.com/
THALES	2023	
Thycotic Software Ltd.	2355	http://www.thycotic.com/
Titus	1837	
Townsend Security	439	http://townsendsecurity.com/
Trend Micro	1929	http://us.trendmicro.com/us/home/
Tripwire, Inc.	1332	http://www.tripwire.com/

Company Name	Booth Number	Website
Triumfant Incorporated	438	http://www.triumfant.com/
Trustwave	817	https://www.trustwave.com/
Tufin Technologies	2551	http://www.tufin.com/
TÜV Informationstechnik GmbH	1344	http://www.tuvit.de/english/Home.asp
University of Denver	2421	http://www.du.edu/
University of Maryland University College	2628	http://www.umuc.edu/
VCE	1549	http://www.vce.com/
Venafi, Inc.	1843	http://www.venafi.com/
Veracode, Inc.	629	http://www.veracode.com/
Verizon Business	323	http://www.verizonbusiness.com/
Vineyard Networks	2454	http://www.vineyardnetworks.com/
VMWare	1051	http://www.vmware.com/
Vormetric, Inc.	445	http://www.vormetric.com/
VSS Monitoring	2747	http://www.vssmonitoring.com/
WatchGuard Technologies	1454	http://www.watchguard.com/
Wave Systems Corp.	939	http://www.tvtonic.com/
Webroot, Inc.	1045	http://www.webroot.com/
Websense Inc.	1129	http://www.websense.com/
WinMagic Data Security	839	http://www.winmagic.com
Xbridge Systems, Inc.	655	http://www.xbridgesystems.com/
yaSSL.com	330	http://yassl.com/
Zix Corporation	954	http://www.zixcorp.com/
Zscaler, Inc.	317	http://www.zscaler.com/

About Securosis

Securosis, L.L.C. 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.

Our services include:

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

Our clients range from stealth startups to some of the best known technology vendors and end users. Clients include large financial institutions, institutional investors, mid-sized enterprises, and major security vendors.

Additionally, Securosis partners with security testing labs to provide unique product evaluations that combine in-depth technical analysis with high-level product, architecture, and market analysis.

Securosis, L.L.C.
515 E. Carefree Highway
Suite #766
Phoenix, AZ 85085
Office: +1-602-412-3051
info@securosis.com
http://www.securosis.com