



# Securosis Guide to the RSA Conference 2010

# Welcome to RSA 2010!

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, since the 3 days tend to go by quickly. Your friends at Securosis decided to kickstart your planning efforts with our inaugural version of the "Securosis Guide to the RSA Conference."

Over the 12 years we've been going to the show, it's gotten bigger and harder to navigate as the security industry has gotten bigger and harder to navigate. This guide should give you a good idea about 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 at the show.

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

<b>Key Themes</b>	<b>3</b>
<b>Securosis Coverage Areas</b>	<b>5</b>
<b>Network Security</b>	<b>6</b>
<b>Endpoint Security</b>	<b>8</b>
<b>Email/Web (Content) Security</b>	<b>10</b>
<b>Data Security</b>	<b>12</b>
<b>Application Security</b>	<b>14</b>
<b>Security Management</b>	<b>16</b>
<b>Compliance</b>	<b>17</b>
<b>Virtualization and Cloud</b>	<b>19</b>
<b>See Securosis at RSA 2010</b>	<b>20</b>
<b>Upcoming Research</b>	<b>21</b>
<b>About Securosis</b>	<b>22</b>

# Key Themes

How many times have you shown up at the RSA Conference to see the hype machine fully engaged about a topic or two? Remember 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 in 2010? Here is a quick list of three topics that will likely be top of mind at RSA, and why you should care.

## Cloud/Virtualization Security

Cloud computing and virtualization are two of the hottest trends in information technology today, and we fully expect this trend to extend into RSA sessions and the show floor. There are few topics as prone to marketing abuse and general confusion as cloud computing and virtualization, despite some significant technological and definitional advances over the past year. But don't be confused — despite the hype this is an important area; virtualization and cloud computing are fundamentally altering how we design and manage our infrastructure and consume technology services — especially within data centers. This is definitely a case of “where there's smoke, there's fire”.

Although virtualization and cloud computing are separate topics, they have a tight symbiotic relationship. Virtualization is both a *platform for*, and a *consumer of*, cloud computing. Most cloud computing deployments are based on virtualization technology, but the cloud can also host virtual deployments. We don't really have the space to fully cover virtualization and cloud computing in this guide, though we will dig a layer deeper in a few pages. We highly recommend you take a look at the architectural section of the [Cloud Security Alliance Security Guidance for Critical Areas of Focus in Cloud Computing](#). We also draw your attention to the *Editorial Note on Risk* on pages 9-11, but we're biased because Rich wrote it.

## Cyber-crime & Advanced Persistent Threats

Since it's common knowledge that not only government networks but also commercial entities are being attacked by well-funded, state-sponsored, and very patient adversaries you'll hear a lot about APT (advanced persistent threats) at RSA. First let's define APT, which is an attacker focused on **you** (or your organization) with the express objective of stealing sensitive data. APT does not specify an attack vector, which *may or may not* be particularly advanced — the attacker will do only what is necessary to achieve their objective. (Among those that respond to these incidents, APT often refers only to a specific country, not a general class of attacker.)

Where customer fear emerges the vendors circle like vultures, trying to figure out how their existing widgets can be used to address the new class of attacks. But to be clear, there is no silver bullet to stop or even detect an APT — though you will likely see a lot of marketing buffoonery discussing how this widget or that could have detected the APT. Just remember the Tuesday morning quarterback always completes the pass, and we'll see a *lot* of that at RSA.

It's not likely any widget would detect an APT because an APT isn't an *attack*, it's a category of attacker. And yes, although China is usually associated with APT, it's bigger than one nation-state. **It's a totally different threat model**, first identified around 2006. This nuance is important, because it means the adversary will do what is necessary to compromise your network. In one instance it may be a client-side 0-day, in another it could be a SQL injection attack. If the attack can't be profiled, then there is no way a vendor can “address the issue.”

But there are general areas of interest for folks worried about APT and other targeted attacks, and those are detection and forensics. Since you don't know how they will get in, you have to be able to detect and investigate the attack as quickly as possible — we call this “React Faster”. Thus the folks doing full packet capture and forensic data collection should be high on your list of companies to check out on the show floor. You'll also want to check out some sessions, including Rich and Mike's Groundhog Day panel, where APT will surely be covered.

## Compliance

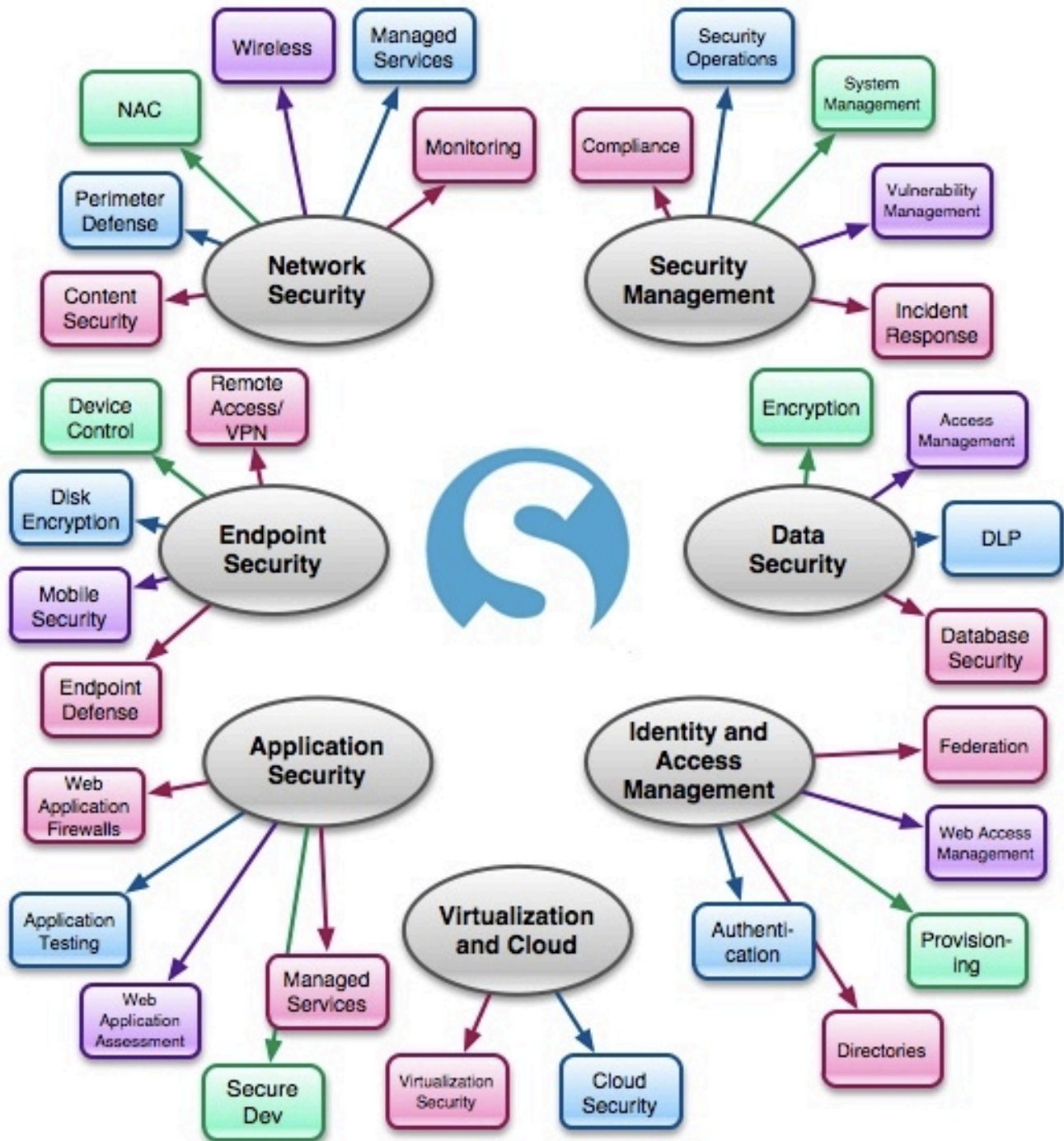
Compliance as a theme for RSA? Yes, you have heard this before. Unlike 2005, though, ‘compliance’ is not just a buzzword, but a major driver for the funding and adoption of most security technologies. Assuming you are aware of current compliance requirements, you will be hearing about new requirements and modifications to existing regulations (think PCI next or HIPAA/HiTech evolution). This is the core of IT's love/hate relationship with compliance. Regulatory change means more work for you, but at the same time if you need budget for a security project in today's economy, you need to associate the project with a compliance mandate and cost savings at the same time. Both vendors and customers *should* be talking a lot about compliance because it helps both parties sell their products and projects, respectively.

The good news at this point is that security vendors do provide value in documenting compliance. They have worked hard to incorporate policies and reports specific to common regulations into their products, and provide management and customization to address the needs of other constituencies. But there will still be plenty of hype around ease of use and time to value. So there will be lots of red “Easy PCI” buttons to bring back for your kids, and promises of “Instant Sarbanes-Oxley” and “Comprehensive HIPAA support” in every brochure.

We also expect to see considerable hot air directed towards Massachusetts 201 CMR 17.00 privacy and disclosure regulation, but it's not clear how it will be really enforced. At this point, focus on understanding the requirements, and definitely don't let the vendors be your source of education. In general, you already know the regulations you need to worry about, so don't get too excited when someone tells you compliance with GBRSH 590 or FUBR 140 is mandatory. There are lots of proposed ‘standards’ out there, but questions of ‘if’, ‘when’, and ‘how’ regarding compliance are less certain.

Also keep in mind that Securosis is sticking to its *Security First* mindset. Focus on protecting private and sensitive data with security controls you can document, and your compliance efforts will be significantly streamlined.

# Securosis Coverage Areas



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

# Network Security

Since we've been connecting to the Internet, people have been focused on network security, so the sector has gotten reasonably mature. As such, there has been a distinct lack of innovation over the past few years. There have certainly been hype cycles (NAC, anyone?), but most organizations still focus on the basics of perimeter defense. That means intrusion prevention (IPS) and reducing complexity by collapsing a number of functions into an integrated unified threat management (UTM) device.

## What We Expect to See

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

- **Application Awareness:** This is the ability for devices to decode and protect against application layer attacks. Since most web applications are encapsulated in HTTP (port 80) or HTTPS (port 443) traffic, to really understand what's happening it's important for network devices to dig into each packet and understand what the application is doing. This capability is called deep packet inspection (DPI) and most perimeter devices claim to provide this capability, making for a confusing environment, with tons of unsubstantiated vendor claims.

The devil is in the details of how each vendor implements DPI, so focus your questions on which protocols they understand and what kinds of policies and reporting are available on a per-protocol basis.

- **Speeds and Feeds:** As with most mature markets, especially on the network, at some point it gets down to who has the biggest and fastest box. Doing this kind of packet decodes and attack signature matching requires a lot of horsepower, and we are seeing 20gbps IPS devices appear. You will also see blade architectures on integrated perimeter boxes, and other features focused on adding scale to the environment as customer networks continue to go faster.

Since every organization has different requirements, spend some time ahead of the show on understanding what you need and how you'd like to architect your network security environment. Get it down on a single piece of paper and head down to the show floor. When you get to the vendor booth, find an SE (don't waste time with a sales person) and have them show you how their product(s) can meet your requirements. They'll probably want to show you their fancy interface and some other meaningless crap. Stay focused on your issues and don't leave until you understand in your gut whether the vendor can get the job done.

- **Consolidation and Integration:** After years of adding specific boxes to solve narrow problems, many organizations' perimeter networks are messes. Thus the idea of consolidating both boxes (with bigger boxes) and functions (with multi-function devices) continues to be interesting. There will be lots of companies on the show floor talking about their UTM devices, targeting small companies and large with similar equipment. Of course, the needs of the enterprise fundamentally differ from small business requirements, so challenge how well suited any product is for your environment.

That means breaking out your marker again, and having the SEs on the show floor show you how their integrated

solutions can solve your problems. Also challenge them on architecture, given that the more a box needs to do (firewall, IPS, protocol decode, content security, etc.) the lower its throughput. Give vendor responses the sniff test and invite those that pass in for a proof of concept.

- **Forensics:** With the acknowledgement that we cannot detect some classes of attacks in advance, forensics and full packet capture gear will be high profile at this year's conference. This actually represents progress, although you will see a number of vendors talking about blocking APT-like attackers. The reality is (as we've been saying for a long time via the React Faster doctrine) that you can't stop the attacks (not all of them, anyway), so you had better figure out sooner rather than later that you have been compromised, and then act accordingly.

The key issues around forensics are user experience, chain of custody, and scale. Most of today's networks generate a huge amount of data, and you'll have to figure out how to make that data usable, especially given the time constraints inherent to incident response. You also need to get comfortable with evidence gathering and data integrity, since it's easy to say the data will hold up in court, but much harder to make it do so.

### Securosis Research on Network Security

For more depth on this topic, check out the blog posts, papers, webcasts, and other content we post in the Securosis Research Library: <http://securosis.com/research/network-security>.

Firewalls	IDS/IPS	Remote Access	Threat Mgmt
ALGOSEC (2529)	Alert Logic (2550)	Barracuda (1549)	Blue Coat (1139)
Astaro (1855)	Check Point (1929)	Check Point (1929)	Cisco (831)
Check Point (1929)	Crossbeam (525)	Cisco (831)	ForeScout (739)
Crossbeam (525)	Endace (2151)	Gemalto (1923)	Fortinet (2225)
Fortinet (2225)	FireEye (332)	SonicWALL (2551)	IBM (1316)
Matasano (554)	Net Optics (2339)		Net Optics (2339)
McAfee (1117)	Nitro Security (2051)		Rapid7 (328)
Palo Alto Networks (539)	Palo Alto Networks (539)		Solera Networks (439)
Secure Passage (655)	SourceFire (1831)		SonicWALL (2551)
SonicWALL (2551)	StillSecure (2228)		WatchGuard (617)
TippingPoint (1825)	TippingPoint (1825)		
Tufin (333)	Top Layer (317)		
WatchGuard (617)			

# Endpoint Security

Anti-virus came onto the scene in the early 90's to combat viruses proliferated mostly by sneakernet. You remember sneakernet, don't you? Over the past two decades, protecting the endpoint has become pretty big business, but we need to question the effectiveness of traditional anti-virus and other endpoint defenses, given the variety of ways to defeat those security controls. This year we expect many of the endpoint vendors to start espousing "value bundles" and alternative controls (like application whitelisting), while jumping on the cloud bandwagon to address the gap between claims and reality.

## What We Expect to See

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

- **The Suite Life:** There are many similarities between current endpoint security suites and office automation suites in the early part of the decade. The applications don't work particularly well, but in order to keep prices up, more and more stuff you don't need gets bundled into the package. There is no end to that trend, as the leading endpoint agent companies have been acquiring new technologies (such as full disk encryption and DLP) to broaden their suites and maintain their price points. But at the show this year, it's reasonable to go to your favorite endpoint agent vendor and ask them why they can't seem to "get ahead of the threat." Yes, that is a rhetorical question, but we Securosis folks like to see vendors squirm, so that would be a good way to start the conversation.

Also be on the lookout of the folks offering "Free AV" and talking about how ridiculous it is to be paying for AV nowadays. Just be aware, the big booths with the Eastern European models don't come cheap, so they will get their pound of flesh in the form of management consoles and upselling to more full-featured suites (which actually may do something).

- **The Cloud Messiah:** Endpoint vendors aren't the only ones figuring the 'cloud' will save them from all their issues, but they will certainly be talking about how integrating malware defenses into the 'cloud' will increase effectiveness and keep the attackers at bay. This is another game of three-card monty, and the endpoint vendors are figuring you won't know the difference. After you've asked the vendor why they can't stop even simplistic web attacks or detect a Zeus infection, they'll probably start talking about "shared intelligence" and the great googly-moogly malware engine in the sky. At this point, ask a pretty simple question: "How do you win this arms race?" With 2-3 million new malware attacks happening this year, how long can this signature-based approach work? That should make for more interesting conversation.
- **Control Strategies:** Given that traditional anti-virus is mostly useless against today's attacks, you are going to hear a number of smaller application whitelisting vendors start to go more aggressively after the endpoint security companies. Yet, this category (along with USB device control technologies) suffers from a perception that the technology breaks applications and impacts user experience. As with every competitive *tete-a-tete*, there is some truth to that issue. So challenge the white listing vendors to prove how they impact the user experience (or not) and can provide similar value to an endpoint security suite (firewall, HIPS, full disk encryption, etc.).

- Laptop Encryption:** You'll likely also be hearing about another feature of most of the endpoint suites: full disk encryption (FDE). There will be lots of FUD about the costs of disclosure and why it's just a lot easier to encrypt your mobile devices and be done with it. For once, the vendor mouthpieces are absolutely right. But it brings up the question of what features you need, whether FDE should be bundled into your endpoint suite, and how you can recover data when users inevitably lose passwords and devices are stolen. So if you have mobile users (and who doesn't?), it's not an issue of whether you need the technology — it's the most effective way to procure and deploy.

### Securosis Research on Endpoint Security

For more depth on this topic, check out the blog posts, papers, webcasts, and other content we post in the Securosis Research Library: <http://securosis.com/research/endpoint-security>.

Anti-Malware	Disk Encryption	Mobile Security
Bit9 (322)	BeCrypt (239)	Cellcrypt (2359)
BeyondTrust (2433)	Check Point (1929)	Device Lock (2232)
Blue Coat (1139)	Entrust (717)	IronKey (2333)
CoreTrace (1963)	McAfee (1117)	Kaspersky (1145)
ESET (1751)	Microsoft (1517)	PGP (1324)
Kaspersky (1145)	PKWare (2045)	RIM (445)
Lumension (923)	PGP (1324)	Safend (2616)
McAfee (1117)	Safend (2616)	
Microsoft (1517)	Sophos (1817)	
Norman Data Defense (2517)	Symantec (1416)	
Sophos (1817)	Wave Systems (1849)	
Sunbelt (651)	WinMagic (939)	
Symantec (1416)		
Trend Micro (1837)		
Webroot (828)		

# Email/Web (Content) Security

In case you missed it, every email security vendor on the planet offers web content filtering within their portfolio of products and — for better or worse — the combination is now known as content security. No other security market has embraced the concept of ‘the cloud’ and SaaS offerings as readily as content security providers. In an effort to deal with increasing volumes of spam and malware without completely overhauling all your hardware, outsourced content filtering is a cost effective way to add both capacity and capabilities. Almost all vendors offer traditional on-premise software or appliance offerings that are fortified with cloud based services (most refer to this as a hybrid model) for additional screening of content.

## What We Expect to See

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

- **Fully Integrated Platforms:** As you wander the show floor at Moscone Center, we expect every vendor to say that their web and email security platforms are completely integrated. What this usually means is that your reports are shared, but cloud and appliance consoles are separate, as is policy management. It’s funny how the vendors have such a flexible definition of “integrated.” If you are looking at migrating to a combined solution, you need to dig in to see what is really integrated and what simply shares the same dashboard, how your user experience will change (for the better), and how effectiveness & clean their results are — end users get grumpy if their favorite web sites are classified as unsafe or they get spam in their inboxes.
- **Hybrid Cloud Services:** We expect every vendor to offer a ‘cloud’ service in order to jump on the cloud bandwagon. This may be nothing more than an anti-spam or remote web filtering gateway deployed on shared infrastructure as a hosted service. The quality and diversity of cloud services varies greatly, as does the level of security provided by different cloud hosting companies. Once you get past the hype of certifications and technobabble, ask the vendors what types of audits and third party security certifications they will allow. Ask what sort of financial commitments they will make in the event that they fail to live up to their service level agreements, and what their service level agreements with the cloud infrastructure providers look like. Those two questions usually halt the discussion, and you will quickly identify hype mongers versus the folks who have really thought through cloud deployment.
- **DLP Lite:** As we’ll see in the Data Security section, DLP is hot again. Thus we expect to see every content security vendor offering “DLP” or “Data Loss Prevention” within their products, but in reality most only offer regular expression checks of network content. Yes, they’ll be able to detect an account number or a social security number, but that is only a sliver of what DLP needs to be. Content discovery and more advanced forms of content inspection (heuristic, lexical, cyclic hash, etc) will be noticeably absent. Again, we recommend you challenge the content security vendor to dig into their discovery and detection capabilities and prove it’s more than regular expressions. Keep in mind a trade show demo is probably not adequate for you to sufficiently explore the advanced features, so your objective should be to identify 3-4 vendors for deep dives after the show.

## Select Securosis Research on Content Security

For more depth on this topic, check out the blog posts, papers, webcasts, and other content we post in the Securosis Research Library: <http://securosis.com/research/web-email-and-data-portal-security>.

Email Security Gateway	Web Security Gateway	Managed Services
Astaro (1855)	Astaro (1855)	AppRiver (2159)
Barracuda Networks (1549)	Barracuda Networks (1549)	Barracuda Networks (1549)
Cisco (831)	Blue Coat (1139)	Cisco (831)
M86 Security (1151)	Cisco (831)	Google (1917)
McAfee (1117)	M86 Security (1151)	M86 Security (1151)
ProofPoint (1132)	McAfee (1117)	McAfee (1117)
Red Condor (529)	ProofPoint (1132)	ProofPoint (1132)
RIM (445)	Sophos (1817)	Symantec (1416)
SonicWALL (2551)	Symantec (1416)	Webroot (828)
Sophos (1817)	Websense (1129)	Websense (1129)
Symantec (1416)		Zscaler (2145)
Trend Micro (1837)		
Websense (1129)		

# Data Security

Although technically nearly all of Information Security is directed at protecting corporate data and content, in practice our industry has historically focused on network and endpoint security. At Securosis we divide up the data security world into two major domains based on how users access data — the data center and the desktop. This reflects how data is managed far more practically than “structured” and “unstructured”. The data center includes access through enterprise applications, databases, and document management systems. The desktop includes productivity applications (the Office suite), email, and other desktop applications and communications.

## What We Expect to See

There are four areas of interest at the show relative to data security:

- **Content Analysis:** This is the ability of security tools to dig inside files and packets to understand the content inside, not just the headers or other metadata. The most basic versions are generally derived from pattern matching (regular expressions), while advanced options include partial document matching and database fingerprinting. Content analysis techniques were pioneered by Data Loss Prevention (DLP) tools; and are starting to pop up in everything from firewalls, to portable device control agents, to SIEM systems.

The most important questions to ask identify the kind of content analysis being performed. Regular expressions alone can work, but result in more false positives and negatives than other options. Also find out if the feature can peer inside different file types, or only analyze plain text. Depending on your requirements, you may not need advanced techniques, but you do need to understand exactly what you’re getting and determine if it will really help you protect your data, or just generate thousands of alerts every time someone buys a collectable shot glass off Amazon.

- **DLP Everywhere:** Here at Securosis we use a narrow definition for DLP that includes solutions designed to protect data with advanced content analysis capabilities and dedicated workflow, but not every vendor marketing department agrees with our approach. Given the customer interest around DLP, we expect you’ll see a wide variety of security tools with DLP or “data protection” features, most of which are either basic content analysis or some form of context-based file or access blocking. These DLP features can be useful, especially in smaller organizations and those with only limited data protection needs, but they are a pale substitute if you need a dedicated data protection solution.

When talking with these vendors start by digging into their content analysis capabilities and how it really works from a technical standpoint. If you get a technobabble response, just move on. Also ask to see a demo of the management interface — if you expect a lot of data-related violations, you will likely need a dedicated workflow to manage incidents, so user experience is a big deal. Finally, ask them about directory integration — when it comes to data security, different rules apply to different users and groups.

- **Encryption and Tokenization:** Due to a combination of PCI requirements and recent data breaches, we are seeing a ton of interest in application and database encryption and tokenization. Tokenization replaces credit card numbers with random token values (that may match the credit card format) matched to real numbers only in a centralized, highly secured database. Format Preserving Encryption encrypts the numbers so you can recover them in place, but the

encrypted values share the credit card number format. Finally, newer application and database encryption options focus on improved ease of use and deployment compared to their predecessors.

You don't really need to worry about encryption algorithms, but it's important to understand platform support, management user experience (play around with the user interface), and deployment requirements. No matter what anyone tells you, there are always requirements for application and database changes, but some of these approaches can minimize the pain. Ask how long an average deployment takes for an organization of your size, and make sure they can provide real examples or references in your business, since data security is very industry specific.

- **Database Security:** Due partially to acquisitions and partially to customer demand, we are seeing a variety of tools add features to tie into database security. Latest in the hit parade are SIEM tools capable of monitoring database transactions and vulnerability assessment tools with database support. These parallel the dedicated Database Activity Monitoring and Database Assessment markets. As with any area of overlap and consolidation, you'll need to figure out if you need a dedicated tool, or if features in another type of product are good enough. We also expect to see a lot more talk about data masking, which is the conversion of production data into a pseudo-random, but still usable format for development.

The key issue is how well the tools interface with different database platforms. For any tool, find out which database management systems are supported on which host operating systems. For monitoring tools, ask if they understand all SQL or rely on audit logs. Also ask how they collect the data — if it is from networking monitoring or requires an agent (both may be acceptable, depending on your needs). For assessment, ask if they perform credentialed database scans via SQL, or just look at configuration files (which provide a lot less information).

### Select Securosis Research on Data Security

For more depth on this topic, check out the blog posts, papers, webcasts, and other content we post in the Securosis Research Library: <http://securosis.com/research/data-security>.

DLP	Database Security	Encryption
CA (1533)	Application Security (2539)	CipherOptics (528)
McAfee (1117)	dataguise (544)	Entrust (717)
RSA (1725)	Guardium/IBM (632)	Ipswitch File Transfer (442)
Symantec (1416)	Imperva (417)	nuBridges (532)
Websense (1129)	LogLogic (633)	PGP (1322)
	Netezza (657)	Protegrity (1029)
	Nitro Security (2051)	RSA (1725)
	Protegrity (1029)	SafeNet (1039)
		THALES (2123)
		WinMagic (939)

# Application Security

Application Security is a nascent market, but data from several recent data breach reports and OWASP studies have broken the myth of the “Insider Threat”. The primary cause of breaches is poorly executed applications, specifically web applications that rely upon complex multi-layered infrastructure. While there is no agreement on which methods or technologies and ‘best’ for securing applications, there is growing interest in the application development community in learning about the available options.

## What We Expect to See

- **A Focus on Web Application Security:** As a general rule we don’t have very good statistics in security and risk management, but this trend is changing. With better forensic information we are showing that web application breaches are the leading cause of security breaches. While this has not yet translated into a significant change in security spending, expect to see long lines and greater interest in code security products and education.
- **Anti-exploitation:** While education in the development community lags regarding what constitutes risky code, tools that identify poor code or provide anti-exploitation will see a lot of attention. The tools vary greatly in the depth of their features, and where in the development cycle they fit. For example, some examine source code, some examine objects while they are compiled or linked, and others offer run-time protection. You will need to ask the vendor what classes of anti-exploitation they provide, and see if their deployment model fits your development framework.
- **Integrated Assessment and Firewall Technologies:** Web application development cycles are so short that full regression testing of new functions is near impossible. More, test systems fail to mimic live production sites, so many vulnerabilities are missed prior to deployment. This has increased demand for application scanning, and changed it into a never-ending task. The window of time between when a vulnerability is introduced and when it is discovered is very small. In most cases exploitation begins *before* a fix can be identified, implemented, tested, and rolled out to production servers. To fill the gap, vulnerabilities discovered by application scanners are being fed into web application firewall (WAF) platforms in near-real-time to block while the application fix is underway. Since the 2009 RSA show, the number of WAF vendors who offer dynamic blocking has tripled. The quality of the assessment is still key, but investigate what your WAF provider is offering, how quickly new policies can be deployed, and what the performance impact will be. This is an effective security feature but has potential policy management and performance impacts which you need to understand.

## Select Securosis Research on Application Security

For more depth on this topic, check out the blog posts, papers, webcasts, and other content we post in the Securosis Research Library: <http://securosis.com/research/application-security>.

Web App Firewalls	Application Testing	Application Assessment
art of defense (342)	CENZIC (2624)	Independent Security Evaluators (2454)
Barracuda Networks (1549)	Fortify (2037)	IOActive (2133)
Breach Security (629)	HP (1440)	Matasano (554)
Fortify (2037)	IBM (1316)	CENZIC (2624)
Fortinet (2225)	nCircle (1023)	
Imperva (417)	Qualys (1432)	
Protegrity (1029)	Rapid7 (328)	
	Tenable (956)	
	Veracode (729)	

# Security Management

For the past 20 years, we've been buying technologies to implement security controls. Yet management of all this security tends to be considered only when things are horribly broken — and they are.

## What We Expect to See

There are four areas of interest at the show relative to security management:

- **Log Religion:** Driven by our friends at the PCI Security Standards Council, the entire industry has gotten the need to aggregate log data and do some level of analysis. Thank you, Requirement 10! So at the show this year, it'll be a log management infestation, with a new vendor poking out of every nook and cranny to espouse a new architecture, disruptive pricing, or some other eye candy. And yes, you do need to collect logs, so focus your efforts at the show on figuring out what is the best fit for your organization. Are you just collecting logs or do you need to correlate and alert? What are your volume and scalability requirements? What kind of reporting do you need? What about integration with the rest of your infrastructure? The point here is not to make a decision but to establish a short list of 3-4 vendors to dig deeper into after the show.
- **Platform Mentality:** Since security management is supposed to make your life easier, you don't need to be a genius to realize that having a management console for every device type in your network doesn't make a lot of sense. So you'll hear a lot about SIEM + Log Management + Configuration Patch + Vulnerability + Network Flow = Nirvana. To be clear, management leverage is good. Doing so by adding even more complexity to your environment — not so much. So to the degree that you are ready to start integrating management disciplines, focus your discussions on migration. How do you get to the promised land? Which hopefully doesn't involve a truckload of high priced consultants to do the 'customization'.
- **Risk Mumbo Jumbo:** Risk is likely to be a hot topic at RSA as well. The more mature security programs have figured out that 'security' means nothing to senior management, but C-level folks get 'risk'. Unfortunately, there are no accepted mechanisms to define or quantify risk. So when a vendor starts talking about "risk scores" you should focus on the amount of effort to get a risk model set up and what's required to keep it up to date. You can't go down to Best Buy and get Risk Management in a box, so the question is how much effort you are willing to put in to show a graph to the CFO, which may or may not reflect reality.
- **Operational Efficiency:** Finally, you'll likely hear a lot about improving the operations of your environment. That was a major theme last year in the depths of the recession, but the issue hasn't gone away. The plays into the themes around integration and platforms, but ultimately there will be a number of niche tools (like firewall policy managers) designed to make your operational teams more efficient, saving money. Depending on the size and/or maturity of your security program, some of these tools may yield value. But adding yet another widget isn't a good thing unless you can redeploy resources onto other functions by taking advantage of automation.

# Compliance

Compliance isn't merely a major theme for the show, it's also likely the biggest driver of your security spending. While there's no such thing as a compliance solution, many security technologies play a major role in helping you achieve and maintain compliance.

## What We Expect to See

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

- **New Regulations/Standards:** Over the past year we've seen the passing or increased enforcement of a handful of new regulations with security implications — the HITECH act in healthcare, NERC-CIP for energy utilities, and the Massachusetts data protection law (201 CMR 17.00). Each of these adds either new requirements or greater penalties than previous regulations in their industries, which is sure to get the attention of senior management. While PCI is still the biggest driver in our industry, you'll see a big push on these new requirements.

If you are in one of the targeted verticals, we suggest you buff up on your specific requirements. Many of the vendors don't really understand the specific industry requirements and are pushing hard on the FUD factor. Ask which requirements they meet and how, then cut vendors who don't get it. Your best bet is to talk with your auditor or assessor before the show to find out where you have deficiencies, and focus on addressing those issues.

- **The 'Easy' Compliance Button:** While it isn't a new trend, we expect to see a continued push to either reduce the cost and complexity of compliance, or make you think they do. Rapid deployment, checkbox rules sets, and built-in compliance reports will top of the feature lists. While these features might help you get off to a good start, even checkbox regulations can't always be satisfied with checkbox solutions.

Instead of focusing on the marketing messaging, before you wander the floor have an idea of the areas where you either need to improve efficiency or have an existing deficiency. Many of the reporting features really can reduce your overhead, but enforcement features are usually trickier. Also, turning on all those checkboxes (especially in tools with alerts) might actually increase the time the tool eats up. Ask to walk through the interface yourself rather than sticking with the canned demos — that will give you a much better sense of whether the product can help more than it hurts. Also check on licensing, and whether you have to pay more for each compliance feature or rule set.

- **IT-GRC and Pretty Dashboards:** Even though only a handful of large enterprises actually buy GRC (Governance, Risk, and Compliance) products, plan on seeing a lot of GRC tools and banners on the show floor. Most of you don't need dedicated IT-GRC tools, but you do need good compliance reporting in your existing security tools. Dashboards are also great eye candy — and some can be quite useful, but many are more sales tools for internal use than to improve the security of your environment.

Dig in past the top layer of GRC tools and security dashboards. Are they really the sort of thing that will help you get your job done better or faster? If not, focus on obtaining good compliance reports using your existing tools. You can use these reports to keep assessors/auditors happy and reduce audit costs.

## Select Securosis Research on Security Management and Compliance

For more depth on this topic, check out the blog posts, papers, webcasts, and other content we post in the Securosis Research Library: <http://securosis.com/research/security-management> and <http://securosis.com/research/compliance>

SIEM/Log Management	Configuration/ Patch Management	Vulnerability Assessment	Network Packet Capture	Compliance
AlienVault (553)	Lumension (923)	Application Security (2539)	Narus (2117)	Agilance (216)
ArcSight (931)	Microsoft (1517)	Lumension (923)	PacketMotion (2619)	CA (1533)
CA (1533)	Novell (1344)	nCircle (1023)	Solera Networks (439)	Archer/RSA (1338)
Intellitactics (652)	Symantec (1416)	Qualys (1432)		Modulo (639)
LogLogic (633)		Rapid7 (328)		
LogMatrix (330)		StillSecure (2228)		
LogRhythm (2158)		Tenable (956)		
netForensics (832)				
Nitro Security (2051)				
RSA (1725)				
SenSage (845)				
Splunk (2544)				
Symantec (1416)				
Tenable (956)				
TriGeo (817)				

# Virtualization and Cloud

The thing about virtualization and 'cloud' is that they really cut across pretty much every other coverage area. But given they're new and shiny — which really means confusing and hype-ridden — we figured it was better to split out the topic to provide proper context on what you'll see, what to believe, and what is important.

## What We Expect to See

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

- **Virtualization Security:** The tools and techniques for locking down virtual machines and infrastructures. Most virtualization risk today is around improper management configuration and changes to networking, which may introduce new security issues or circumvent traditional network security controls. Focus on virtualization security management tools — especially configuration management that can handle the virtualization configuration, not just the operating system configuration and network security. Be careful when vendors over-promise on network security performance — you can't simply move a physical appliance into a virtual appliance and expect the same performance.
- **Security as a Service:** A variety of new and existing security technologies can be delivered as services via the cloud. Early examples included cloud-based email filtering and DDoS protection, and we now have options for everything from web filtering, to log management, to vulnerability assessment, to configuration management. Many of these are hybrid models, which require some sort of point of presence server or appliance on your network. Security as a Service is especially interesting for mid-sized enterprises, since it's often able to really reduce management and maintenance costs. Although many of these offerings don't technically meet the definition of cloud computing, don't tell the marketing departments.
- **Cloud-Powered Security:** Some vendors are leveraging cloud-based features to enhance their security product offerings. The product itself isn't delivered from the cloud or aimed at securing the cloud, but uses the cloud to enhance its features. For example, an anti-malware vendor that leverages cloud technologies to collect malware samples for signature generation. This is where we see the most abuse of the term 'cloud', and you should push the vendor on how the technology really works rather than relying on branding vapor.
- **Cloud Security:** The tools and techniques for securing cloud deployments. This is what most of us think of when we hear "cloud security", but it's what you'll see the least of on the show floor. We suggest you attend the [Cloud Security Alliance Summit on Monday](#) (if you're reading this before then) or Rich's presentation with Chris Hoff on Tuesday at 3:40. You can also visit the Cloud Security Alliance in booth 2641.

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.

## Select Securosis Research on Virtualization and Cloud Security

For more depth on this topic, check out the blog posts, papers, webcasts, and other content we post in the Securosis Research Library: <http://securosis.com/research/cloud-and-virtualization>.

# See Securosis at RSA 2010

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

## Speaking Sessions

- **STAR-106:** [Security Groundhog Day — Third Time's a Charm](#) — Mike and Rich (Tuesday, March 2 @ 1 PM)
- **P2P-304A:** [Security Posture: Wading Through the Hype...](#) — Mike (Thursday, March 4 @ 1 PM)
- **EXP-108:** [Winnovation- Security Zen through Disruptive Innovation and Cloud Computing](#) — Rich (Tuesday, March 2 @ 3:40 PM)
- **END-203:** [How to Expedite Patching in the Enterprise? A View from the Trenches](#) — Rich (Wednesday, March 3 @ 10:40 AM)
- **DAS-403:** [Securing Enterprise Databases](#) — Adrian (Friday, March 5 @ 11:20 AM)

## Other Events

- **Security Blogger Meet Up:** Securosis will be at the 3rd annual [Security Blogger Meet Up](#) at the classified location. You need to have a blog and be pre-registered to get in.
- **Securosis and Threatpost Disaster Recovery Breakfast:** Once again this year Securosis will be hosting the [Disaster Recovery Breakfast](#) on Thursday, March 4 between 8 and 11. 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.
- **PechaKucha (PK) Happy Hour** - Rich will be presenting at the [PK Happy Hour](#) on Thursday, March 4 between 5 and 6:30 PM in the Crypto Commons. See if he can get through 20 slides in about 6 1/2 minutes. Fat chance, but Rich is going to try.

# Upcoming Research

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, and follow our [Totally Transparent Research](#) policy.

Our plan for the next few months is to publish the following papers:

- Understanding and Selecting a Database Encryption or Tokenization Solution
- Understanding and Selecting a Database Assessment Solution
- Project Quant for Database Security
- Quick Wins with DLP
- Pragmatic Data Security
- Network Security Fundamentals
- Endpoint Security Fundamentals
- Understanding and Selecting a SIEM/Log Management product
- Understanding and Implementing Network Segregation
- Data Security for the Cloud

You can check out the most recent plans for our upcoming research at <http://securosis.com/research/upcoming-research-agenda>.

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](#).

# 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.  
20930 North Tatum Blvd  
Suite #110-116  
Phoenix, AZ 85050  
Office: +1-602-412-3051  
[info@securosis.com](mailto:info@securosis.com)  
<http://www.securosis.com>