Security Analytics
Team of Rivals

Version 1.4
Released: March 16, 2017

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

Author's Note

The content in this report was developed independently of any sponsors. It is based on material originally posted on the Securosis blog, but has been enhanced, reviewed, and professionally edited.

Special thanks to Chris Pepper for editing and content support.

This report is licensed by Intel Security.

www.intelsecurity.com

McAfee is now part of Intel Security. With its Security Connected strategy, innovative hardware-enhanced security, and unique Global Threat Intelligence, Intel Security develops proactive, proven security solutions and services to protect systems, networks, and mobile devices for business and personal use all over the world. www.intelsecurity.com.

Copyright

Security Analytics Team of Rivals

Table of Contents

Everything Changes

Security monitoring has been a foundational element of security programs for over a decade. The initial driver for separate security monitoring infrastructure was the overwhelming amount of alerts flooding out of intrusion detection devices, requiring some correlation to determine which mattered. Soon compliance mandates (primarily PCI-DSS) emerged as a forcing function, providing a clear requirement for log aggregation — which SIEM already offered. As the primary security monitoring technology, SIEM became entrenched for alert reduction and compliance reporting.

Attacks have become much more sophisticated, and detection now requires a level of advanced analysis that is difficult to achieve using older technologies. So a new category of technologies dubbed Security Analytics has emerged to fill the need.

But everything changes, and requirements have evolved. Attacks have become much more sophisticated, and detection now requires a level of advanced analysis that is difficult to achieve using older technologies. So a new category of technologies dubbed *Security Analytics* has emerged to fill the need, addressing specific use cases which require advanced analysis — such as User Behavior Analysis, insider threats, and network-based malware detection. These products and services are all based on sophisticated analysis of aggregated security data, using "big data" technologies which did not exist when SIEM initially appeared in the early 2000s.

The age-old cycle should be familiar: existing technologies struggle to maintain relevance and effectiveness as requirements evolve, so new companies innovate to fill the gap. Enterprises have seen this movie before, including new entrants' inflated claims to address all the failings of last-generation technology, with little proof but high prices. To avoid the disappointment that inevitably follows throwing the whole budget at an unproven technology, we recommend organizations ask a few questions:

1. Can we meet this need with existing technology?
2. Can these new offerings definitively solve the problem in a sustainable way?
3. How will we know if and when the new can supplant the old?

Of course the future of security monitoring is cloudy (just like everything else), so we do not have all the answers today. But you can understand how security analytics works, why it's different (sometimes better), whether it can help you, where in your security program the technology can provide value, and how soon.

But we need to be very clear: security analytics is not a replacement for SIEM — at least today. For some time you will need both technologies. The role of a security architect is basically to assemble a set of technologies to generate actionable alerts on specific threat vectors relevant to the business, investigate attacks in process and after the fact, and generate compliance reports to streamline audits. These technologies compete to a degree, so we like the analogy of a *Team of Rivals* working together to meet requirements.

It gets better: many current security analytics offerings were built and optimized for a single use case — typically advanced threat detection, User Behavior Analysis, or insider threats. The Team of Rivals is especially appropriate for organizations facing multiple threats from multiple actors, who understand the importance of detecting attacks sooner and responding better. As the movie *Contact* asked, "Why buy one, when you can buy two for twice the cost?" Three or four have to be even better, right?

On Security Analytics

Before we dig too deeply into technology we need to clarify our position on security analytics. It's not something you just buy. Not for a long while, anyway. Security analytics is a way you can accomplish something important: detecting attacks in your environment. But it's not an independent product category.

Security analytics is not something you just buy. Not for a long while, anyway. It is a way you can accomplish something important: detecting attacks in your environment. But it's not an independent product category.

That doesn't mean security analytics will become subsumed into an existing SIEM technology or other security monitoring product/service stack, although that's one possibility. We can easily argue these emerging analytics platforms should become the next-generation SIEM. But the Security Analytics Team of Rivals is not a long-term solution. At some point organizations need to simplify and consolidate vendors and technologies. They will pick one security monitoring platform, but we are not taking bets on which.

But an integrated solution *someday* won't help you detect attackers in your environment *today*. So let's define what we mean by security analytics, and then focus on how these technologies work together to meet today's requirements, with an eye for the future.

To call itself a security analytics offering, a product or service must address:

- **Data Aggregation:** It's impossible to analyze without data. Of course there is some question whether the security analytics tool needs to gather its own data, or can just integrate with an existing security data repository like your SIEM.
- **Math:** We joke a lot that math is the hottest thing in security lately, especially given how early SIEM correlation and IDS analysis were based on math too. But this new math is different, based on advanced algorithms and data management to find patterns within data volumes which were unimaginable 15 years ago. The key difference is that you no longer need to know what you are looking for to find useful patterns, a critical limitation of today's SIEM. Modern algorithms can help you spot unknown unknowns. Looking only for known and profiled attacks (signatures) is clearly a failed strategy.
- **Alerts:** These are the main output of security analytics, and you will want them prioritized by importance to your business.
- **Drill down:** Once an alert fires analysts need to dig into the details, both for validation and to determine the most appropriate response. So analytics tools must be able to drill down and provide additional detail to facilitate response.
- **Learn**: This is the tuning process, and any offering needs a strong feedback loop between responders and the folks running it. You must refine analytics to minimize false positives and wasted time.
- **Evolve:** Finally the tool must improve, because adversaries are not static. This requires a threat intelligence research team at your security analytics provider constantly looking for new categories of attacks, and providing new ways to identify attacks.

We could write a book about the nuances which distinguish the different approaches to security analytics, arguing whether the criteria above are sufficient. Or perhaps these are still too broad. The point is that as security analytics products evolve to track market requirements, the market will identify the most important criteria and determine which analytics approach survives. We will stick to the tactical level in this paper, concerning ourselves only with how you can align your security monitoring technologies and emerging analytics capabilities to better identify attacks in your environment.

Coexistence Among Rivals

As described above, any single approach to security monitoring probably cannot satisfy all your requirements. So you need a set of complimentary technologies which can coexist. Either the old guard evolves to meet modern needs or the new guard supplants them — the technology industry is notably Darwinian. But in the meantime you need to figure out how to solve a problem: detecting advanced attackers and insiders who use increasingly sophisticated techniques.

We don't claim to be historians, but Lincoln's Team of Rivals (Hat tip to Doris Kearns Goodwin) seems interestingly relevant. Briefly, President Lincoln needed to make a divisive political organization work. So he named rivals to his cabinet, making sure everyone was accountable for the success of his administration. There are parallels in security — a security program must, first and foremost, protect critical data, although from hackers rather than Confederate spies and sympathizers. So our primary focus must be on protection, while ensuring our ability to respond and generate compliance reports. Different tools (today, at least) specialize in different aspects of the security problem, and fit into a program in different places, but ultimately they must work together. Thus the opportunity for a Team of Rivals to address the security monitoring challenge.

President Lincoln needed to make a divisive political organization work. So he named rivals to his cabinet, making sure everyone was accountable for the success of his administration.

How can you get these very different and sometimes oppositional tools to work together, often despite vendors' best interests? Most SIEM vendors are working on a security analytics strategy, so they aren't likely to be enthusiastic about working with a third-party analytics offering — which is intended to replace them. Likewise, security analytics vendors want to marginalize the old guard as quickly as possible, leveraging SIEM capabilities for data collection/aggregation and then taking over the heavy analytics to deliver value independent of the SIEM, and stealing that budget.

But trying to pick winners and losers in security markets is not a great use of time. We recommend you focus on identifying your organization's problems, then choosing technologies to address them. That means starting with use cases, letting them drive which data must be collected and how it should be analyzed.

Revisiting Adversaries

When evaluating security use cases we always recommend starting with adversaries. Your security architecture, controls, and monitors need to factor in the tactics of likely attackers, because you

don't have time or resources to address every possible attack. We researched this extensively for The CISO's Guide to Advanced Attackers, but in a nutshell adversaries can be broken into a few different groups:

1. **External Actors**
2. **Insider Threats**
3. **Auditors**

You can break external actors down further into a bunch of subcategories, but for this research that would be overkill. External actors needs to gain a foothold in the environment by compromising a device, move laterally to achieve their mission, and then connect to a command and control network for further instructions and exfiltration. This is your typical adversary in a hoodie and mask, featured in every vendor presentation.

Insiders are a bit harder to isolate because they are often authorized for access, so detecting misuse requires more nuance — and likely human validation. In this case you look for signs of unauthorized access, privilege escalation, and ultimately exfiltration.

The third major category of adversaries is auditors. Okay, don't laugh too hard. Auditors are not quite adversaries, but more precisely a constituency you need to factor into your data aggregation and reporting efforts. These folks are predominately concerned with checklists. So you need to make sure to substantiate work instead of just focusing on results.

The third major category of adversaries is auditors. Okay, don't laugh too hard. Auditors are not quite adversaries, but more precisely a constituency you need to factor into your data aggregation and reporting efforts.

Using the right tool for the job

You already have a SIEM so you might as well use it. Its strength is in data aggregation, simple correlation, forensics & response, and reporting. But what kinds of data do you need? A lot of stuff we have been talking about for years.

- Network telemetry, with metadata from network packet streams at minimum
- Endpoint activity, including processes and data flowing through the device's network stack
- Server and data center logs, and change control data
- Identity data, especially around privilege escalation and account creation
- Application logs — most useful are access and bulk data transfer logs
- Threat intelligence to identify attacks seen in the wild, but not necessarily yet by your organization

This is not brain surgery, and you are doing much of it already. Security monitors to find simple attacks have been deployed and still require tuning, but should work adequately. The key is to leverage the SIEM for what it is good at: aggregation, simple correlation (of indicators you know to look for), searching, and reporting. SIEM's strength is not discovering patterns within massive volumes of data.

Now let's consider how security analytics impacts the discussion, although there is significant confusion as to what security analytics even is. Basically, any product that analyzes security data now seems to be positioned as "security analytics." So how do we define these products? Security analytics uses a set of purpose-built algorithms to analyze massive amounts of data, searching for anomalous patterns of activity, misconfiguration, or privilege escalation (among other indicators) which may indicate misuse or malicious activity.

There are a variety of approaches, and even more algorithms, for finding such patterns. We find the best way to categorize analytics approaches is to focus on use cases rather than underlying math; we'll explain why below. We will assume the vendor chooses appropriate algorithms and computational models to address each use case — otherwise their tech won't work and Mr. Market will grind them to dust. Darwin in action!

Security Analytics Use Cases

When we think about security analytics use cases a few bubble to the top. There are many ways to apply math to a multitude of security problems, so you are welcome to quibble with these simplistic categories. But these are the most common we hear about, and they nicely cover the key requirements.

We need advanced analytics to detect advanced attacks because older monitoring platforms are driven by rules — you need to know what you are looking for before you can find it. Unfortunately, as we have all learned, modern attackers don't follow a single playbook, so looking for yesterday's attacks is lousy strategy.

Advanced Attack Detection

We need advanced analytics to detect advanced attacks because older monitoring platforms are driven by rules — you need to know what you are looking for before you can find it. Unfortunately, as we have all learned, modern attackers don't follow a single playbook, so looking for yesterday's attacks is lousy strategy. Advanced attack detection runs against data from traditional logs, as well as endpoint and network telemetry. This breadth of collection provides adequate data to build baselines and models, which then enable an analytics product to find anomalous behavior which may represent a threat.

User Behavior Analysis

UBA has a lot in common with advanced attack detection, but focuses on user behavior to detect malicious activity. This approach works because at some point every attack compromises a user, so tracking and analyzing user activity is an excellent way to detect malicious activity. But this analysis is complicated by the fact that users interact with systems both inside and outside your organization.

They use SaaS services which often do not provide adequate visibility into their activity. And they connect with multiple devices. So you need to move past a device-centric perspective to evaluate behavior across many devices, understand a user's typical behavior, and recognize abnormal activity. Further complicating matters is location — users access systems from different locations. UBA runs on data gathered using a number of different collection techniques, including but not limited to: log analysis, endpoint telemetry, mobile device analysis, and geolocation. Network data can also be factored in for users running through a proxy (either on-premise or within the cloud) to collect activity.

Insider Threat

Our final use case involves looking specifically for malicious insiders, which is challenging because they are authorized to access internal data. As with the other two cases, this analysis encompasses user behavior and network telemetry, but may also involve internal system access (especially Finance and HR) as well as physical access. Physical access and accessible systems vary widely between organizations so analytics must be customized for each organization. Legitimate use also varies by company and user, so indicators of misuse must be tuned and optimized to a much greater degree, increasing deployment time and necessary customization.

The Reality of Security Analytics Use Cases

Being a bit more creative, we could add cognitive analysis, web behavior, identity analytics, application usage, cloud security analytics, and a variety of other use cases for security analytics. But that becomes overkill because these use cases all leverage advanced mathematical analysis of aggregated security data. The use cases differ mostly on which data they analyze. But they all overlap considerably, so soon enough we expect all security analytics vendors to roll out solutions addressing all useful use cases.

How can we be so dismissive of the tremendous work data scientists devote to making these tools possible? Mostly because the work of data scientists has made detecting advanced attacks achievable without a Ph.D. in Math.

In the heat of a buying cycle you will hear a lot about a variety of mathematical techniques. We recommend you disregard this. Unless you have a Ph.D. in Mathematics it will likely only distract from your mission: to find a tool which detects attacks.

How can we be so dismissive of the tremendous work data scientists devote to making these tools possible? Mostly because the work of data scientists has made detecting advanced attacks achievable *without* a Ph.D. in Math. You need to look for patterns which indicate an active threat actor. Follow the kill chain looking for indications of reconnaissance, privilege escalation, configuration drift, command and control traffic, and exfiltration. The sooner you detect an attack, the more likely you can intervene *before* a data breach. Easier said than done, but you don't need to overcomplicate your decision.

Coexistence

Returning to the right tool for the job, security analytics offerings aren't really designed to provide a clear way to search for and pivot on an alert, and then drive an incident response process. They also don't lend themselves to easy compliance reporting. Of course that does not mean tools won't extend functionality to address those requirements over time.

But today in early 2017, analytics tools aren't built to address all the security monitoring use cases. You cannot yet choose one or the other — you need both to work together for the foreseeable future. So look for logical integration points, including:

1. **Data:** Your SIEM has been collecting and aggregating security data for a long time. Messing with it now doesn't make much sense. Extracting data to drive security analytics is much like data extraction for non-security business intelligence. Extraction can be time-consuming so ensure you automate sufficiently.

2. **Alerts:** You will be getting alerts from both systems, so you need to figure out what will happen when an alert fires. Where will operations folks and responders spend the majority of their time? What's important here is bi-directional information sharing between the SIEM and security analytics offering. You should be able to move back and forth between tools, maintaining context.

Heterogeneity

One characteristic of the security market is that consolidation and partnership continuously drive larger security vendors to offer something in pretty much every product category. SIEM and security analytics are no different. The question is whether you will go with a single vendor or more than one. Is this a market for best of breed? Your answer depends on which problems you are trying to solve. Many SIEM vendors offer security analytics capabilities, either via separate offerings or partnerships with smaller companies. As we mentioned earlier, inevitably upstart security analytics players will add SIEM capabilities, because the market is too big to ignore. But what does that mean for enterprises?

At risk of sounding like a broken record, go back to your requirements. If you can get the security analytics you need for your use cases from your SIEM vendor, that's a no-brainer. Likewise, if a security analytics vendor proves they can detect relevant attacks you highlighted during adversary analysis, roll with that offering and ensure it coexists with the existing SIEM.

But even if you go with a single vendor today, plan for heterogeneity. Demand flexible integration points between disparate monitoring technologies, *even if you don't need that today*. You will add cloud security

But even if you go with a single vendor today, plan for heterogeneity. Demand flexible integration points between disparate monitoring technologies, even if you don't need that today. You will add cloud security monitoring soon, if you don't have it already, and may reopen your analytics decision.

monitoring soon, if you don't have it already, and may reopen your analytics decision. The only things we can guarantee are that your attack surface will be different tomorrow and that adversaries will get better, so at some point a new analytics offering may make sense. Don't paint yourself into a corner by losing any access to your data.

By the way, heterogeneity doesn't pertain only to analytics vendors and SIEM. Given the severe and increasing skills gap we see when searching for security professionals, you may want a service provider for some of these functions. Considering the advanced nature of security analytics, and the customization it requires, that function is likely too immature for a managed service. But we recommend evaluating services which provide traditional SIEM capabilities.

As an additional caveat on the services discussion, many MSSPs aren't very effective at keeping a SIEM tuned to detect attacks or adding use cases. But operating the system and making sure data gets to the right place is a reasonable task for a service provider. Regardless, as with any service provider, care and diligence are required: in this case pay attention to proper alert handoffs and access to SIEM data to facilitate forensics and incident response.

A Glimpse of the Future

A lot of our research is conceptual so we like to wrap up with a scenario. This helps make ideas a bit more tangible and provides context for you to apply them to your particular situation. To illuminate how the Security Analytics Team of Rivals can work, let's consider a scenario involving a high-growth retailer who needs to maintain security while scaling operations which are being stressed by growth.

Our company, which we'll call *GrowthCo,* has made technology a key competitive lever, especially around retail operations, to keep things lean and efficient. As scaling issues become more serious they realize their attack surface is growing, and that may force shortcuts which expose critical data. They have always invested heavily in technology, but less in people. So their staff is small — especially in security.

In terms of security monitoring technologies, GrowthCo has had a SIEM for years (thanks, PCI-DSS). They have very limited use cases in production due to resource constraints. They do the minimum required to meet their compliance obligations.

To address staffing limitations and the difficulty of finding qualified security professionals, they decided to co-source their SIEM with an MSSP a few quarters ago. Their SIEM runs both on-premise and within the MSSP's SOC; the MSSP takes point on running the tool and generating alerts. The goal was for the MSSP to help expand use cases and take over first and second tier response. Unfortunately the co-sourcing relationship didn't completely work out. GrowthCo doesn't have the resources to closely manage the MSSP, who isn't as self-sufficient as they portrayed themselves during the sales process. Sound familiar?

The internal team had some concerns whether the SIEM can detect the attacks they expect to see as a high-profile retailer based on years of using it, so they also deployed a security analytics product for internal use. Their initial use case focused on advanced detection, but they want to add UBA (User Behavior Analysis) and insider threat use cases quickly to broaden the usage of security analytics.

The challenge facing GrowthCo is to get its Security Analytics Team of Rivals — which includes the existing SIEM, the new security analytics product, the internal team, and the co-sourcing MSSP — all on the same page and working together on the same issues.

The challenge facing GrowthCo is to get its Security Analytics Team of Rivals — which includes the existing SIEM, the new security analytics product, the internal team, and the co-sourcing MSSP — all on the same page and working together on the same issues. Let's consider a few typical use cases for how this can work.

Detecting Advanced Attacks

GrowthCo's first use case, detecting advanced attacks, kicks off when their security analytics tool produces an alert. The alert points to an employee making uncharacteristic requests on internal IT resources. The internal team quickly determines it seems real. That user shouldn't be probing the internal network, and their traffic has historically been restricted to a small set of (different) internal servers and a few SaaS applications.

To better understand the situation, the internal team asks the MSSP to provide some data from the SIEM to offer some insight into what the adversary is doing across the environment. This is an unusual role for a service provider. Normally the MSSP gets the alert directly, has no idea what to do with it, and then sends it along to GrowthCo's internal team to figure out. But that doesn't reduce demand on internal resources.

But giving the MSSP discrete assignments like this enables them to focus on what they are capable of, while saving the internal team a lot of time assembling context and supporting information for eventual incident response.

But giving the MSSP discrete assignments like this enables them to focus on what they are capable of, while saving the internal team a lot of time assembling context and supporting information for eventual incident response. Returning to our scenario: this time the MSSP identifies a number of privilege escalations, configuration changes, and activity on other devices. Their report details how the adversary gained presence and then moved internally, ultimately compromising the device which triggered the SIEM alert.

This scenario could just as easily have started with an alert from the SIEM sent over from the MSSP (hopefully with some context), then used as the basis for triage and deeper analysis on the security analytics platform. *The point is not to be territorial about where each alert comes from, but to use available tools as effectively as possible.*

Hunting for Insiders

Our next use case involves looking for malicious employee activity. This situation blurs the line between User Behavioral Analysis and Insider Threat Detection. The security analytics product first associates devices in use with specific users, and then combines device telemetry with other data sources to provide a baseline of normal activity for each user. By comparing activity to baselines the internal team can look for uncharacteristic activity for each employee, regardless of device or location. If they find something they can dive into user activity or pivot into the SIEM, using its broader data set to search and drill down into devices and system logs for more evidence of attacker activity.

This kind of analysis tends to be difficult with only a SIEM, because their data model is keyed to devices and not designed to correlate data across them. That does not mean it is impossible, or that SIEM vendors aren't adding more flexible analysis, but SIEM tends to excel when rules can be

defined and threat vectors modeled into the tool in advance. This is an example of choosing the right tool for the right job. Once you know what you are looking for, a SIEM can very effectively mine aggregated security data.

Streamlining Audits

Finally, you can also use a Team of Rivals to deal with the other class of 'adversary': auditors. Instead of having an internal team spend a great deal of time mining security data and formatting reports, you could have an MSSP prepare initial reports using data collected in the SIEM, and then have the internal team perform some quick Q/A, to optimize use of scarce security resources. Of course a service provider will have less understanding of the environment because they aren't employees, but they can start with the deficiencies identified in the last audit and SIEM reports to substantiate improvements.

Once again, a little creativity and intelligence enable us to leverage the varied strengths of an extended security team. The payoff is less time and effort spent on frustrating compliance reporting, with full advantage taken of the service provider and reduced load on the internal team. But the internal team bears ultimate responsibility and accountability for audits, so they must still ensure the completeness and quality of reports, and provide additional documentation as necessary.

Once again, a little creativity and intelligence enable us to leverage the varied strengths of an extended security team. The payoff is less time and effort spent on frustrating compliance reporting, with full advantage taken of the service provider and reduced load on the internal team.

Summary

As we have said through this paper, it is no longer an either/or choice between security analytics and SIEM. Or even between insourcing and outsourcing security monitoring. You need to establish a team with complimentary capabilities, skills, and resources; then leverage each part for what it does best. It is frustrating to use a technology for something it's not built to do, and just as frustrating to expect a service provider to do things beyond their capability — regardless of their claims during the sales cycle. So don't do that — build your security monitoring program to give all parties the best chance of success.

The goal is not, of course, to run multiple overlapping technologies in parallel forever. Eventually you will be able to move to a single strategic security monitoring platform. But not today, so in the meantime you need to wrangle a Security Analytics Team of Rivals.d

This paper explains why these technologies aren't mutually exclusive, and how you can leverage them both, across a variety of internal and external teams and tools, to address your security monitoring requirements. The goal is not, of course, to run multiple overlapping technologies in parallel forever. Eventually you will be able to move to a single strategic security monitoring platform. But not today, so in the meantime you need to wrangle a Security Analytics Team of Rivals.

If you have any questions on this topic, or want to discuss your situation specifically, feel free to send us a note at info@securosis.com.

About the Analyst

Mike Rothman, Analyst and President

Mike's bold perspectives and irreverent style are invaluable as companies determine effective strategies to grapple with the dynamic security threatscape. Mike specializes in the sexy aspects of security — such as protecting networks and endpoints, security management, and compliance. Mike is one of the most sought-after speakers and commentators in the security business, and brings a deep background in information security. After 20 years in and around security, he's one of the guys who "knows where the bodies are buried" in the space.

Starting his career as a programmer and networking consultant, Mike joined META Group in 1993 and spearheaded META's initial foray into information security research. Mike left META in 1998 to found SHYM Technology, a pioneer in the PKI software market, and then held executive roles at CipherTrust and TruSecure. After getting fed up with vendor life, Mike started Security Incite in 2006 to provide a voice of reason in an over-hyped yet underwhelming security industry. After taking a short detour as Senior VP, Strategy at eIQnetworks to chase shiny objects in security and compliance management, Mike joined Securosis with a rejuvenated cynicism about the state of security and what it takes to survive as a security professional.

Mike published The Pragmatic CSO <http://www.pragmaticcso.com/> in 2007 to introduce technically oriented security professionals to the nuances of what is required to be a senior security professional. He also possesses a very expensive engineering degree in Operations Research and Industrial Engineering from Cornell University. His folks are overjoyed that he uses literally zero percent of his education on a daily basis. He can be reached at mrothman (at) securosis (dot) com.

About Securosis

Securosis, LLC is an independent research and analysis firm dedicated to thought leadership, objectivity, and transparency. Our analysts have all held executive level positions and are dedicated to providing high-value, pragmatic advisory services. 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 conform to 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 assessment.
- **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. Services available as part of a retainer package include market and product analysis and strategy, technology guidance, product evaluation, and merger and acquisition assessment. 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 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 tend to be customized to meet a client's particular 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. For more information about Securosis, visit our website: <http://securosis.com/>.