The Evolution of Data Driven Security

By David Monahan

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) Research Report

June 2014

Sponsored by:

BAY DYNAMICS™

Guidance® SOFTWARE

EMA™ IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

Table of Contents

Executive Summary

Information is data with context. The number 42 is a data point. Once given a context of "age" or "house number", it becomes information and more easily identified as useful or valuable. Information Security has always been a large consumer of *data*. More sophisticated best practices combined with expanding compliance and regulatory requirements have almost exponentially accelerated the production and consumption of data but they have also driven the need for better context and creating information. Event and activity *data* have grown to "Big Data" proportions. As a result, traditional log and event management tools and monitoring practices are insufficient because of their increasing inability to wade through the *data* to present the key *information* to those who need it.

Management and operations level IT and information security practitioners perceive the change in the volume and types of data available and tools required to provide analysis and context to create usable information. A multitude of tools exist that can provide practitioners a means to meet their informational and response needs to prevent attacks from becoming breaches or, at a minimum, significantly decrease the lag between breach and detection to reduce impacts and associated remediation costs. Enterprise Management Associates® (EMA) has partnered with its sponsors to provide this research, which clearly shows that the information security discipline needs next generation analytics capabilities to be successful in the age of Big Data.

> The era of Big Data has begun demonstrating to information security that there is more that can, and must, be done to identify threats, reduce risk, address fraud and improve compliance monitoring activities by bringing better context to data creating information for actionable intelligence.

EMA conducted a research survey to study how Security and IT practitioners at all levels are dealing with the ever increasing data volumes and diversity. From the research, EMA understands that all IT and Security organizations are really not much different from Target Corp. IT and Security are deluged with thousands of alerts daily, a majority of which appear to be critical, making response an insurmountable task with affordable staff levels and traditional tools. With so many critical alerts, they have moved from the analogy of finding the needle in the haystack to identifying and prioritizing THE needle in the stack of needles. The survey consisted of over 200 random IT and security respondents. A representative cross section of industries and company sizes ranging from SMB and SME to large enterprises and government were included. This report represents findings from an in-depth study of the responses.

The research analyzed various aspects of 13 security technologies used in Security Management. These technologies included tools that have been in use for over ten years such as Web Security Gateways, Network Admission Control (NAC) and Security Event & Incident Management (SIEM), as well as many newcomers such as Advanced Persistent Threat (APT)/ Advanced Targeted Attack (ATA) detection, Cloud Application Security and Advanced Security Analytics (SA) or Threat Analytics (TA). The era of Big Data has begun demonstrating to information security that there is more that can, and must, be done to identify threats, reduce risk, address fraud and improve compliance monitoring activities by bringing better context to data creating information for actionable intelligence. Practitioners can reap the security value of new forms of structured and unstructured information such as Human Resources records, employee calendars and email, and other sources not consumed by traditional log management and SIEM technologies. New adaptive algorithms called Machine Learning and Big Data analysis techniques can be utilized to identify abstract data relationships, anomalies, trends, fraudulent and other behavioral creating information where only data existed. The era of Big Data is driving the next technology evolution.

Key findings include:

1. Over 50% of organizations have *not* deployed SIEM, a foundational security technology.
2. Forty six percent of respondents believe SA/TA is the next evolution in SIEM.
3. Ninety five percent of SA/TA users received "Expected" to "Greater than expected" value from their solutions.
4. Sixty five percent of respondents said they NEED advanced automated responses to keep up with security alerts.
5. Sixty nine percent of respondents were "less than confident" to "highly doubtful" they could detect an important security issue before it had significant impact.
6. Ninety percent of organizations that have deployed a combination of SIEM, SA/TA and/or APT/ATA experienced reduced false alerts or improved actionable alerts; 100% of organizations that deployed only SA/TA experienced the reduction/improvement while only 60% of organizations that deployed only SIEM said they experienced reduced false alerts or improved actionable alerts.

This report sets the stage and provides insights into IT and Information Security practitioners' perceptions of their impediments to, and the solutions necessary for, success during this time of the Evolution of Data Driven Security.

Findings

Information Security has seen significant evolution in the last 25 years. Initially there were few systems, users, and access points making the task pretty straight forward and achievable with manual file reviews and a few homemade scripts. As the numbers of systems and applications increased so did the charting requirements forcing a change to log management systems. These helped by consolidating logs and including data searching and filtering tools. With the data explosions of the 1990s, caused by the expansion of Internet access and e-commerce, the market evolved again with the creation of Security Incident and Event Management (SIEM) tools. Over the last 15+ years, SIEM has evolved into a mainstay of security operations. SIEM provides event prioritization, suppression, correlation and normalization to reduce the volumes of alerts, as well as more advanced graphical reporting and various forms of search and data mining capabilities. With these tools, those responsible for information security have found many needles in the haystacks.

Demographics

Respondent Role and Association with Security

The top 10 functional areas represented 81% of the total respondents. The largest single group was Executive Management at the CIO/CTO level. This is a rare occurrence for random surveys but as a result, EMA was able to gather excellent insight into the budget holders and key decision makers' perceptions. Additionally, regardless of title, 62% of the respondents indicated that Information Security was part of their primary area of responsibility with another 20% indicating that though security was not their primary role, they were significantly involved in security in their organizations.

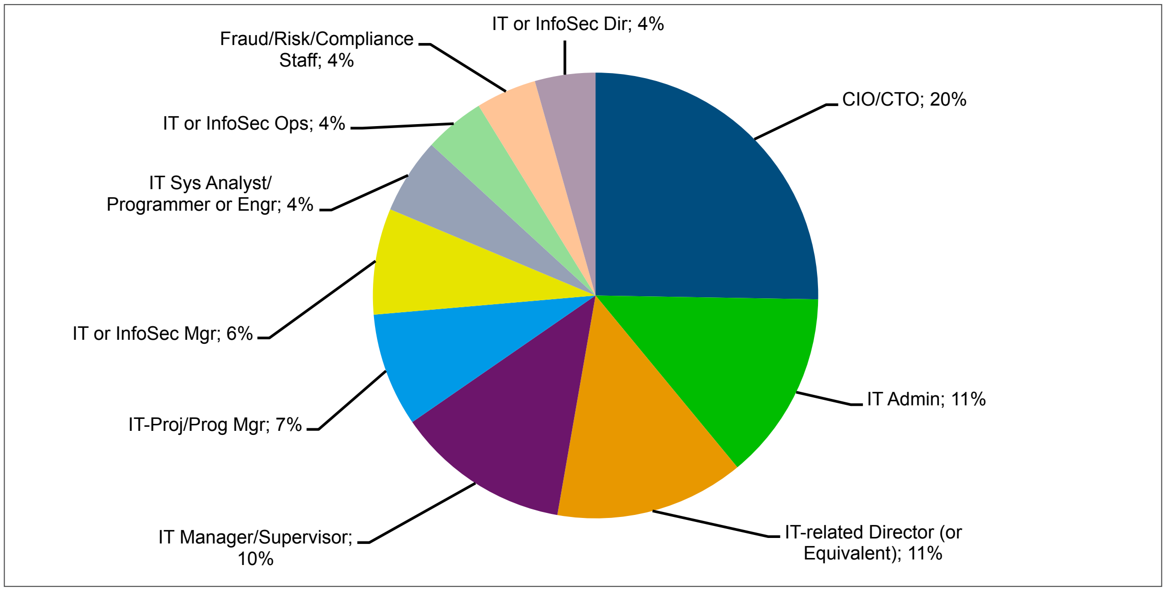

Figure 1a. Top 10 Respondents by Function

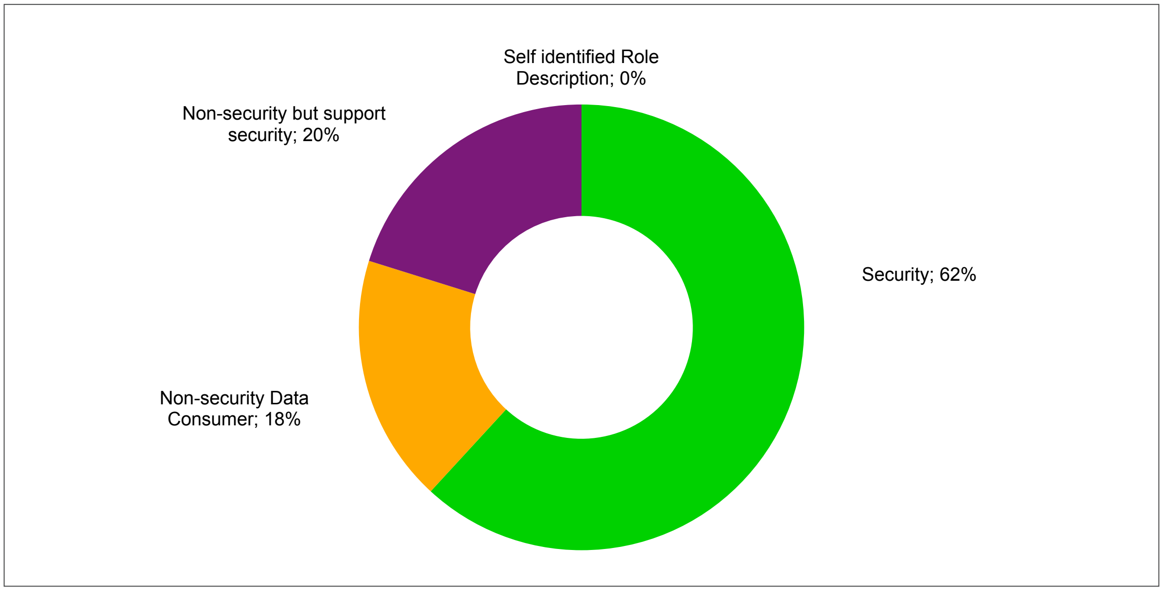

Figure 1b. Role with regards to Security

Additionally, when queried about their involvement in security projects, 74% said they had direct involvement with or a working knowledge of current security initiatives, putting them in a position to understand the issues involved with delivering security to the enterprise. This is a key point for the research. EMA asked this question and correlated it with the question on their association with security, represented in figure 1b above, to better isolate how much involvement the respondent really had. Generally, it is better to go on the conservative side and use the smaller number as the indicator. In this case, the smaller number of 74% still demonstrates a large percentage that are able to speak to the organizational security challenges, giving EMA a higher probability of accuracy in the other findings.

Operating Geographies

The operational geography of the companies represented by the respondents were heavily weighted on North America, as expected, but also showed a very strong representation globally with over half of the companies each operating in EMEA and APAC. This was useful to note because it showed perspectives on technology uses outside of NA centric companies.

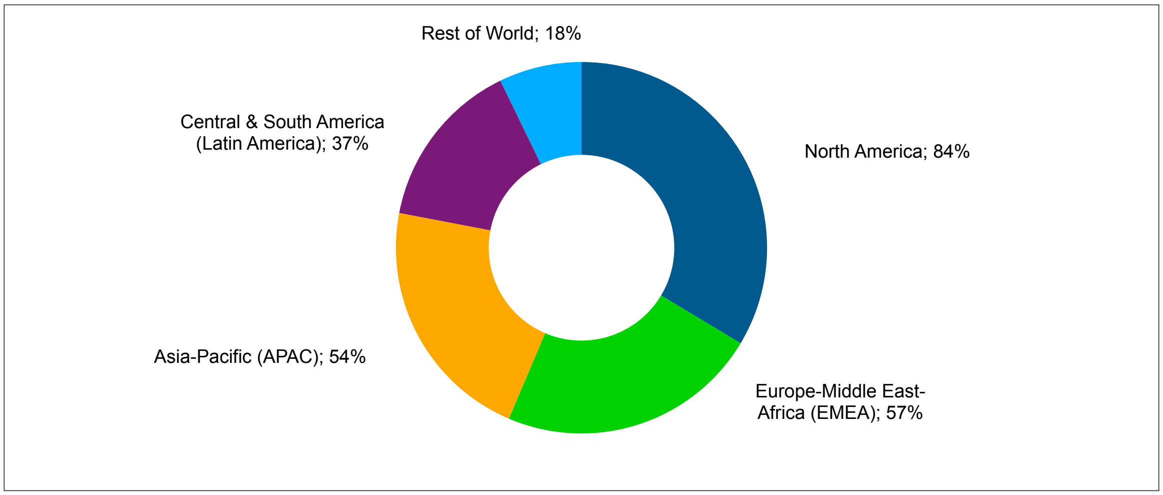

Figure 2. Operating Geographies for Respondent Organizations

Industry Representation

Respondents were nicely distributed across major industry verticals providing a solid cross-section of responses. Category "All Other" includes: Media, Legal, Education, Hospitality, Transportation, Telecomm, and Energy. These had small representation and were combined to gain a statistically relevant sample.

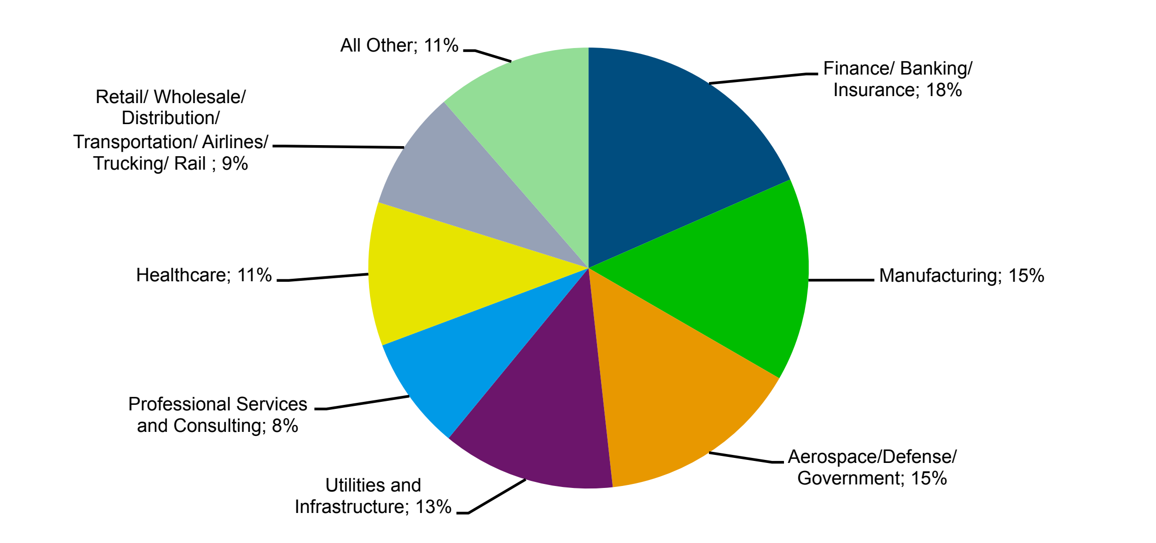

Figure 3. Represented Industries

Organizational Size

In reviewing the company demographics, EMA identified a good spread with 31% of respondents from enterprise environments, 53% from small to medium *enterprises*, and 16% coming from the small to medium *business* environments.

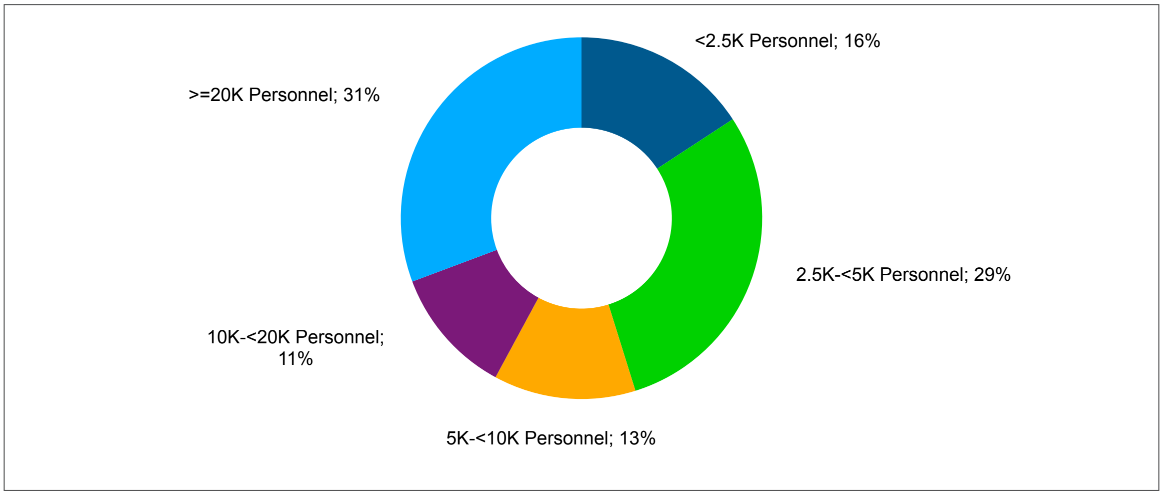

Figure 4. Organization Size

Budgetary

With all of the fervor around "It's not *IF* I'll get hacked but *WHEN* I get hacked", it is good to see that 53% of organizations reported budget increases while only 7% reported decreases. This is excellent for the security organizations. What was interesting to note was that the percentages moved slightly downward from the 2012 study. Though small enough that it is not statistically significant, it should continue to be tracked in future studies to identify the longer term trend.

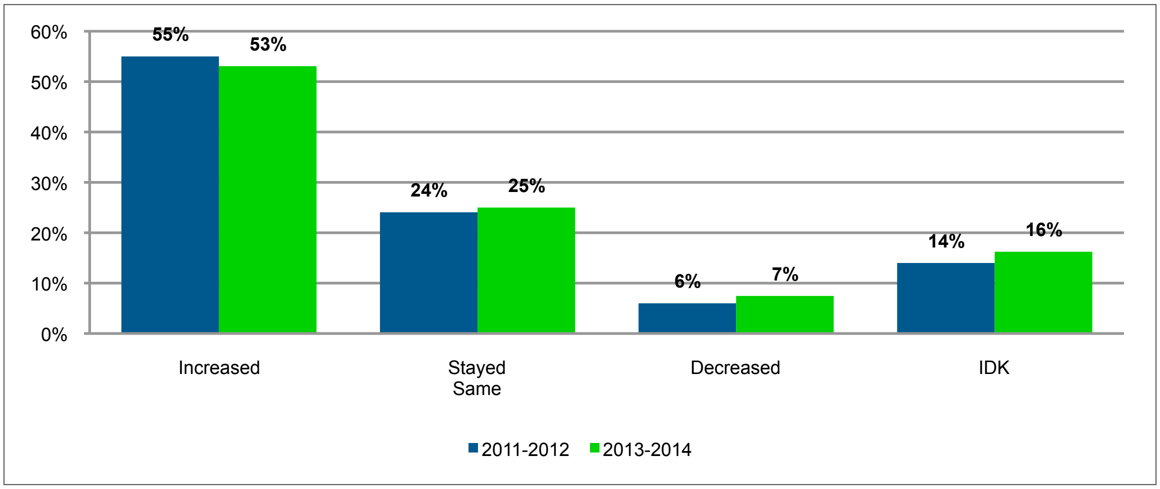

Figure 5. IT Security Budget Status

When analyzing the percent increase/decrease of the budgets, EMA found that the majority of the budget increases fell into the 10% to 25% range. This is a 10 point increase over the last study. Seven of those points came from the "Increased > 25%" category while the other three moved up from the "Increased <10%" category indicating that spikes in budget increases came in the 2011-2012 time frame and the increases are beginning to level out. Subsequent iterations of this research should bear this out.

The study dug down into the budget changes to determine how significant the changes were. Respondents indicated that overall, their budgets had shifted to be between 10% and 19% of the total IT budget. When drilling down by market vertical, this range was the highest for all markets except Manufacturing which made a surprisingly stronger than expected showing in the report. Manufacturing reported having 32% of its security budgets being 20%-30% of the IT budget. This was its highest single category and further supports that Manufacturing may be emerging from a laggard state in IT Security. With rapid manufacturing expansion in other countries, attackers have been putting increasing pressure on manufacturing companies to steal both product and production technique intellectual property. Infrastructure and Utility respondents reported 17% of their organizations having IT security budgets exceeding 30% of the IT budgets. This was the highest single group in the >30% category and also follows current information since non-monetarily based hacking from nation state, terrorist, political or religious factions are stepping up their attacks on national infrastructure world-wide.

> Manufacturing reported having 32% of its security budgets being 20%-30% of the IT budget. This was its highest single category and further supports that Manufacturing may be emerging from a laggard state in IT Security.

Security's Political and Financial Supporters

Knowing Security is a form of insurance and should therefore be a prevention game, it is often difficult to garner support, especially financial support from the appropriate executive stakeholders. The research asked several question in this area to ferret out the problems security faces in getting the budgets and attention it needs. First the survey asked, "In general, which of the following are among your most significant frustrations with IT Security practices in your organization?" The 4th highest issue, with 33% of the respondents, was, "Inadequate ability to /communicate meaningful information to business stakeholders". The survey also asked, "In general, what is your most significant frustration with IT Security technologies?" This is definitely an underlying issue of the first question since poor tooling will produce poor practices. The responses to this question yielded a common message, "Tools are unable to provide appropriate reporting to communicate information meaningful to business stakeholders". It was the 5th highest frustration with 29% of respondents rating it as an issue. From 1st highest to 5th highest frustrations there was only a 7-point gap. The lack of a significant leader indicates that all of them should be considered significant user perceptions.

The following graph shows where vocal (political) and financial support come into play within the organizations. The discouraging part is that based upon the numbers, it seems clear that a significant portion of the respondents' security efforts are hampered by an inability to communicate needs and/or impacts as discussed in the previous paragraph.

The greatest political support came from mid-level managers either internal or external to security. Between 41% and 43% of those managers expressed vocal support for security. This is good because it means those managers recognize the value of the services security provides. Mid-level managers are also significantly closer to the front lines so they also need less "convincing" than higher level managers who do not see the details of what is going on, being more focused on business level performance outside security. Beyond the senior managers, organizations are slower to provide political support with only about a third of management expressing vocal support. This goes back to inability to communicate the program benefits to the rest of the business.

When evaluating the feedback on who provides security vocal and financial support for activities, EMA found that CIOs were the largest single financial backer for security with 44% of them chipping in while only 32% felt their CISO/CSOs were supportive. It is actually not surprising that the number of CISO/CSOs providing financial support is lower than CIOs because many organizations do not have CISO/CSOs and EMA did not ask distinguishing questions on whether or not the role existed. Though 44% is a strong number for CIOs providing financial backing for projects, the actual number is most likely higher because of interpretation of the question. Many SMBs and smaller SMEs do not have an officially titled CIO. Though that fact may raise the number slightly, that still leaves many security organizations insufficiently represented by executive level financial backers. This is also directly affected by security's inability to communicate the program benefits to the management team.

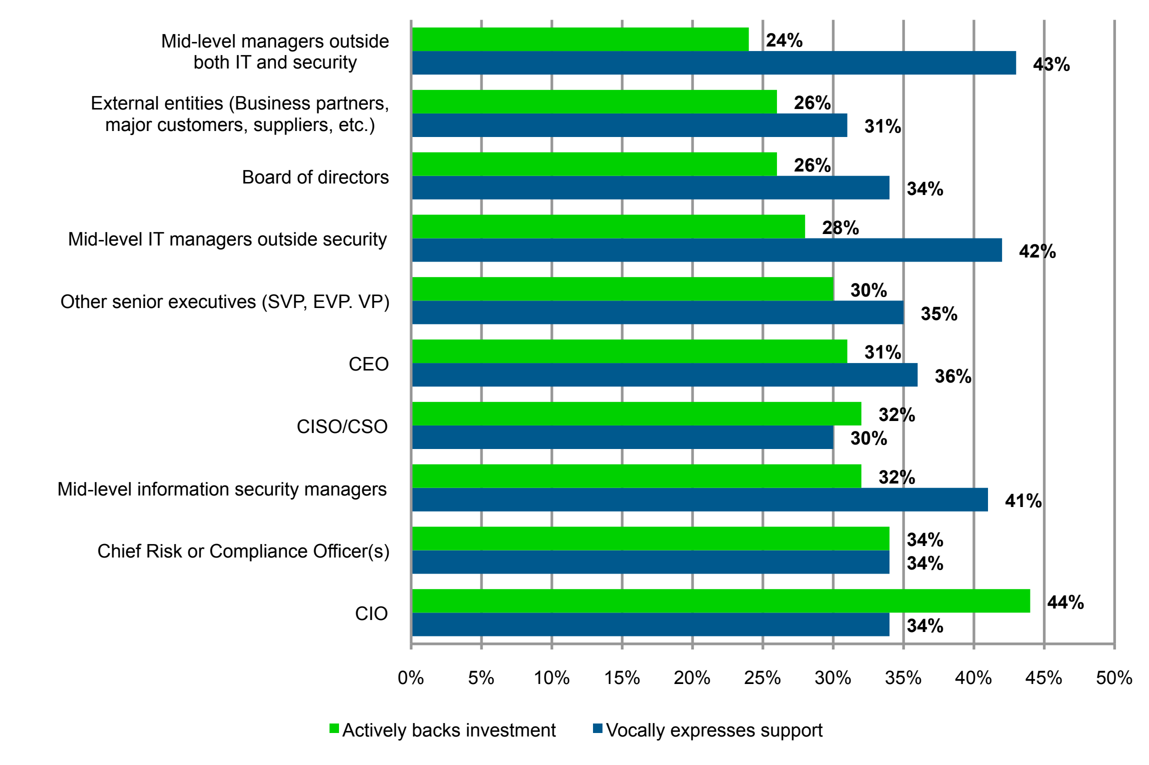

Figure 6. Security Support- Financial and Political

Security Staffing

The need for qualified security personnel has revived a problem from yesteryear. The acknowledgement that all organizations are targets has increased demand for qualified security personnel beyond the workforce capacity to deliver those skills. This is similar to the beginnings of the dot.com boom, when Internet growth drove the need for qualified IT and security staff beyond workforce capacity. This can be seen represented in the cumulative data collected beginning with the staffing graph below. Based upon the budget questions previously discussed, EMA knows that security is getting funded but it was evident that security teams are getting smaller in the larger companies with more transition in the security staffing. Job hopping for perceived better compensation, more agreeable managers and/or more enjoyable working environments is increasing, so companies are going to experience more difficulty in retaining their qualified staffs. As a side note, based upon other studies, companies should be reviewing their compensation and work requirements now to either look at how they can prepare for this increased modality or risk having not only an increase in employees' salaries but also a reduction in productivity from having to get new staff up to speed.

The survey identified that 43% of respondents said their largest frustration with IT Security at this time was, "Insufficient security personnel for the workload". (See figure 7b below.) The 3rd largest frustration, listed by 34% of respondents, was, "Too difficult to find and retain security expertise". Together these facts corroborate lack of qualified staff as a significant causality over lack of budgets/layoffs.

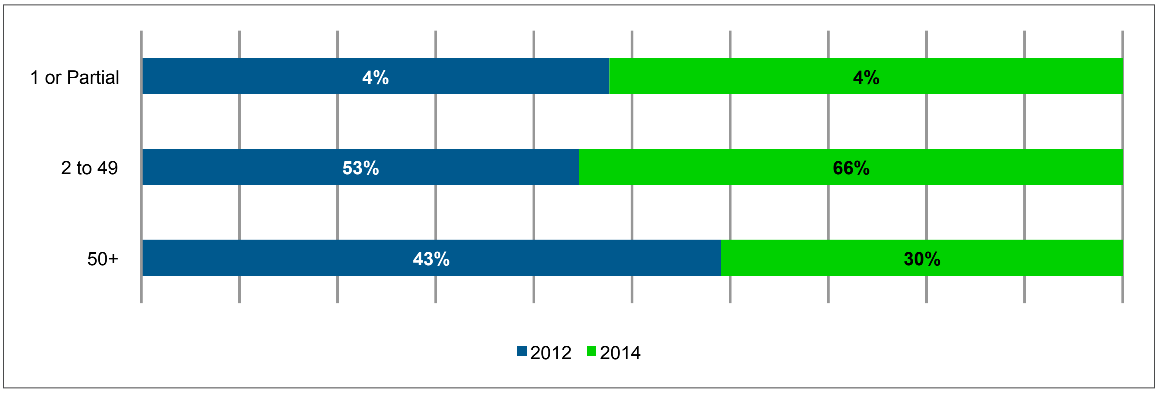

Figure 7a. Security staff sizes

Security Frustrations

In addition to the qualified staffing issues mentioned above, respondents identified organizational, technology, and practices issues that impede their success and create friction in their positions. Figure 7b indicates that outside of staffing issues the next three most frustrating practices within their organizations are: "Too difficult to separate legitimate from malicious activities", "Inability to report meaningful information to stakeholders" and "Compliance gets in the away of security". The first two issues are indicative of either a lack of technology availability or market awareness of the tools available or in some cases, impacted by the lack of qualified staff. Generally the mentality is "no tools out there can do the job", or "no tools out there that I know of can do the job", or "the tools exist but I can't afford them". Given the research, it is evident that the tools are out there so it is not a technology issue; it is because the technology to render better visibility are not well publicized in the market or budgets are not there. Generally the budgets are being funded and the research shows amazing growth in this technology area so it comes down to a combination of more that needs to be done to get the message out there and some retooling issues. Despite budget funding, retooling is often a far more expensive and greater issue than just the cost of the tools themselves. This means that the solutions vendors had better be improving their communications focus on implementation costs and timeframes. How well their solutions bolt into the existing tools and augment what customers already have is a key discussion. If the tools can get up and running quickly to product ROI in days to weeks rather than the traditional weeks to months (or longer in the large enterprise), prospective customers will be far more interested. The other side of the coin is that the vendors must also be able to state what technologies can be replaced by their solutions. Even if the initial investment is relatively inexpensive, management knows it cannot keep expanding its operational expenses (op-ex) for service contracts because that ties up too much of the budgets on an ongoing basis.

The second issue is created by one or both of two primary factors. One is the lack of proper tooling that was just discussed; the other can be the lack of experienced personnel, that was also discussed earlier, both at the operational and management level. If the Security managers and above do not understand what is important to the business and/ or do not have the experience to implement the proper controls and associated measurements, better tooling will do them only limited good. Security management needs to understand that it deals with insurance. If successful, then there are few to no actual incidents. Communicating attempts at controls violations as well as actual violations can be very useful. Identifying areas of risk is also critical but often, the ability to provide that level of information is a daunting task in the catch 22 world of lack of tooling. Given their environmental, time and resource constraints, security often puts itself in the predicament of trying to attempt too many improvement projects at once causing inefficiencies, delays or poor controls. Security organizations must, like every other business organization, use basic block and tackle methods to identify the areas of control that are necessary and prioritize them. Then present that prioritized list to the proper management letting them decide where to draw the cut off line of what they are willing to invest in.

Compliance is necessary in today's world. Interesting to note is that security professionals feel that, "Compliance gets in the way of security". It is actually pretty straight forward. If organizations are too focused on checking the compliance boxes without making the real investment in security then security is compromised for the sake of compliance. This is especially true in the area of security awareness. See EMA's Webinar on the negative effects of poor security awareness training on an organization here. Compliance covers critical areas but if practitioners are restricted to the bare minimum in any or all of these areas, a false sense of security is created and problems will occur. Remember, Target Corp. was compliant before its breach.

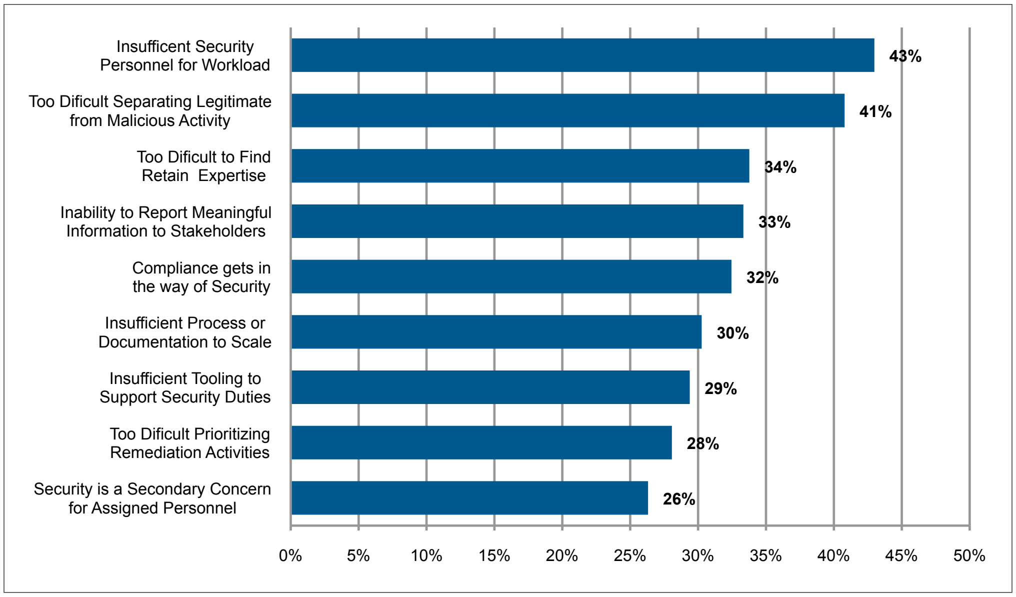

Figure 7b. Frustrations with IT Security Practices

Figure 7c, below, augments the information in figure 7b, above. Practitioners and management believe that their tools cannot identify attacks soon enough and the vendors are not quick enough to respond when emerging attacks are identified. The latter seems to be more a factor of a reliance on signature-based technology or technology that is insufficiently robust to adapt to the emerging attacks. The third item speaks for itself. Despite increased budgets, many feel that tools can be too expensive compared to their return on investment (ROI). Later in this Paper the study addresses technologies that received very high value ratings from their customers, which may help others in choosing technology for their own needs.

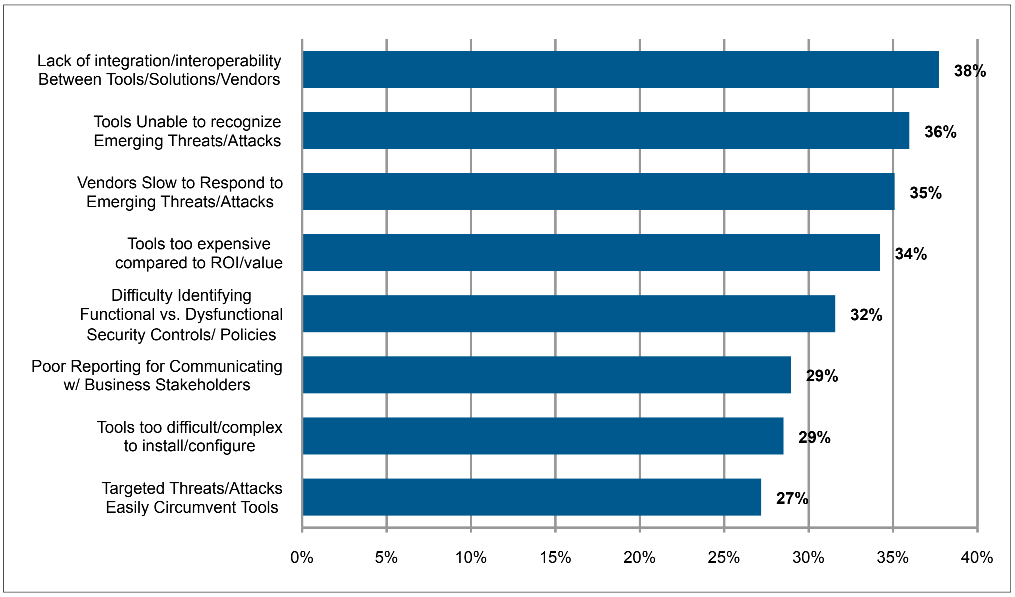

Figure 7c. Frustrations with IT Security Technology

Forty-three percent of respondents saw, "increased ability to recognize targeted threats" as the most significant need for improvement in security. This is very important issue but the good news is technology is catching up in its ability to provide that support. As a sad dichotomy, many organizations aren't ready to address the advanced problems. They still are having difficulty with foundational items. Research showed there was no improvement between 2012s report and this one in organizations defining a security configuration baseline for themselves. In fact, the organizations reporting that they had created a comprehensive security baseline went down from 41% to 38% and correspondingly, the organizations reporting limited or no security baselines went up 1 point each. This is a daunting task for resources if it must be done manually. However, this is an area where solutions such as IT-GRC or possibly a Configuration Management Database (CMDB) may be able to help. Part of completing the security configuration baselines is the ability to define normal operational states and secure operational states within the environment. It was interesting that respondents chose to focus on a "secure state" rather than a "normal operational" state almost like they perceived them as unrelated. To get to a secure state, practitioners must identify how not only individual users but groups of peers "normally" operate. That can be both people and systems. If a person is suddenly acting out of character, it could be indicative of new responsibilities, a change in personal behavior due to outside influences or that the identity has been compromised. Similarly, if a system begins behaving differently it can indicate a change in function or configuration or that it has been compromised.

Forty percent of practitioners were concerned about "improved integration of security technologies". They have been clamoring for years about getting information into a "single pane of glass" or single user interface. This has improved to some degree but the conflicting issue is that with the era of Big Data, the volumes and types of information that can be gathered or correlated has exploded. Without the ability for ingestion of more data types and compiling it into one place for evaluation, there is no way security practitioners can keep up.

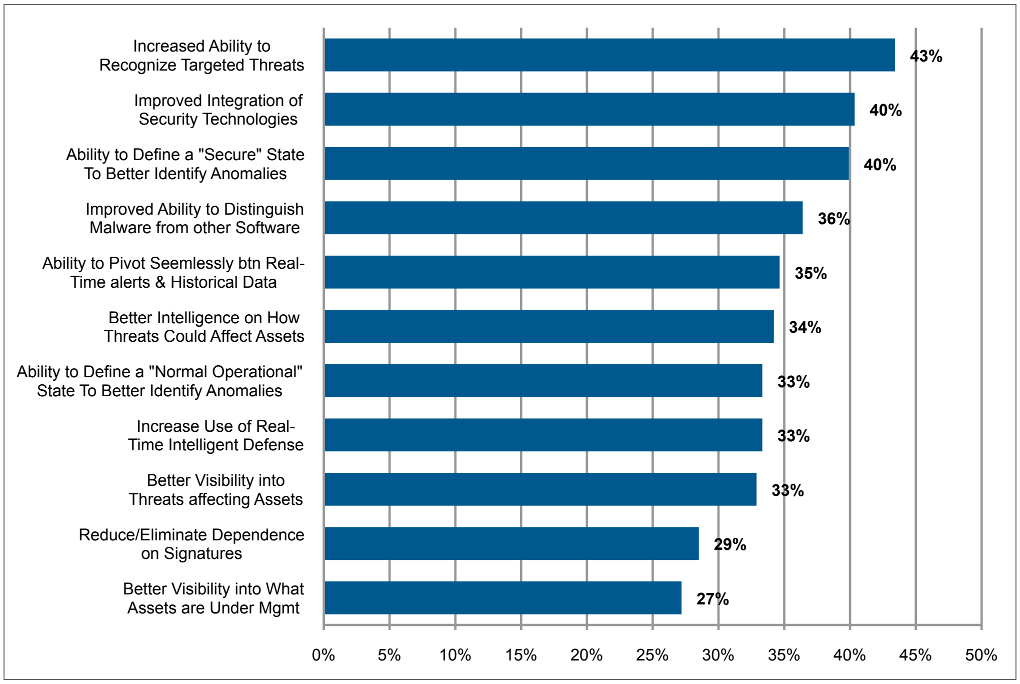

Figure 7d. Most needed improvements of Infosec as a discipline

As the follow up for asking about frustrations and improvement areas, respondents were asked where they thought the onus of improving security would fall for improving data analysis over the next 1-3 years. Given that, a shift in opinions was seen from 2012 to 2014. Respondents remained steadfast in their focus on vendors in this study. The belief that vendors had the responsibility to improve the state of security rose 9 points from 48% in 2012 to 57% in 2013. Part of this stems from the understanding that people cannot do it all alone. Respondents feel that security technology has to get better so the vendors have to get better to meet that need.

Respondents put an increased stress on standards organizations with a 5 point increase from 38% in 2012 to 43% in 2014, indicating that they need to do more. This is interesting timing with both the PCI standard being updated in late 2013 and NIST releasing both new and updated security standards such as SP 800-160 and SP 800-82 Revision 2. Better standards would hopefully result in getting farther away from "Compliance getting in the way of security".

There was a similar drop in expectations for creating leadership improvements in security from Managed Security Service Providers (MSSPs) and Professional Services vendors outside of security. There is no indication of why these changes occurred and there is something of a dichotomy since MSSPs are doing well and fewer personnel available on the market makes MSSPs a more attractive option.

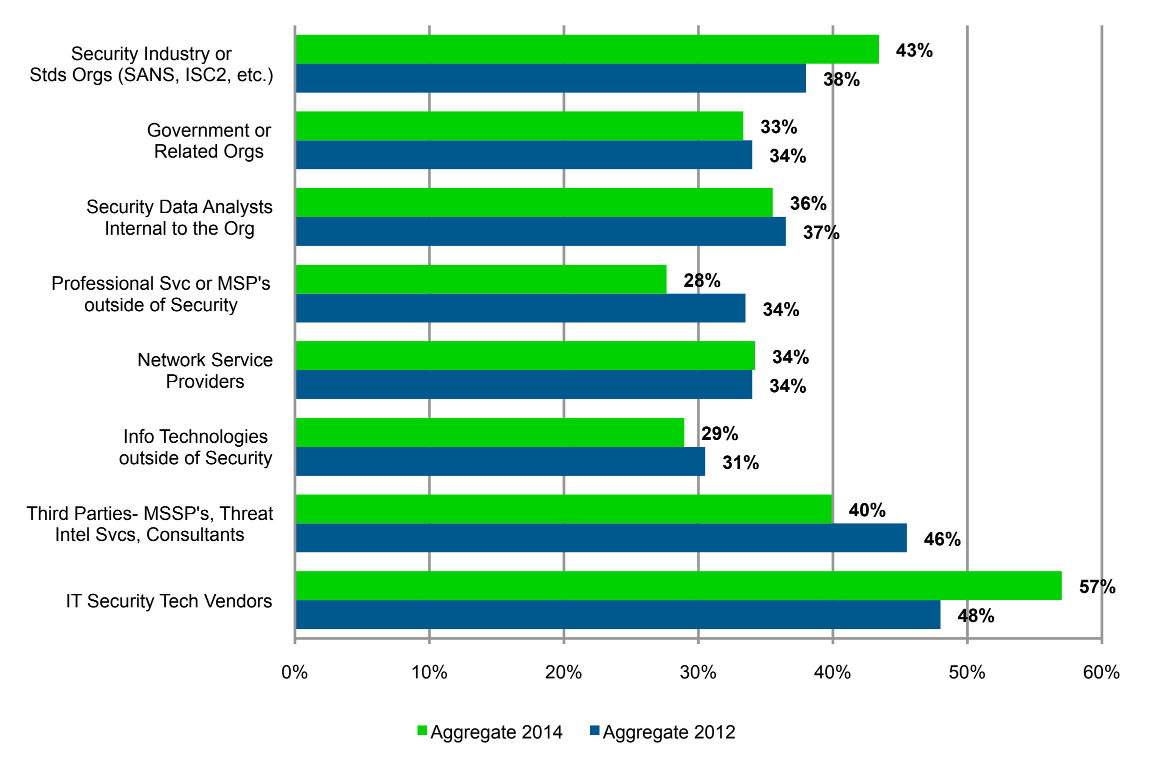

Figure 8. 2012 vs. 2014 Perception of greatest responsability to improve data analysis for Infosec

Security Technologies

The research asked participants about 13 areas of technology to determine more about if, why and how these technologies affect data driven security. There were a number of significant findings that EMA drilled into so to better understand more about the various factors influencing the respondents' choices. There are literally hundreds of security solutions and thousands of vendors supplying security technology. In defining the list of technologies, EMA tried to include technologies that it thought would enhance the topic of data driven security by addressing the need for more and better information creation and/or processing. It also explored technology sectors that appeared to be more innovative in their approach to solving the problems security is facing. There was no way, or attempt, to include all technologies that might have been included without making this a product survey, which was outside the intended scope. Given perceptions offered, EMA found a number of interesting and compelling variants from what was expected.

A key take-away from the technology questions is that respondents require technology that is a force multiplier, not a workload multiplier. Technologies or solutions that just provide more data (not information) or provide poor reporting, cumbersome work flows, unintuitive or multiple interfaces, or poor data/alert management capabilities were a significant frustration and if identified before purchase, were deal breakers. Relating to the data/alert management aspects, technologies that over-alert, with [too many] false positives or an inability to properly rank alerts for response were also a key frustration. Organizations were loud and clear that they need enabling technology that provides accurate, actionable alerting in a timely manner, thus becoming a force multiplier for them to address the "worst first" in minutes to days, not weeks to months.

Technology Details

The thirteen solutions that we included are listed next, in alphabetical order: Adv. Endpoint Protection (AEP), Adv. Security/Threat Analytics (SA/TA), Advanced Persistent Threat/Advanced Targeted Attack (APT/ATA), Cloud Application Security Management (CASM), Cloud/Premises-based Anti-DDoS (A-DDoS), Data Classification (DC), Information Technology- Governance, Risk and Compliance (IT-GRC), Mobile Device Management (MDM), Network Admission Control (NAC), Next Generation Firewall (NGFW), Security Incident and Event Management (SIEM), Web Application Firewall (WAF), and Web Security Gateway (WSG).

Please note for the following section, when discussing customer value, EMA has two metrics. The first is the percentage of respondents that answered, "provided expected value" or, "exceeded expected value", which could be from 0% to 100%. The second is the mathematical mean with a range from 0 to 3 where 0 indicated, "no value"; 1 indicated, "less than expected value"; 2 indicated, "provided expected value" and 3 indicated, "exceeded expected value". Due to four ties in weighting values there were only 9 ranks in the final outcomes.

The selected technologies have had a significantly varied lifespan. Web Security Gateways have been deployed for 20+ years while Cloud Application Security solutions have only existed for a year or two with most of the vendors appearing in the last 8-10 months. The other technologies arrived somewhere in between with a number of them still defining their market space. The numbers on deployment speak for themselves; however there are some considerations that must be pointed out.

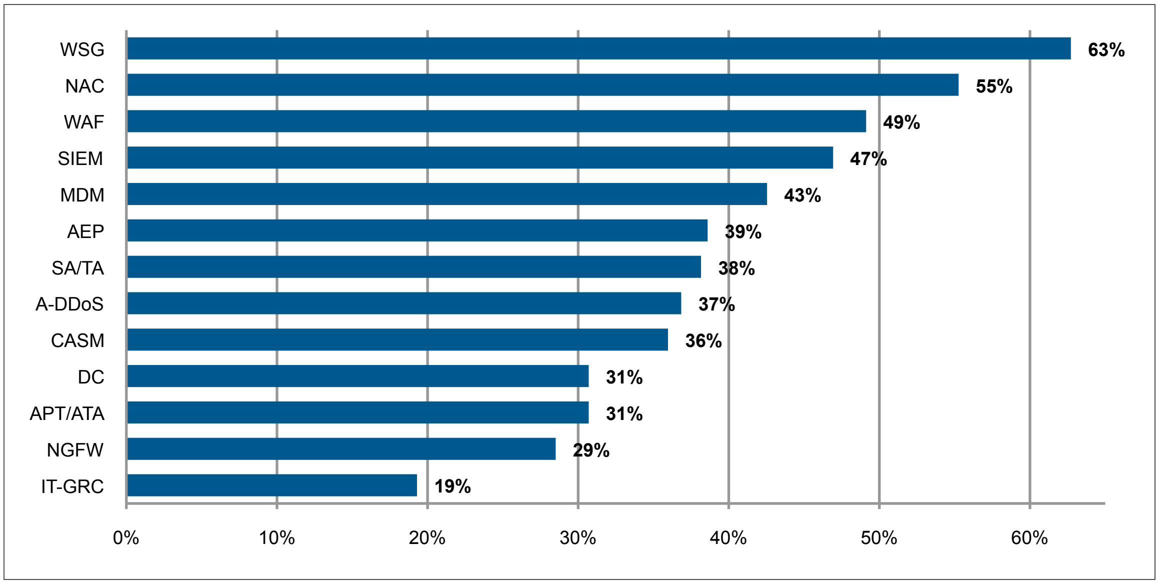

Figure 9a. Technology deployments in respondent organizations

Web Security Gateway (WSG)

WSGs had the highest deployment at 63% of organizations and, oddly enough, also received the lowest overall value (8th place) with a weighted score of 2.09 out of 3 putting it in a tie for last place for weighted score with AEP. It's combined "expected or greater than expected value" of 86% was only 1 point lower than AEP. A few possible explanations for this would be the legacy install base, deployment costs for large multi-gateway organizations, and lack of specific internal network coverage. WSGs have had almost double the time in market than the next closest technology. Having existed for the longest, it has had time to amass more deployments. Next, most of the solutions out there require a fairly substantial investment to meet the demand loads of larger Internet access connections and where customers have deployed in a geographically dispersed or other multi-connection architecture the deployment, costs can lead to a value crisis depending upon how well the purchaser matched requirements to the solution features and cost. Lastly, these solutions only capture communications going through them and as they are usually attached to the external network egress point or Internet, do not monitor activities inside the core network, giving malicious activities starting from the inside, more time to expand and get a foothold before identification. Other solutions must be deployed to identify internal issues more quickly. However, for their intended purpose of capturing network activities across the gateway, they can offer a very robust solution set including logging and notifications, and in some cases, inspection of SSL traffic and automatic blocking of communications that violate policy.

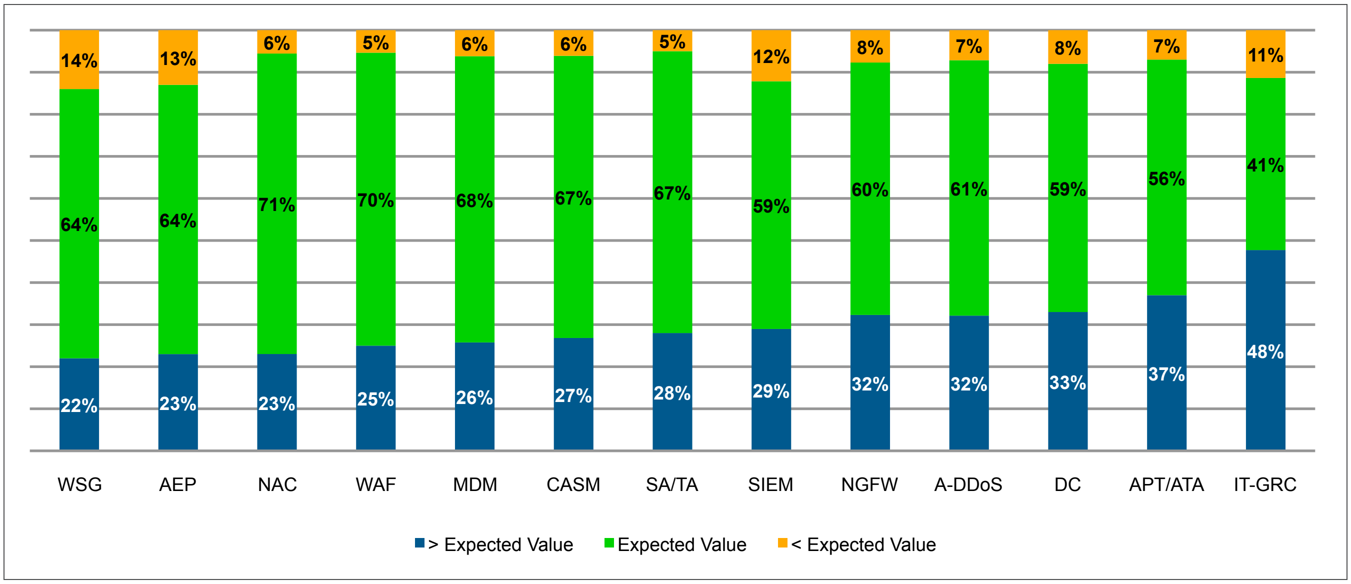

Figure 9b. Perceived value of deployed technologies

SIEM

The next big surprise was the lack of SIEM deployment. Given that logs have been expanding at a significant pace since the mid-1990s and SIEM has been out there since the early 2000s, it was expected that the market penetration would be much greater than 47%. Deployment expectations were more in the neighborhood of where WSGs came in. SIEM placed 8th, tying with SIEM, on the weighted value rankings with a score of 2.17 out of 3 and 88% combined "expected or greater than expected value", ranking it 6th in overall value.

Solution configuration and tuning complexity can make SIEM time consuming requiring more personnel to support in large or dynamic environments making organizations with financial headcount restrictions less likely to adopt SIEM. Respondents supporting home-grown or custom solutions might not include them as SIEM because they are not vendor supported and may not function exactly as commercial SIEM. Cost of entry and maintenance can be high. Many SIEM vendors charge by the number of logging systems or the volume of alerts per second or the log volumes collected per month. These pricing models most significantly affect the SMB and larger SME organizations.

The research supports these conclusions. The top three frustrations for SIEM owners for 2014 were, "too much cost/effort to deploy and manage relative to benefit" (41%), "does not integrate well with the as many data sources as we need" (38%), and, "we don't have enough people or expertise to get the ROI from it" (36%). Due to the historic complexity involved with configuration and tuning, getting full value and ROI have been issues. SMBs and larger SMEs had the lowest overall adoption rates at 39% and 35% respectively. SMBs have smaller budgets to utilize on non-revenue driving technology and the larger SMEs have larger system deployments and logging volumes that their budgets have difficulty supporting. Mid-size SMEs had the greatest penetration at 59%.

It is certain that these factors have affected market penetration and value propositions for owners. One significant recommendation for those considering SIEM, is that they should understand the operational requirements across all groups that could use it so they know what features to look for to support the greatest number of operations teams (security, IT, application, network, storage, etc.) with the single purchase. All SIEMs are not created equal. Their cost and usefulness will vary based upon those organizational requirements, not external evaluation criteria. A good SIEM should be able to readily consume alerts from all common infrastructure systems and common applications then provide alerts to key events relevant to the particular environment. A great SIEM provides the ability to query the data to retrieve answers to complex questions about the specific environment.

Advanced Endpoint Protection (AEP)

This category does NOT consider antivirus (AV) as an AEP function since AV is considered base table stakes across the enterprise. AEP is delivered in several ways; most solutions are agent-based monitoring system configuration parameters, file integrity management (FIM), data movement (Host-DLP), process and application behavior, and user activities. There are standalone/pure-play vendors, but most of the market receives the services delivered in combination with traditional AV by the larger security vendors in that space to increase their value to the customer from the added functionality within the same footprint. It is because of that integration with traditional AV agents that the low level of deployment (39%) was surprising. However, in performing more investigation, EMA identified that many organizations that have deployed the full agent have not enabled the broader protection. A few key reasons for this were the traditional perception of deployment complexity and the difficulty in maintaining agent operation. Due to this, a significant number of customers do not upgrade to current versions to avoid the headaches. The issues are not necessarily in line with current technology but legacy perceptions are a formidable adversary. At least one vendor interviewed was so confident in the current product improvements a customer support program is being implemented that provides resources to help customers upgrade to the current versions in order to prove the value statement and overcome the negative perception.

The historical perceptions were a significant factor on the value proposition for AEP. Total combined "expected or greater than expected value" was the second lowest at 87% and its weighted score tied with WSG for 8th out of 8th place with a rating of 2.09 out of 3. Note again that an 87% value rating is not something to be trivialized; it just happens to be the lowest total satisfaction rating in the technologies queried.

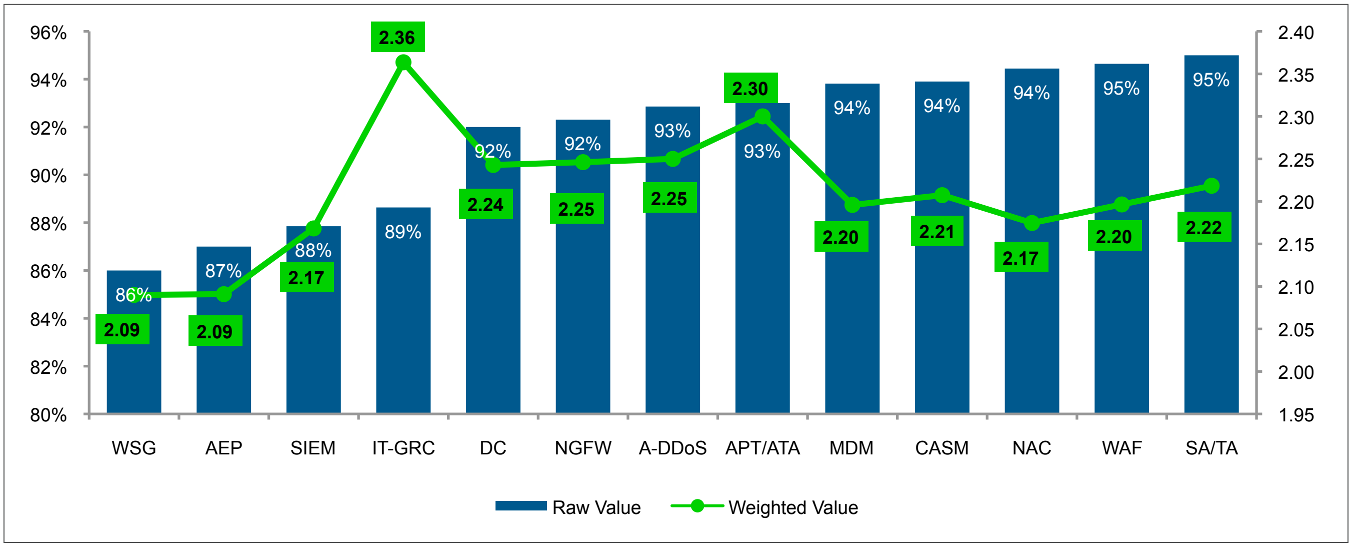

Figure 9c. Overall value and weighted value of deployed technologies

Advanced Security/Threat Analytics (SA/TA)

SA/TA was the sleeping giant of the study. Given the answers received from respondents on the frustrations and issues they are experiencing and the additional support they need, this category has the greatest possibility to address those frustrations and concerns to be a true force multiplier.

Studying the deployment information, we were surprised that SA/TA solutions were deployed in 38% of the organizations represented by respondents. Given that SIEM, considered a long term staple in security, had only 9 points higher market deployment with about a 10 year head start, it seems that it is gaining adoption fast. This accelerated growth was not unique to SA/TA but several combinations were. It tied with Web Application Firewalls (WAF) for the highest combined "expected or greater than expected value" at 95%. It was 5th in weighted value at 2.22 out of 3. Its "higher than expected value" was 3 points higher than that of WAF, pushing it slightly ahead of WAF in overall value. This is an unusually high value rating showing that the majority of the solutions out there can be deployed and configured fairly easily returning actionable results in a short time with low staff overhead.

SA/TA technology covers a broad swath of capabilities. At their root, these capabilities focus on data internal to the purchasers' environments. They can ingest external threat [service] information as corroborating evidence or to influence overall asset risk but that is not their primary focus. (Technologies focusing on external threat information should generally fall under Security Intelligence or Risk Intelligence.)

EMA asked research participants if they had heard about SA/TA as a field of technology and whether they were considering an investment in this area. 96% of respondents said they had heard about the technology. Eighty-six percent said they have enough knowledge about it to determine whether they have a need for it. Within that same context, 70% of the respondents said they either had already invested in the technology or were seriously pursuing a project to invest in it. Only 17% have thus far determined they don't see a need for the technology in their environment. For a market that has only existed for a couple of years and is really only taking off now, that is incredible.

EMA drilled down a little further asking the 86% of participants that had heard of the technology what they thought about it, whether SA/TA was all marketing hype and mere rebranding or whether they thought there was a true difference in the technology. The response revealed several key items for the space. First of all, only 1% of the respondents thought that SA/TA was a rebranding attempt with no additional value in the product. That is tremendous because it means that the vendors creating this technology have demonstrated out of the gate that they have additional value.

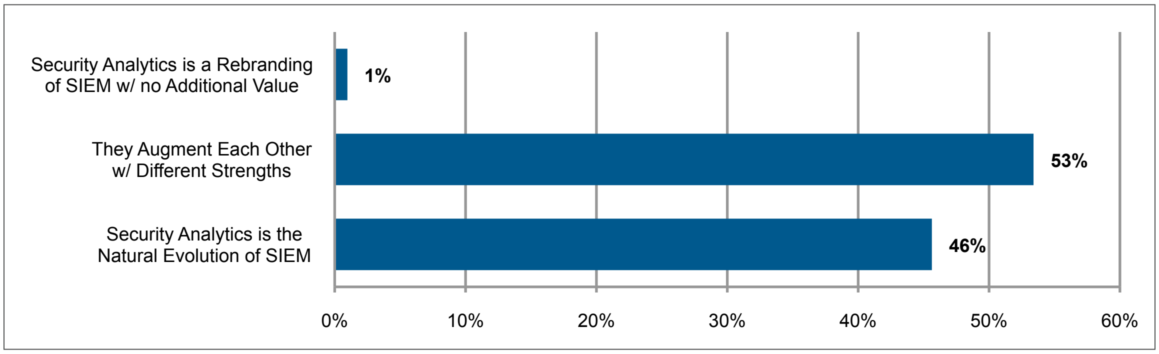

Figure 10a. Perspective on SA/TA vs. SIEM

EMA has spoken with many of the vendors in this space. Virtually all of them said the same thing. They are not looking to replace SIEM technology but to augment it. Let SIEM continue to be the collection and aggregation point and they will sit on top of that engine providing further analytics and pumping that back into the SIEM with better context for response. That doesn't mean that SA/TA cannot replace SIEM in the correct context for organizations looking to cut costs but, if that is a consideration then security must be sure to investigate the SA/TA capacities and other capabilities as they are not all designed to handle high volume bulk data ingestion in real-time.

SA/TA vendors Though SA/TA solutions have similarities to AEP and APT/ATA solutions in some of the information they collect, the scope of that data collection, correlation and analysis is broader than AEP and ATA/APT solutions. Partnerships with other vendors that create and/ or collect security data/ logs are more prevalent and farther reaching with SA/TA solutions. SA/TA solutions exceed APT/ATA solutions addressing malicious and/or anomalous behaviors produced by malware because they include malicious/rogue users, systems and applications activities that do not exhibit the signs of malware but exhibit signs if "abnormal behavior" when compared to their historical behavior or to their peers' current and/or historical behavior. They exceed AEP by including the correlation of off endpoint information and activities either on or off system natively or through partnership.

SA/TA solutions are required to rapidly analyze massive amounts of data, gathering it from across the entirety of the environment and coalescing it into information that is readily used by analysts and responders. By harnessing large amounts of contextual based data they transform the analyst's response capabilities providing true visibility into the behavioral risk associated with activities simultaneously enhancing security practitioners' ability to cut through the noise and address the highest risk items first. It provides multi-dimensional analysis to quickly expose hard-to-detect risks presenting relevant information in a highly visual manner. It correlates and categorizes alerts and information across disparate data types and systems, enabling analysts and responders to spend more time addressing the most critical issues and less trying to identify if something happened or which of the alerts received is most important. It leverages interactive interfaces, allowing on-the-fly adjustments/pivots and drill down to zero-in on threats. Another key feature is that these systems cannot be constrained by reliance on signatures, predefined indicators or archaic heuristic models.

Respondents identified important data sources in the survey from two different perspectives. The first is data they would like to collect but cannot currently process. The second is the ranked importance of each on the ability to improve incident response. Respondents rated Machine Learning Tools as the data source they feel is most desired because they feel it is the most relevant and accurate. For improving response, risk analysis and fraud management ranked the highest.

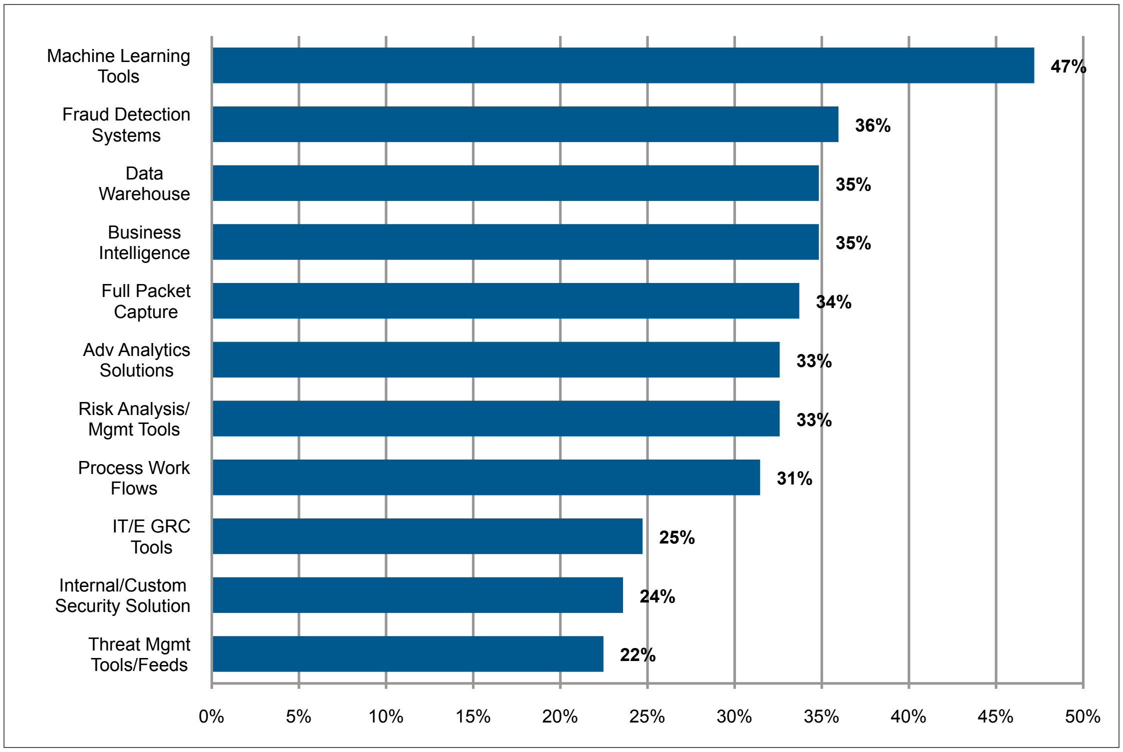

Figure 10b. Desired data sources not supported by SIEM

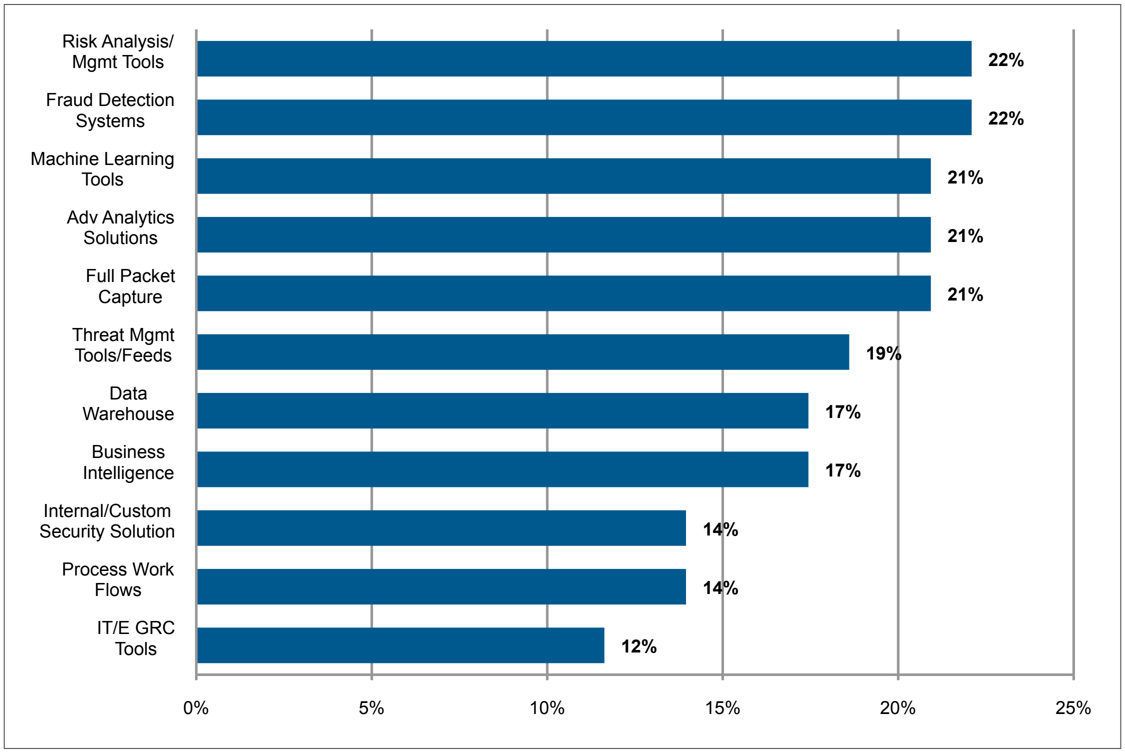

Figure 10c. Data sources dsired to improve response

Beyond data types, participants indicated their most significant desired functionality. In the figure below, 65% of the respondents stated they needed, "advanced automated response capabilities". Many of the other technologies identified have various forms of remediation built-in but using the term "advanced" implies greater than existing capabilities and, when taken in context with the required reductions in false positives, greater accuracy than is found in many technologies.

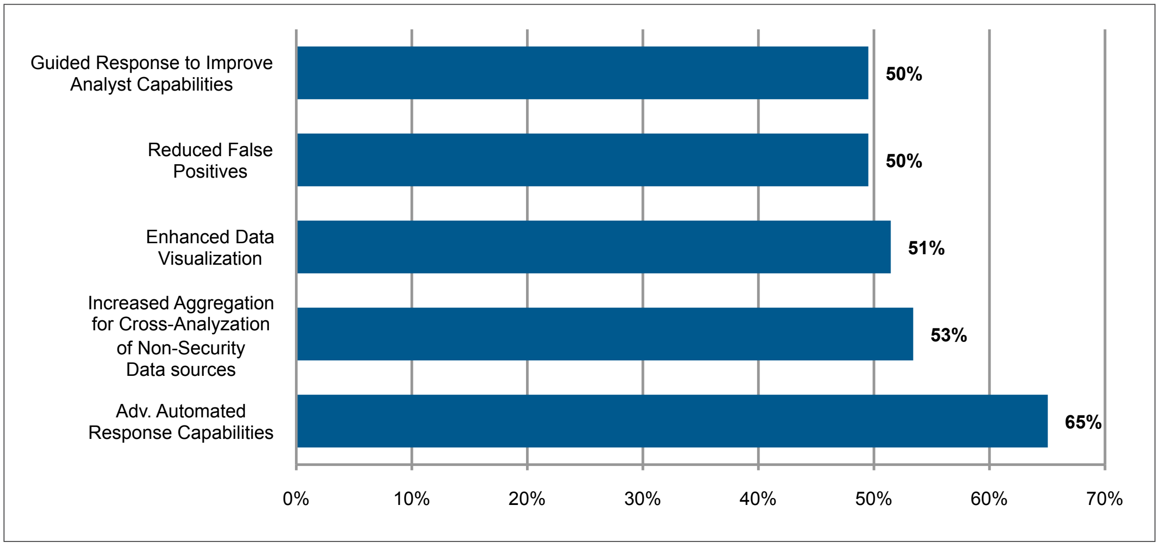

Figure 10d. Desired Features Filled by Security Analytics

Part of the rapid adoption is riding the wave of Business Intelligence and Big Data. An Advanced Security\Threat Analytics solution is very similar to a Business Intelligence engine and delivers similar results, though focused on security. Once running, they seem to have very low false positive rates and yet return useful information in nearly real-time. (See the Security Confidence section below.) The compromise for these sorts of systems is speed vs. accuracy. The faster the system returns a result, the less time it has to accumulate corroborating evidence and vice versa. The more evidence it gathers to support its finding of "bad" activity, the slower the response. As with Big Data and Business Intelligence engines, SA/TA are designed to ingest data quickly from diverse sources, giving them something of a leg up on traditional SIEM.

The most significant issue for consumers of this branch of technology is its newness. Most of the vendors in this space are less than 2 years old. There are a few that have existed for several years, but those often started out focusing on another area, either internal or external to security, and then underwent an evolution and/or rebranding of one kind or another in the last couple of years. Because of the newness, there is a lot of marketing fervor, positioning hype and copycatting going on. There are various class names for solutions and technologies, some of which would fall into this category while others do not. This creates confusion with potential customers. Names such as Security Analytics, Threat Analytics, Security Intelligence, Threat Intelligence and Risk Intelligence are currently used to describe systems that would fall into this area as well as APT/ATA detection and other response and risk functions.

A good overall definition with which to measure these technologies is, a good Security/Threat Analytics solution uses technology often referred to as "machine learning", to adapt to the activities and behaviors within its monitored environment providing improved visibility into activities and why they should be investigated. A great Security/Threat Analytics solution can also ingest non-standard data types that could include Big Data repositories and other unstructured data using those data points to provide visibility into abstract data relationships and behaviors. In some cases it can even provide semi or fully automated response. Unlike SIEM, SA/TA solutions bring visibility to problems that operators and administrators hadn't even questioned.

Advanced Persistent Threat/Advanced Targeted Attack (APT/ATA)

APT/ATA is also a fairly newcomer to the security scene as a category of products. The most prominent vendor in the space was founded about 10 years ago, releasing its first product about 8 years ago but gained little market traction in terms of defining its technology as a category until the last few years when the industry began seeing an increase in the volume and complexity of malware.

The term used by a number of the vendors in this space to describe their function or category is Threat Intelligence. As with the SA/TA space, the newness of this term makes its use fairly fluid. Vendors in both the SA/TA and APT/ATA space use it to describe their products, which perform very differently.

The core value proposition of this genre is using multiple methodologies to identify the presence of malware and associated constructs like botnets within computing environments. They can use signature-based malware and file integrity checking as well as network packet and protocol analysis, file execution in contained environments called, sandboxes and others to coerce malware to demonstrate its function, capabilities and purpose.

Despite the relatively short runway APT/ATA has had as a market space and given the fervor around the proliferation of malware, it is not surprising that APT/ATA had a market penetration of 31%. It scored well in both value rankings with a combined "expected or greater than expected value" of 93%, ranking it third, tying with A-DDoS and achieving a weighted value of 2.3 out of 3, ranking it second to IT-GRC.

There are a number of vendors in this space to choose from with a wide variety of implementations to support prevention, detection, and response/remediation capabilities. Malware is evolving quickly and the value of using VM sandboxes alone is waning. Vendors have deployment options ranging from dedicated appliances to software installation on standard hardware to virtual machine (VM) images.

These solutions are primarily deployed on the network perimeter due to cost of appliances, though the software and VM deployment options are now becoming more available. Prospective customers should understand not only their current environment(s) but also where they intend to be with adoption of cloud and hosted data centers before settling on a solution. Depending upon the deployment option, buyers will need to consider a trade-off between higher performance and price of an appliance and the associated deployment limitations vs the software and VM options. These may have less performance but can be deployed with greater density within the infrastructure to detect malware earlier.

Cloud Application Security Management

This market is very new, probably the newest of all of the technologies included for feedback. The oldest vendor is less than 2 years old with most of the other key players in existence at the time of writing of this report coming out of "stealth mode" between September 2013 and February 2013. The vendors have slightly different fortes within their solutions but core to them all is cloud application discovery and reporting so the organization can identify how the cloud is being used and manage how users utilize to the authorized cloud applications. Without making this a discussion of those nuances, it is clear that this is an up and coming area. CASM scored a 94% on the combined "expected or greater than expected value" making it the 2nd place in overall value, tied with MDM and NAC; it had a weighted score of 2.21 out of 3 making 6th in weighted value. Thirty-six percent of respondents said they had deployed some form of solution in this area with 65% of the Retail/Wholesale/Distribution/Trucking respondents and 50% of the healthcare respondents indicating adoption. Forty-nine percent of the respondents that indicated "adoption" were from the SME space with 2,500-4,999 personnel. There is no clear indicator as to why this particular range of SME had a significantly higher adoption of these services.

This particular technology is ripe for adoption. Healthcare has plenty of regulatory concerns with sharing data in the cloud making monitoring an easy argument; the retail/distribution are highly mobile making use of cloud apps highly appealing and monitoring a solid control. Other cloud enabled businesses using services such as SalesForce.com, should consider whether the value of that data could make CASM a valuable investment. Since all of the major players in this space provide a similar foundational service, potential buyers should investigate the vendors to determine which of the differential features and delivery methods will be most valuable.

Next Generation Firewall (NGFW)

NGFW had a lower than expected market penetration at 29%. It tied with Anti-DDoS for 3rd highest weighted value rating, earning 2.25 out of 3 and received an "expected or greater than expected value" of 92% making it the 4th place in overall value and tied with Data Classification. The NGFWs have a significantly broader set of capabilities than their predecessors, which would align with their value ratings. Manufacturing organizations and organizations of between 5,000 and 9,999 people had the highest adoption at 44% and 34%, respectively. One of the mitigating factors for adoption here could also be the generally perceived difficulty and impact of replacing a firewall installation. Though NGFWs do provide greater protection and security visibility than their predecessors, the business impact of downtime associated with a rip and replace is often extremely daunting and demotivating to technologists limiting overall adoption without a very strong business driver.

Information Technology- Governance, Risk & Compliance (IT-GRC)

IT-GRC was the "Cinderella story" of the report. Historically, there were GRC solutions that were monolithic endeavors with which to gather all enterprise data into one place to quantify and manage risk to use that for the purpose of addressing governance and compliance concerns and requirements. These solutions have advanced significantly, evolving primarily into two camps, e-GRC and IT-GRC. EMA asked about the latter. These are focused on IT assets and their associated risks.

IT-GRC had the lowest adoption rate of all of the technologies (19%) indicating that there is significant hesitation to deploy the technology. Though it only achieved a combined "expected or greater than expected value" of 89% putting it in 5th place for overall value, the deployed solutions achieved 48% "greater than expected value", which was the highest single value in that category, 20 points higher than the next closest "greater than expected value" and enough to push IT-GRC to the highest weighted value 2ith a score of 2.36 out of 3.

The low installation percentage indicated that only organizations that are higher on the maturity scale are adopting the technology while the very high "greater than expected value" demonstrates that the current IT-GRC tools prove to be significantly better to use than their predecessors.

Network Admission Control (NAC)

NAC had the second highest deployment in the survey, 55%, only 8 points behind WSG. It also achieved the second highest combined highest "expected or greater than expected" value, 94%, tying with MDM and CASM for overall value. NAC had the distinction of having the highest, "provided expected value" rating, coming in at 71%. Its weighted value rating was 2.17 out of 3 where it tied with SIEM for next to last.

Though NAC initially gained ground about 10 years ago, most of the original vendors have either been bought and consumed or gone out of business. Currently, NAC technology is available from a number of infrastructure vendors as well as pure-play companies. In the last few years, it has gained significant attention to deal with the exploding bring your own device (BYOD) trend. Among other things it facilitates asset identification and management with policy-based controls for assets. Policies and controls may be applied to devices that reside within or, more importantly, move in and out of the environment. Unknown, unmanaged, or rogue devices can be quickly identified by the other devices in the environment. Devices configured or behaving "abnormally" based on the defined policies can be ferreted out as well.

When selecting a vendor for NAC, prospects would be wise to consider the possible impacts or limitations of going with an infrastructure vendor as in many cases one has to stay with that vendor to maintain NAC functionality. Other primary considerations are whether the vendor requires agent based installation, which can be a significant impediment in large deployments, or if they only function with 802.11 operational in the environment.

Security Confidence

Security seems to be at a somewhat of a stall when it comes to dealing with the volume of alerts that they receive. Recent revelations from the Target Corp breach display that its security organizations was receiving tens of thousands of alerts that it could not cope with even with extensive resources. The vast data creates a common inability to identify, prioritize and respond to alerts and the corresponding threats in the environment. Previously in this report, EMA identified a number of frustrations that security practitioners are experiencing. The lack of qualified staff and inability to separate the real threats from the other environmental activities have created a situation where only 31% of respondents felt highly confident they could, "detect an important security issue before it had significant impact" leaving 69% feeling between "somewhat confident" and "not confident" that they could detect the issues before it became a serious breach.

When EMA analyzed the data by technology type, there was a significant difference in the answers. The figure below displays the differences when the technologies were deployed. The largest increase in confidence came from the deployment of a Security or Threat Analytics solution boosting confidence 14 points, an almost 50% increase over the aggregate and 16 points higher than Web Security Gateways alone.

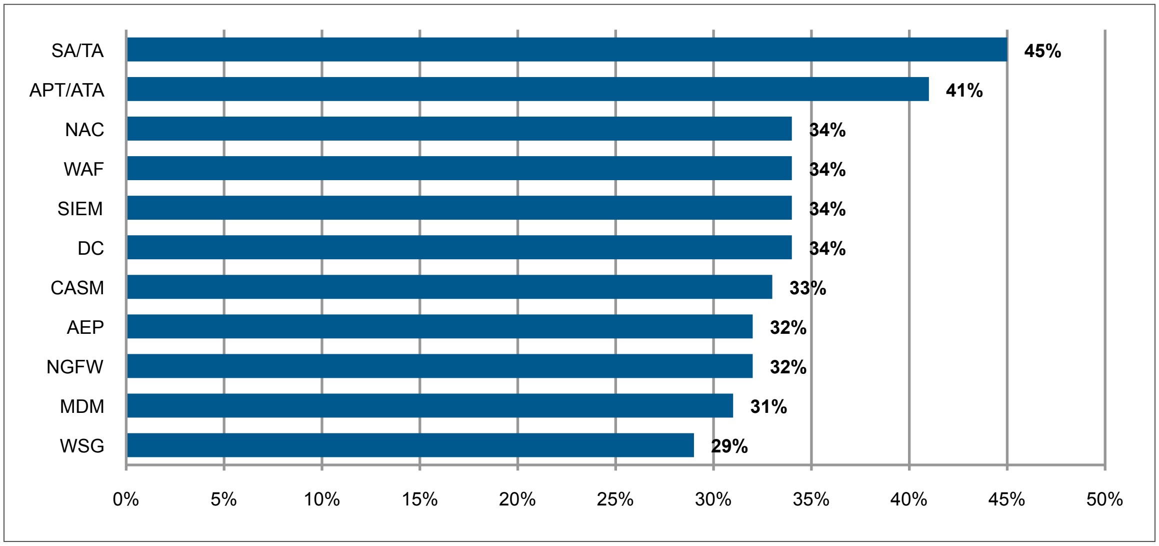

Figure 11a. Security issue detection confidence by technology deployed

Additionally, when asked if the deployment of an SA/TA technology had reduced the false positives or improved actionable alerts experienced, 90% of the respondents said they had experienced a reduction in false positives. This was on top of any other technology installed.

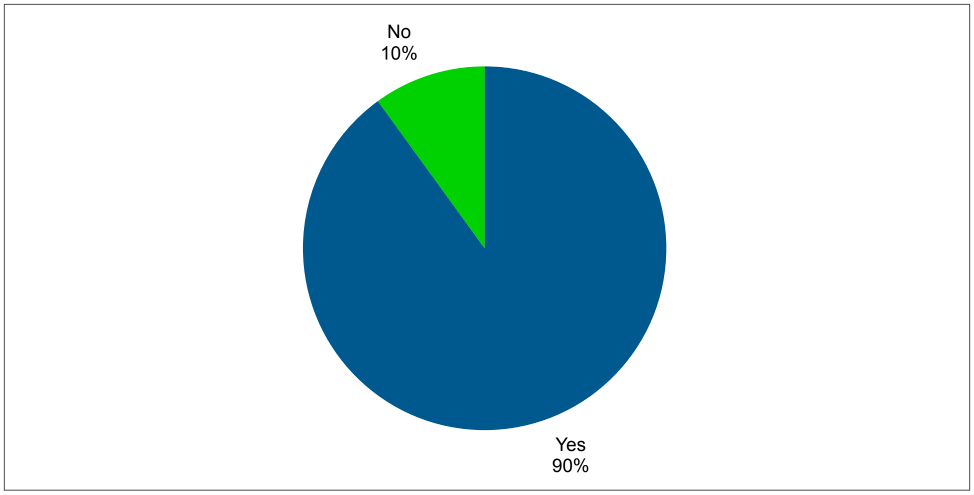

Figure 11b. Affect on false positives and actionable alerts post SA/TA installation

Respondents were also asked if the introduction of SIEM and/or an SA/TA solution had reduced the frequency and/or duration of investigations in their environments. Only 14% said they had experienced no change in either or both. Fifty percent said they had seen a reduction in both!

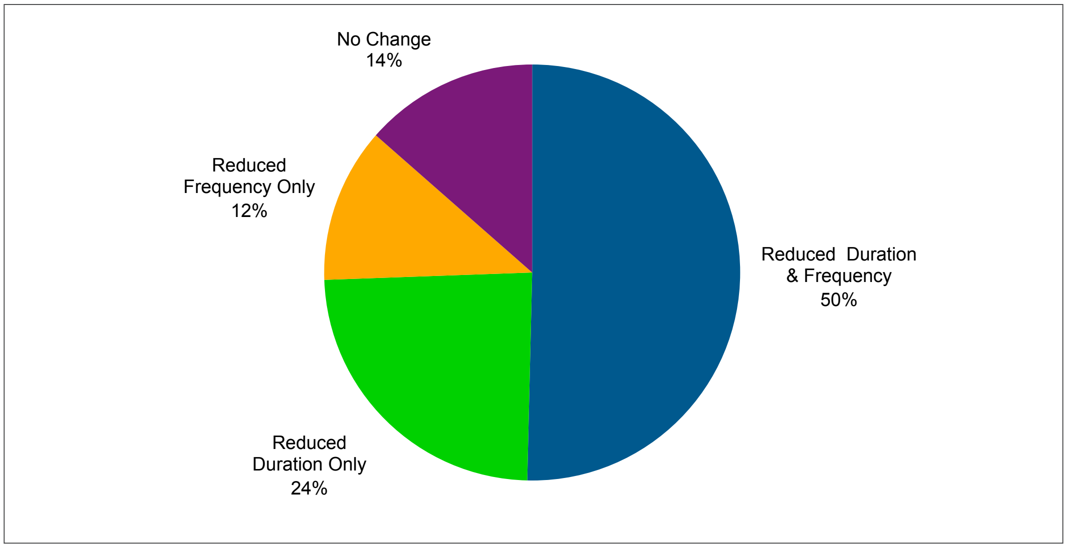

Figure 11c. Impact on security investigations when SIEM and/or SA /TA was deployed

Security is about finding the activities that increase risk and/or result in a loss of some kind. Ultimately, Security Confidence comes from the success the organization has in identifying and stopping incidents. The sooner those activities can be identified and stopped, the less the associated impact. The reduction translates into real dollars. Not only the opportunity cost of time spent for the investigation and remediation that could be used elsewhere but actual dollars that would be spent on customer notification and credit monitoring, fines, lawsuits, revenue loss, etc. should the breach occur.

Below, EMA research shows participants responses on how the introduction of SIEM, APT/ATA and SA/TA have affected their ability to *recover* from an unplanned security event and thus affected their Security Confidence. As a singular technology SA/TA provided a far better ability to resolve, allowing responders to complete 24% of incidents in minutes. This was 1.6x better than SIEM alone, 2x better than having none of the three technologies installed and 4x better than installing APT/ATA alone.

As a singular technology SA/TA provided a far better ability to resolve, allowing responders to complete 24% of incidents in minutes.

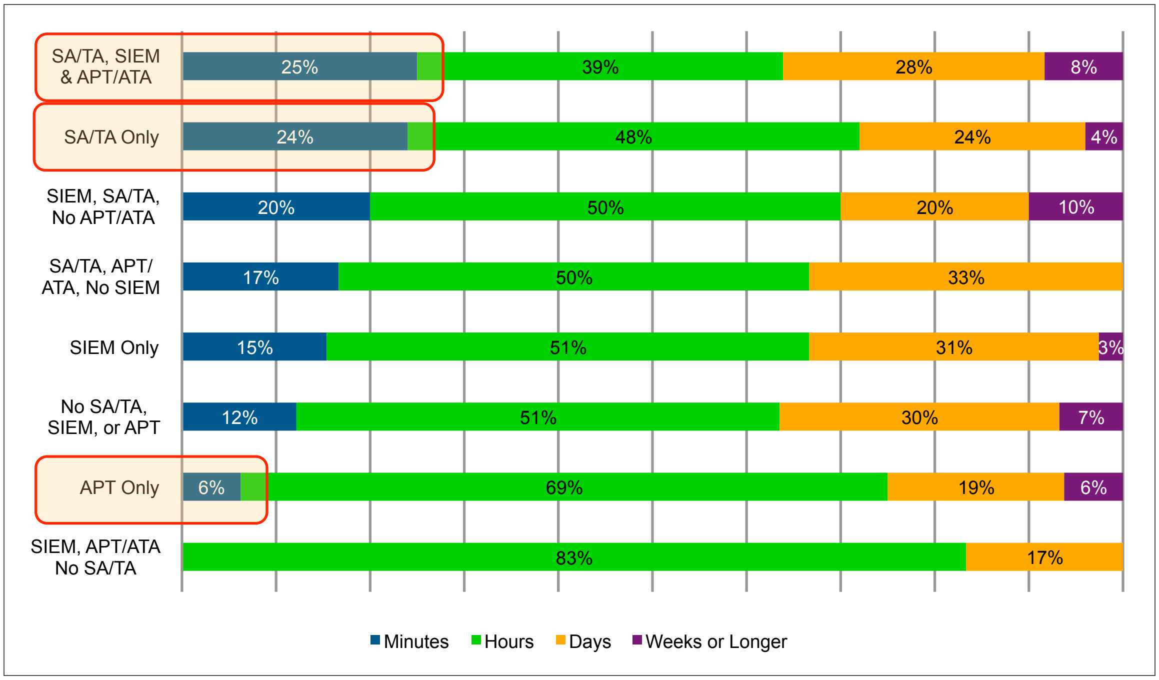

Figure 12. Impact on security investigations when SIEM and/or SA /TA was deployed

The reason for the jump when APT/ATA is introduced alone is that some of the APT/ATA technologies do not produce enough contextual corroborating evidence driving more investigation time, which lengthens the overall remediation cycle. When APT/ATA is combined with SIEM, the SIEM provides the needed correlation (context) to significantly improve the results. At that point, respondents said they could resolve 83% of the identified issues within minutes and none too more than days.

The best result came from combining all three. This pushed the volume of events resolved in minutes to 25% but note that some events were pushed back into the weeks or a longer time frame. A key note on this evaluation is that it was not exactly a like-for-like comparison. As mentioned before in the technology section, SA/TA solutions have a much broader detection scope than APT/ATA. This means that in comparison analysts can be presented with less false positives via better data but also a greater overall workload because SA/TA is detecting more incidents than would be detected by APT/ATA and/or SIEM.

Conclusion

Data is everywhere. However, for the Evolution of Data Driven Security, practitioners have passed the need for more data emerging into the need for better information. If the difference between data and information is understood, some common terms make far more sense. Information Technology and Information Security are the businesses of providing services around information. IT transforms data into information to be consumed by the organizations it supports. Information Security provides various protection services for the information held within the organizations it supports.

Some argue that defense in depth is not working so organizations need to change paradigms. It should come as no surprise to anyone to say that there is no silver bullet for security. Given that, it does not seem wise to shift paradigms and put all of the informational eggs into one basket. However, that being said, there are some very promising technologies that look to be able to provide security practitioners a big step forward. All of the technologies EMA asked about have a place in the environment as do others not included. It is up to the organization to evaluate its risks and must determine if any or all are a good fit.

The lack of deployment of SIEM deployment is surprising. In many ways SIEM is table stakes in security for all but the smallest and simplest environments. Why so many organizations have chosen not to deploy them could be the subject of another research study. What was more surprising was how many organizations believed they had an understanding of Security/Threat Analytics (SA/TA) as an area of technology, especially when the nomenclature is currently so fluid, and how many were considering investment in or had already deployed one of these tools. This indicates two important things. First, it seems that the market has already begun shifting its attention from traditional SIEM to SA/TA. Secondly, the industry is past the early adopters' phase, which has happened very quickly. The attention and development around Big Data analytics and Business Intelligence have most likely played a significant role in this acceleration.

Advanced Security and Threat Analytics solutions are a significant evolution in detection and response capabilities but in many cases, they cannot provide their maximum value, and in some cases do their jobs sufficiently, without the evidence created by other control technologies. They are analysis solutions and need something to analyze.

Some issues to consider when choosing the next technology investment follow.

1. Most SA/TA solutions bill themselves as an augmentation to and intelligence provider for SIEM not the replacement. Before selecting a solution, determine not only the functionality you require but how it fits into your overall security architecture.
2. As time passes we will see a market convergence in SIEM and SA/TA solutions. To continue to maintain, let alone gain, market share we are seeing SIEM vendors touting themselves as Security Analytics. Investigate carefully what they mean by that and refer to the guidelines given in the SA/TA technology section. Aside from increased partnerships, SIEM vendors will either be developing the advanced analytics capabilities themselves or buying up existing SA/TA vendors to compete. Some have already anticipated this need and begin the development transition.
3. APT/ATA can be a valuable detection technology; however, most are fairly narrow in scope. Due to their broader detection scope, we will see the SA/TA vendors expand more rapidly than APT/ATA competing for the same dollars. The APT/ATA vendors, as a market space, will have to expand their capabilities to compete or fall behind. This is evident by a recent acquisition by a major APT/ATA vendor of companies that provide endpoint services and network packet capture services.
4. Advanced Security Analytics fills a need similar to certain Business Intelligence (BI) needs. Some of the underlying analytical capabilities of the vendors are similar as well. Most likely, the SA/TA industry will see incursion into the security space as core BI players adapt their technology and messaging to expand into the security market.

There are very strong indicators that security analytics tools are here to stay. They are assuming a key role in the security tools arsenal facilitating better business decisions around risk and response for the organizations that wisely chose to deploy them.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help its clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com
3003.061714