SECURITY MEGATRENDS

ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) Research
Written by David Monahan
January 2019

SPONSORED BY:

SentinelOne™

EMA™ IT AND DATA MANAGEMENT
RESEARCH | INDUSTRY ANALYSIS | CONSULTING

TABLE OF CONTENTS

Executive Summary

Threats abound, but people are out there trying to deal with them. Organizations continue to fall behind, finding it increasingly difficult to identify and respond to threats in a timely manner. This report delves into several areas of concern today including cloud security issues, SecOps frustrations and tools, the Internet of Things, data sharing and leakage, DDoS, endpoint security, and artificial intelligence. The report identifies challenges and perceptions that enterprises, midmarket companies, and SMBs face across seven industry verticals including manufacturing, financial, and healthcare. The goal is to help readers to understand the common issues and where they are doing a better or worse job than others. Ultimately, the report will help readers understand how to handle threats better, no matter where they stand now.

Demographics

This research report was distributed across North America and is thus focused. Further geographic division was not tracked. The respondents were primarily targeted from IT/ cyber security, with additional extraction from executive management. In this research, line of business personnel were not queried because they do not have enough insight into the desired breadth or depth of security.

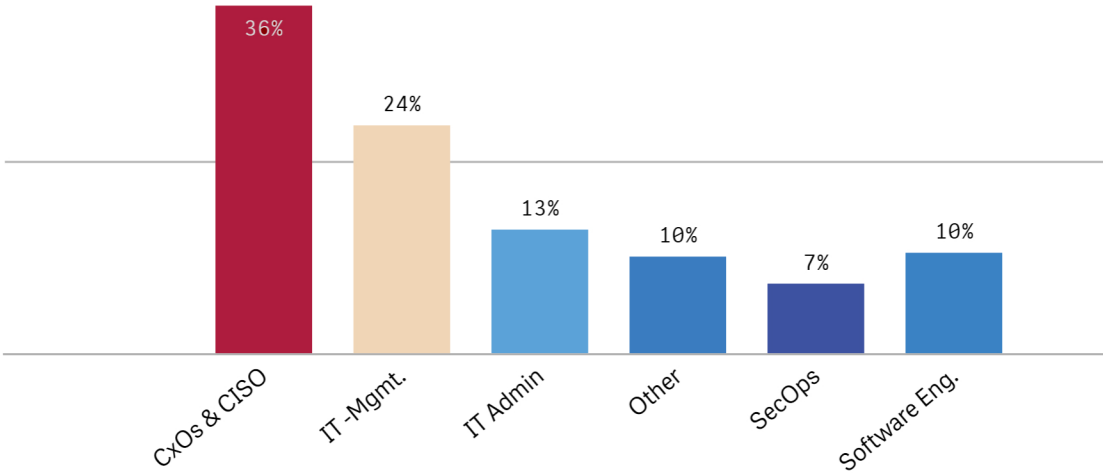

Figure 1 Respondent role

Organizations of all sizes and industry verticals have some security issues and challenges in common, but each also has its own specific challenges. The research looked across SMBs, midmarkets, and enterprises as well as multiple industry verticals to understand the commonalities and divergence in the trends.

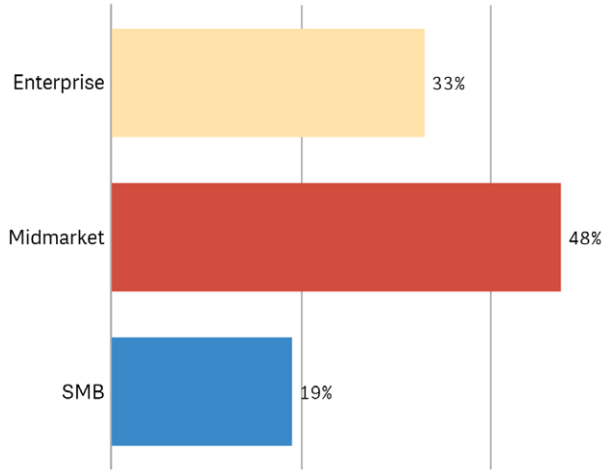

Figure 2 Organization breakout by size

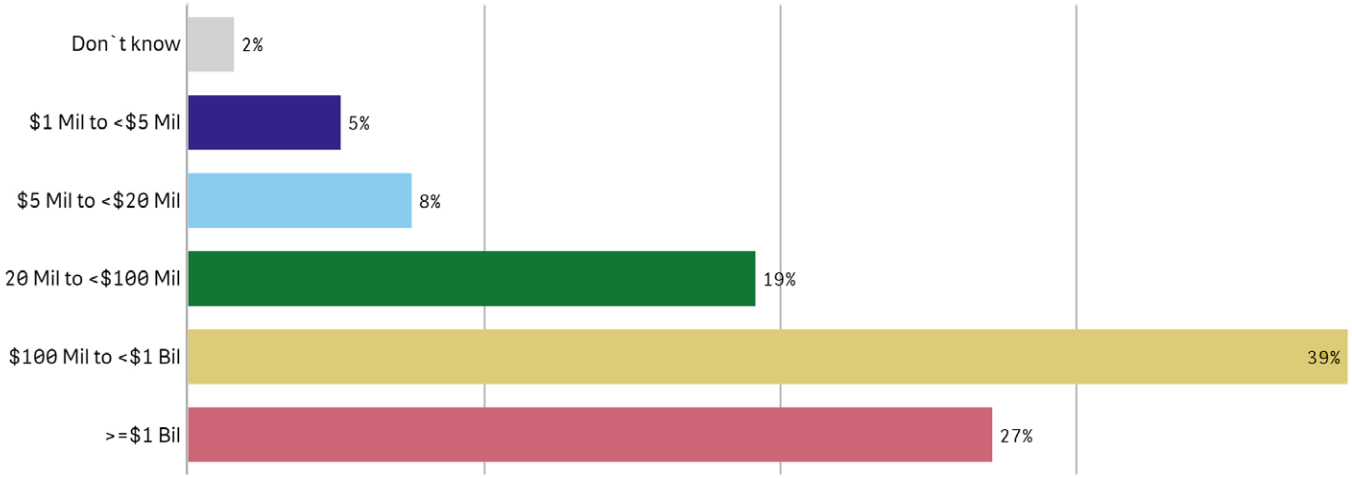

Figure 3 Organizational breakout by revenue

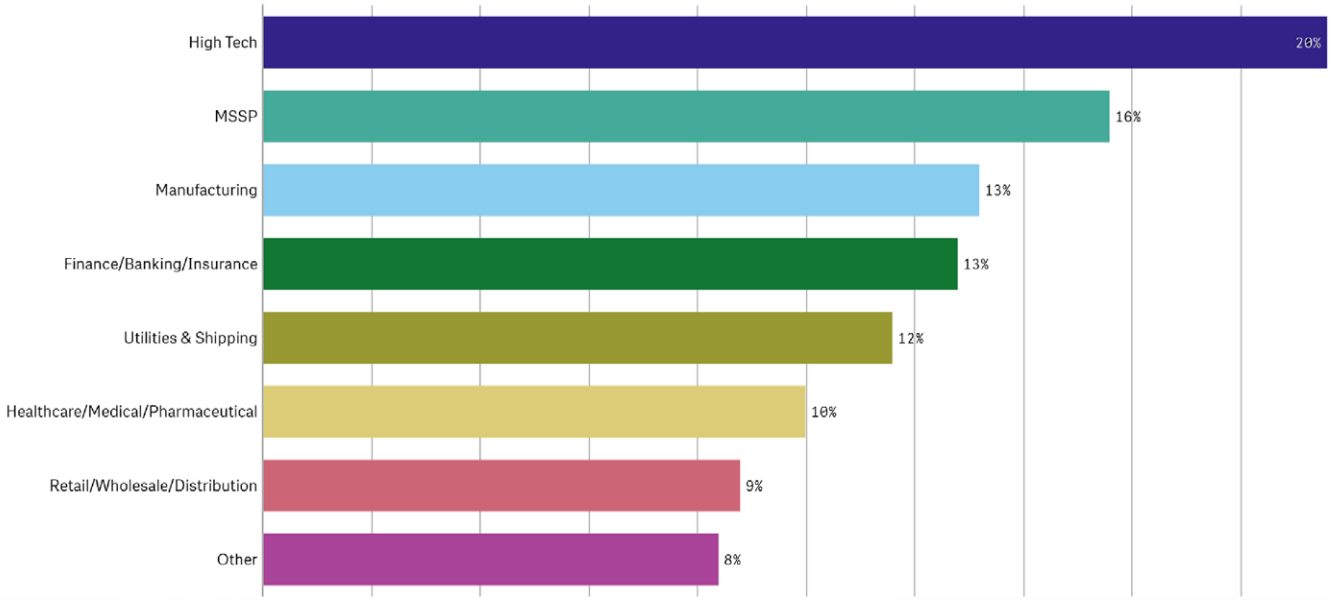

Figure 4 Organizational breakout by industry

IT and Security Budgets

IT and security budgets are looking healthy. EMA has seen consistent growth in both over the last five years. IT budgets have been growing an average of 9 to 13 percent, while security has been higher in the 15 to 20 percent range. In this sample, only one percent of organizations reported a budget decrease for IT and security, which is common at this time. The most common annual IT budget increase was 10 to 24 percent and the average was just shy of 23 percent. The state of security over the last five years, with the changed perspective of assuming that the company has already been breached, pushed those budgets up annually far more significantly than in the previous fifteen years.

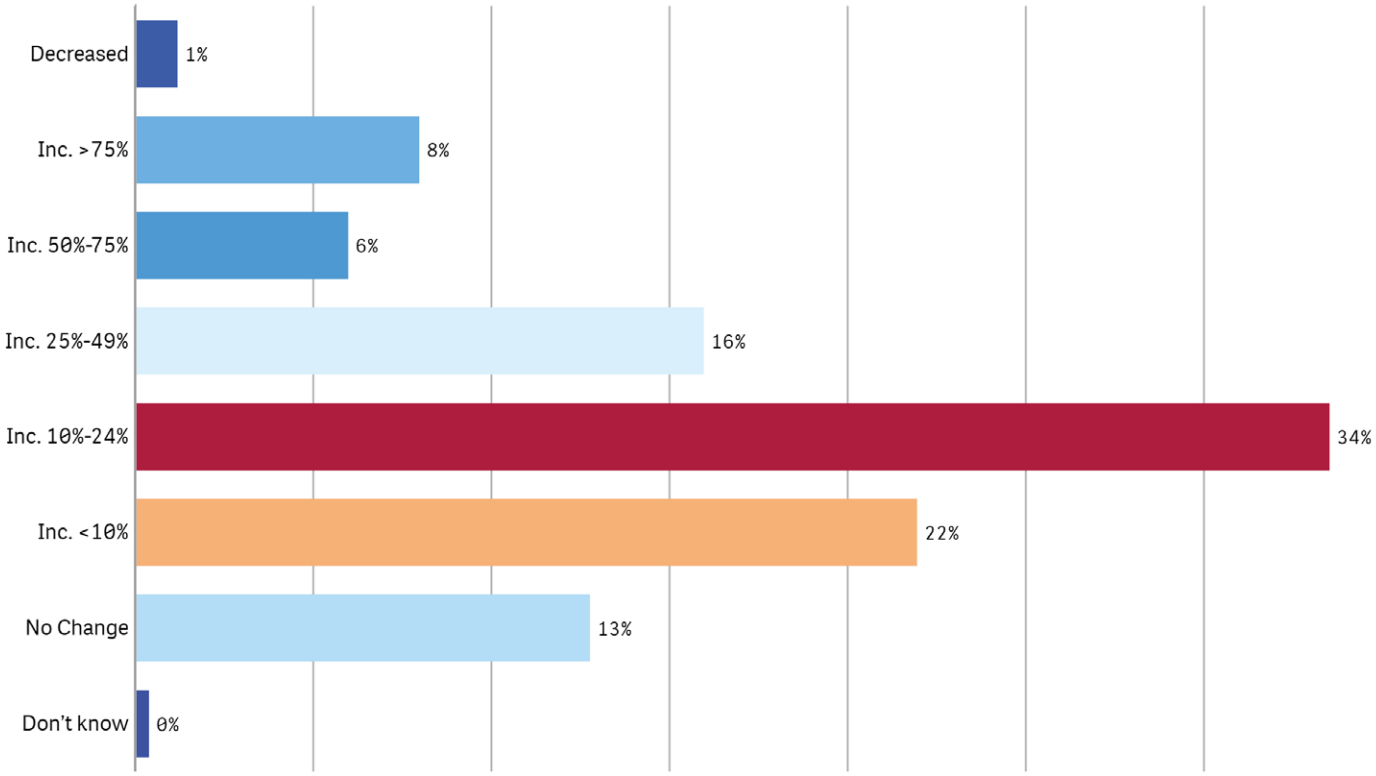

Figure 5 IT budget increases from 2017-2018

By industry, the breakout was quite variant. High tech made a higher increase in investment than the other industries, while manufacturing and healthcare/pharma/medical were significantly below average. Finance/banking/insurance are in a different place. That group has been making larger investments in IT for years, so their proportionate change year over year is not as drastic as some. Though they are at the lower end of the chart, they are actually at the higher end of overall IT and security investments.

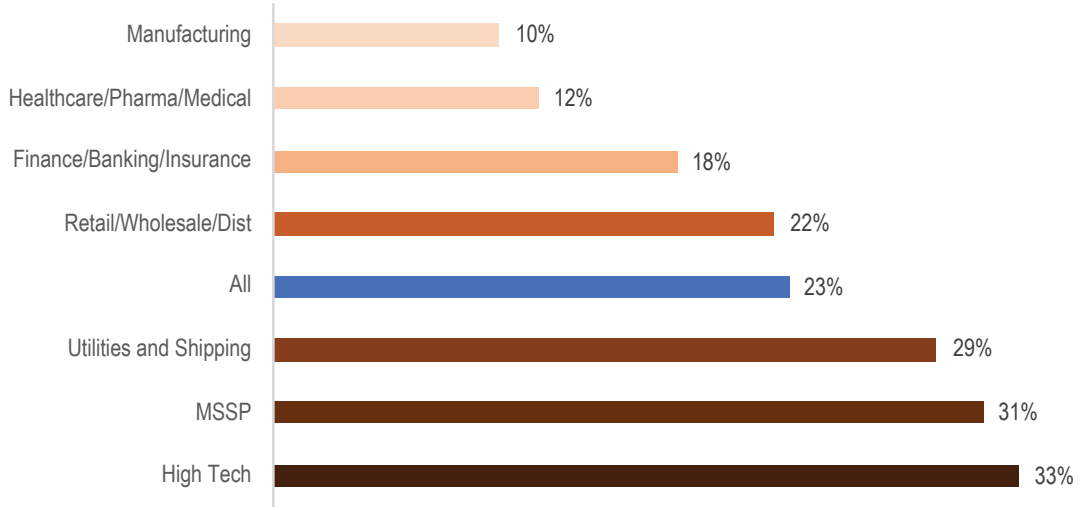

Figure 6 IT budget increases from 2017-2018 by industry

The issue with manufacturing and healthcare/pharma/medical is a significant one. Those verticals have consistently lagged in IT and security, and now hackers target them. Personal health records (PHR) are the most sought-after records. They drove the highest price on the black market because they can be used for the broadest range of theft from opening new credit accounts, to purchases, and even full identity theft. Manufacturing is a target due to the rise in industrialization in third world countries and other countries. The theft of cutting-edge manufacturing techniques is huge business, especially for competing companies in places like China and India.

On the other side of the equation, industries like utilities and shipping are pulling the average up with a nearly 30 percent increase in their budgets. This is in direct response to the need for defense against infrastructure attacks that have been on the rise since the mid-2000s. Hackers in countries like Iran and Russia, among others, have been infiltrating the U.S. power grid and other utilities to understand more about how they operate and, when possible, affect operations.

The Cloud

Application Deployment

In evaluating infrastructure strategies across the board including public cloud, private cloud, hosting, and non-cloud data centers, the spread showed that public and private cloud combined have overcome internal data centers in deployment of workloads.

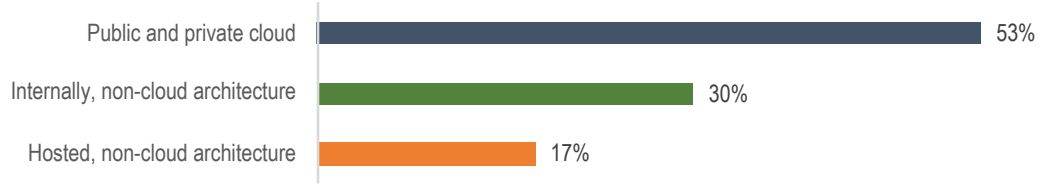

Figure 9 Estimated percentage of applications by deployment architecture

In breakout, none of the enterprises had more than 50 percent of their applications pushed to public cloud, with 78 percent having 25 percent or less. No enterprises represented had more than 25 percent of their application in a hosting center and none of them had more than 50 percent of their applications in a private cloud, leaving internal data centers as the most prominent application deployment environment.

The midmarkets had as many as 75 percent of their apps in the public cloud, private cloud, or traditional data centers. The most common percentages were that 61 percent had 25 percent or fewer applications in an internal data center, 90 percent had 25 percent or fewer applications in a hosted data center, 71 percent had 25 percent or fewer in the public cloud, and 52 percent indicated they had 25 percent or less in a private cloud architecture.

All of the SMBs had no more than 50 percent of their applications in the public cloud. The surprising part was that 79 percent said they had as many as 50 percent in a private cloud. Only seven percent of SMBs indicated they had 90 percent or more of their applications in a traditional data center, and all of them indicted they had no more than 50 percent in a hosted environment.

In evaluating the approach by industry, utilities, finance/banking/insurance, and manufacturing stand out. They engaged private cloud architectures for 76 percent or more of their applications. Finance/banking/insurance had respondents exceeding 90 percent of applications in internally hosted architectures. Manufacturing also highly leveraged private cloud, with respondents indicating they had 76 percent or more of their applications in private cloud.

Use of Cloud for Security Workloads

The cloud is coming on strong. The frequency of cloud adoption for security workloads is more than triple what it was two years ago, and now it appears as though everyone is in the cloud.

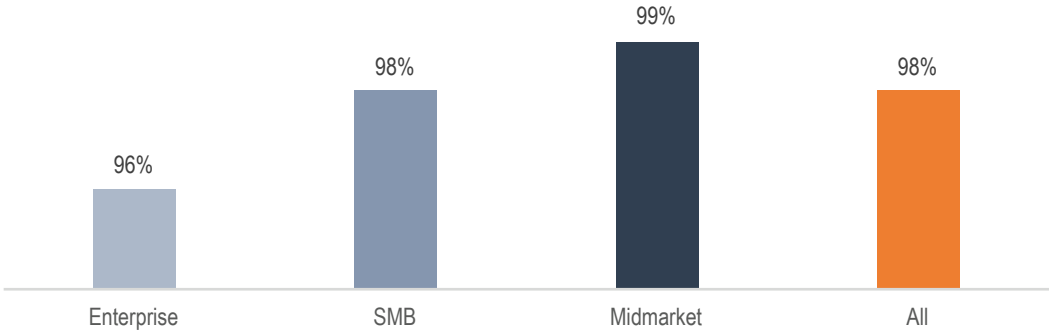

Figure 10 Use of cloud for security workloads

This breakout, though higher than expected, seems to show the correct proportions. Enterprises have an investment in their own data centers, have more complexity in their architectures, and early in the cloud they had a general bias toward cloud, especially for security. At the same time, SMBs and midmarkets dove in to cloud migrate their cost structures from capital to expense and to increase agility of all types of services, security included.

The breakout by industry is also interesting. While it would be easy to expect the high tech industry to all have some kind of security workload in the cloud, it was initially surprising to see manufacturing at nearly 100 percent.

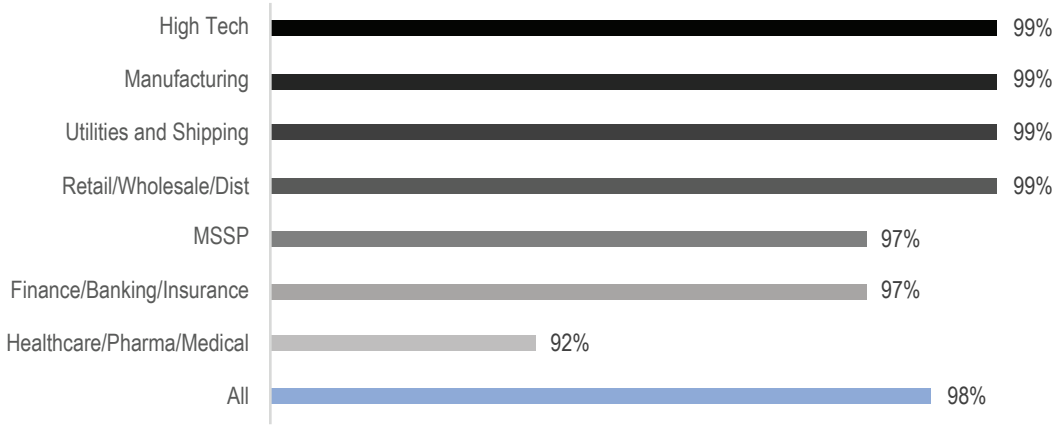

Figure 11 Use of cloud for security workloads by industry

Upon additional investigation, EMA determined that the driver for manufacturing was the lower barrier to entry in the form of reduced capital investment. The same was true for utilities. Large retail/wholesale is trying to scale faster, while small retail/wholesale is just trying to catch up and perform better. Both see the cloud as their avenue for achieving that goal.

Security Participation in Public Cloud Initiatives

Respondents indicated that the security team was involved as a leading player in more than half of the public cloud initiatives.

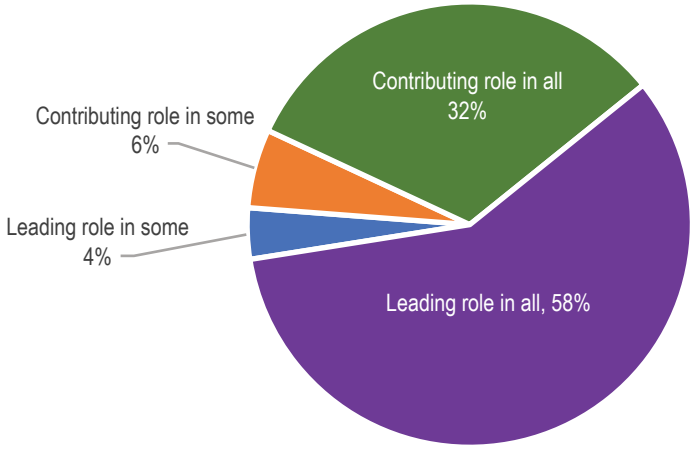

Figure 12 Security team role in public cloud initiatives

One outcome that was totally counterintuitive was that SMBs had their security teams in a leading role at 19 percent (ten points) more often than enterprises. More enterprises have security people than SMBs and enterprises have more overall security people, so that was odd. EMA does not have any additional insights into why that particular situation occurred. Midmarkets fell right in between them.

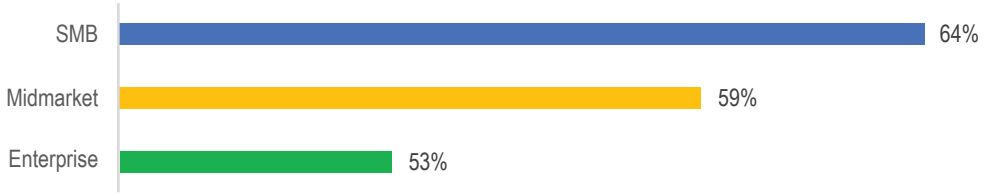

Figure 13 Security taking a leading role in public cloud initiatives

Security Ownership in Public Cloud

The most disturbing thing about the cloud is the assumption around who owns security. With an internal data center ownership is within the company, or has very few exceptions for third-party applications. In the hosted environment, ownership is also “usually” more cut-and-dry, with the hosting provider or managed internal IT managing applications. Whoever manages it is primarily responsible for its security, with the hosting provider supplying some layers as necessary to protect the data center and their other customers.

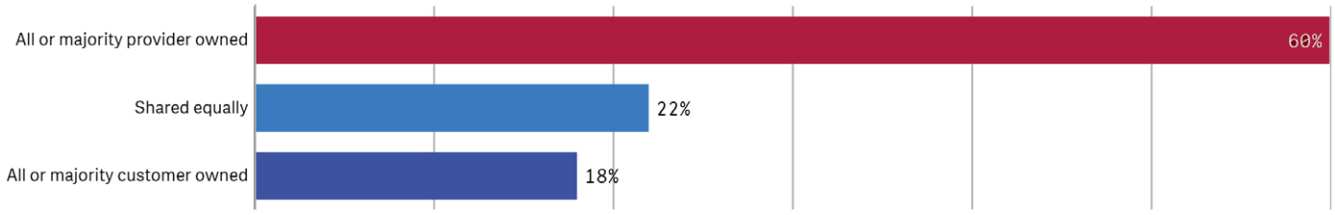

Figure 14 Security ownership within a hosted environment

In the public cloud, however, there is a significant misconception of who owns security. PaaS, IaaS, and SaaS each has different layers of security and different security demarks. Thus, the public cloud has more complex security ownership and management. SaaS providers secure the hardware, network, systems, and underlying applications while the customer is responsible for securing the user access and accessible areas of the application and data. With IaaS services the provider generally stops at the network level, leaving the rest for the customer to maintain. They may provide some underlying system hardening, but the customer is responsible for the operating systems, application installation, and most of the hardening, as well as user access and data. With PaaS, the provider generally maintains everything under the application or development environment and the customer maintains the entirety of the application. These definitions are also somewhat fluid, so it is important to discuss the requirements with the prospective cloud providers before you make a selection and with any current cloud providers to clear up any gaps.

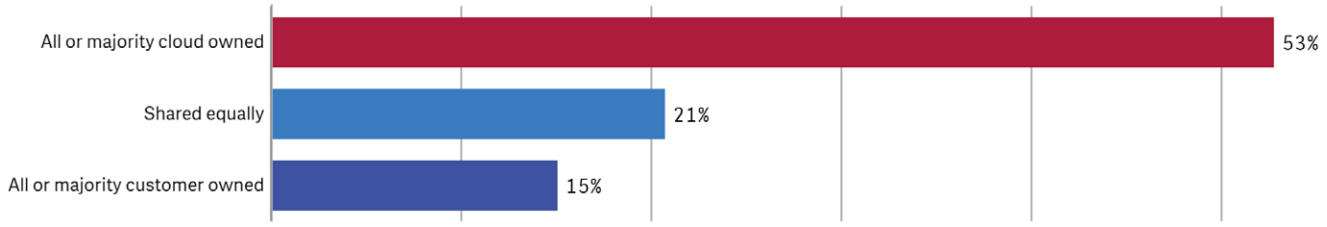

Figure 15 Security ownership within the public cloud

In Figure 15, it is clear that the majority of respondents feel that the security of their cloud environment sits squarely on the shoulders of the providers. It is not uncommon for someone creating shadow IT and relying on the cloud provider to keep that instance secure without realizing the onus is really on them, thus putting business data and operations in jeopardy.

The confusion around security ownership may seem a little surprising given the leading role that security is taking in so many cloud initiatives. However, with the lack of security skills and tenure in so many companies, it is most probable that the people from security involved in these initiatives are often inexperienced and therefore do not understand many of the security nuances.

Security Challenges in Public Cloud

Respondents voiced multiple concerns about their security challenges in the public cloud. The top eight are:

1. Security visibility within the cloud infrastructure due to provider limitations
2. Inability to meet compliance needs
3. Security visibility within the cloud infrastructure due to architecture limitations
4. Threat from crypto-jacking
5. Security visibility within the cloud infrastructure due to tool limitations
6. Need for or lack of cloud data encryption
7. Lack of centralized controls for distributed cloud providers
8. Inability to properly manage cloud encryption key lifecycle

Notice that two of the top three centered around a lack of visibility into the public cloud environments, and the third reflects an inability to have centralized or common controls across the cloud providers. Though cloud providers have come a long way in exposing APIs for better visibility and control within their environments, it appears that there is more to do.

Here are the top three overall security challenges:

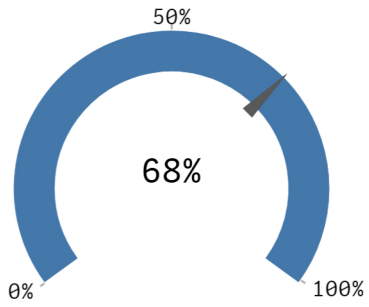

Figure 16 Security visibility within the cloud infrastructure due to provider limitations

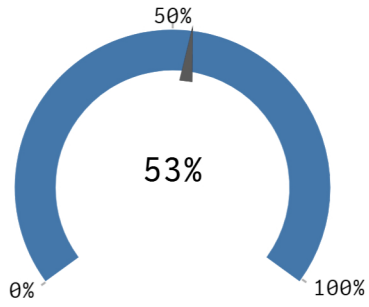

Figure 17 Security visibility within the cloud infrastructure due to tool limitations

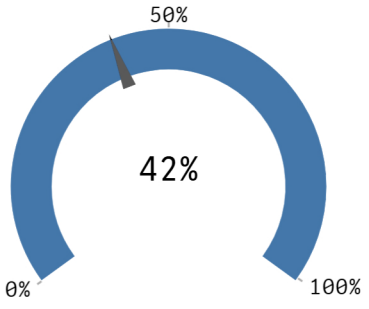

Figure 18 Lack of centralized controls for distributed cloud providers

Though the percentages varied by organization size, the rankings remained consistent across enterprise, midmarkets, and SMBs.

Hybrid Cloud

No discussion of cloud would be complete without including hybrid clouds because there is a lot of activity around hybrid clouds. Ninety-nine percent of organizations are either engaged in a hybrid architecture or are planning to deploy one in the next 24 months.

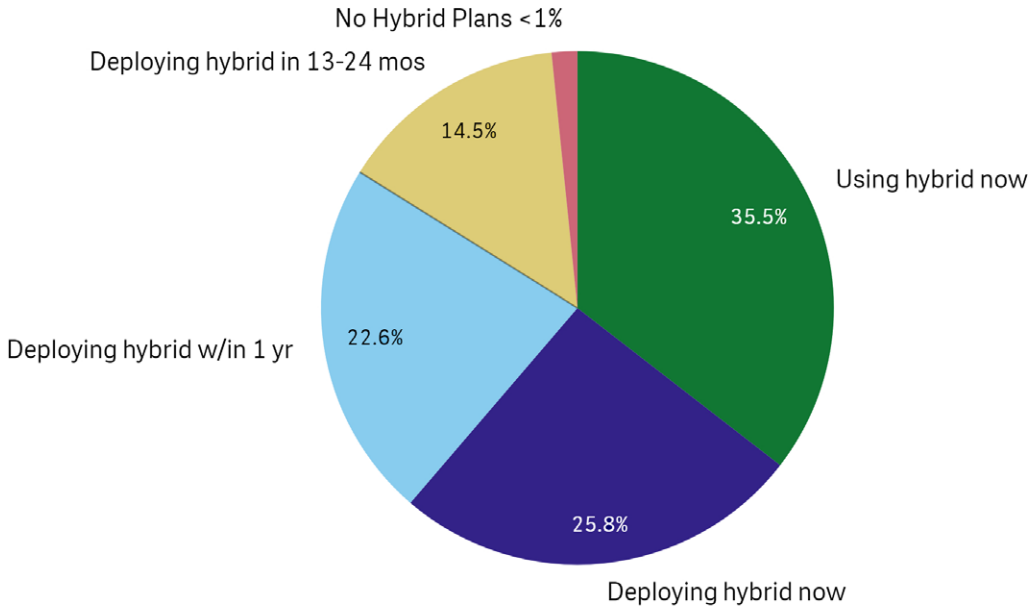

Figure 19 Use of hybrid cloud architecture

While 58 percent of the midmarket respondents indicated they either had a hybrid cloud architecture or are in the process of deploying a hybrid cloud architecture, as expected, enterprises are a bit more bullish with their hybrid cloud projections, with 78 percent either having hybrid cloud or currently deploying hybrid cloud.

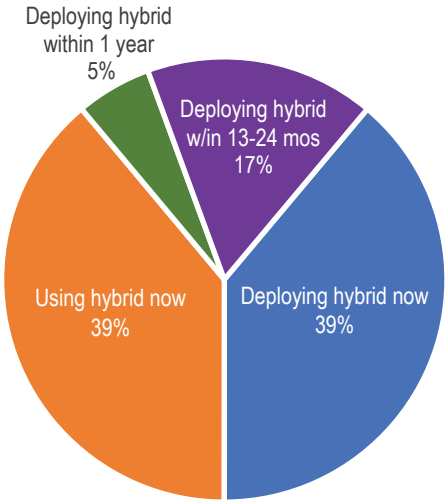

Figure 20 Enterprise use of hybrid cloud architectures

In retail/wholesale none of the respondents indicated they had a current hybrid cloud deployment, but a resounding 80 percent indicated that their companies were currently deploying hybrid cloud architectures. Only 38 percent of healthcare/pharma/medical companies were working on deploying hybrid. The finance/banking/insurance sector had the highest current hybrid cloud deployment, with 60 percent currently leveraging hybrid and the other 40 percent indicating they were either currently deploying hybrid or were going to deploy in the next year.

With all of the cloud activity, EMA asked respondents what the greatest challenges were in their work in hybrid clouds. The top three responses were:

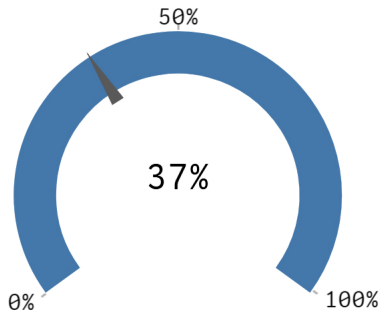

Figure 21 Integrating hybrid cloud security into current on-premises security architecture

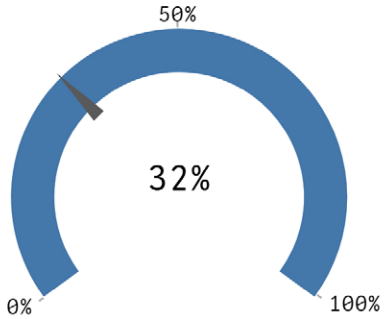

Figure 22 Complexity of multisite security orchestration

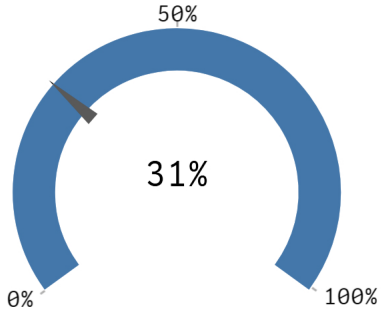

Figure 23 Security latency between internal and external cloud resources

SecOps Frustrations: Tools

One of the reasons there is a huge value opportunity for MSSPs is because of the difficulty and frustration security has with managing all of their tools. Enterprises can have a huge number of management consoles to interact with to do their jobs.

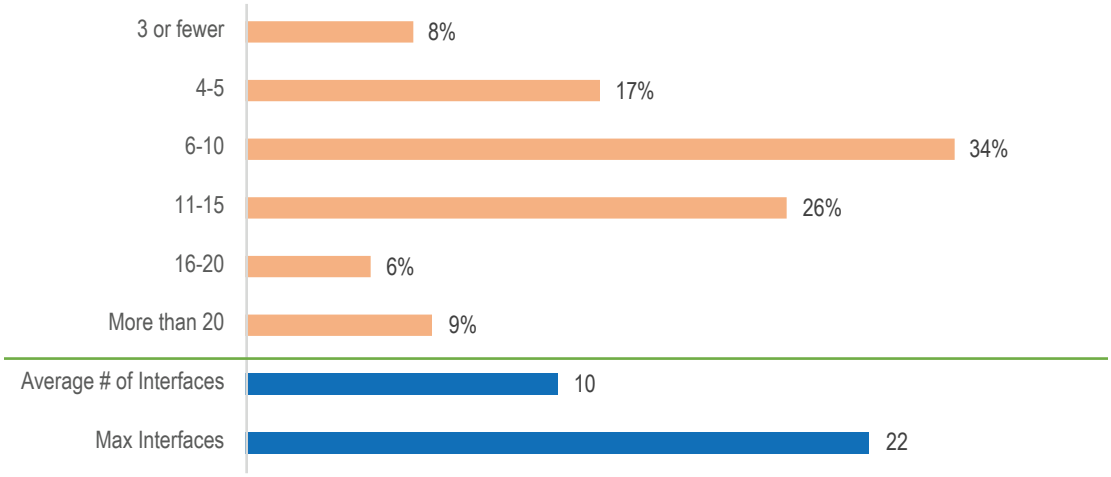

Figure 27 Consoles security teams use to manage programs

SecOps Frustrations: Alert Fatigue

Another area of frustration for security professionals is referred to as alert fatigue. Alert fatigue stems from the large volume of alerts presented to analysts that they are required to validate, identifying whether they are really high severity or at the other extreme—if they are false positives that are really nothing to worry about. In many environments there is highly insufficient context for the systems to properly judge the criticality, so over 95 percent of the tickets that come in are classified as the highest priority.

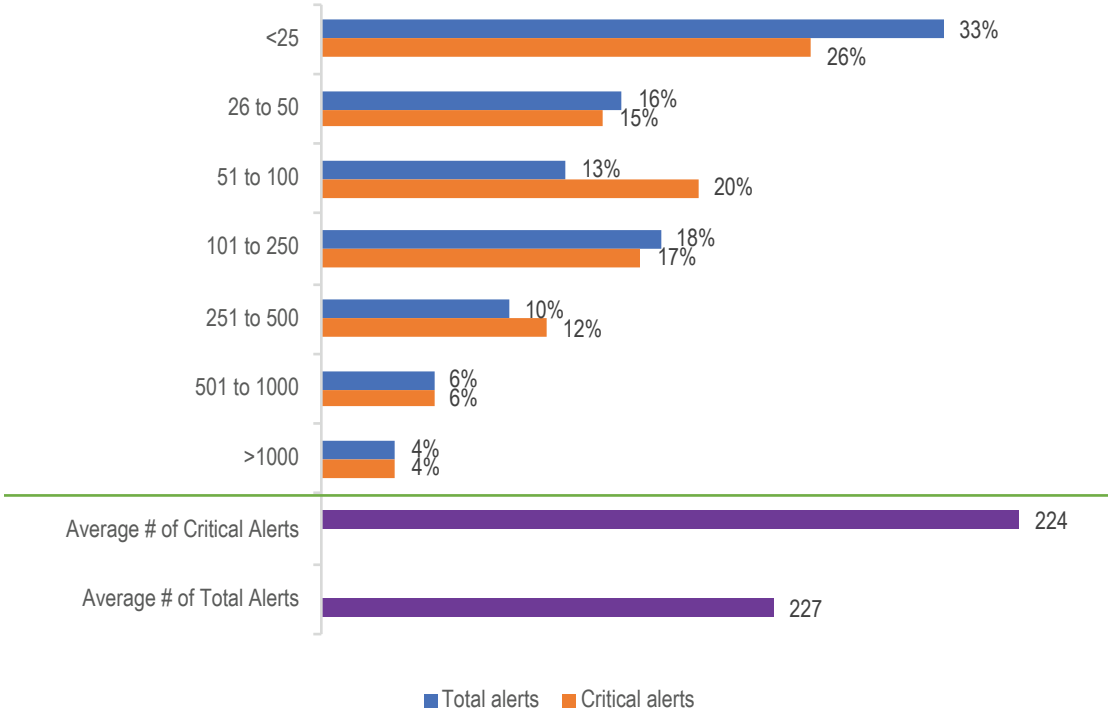

Figure 28 Comparison of severe tickets to overall tickets

SecOps Frustrations: Handoffs

The final area of frustration covered in this report is inter-team handoffs. Seventy-six percent of respondents identified some level of impediment when trying to resolve an incident requiring inter-team handoffs or support.

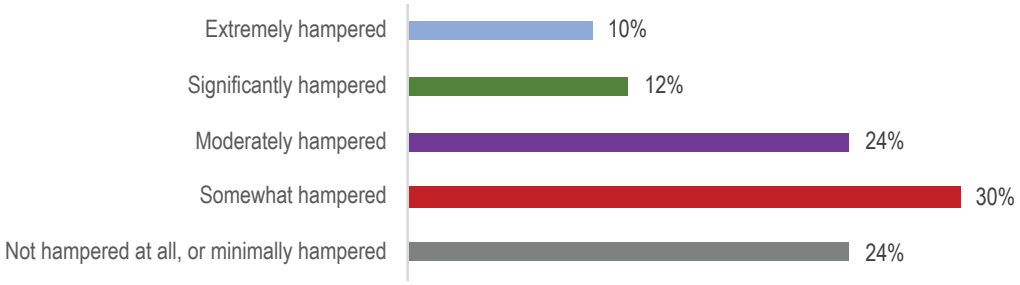

Figure 29 Level of impediment experienced in inter-team handoff for incident investigation

When trying to investigate and resolve an incident, security analysts are often required to engage members of other teams for one or more phases of the incident prior to closing. These frustrations are encountered at some level daily, which leads to job dissatisfaction. After enough frustration, personnel leave. MSSPs alleviate or at least significantly reduce many of these frustrations by handling the incident lifecycle. The degree of reduction is highly dependent upon how much of the lifecycle the MSSP controls.

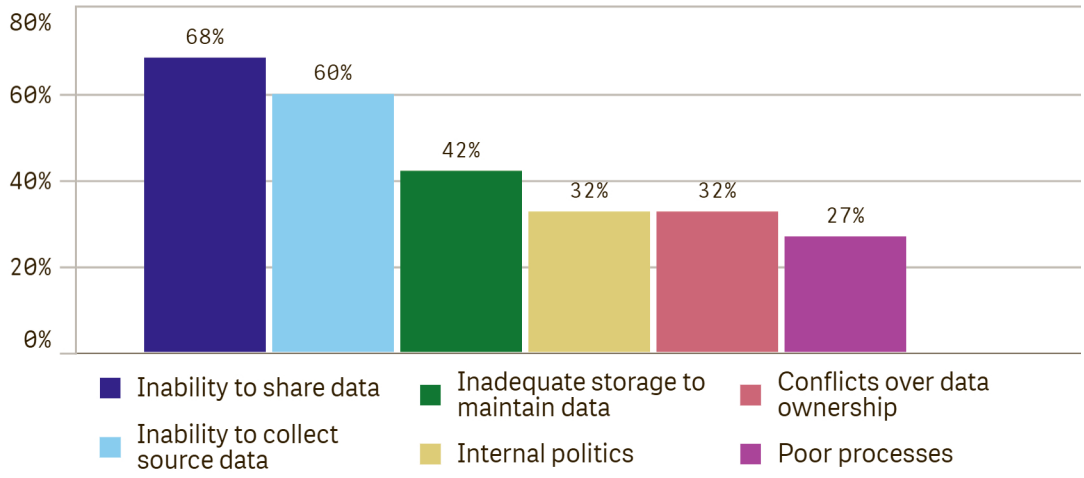

Figure 30 Impediments experienced during incident investigation

Seventy-four percent of enterprises experience the inability to share data, which is the highest impediment for them. Midmarkets identified both an inability to collect and inability to share data equally at 66 percent. Sixty-five percent of SMBs identified data collection as their largest impediment.

SecOps Tools

Consolidation Through Integration and Automation

There are over 1,400 different vendors that supply cyber security tools. SecOps has between 10 and 22 management interfaces to get the security job done. The adoption of niche or point solutions has been tremendous, but is now beginning to contract. Because point solutions were originally seen as better at the job, security shops purchased those to deal with their problems. Now, with the menagerie of point solutions, the problem of paying for and managing those tools has come to a head. To properly couch this, it is important to say that point solution vendors have their place and more often than not solve their problems well, so getting the job done is not generally the problem. However, there is nothing they can do to reduce the number of interfaces used to manage security. Consolidation of tools is the only way to do it. SecOps teams are actively trying to reduce the number of interfaces they deal with.

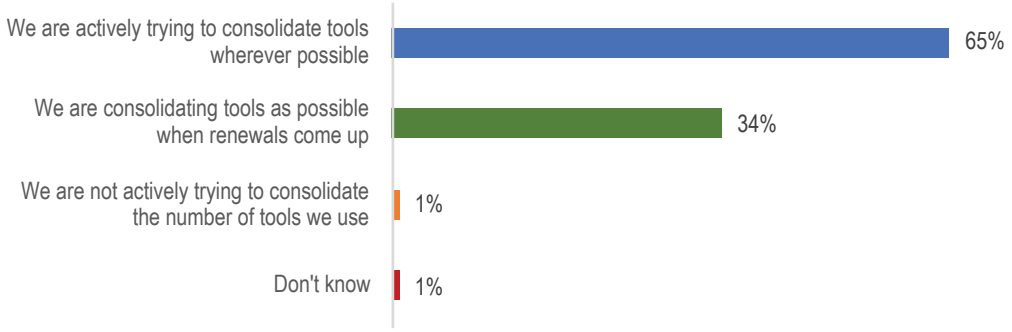

Figure 36 SecOps is consolidating tools

The cloud is solving some of this issue, but not all of it. Platform vendors are also addressing it, probably more so than just using the cloud. There has been significant merger and acquisition activity in the security space over the last five years, with the larger vendors absorbing and integrating smaller vendor functionality. This is a double-edged sword because sometimes vendors purchase other vendors to remove them from the competition—not to integrate. Other times, integrations are not successful and some functionality is lost, as well as larger companies' processes and roadmaps hampering innovation. Partnership is quite appealing to both point solution vendors and the customers because the customers get to keep the solutions they like while improving data sharing and reducing their needed interfaces. Technology consumers are leveraging all of these options to achieve the goals of tools reduction.

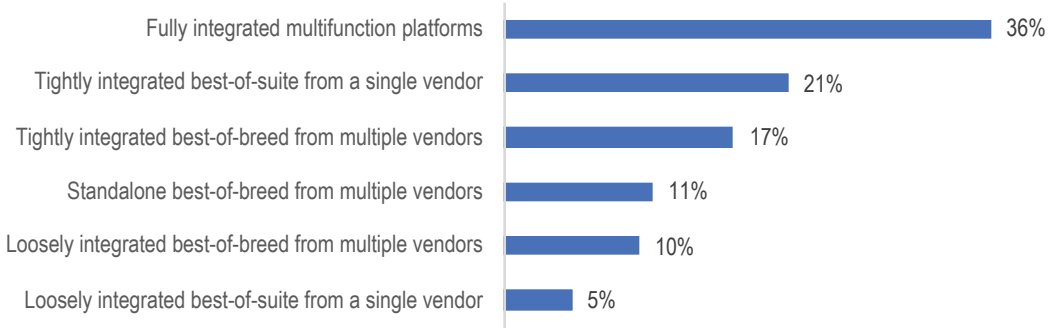

Figure 37 SecOps approaches to consolidating tools

When queried about the most important security management features to meet their business requirements, the majority of respondents said that integration with other IT management products was first order.

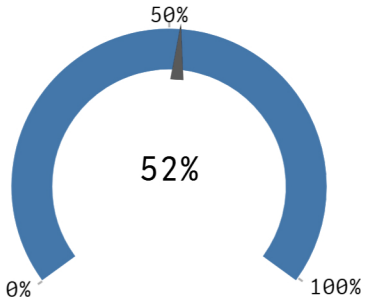

Figure 38 Most important is integration with other IT mgmt. products

Integration with automation and orchestration is the top integration driver. As this movement continues and is successful, it will remove some of the pressures driving customers to MSSPs.

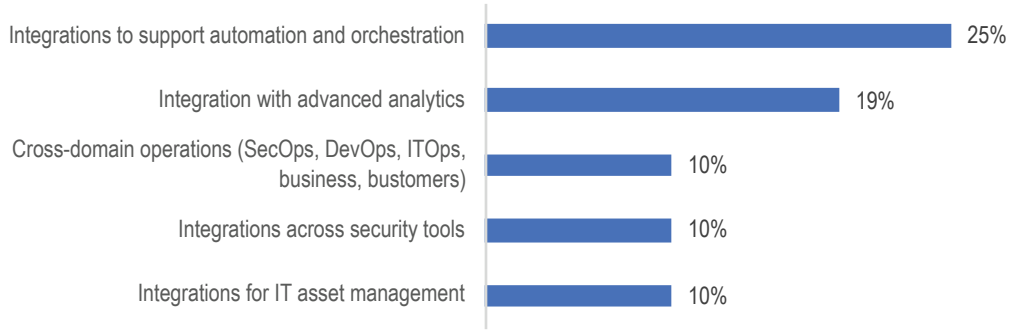

Figure 39 Integration drivers for SecOps

Integrations are a common driver for improving SecOps, and the primary integration driver is for automation and orchestration. Four of the top five monitoring features desired are automations.

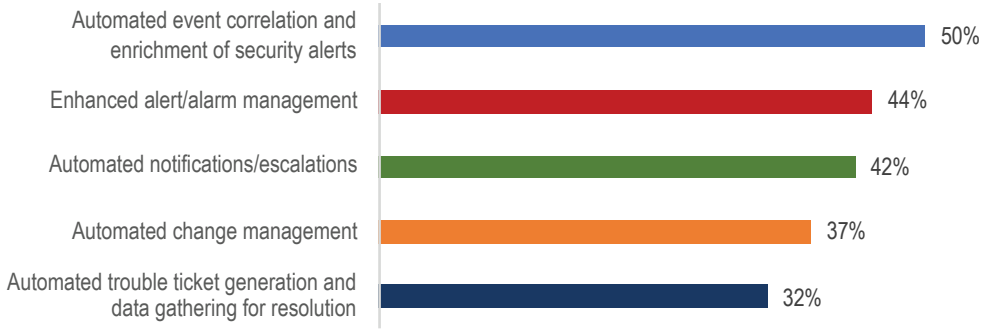

Figure 40 Monitoring features providing the most value to SecOps

Change management has traditionally been a sore spot for the business because poorly affected changes cause the vast majority of unplanned outages or service interruptions. SecOps is also looking at how to be a better internal service provider to the business by automating aspects of change management.

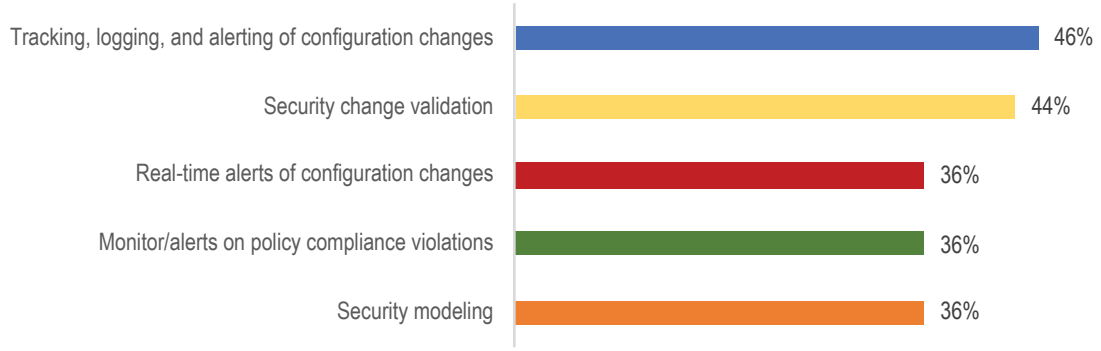

Figure 41 Desired change management automations

Analytics

After automation and integrations, analytics is the next big hitter in security. Though automation and integration scored higher in the polls, there is a strong argument that better analytics should come first. Analytics transforms data into actionable information and intelligence. If companies can reduce the volume of tickets and better categorize them through better analytics, then they reduce the workload and allow SecOps to get the most important work done first. After all, automating a bad process gets business to the wrong places faster and more often.

Good analytics needs two things: good algorithms and as much good data as possible. It is important to understand the types of data a prospective analytics package or platform can ingest before you purchase.

Figure 42 Five types of data most often used in security analytics

Once the data is being ingested, SecOps can get to work. Listed are the top three uses cases for security analytics:

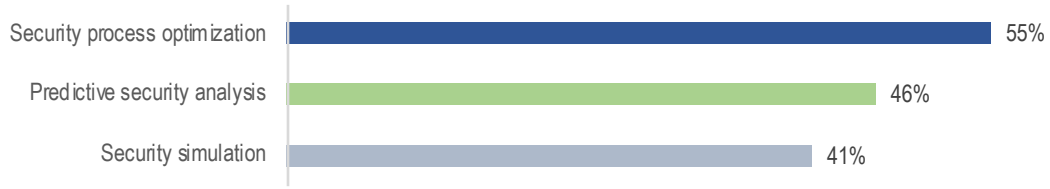

Figure 43 Top three use cases for security analytics

While there is no doubt that these are all valuable, it was surprising that behavioral analytics, though on the list, was not in the top three. The question asked "which were the most important," not "which are the most widely in use," so that could make a difference.

Understanding the importance of analytics, EMA evaluated why more operations do not have them in place. Though budgets are growing they do have limits, so EMA put budgets off to the side and focused on operational impediments.

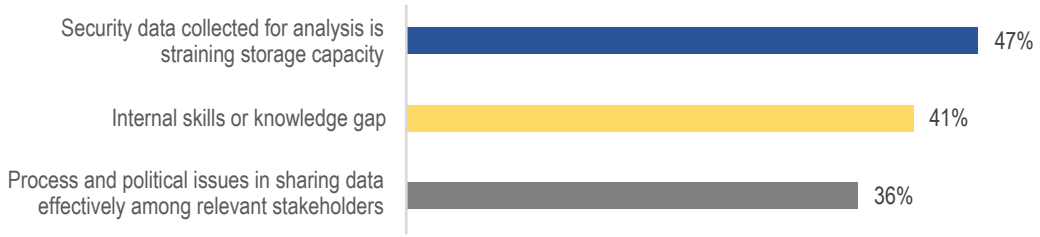

Figure 44 Top three operational impediments to implementing security analytics

Storage is cheap, but when companies start looking at petabytes for larger enterprises to store data for a year, it can put a strain on the budget. Given that sort of constraint, SecOps has to make tougher decisions on whether to reduce the timespan of data stored or whether there are more judicious choices to be made around data selected for ingestion. Not all data is good data. Some definitely provides better telemetry than others.

Endpoint Security

Protection

The modern endpoint is any place data resides or is processed. It is at those points that the vast majority of attackers get to the information they desire. The battle for the endpoint is raging. Across antivirus, detection, prevention, and all combinations thereof, there are approximately 50 companies operating in the endpoint defense space. Seventy-three percent of respondents have been affected by some form of endpoint attack, and only 58 percent of organizations are highly confident they could detect an important security incident before it caused significant impact. When asked how effective their detection and prevention solutions were, respondents felt that detection solutions were only about 71 percent effective and prevention was only about 73 percent effective. Figure 61 shows the kind of infection rates by general malware class. Respondents could select none or any other combination of applicable attacks.

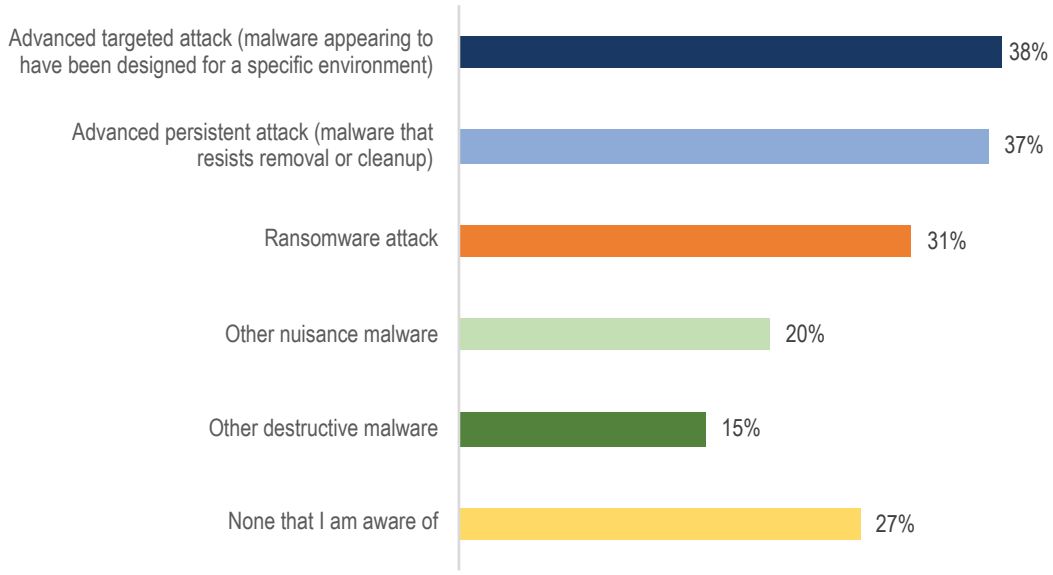

Figure 61 Successful endpoint attacks

Impacts of Attacks

When endpoint attacks occur, even on a single individual, the business impacts can be devastating. The research shows that 28 percent of malware attacks were significant to severe in their impact to the business. Respondents were asked to identify which types of malware attacks created significant to severe impacts. The following data identifies their responses.

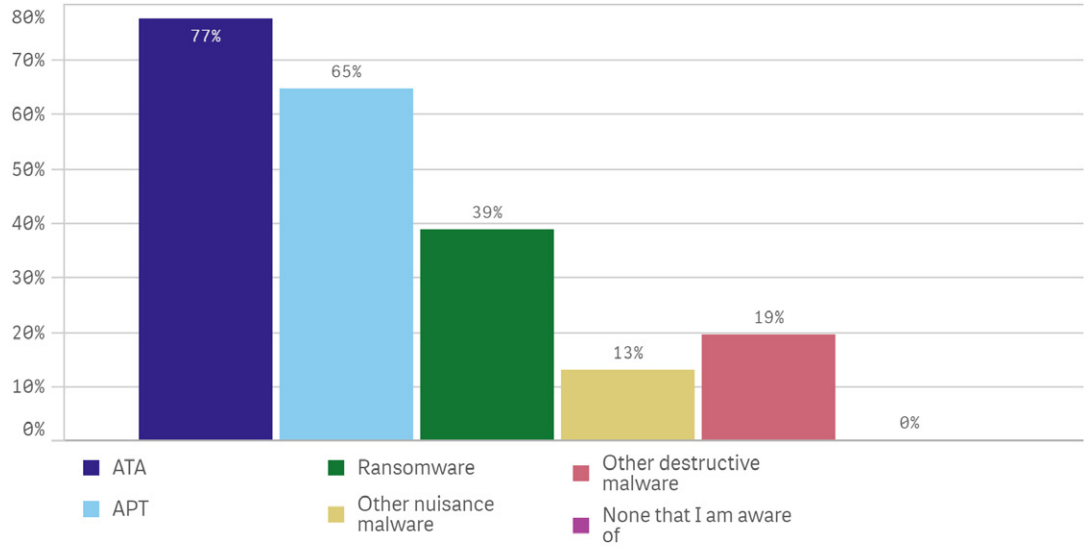

Figure 61a Endpoint incidents that bypassed endpoint security, causing severe damage

It is interesting to see that despite all of the press attention ransomware has, more organizations are experiencing incidents created by ATAs and APTs than ransomware.

A few other salient points in the endpoint research:

- Ninety percent of respondents that experienced an attack causing significant to severe impact believed an advanced endpoint solution would have performed better than traditional AV.
- All of the respondents who experienced severe impacts from a malware attack indicated they now intend to replace their traditional AV product with an advanced endpoint solution.

Clean Up

These types of successful attacks occur all too often, with 48 percent causing moderate to severe business impacts and overall requiring an average of over four man-hours, and in nine percent of cases more than a working day, from both the support team and the employee to resolve and get back into operation.

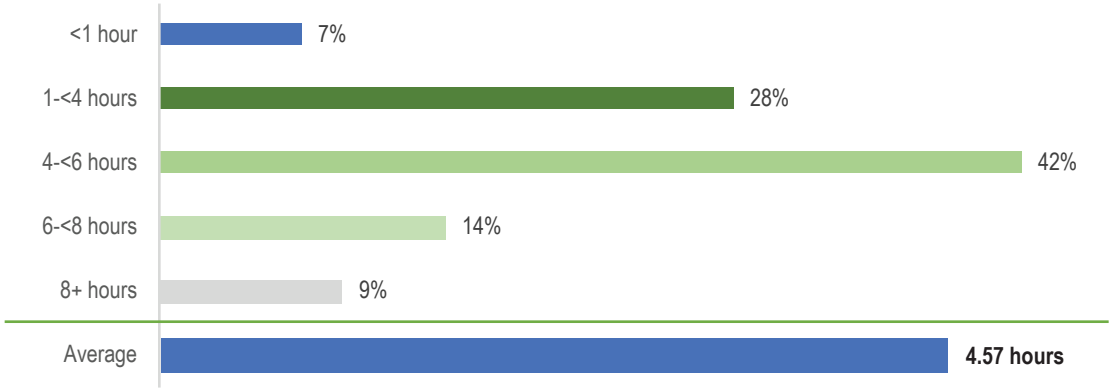

Figure 62 Time to restore an endpoint that a malware attack compromised

Twenty-three percent of respondents identified that their organization had experienced a malware attack that took six or more hours to resolve. Those organizations identified that their current endpoint solution missed the following malware.

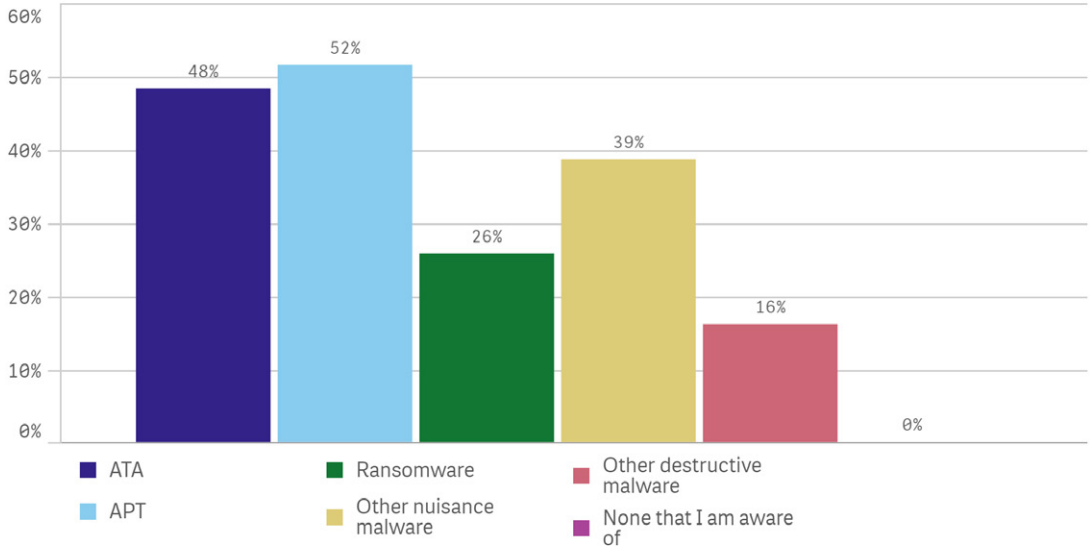

Figure 62a Endpoint attacks bypassing current endpoint solutions that required six or more hours to resolve

Investigations and Forensics

No matter the type of defense you have or choose, a key aspect is the kind of information it provides after initial detection. How did the malware get in? When did it get in and thus, how long has it been inside? What systems has it touched? What has it done on the endpoint? These questions, along with others, are all pertinent and must be answered to successfully declare victory over the infiltration. Full endpoint interrogation data was rated most useful to accelerating incident response and breach detection.

Figure 63 Endpoint data as most useful data for breach detection and incident response

The choice for endpoint protection is a big one. It is the last line of defense for precious information. To that end, companies must detail requirements well. In the author's opinion, detection is good but detection without the proper data collection for full forensics leaves the organization open to a lot of work. Be sure any detection platforms evaluated can provide enough details to understand how the attack executed and proliferated and the attack path.

EMA Perspective

There are a lot of common security problems in the world today. One report can't possibly cover all of them. A key finding is that while there are absolutely nuances to some of the problems that are specific to a vertical, there are very few, if any, security problems totally unique to any company size or vertical. Threat actors may be more persistent and the potential losses may be larger, but a solid security program is based on reducing risk. Each company has to prioritize its risk and address the most significant problems in a way they see most fit. If companies invest appropriately based on their true risk tolerance and follow best practices, they can be compliant and secure without worrying about which compliance regulations they are or are not meeting.

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 EMA's 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 blog.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

3793-SentinelOne.011819