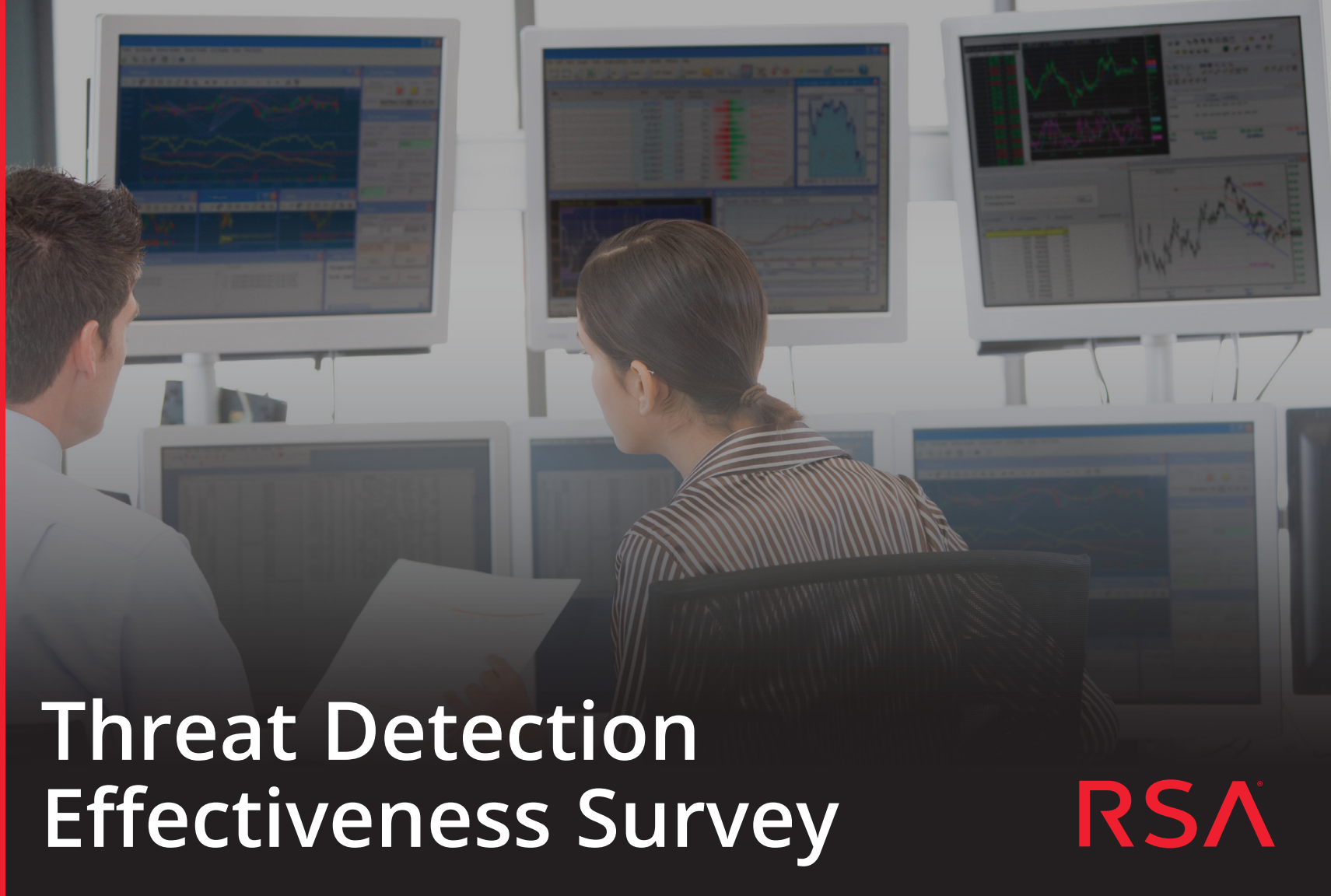


Threat Detection Effectiveness Survey

RSA

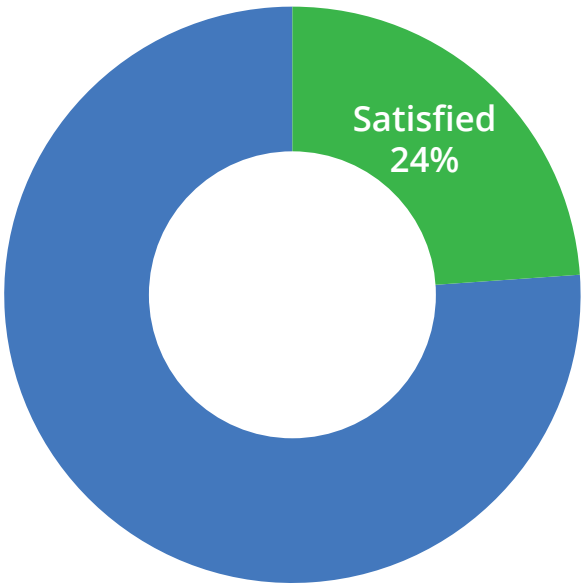
Overview

RSA conducted a global survey to understand how effective organizations are at detecting and investigating cyber threats. The research was designed to provide global insight into what technologies organizations use, what data they gather to support this effort, their satisfaction with the current toolsets, what new technologies they plan to invest in, and how they plan to evolve their strategies going forward.

The survey was completed by more than 160 respondents across 22 different industry sectors in the Americas, EMEA, and APJ from December 2015 through February 2016. The twelve question survey asked respondents to answer rating questions and to input exact percentages for resource allocation and investment. Of the organizations surveyed, about 60% fall into five industry sectors: Financial Services, High Tech, Education, Services, and Government.

Overall: Low Satisfaction for Detection and Investigation

How satisfied are you overall with your ability to detect and investigate threats using your current data and tools?

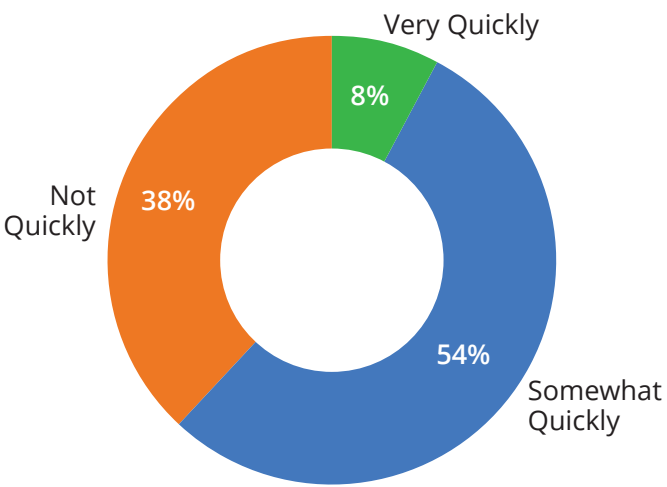


Only 24% of organizations are satisfied with their current ability to detect and investigate threats using their current data and tools.

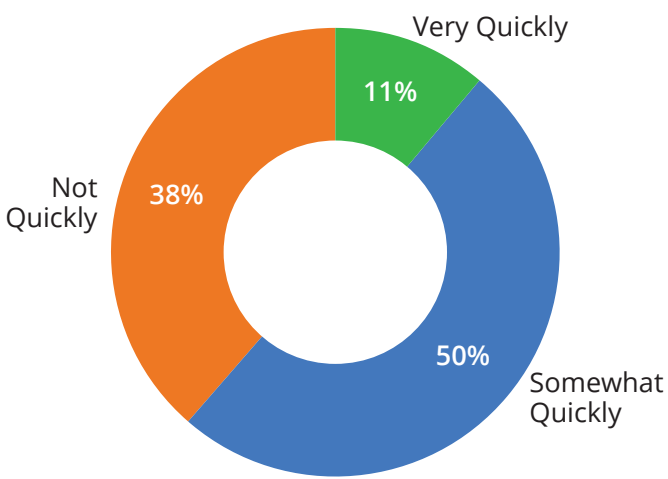
Detection and Investigation Lack Speed

Few organizations are able to detect and investigate attacks very quickly, which can lead to extended adversary dwell time.

How quickly are you able to detect attacks using your current data and tools?



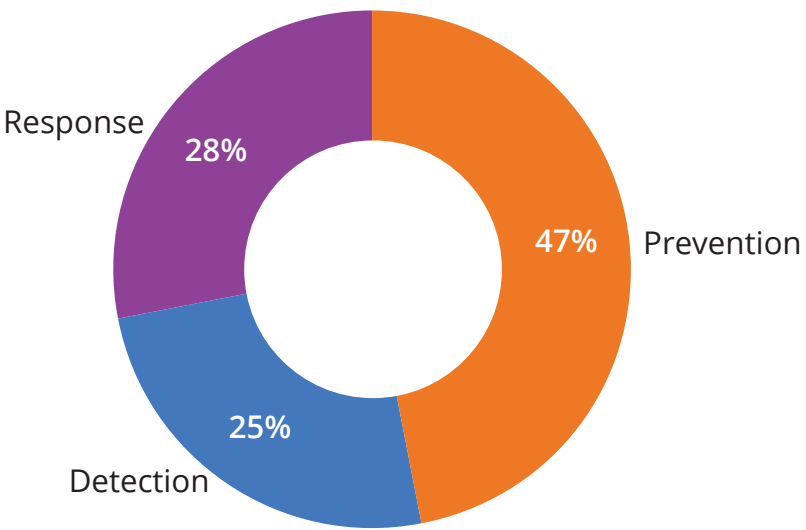
How quickly are you able to investigate attacks using your current data and tools?



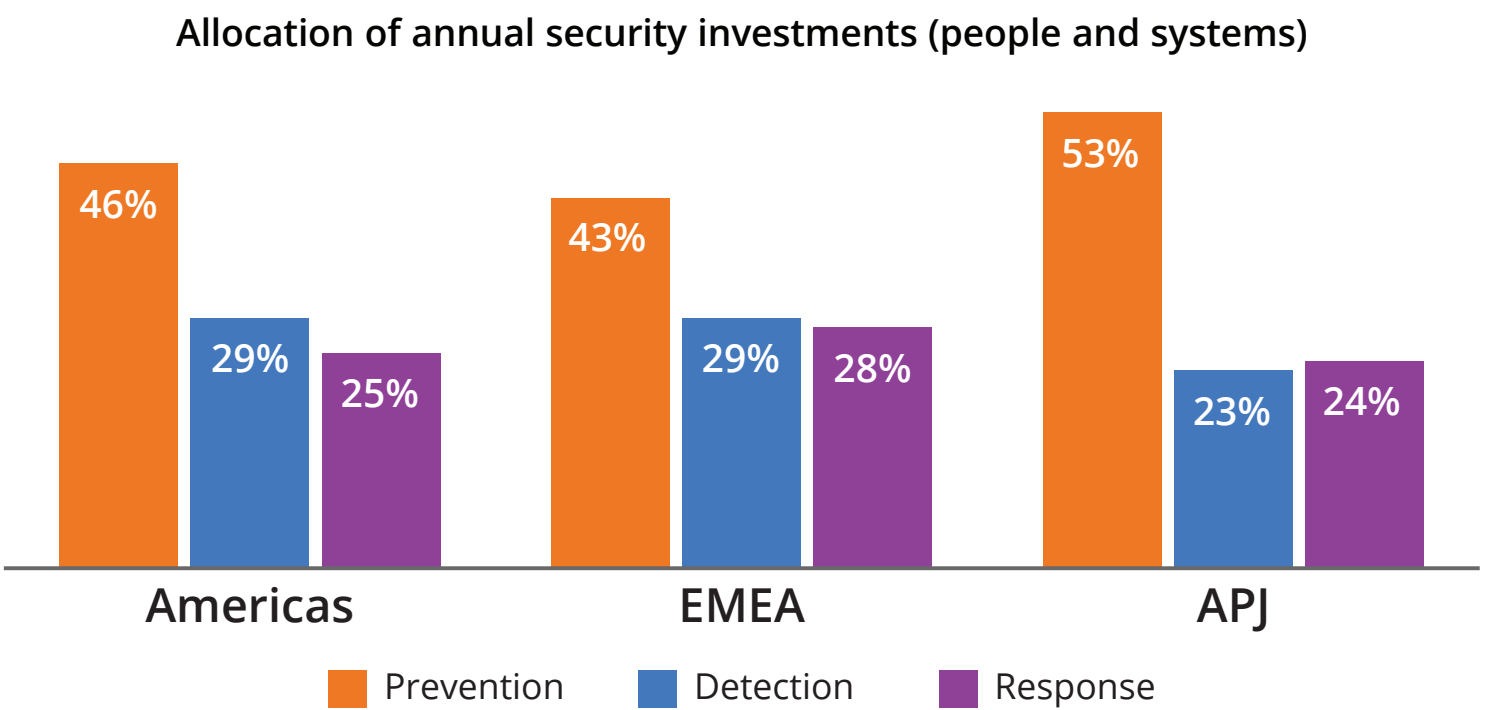
Do We Have the Right Priorities?

Organizations surveyed reported that half of their investment in staff and technology is in preventative technologies and strategies, with little or no plans to increase investment in detection and response over the next 12 months.

Allocation of annual security investments (people and systems)

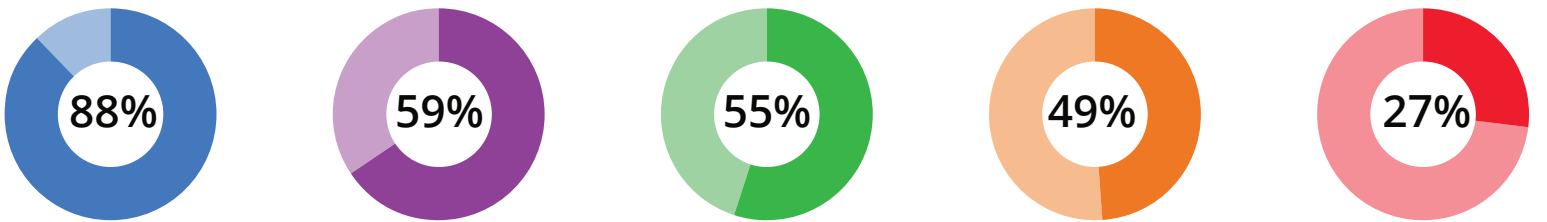


Prevention is the Main Focus Across Geographies



Do We Have the Right Visibility?

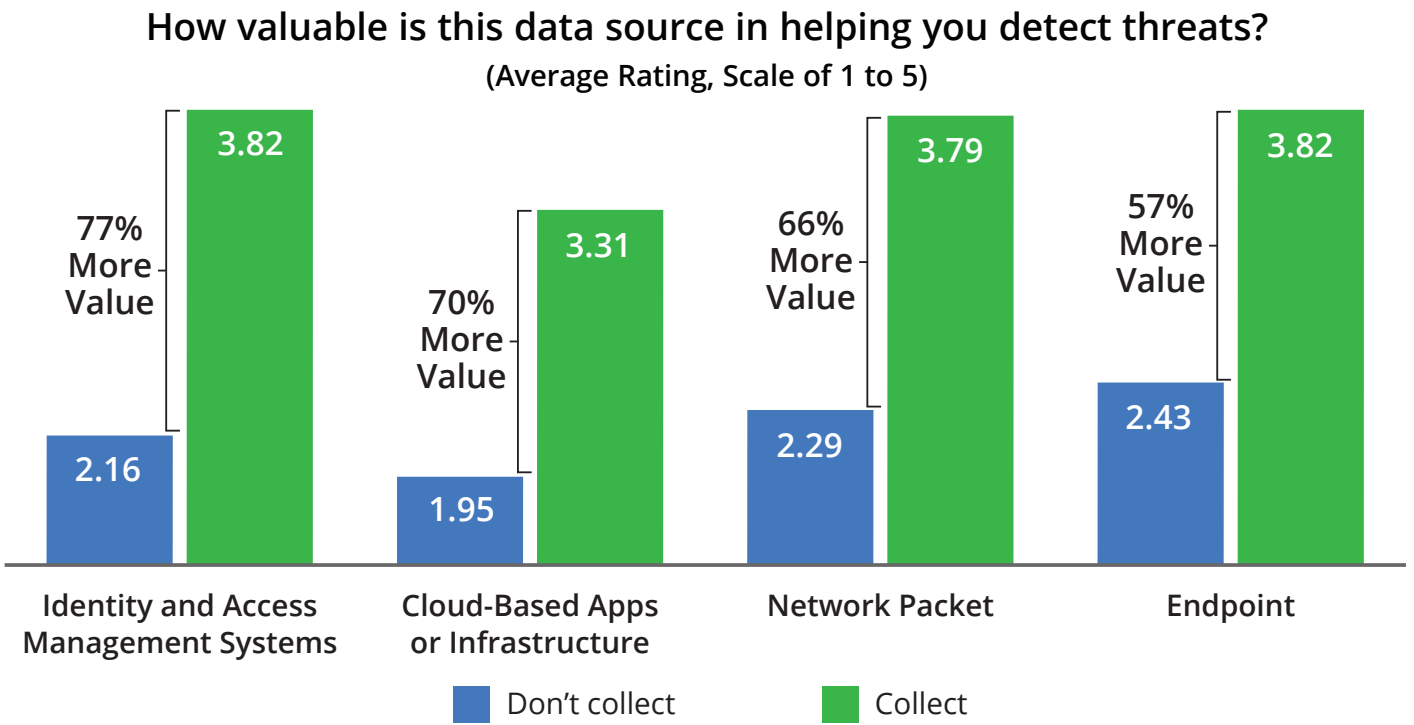
What data sources are organizations collecting from to help them detect threats?



Organizations do not collect some of the most valuable data

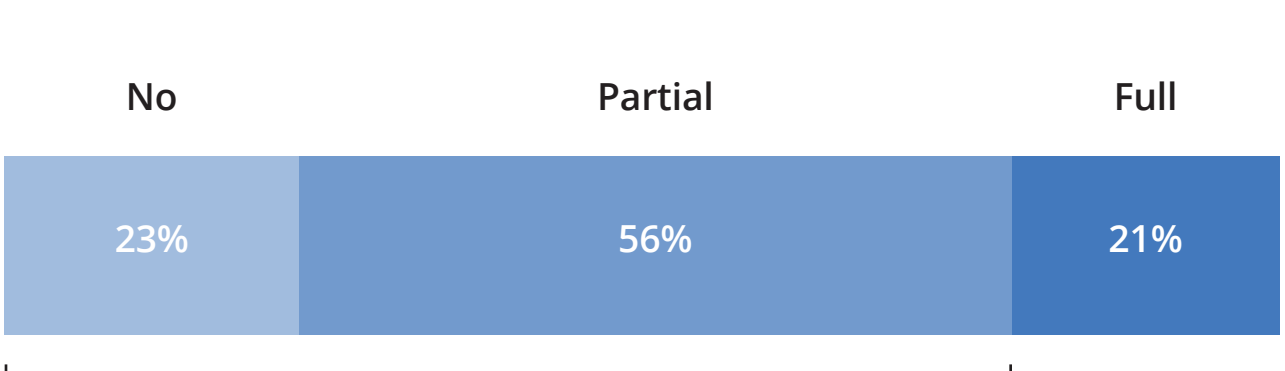
You Don't Know What You Don't Know

Organizations that collect specific types of data find increased value compared to those who don't.



Data Is Collected But Not Integrated

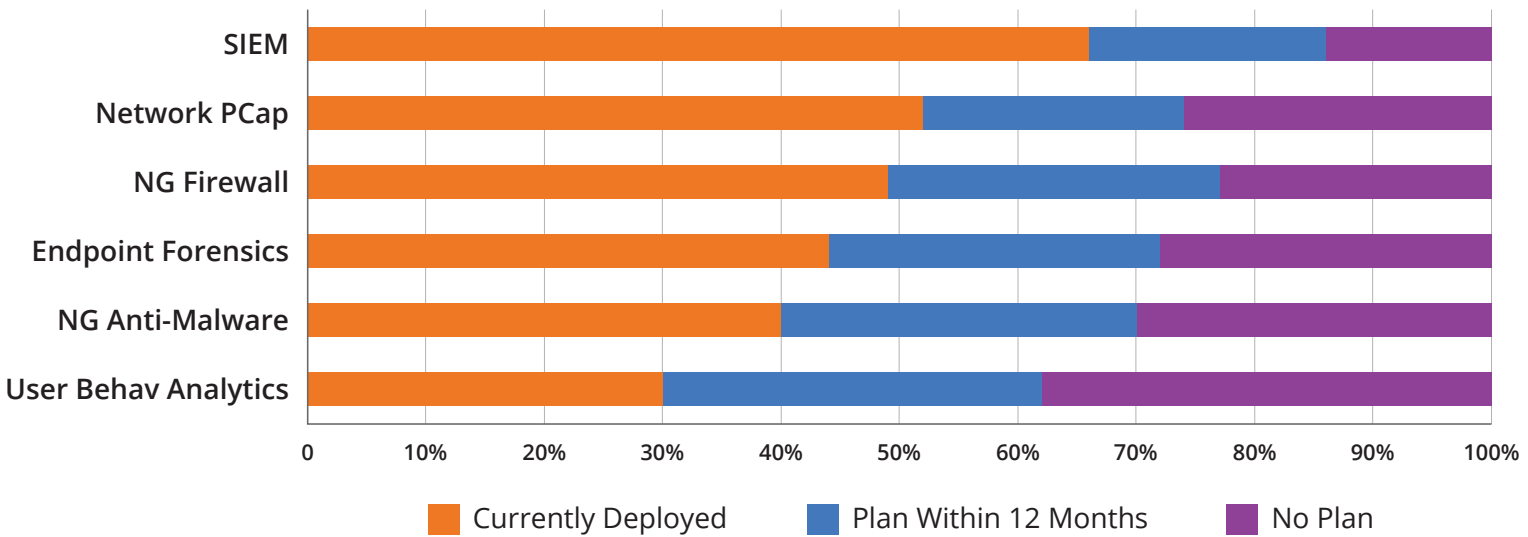
Characterize the extent to which you have aggregated/integrated the data sources you collect for threat detection into a single normalized data structure



Many Technologies Deployed, No Silver Bullets

While SIEM is deployed by the majority of organizations, more effective tools like packet capture, endpoint forensics, and analytics lack the necessary adoption.

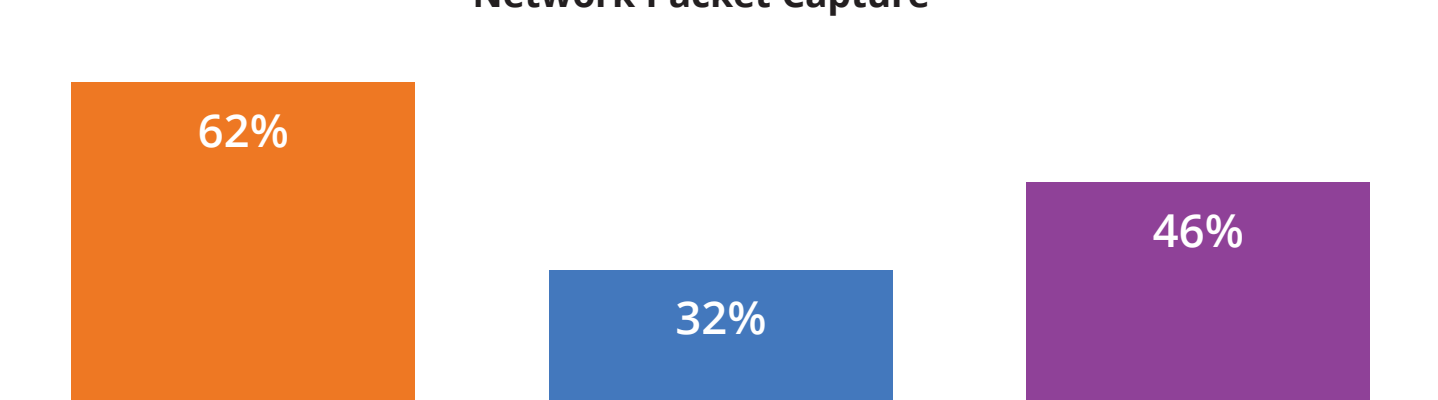
Describe current and planned use: technologies for detection & investigation



Network Packet Capture Use Varies Across Geographies

Organizations in the Americas outpace peers in network packet capture use.

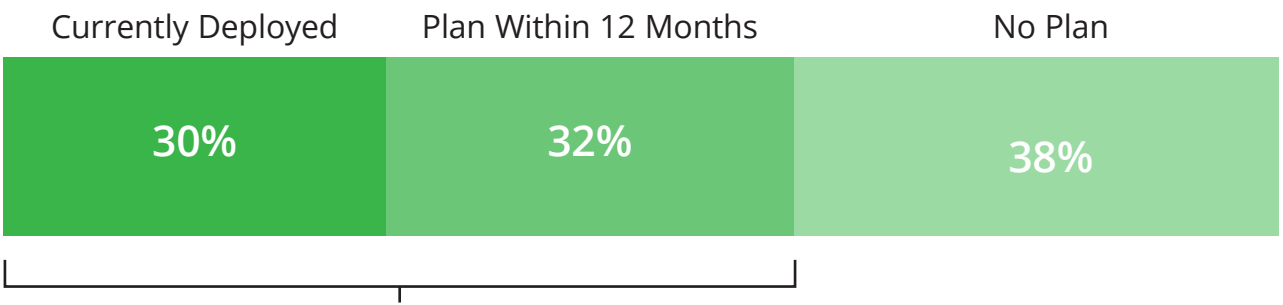
Which of the following data sources do you collect and use in support of your threat detection efforts?
Network Packet Capture



User Behavioral Analytics Is Top Investment Priority

Organizations recognize that increased automation is necessary to spot anomalous activity and aid detection of the most advanced attacks.

Describe current and planned use: Behavioral Analytics



Within the next 12 months, over 60% of organizations are projected to use behavioral analytics.

Conclusion

The survey data shows that organizations are relying on a fragmented foundation of data and technologies for detection and investigation. Because data remains siloed, visibility is incomplete, making it difficult to scope attacker activity. As a result, the speed with which they can detect and subsequently investigate threats becomes a major challenge. Understandably, respondents expressed deep dissatisfaction with their current threat detection and investigation capabilities.

The results show a lack of adoption of technologies that can automate and make detection and investigation more effective. The value of network packet capture and endpoint forensics, are only well understood by the minority of organizations who have incorporated them as part of their strategies. Encouraging data shows an acknowledgement of the importance of identity information for detection, and planned investment in user behavioral analytics.

To successfully move forward, organizations need to plug gaps in visibility, take a more consistent approach to deploying the technologies that matter most, and accelerate the shift away from preventative strategies.

Published in the USA. 02/16 eBook
H14916

RSA