SOLUTION BRIEF | Mid-Market Cybersecurity

ARCTIC WOLF

The State of Mid-Market Cybersecurity: Findings and Implications

50 percent of IT professionals say they don't know where to start to improve their security posture

Perception

- **95%** believe they have above average security posture
- **89%** believe perimeter security products can combat all cybersecurity threats
- **90%** say they have personnel solely dedicated to cybersecurity

Reality

- **72%** report that their role is so broad it's difficult to focus on IT security as much as they should
- **63%** say they may not be able to stop zero-day threats
- **77%** of security alerts are investigated after more than one hour

Mid-market enterprises face the same cybersecurity issues as large enterprises with only a fraction of the budget and less-skilled personnel. A recent survey conducted by Arctic Wolf brings to light many of the challenges that mid-market IT and security professionals face. Smaller companies tend to be overconfident about their security posture—thinking they have rigorous cybersecurity defenses when in fact they do not. Though they may have implemented industry best practices at a higher level, a closer examination of their security operations and processes revealed that they were more vulnerable than they realized. The findings affirm a cybersecurity dissonance among mid-market enterprises, highlighting a disparity between perception and reality.

Perception

Mid-market IT professionals are overly confident when it comes to cybersecurity. Most have invested in perimeter and endpoint security products, and they feel confident that these products can protect them from nearly every threat. 95 percent of respondents believe their cybersecurity posture is above average or great, and 89 percent believe their perimeter security products can combat all cybersecurity threats.

Figure 1: How would you rate your organization's overall IT security posture?

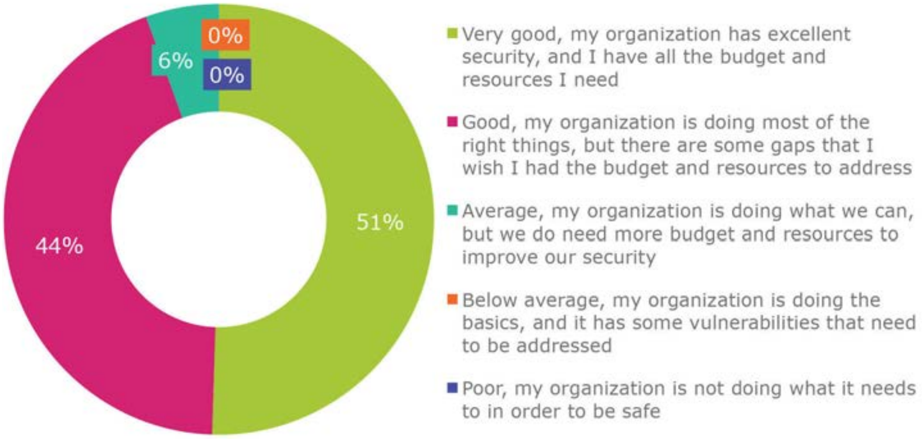
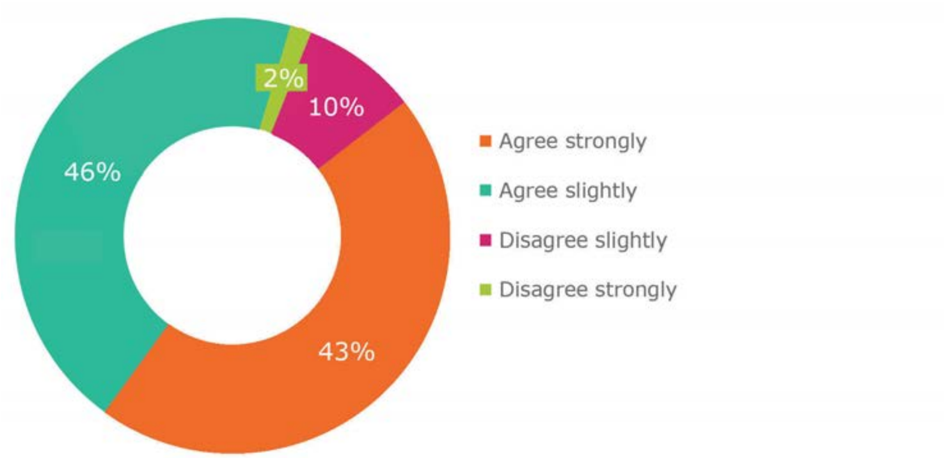
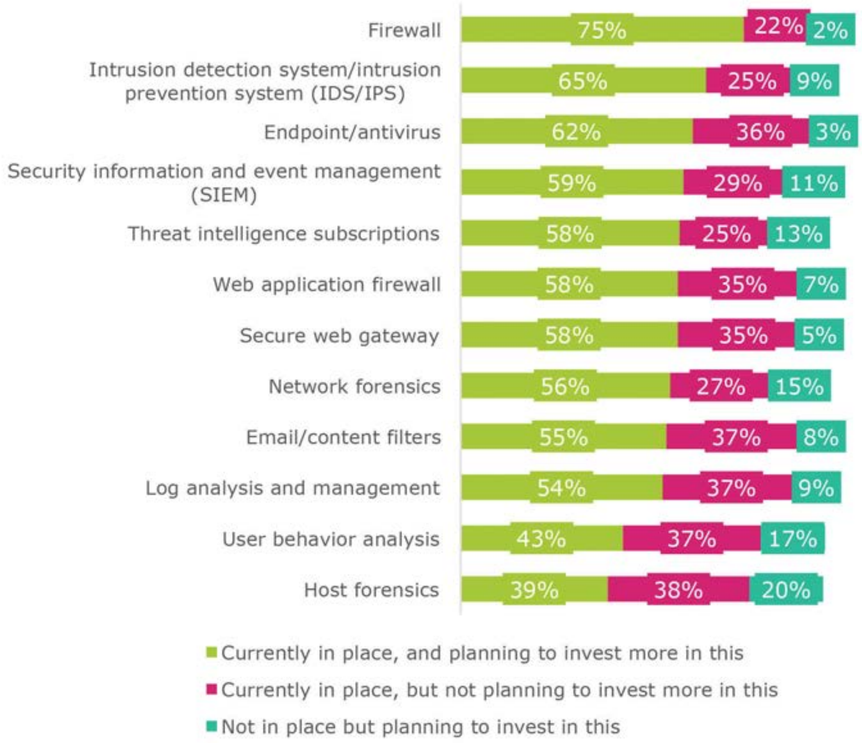


Figure 2: To what extent do you agree with — The perimeter security product/s used by my organization can combat all cybersecurity threats?



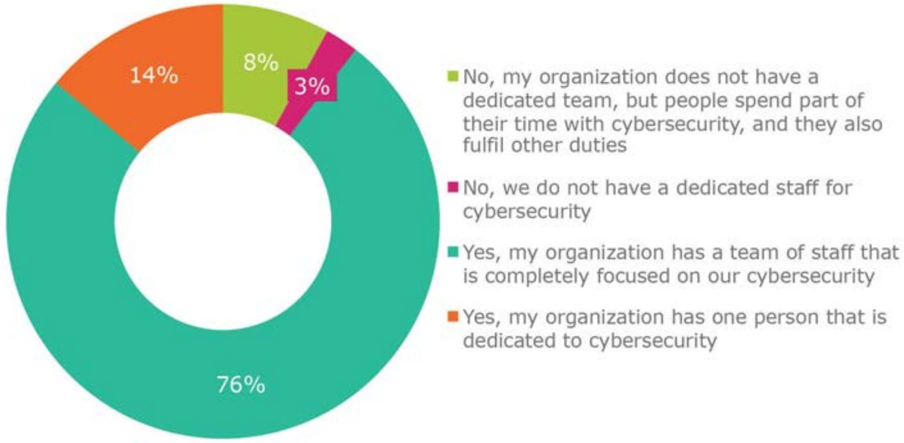
95 percent of respondents expressed high confidence in their cybersecurity defenses, but struggle to defend against malicious activity.

Figure 3: Which of the following cybersecurity elements does your organization have in place, and which is your organization planning to invest more in?



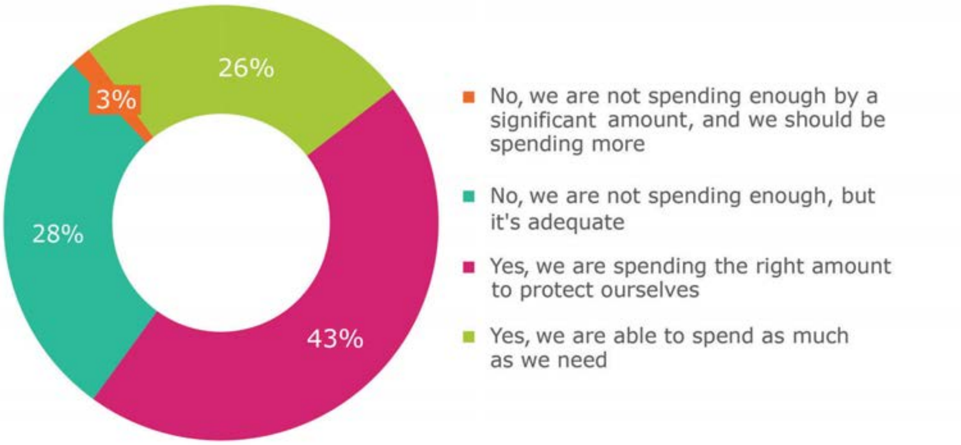
Mid-market enterprises appear to be taking cybersecurity seriously by assigning dedicated personnel. On average, 90 percent of survey respondents indicated they had one or more people completely focused on cybersecurity.

Figure 4: Does your organization have a specific internal role or internal team that is dedicated solely to cybersecurity?



The Arctic Wolf survey also found that IT and security professionals felt that they had sufficient budget for cybersecurity. 97 percent said the spending was adequate.

Figure 5: Do you think you are spending enough on security?



The survey found that overall, IT and security professionals at mid-market companies appear to be very confident that they have the resources to do their job and protect their company from malicious threats. They have a breadth of security products that protect both the perimeter and endpoints. Dedicated cybersecurity staff are available to focus on security, and they have the necessary budget.

Reality

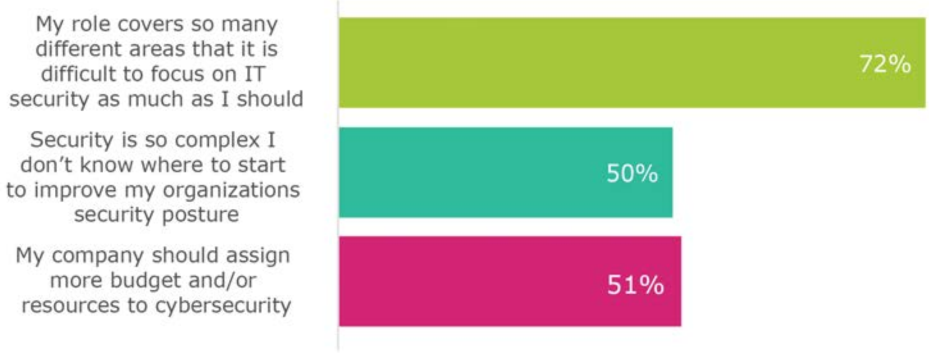
Despite the positive self-assessments of survey respondents, a closer look at the security operations and processes show that mid-market IT and security professionals struggle to defend against malicious activity that has become more sophisticated, more targeted and severe. The reality is that IT and security professionals at mid-market companies have broader responsibilities and do not have the luxury of focusing on cybersecurity. In addition, their expertise tends to be broad versus deep, so they may not have the necessary specialized skills.

Though IT and security professionals feel confident in their security posture, the reality is that they have significant gaps in security and are often unable to adequately deal with the complex threat environment. In fact, 72 percent of respondents report that their role covers so many different areas that it is difficult to focus on IT security as much as they should. 50 percent of the respondents said that security is so complex, they don't know where to start to improve their organization's security posture. 51 percent also said they would like their organization to assign more budget and/or resources to IT security.

"The challenge smaller enterprises face is that they have all the same security challenges as large enterprises with only a fraction of the budget and less skilled personnel."

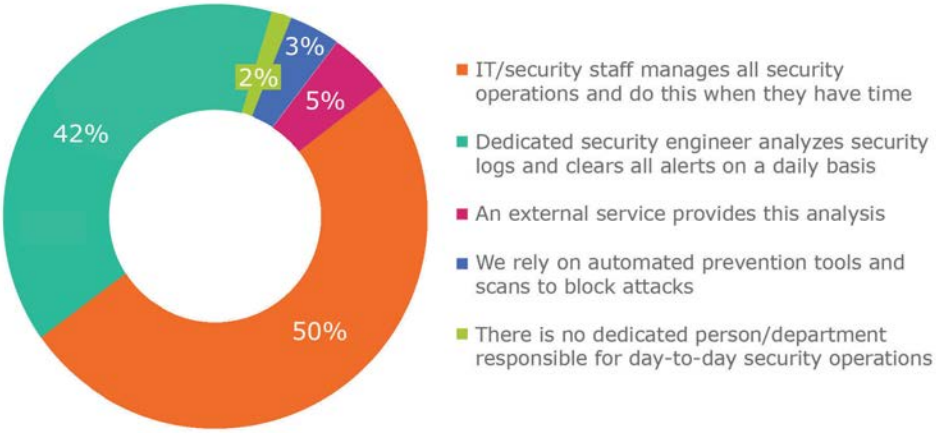
– Brian NeSmith
CEO, Arctic Wolf

Figure 6: Percentage of respondents that agree with the above statements.



The disparity between perception and reality is also reinforced by the survey responses to how security alerts are investigated. Though most respondents indicated they had dedicated security personnel, 50 percent said that security alerts were investigated by IT/security staff when they had time.

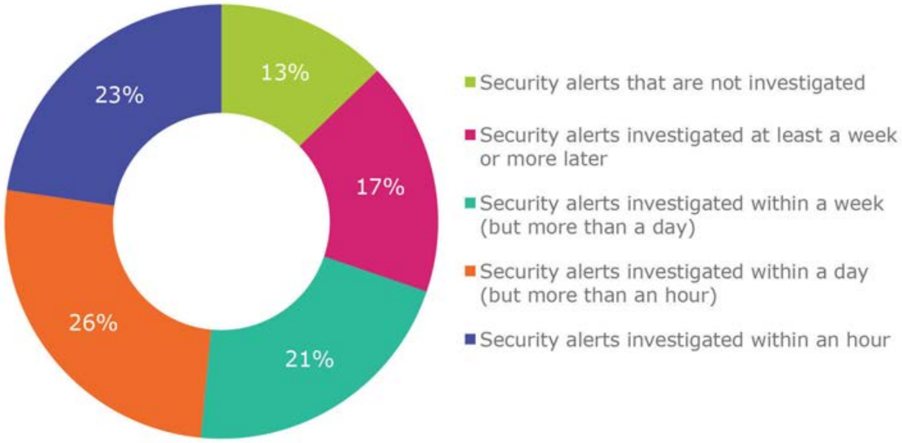
Figure 7: How does your organization usually analyze security alerts and events?



The practice of investigating alerts when staff has the time is dangerous since every minute counts when a company's defenses have been compromised. In the event of a breach, it needs to be contained as quickly as possible, and this is not happening at most mid-market enterprises.

Consistent with security alerts being investigated when IT or security staff have time, 77 percent of security alerts are investigated after more than one hour. Containing a breach within minutes versus hours can make all the difference. For example, in the case of ransomware, once the malware begins the encryption process, it becomes a race against time to stop the encryption to contain the damage. It only takes 16 minutes to encrypt one thousand Microsoft Word documents, so every second matters.

Figure 8: What percentage of your organization's security alerts within the last three months have been investigated, and within what timeframe?

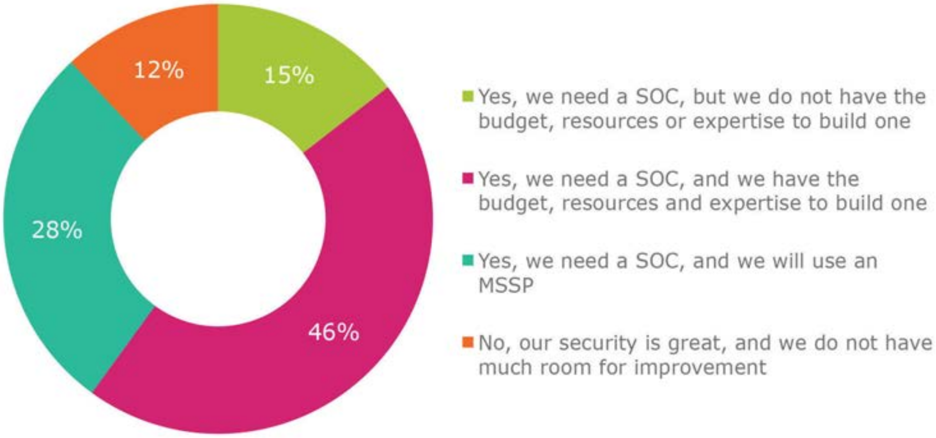


A more detailed look at the survey respondents' security operations show there is a significant gap between how IT and security professionals perceive their security posture and the reality of how secure they really are.

Security Operations Center Improves Cybersecurity

A security operations center (SOC) is the most essential element of modern security, but they are often viewed as very expensive and complicated. The Arctic Wolf survey found that a SOC was highly desired by survey respondents, but largely viewed as being outside of their budget. 88 percent of respondents believed that a SOC would be beneficial for their business, while 59 percent reported that a SOC was too expensive. The data showed that a SOC on average costs $1.4 million to establish, and the ongoing operational costs are also significant.

Figure 9: Would having a security operations center (SOC) with SIEM, threat feed subscriptions, three to four security engineers, log collection, machine learning, user behavior analytics, vulnerability scanning, and data security improve your organization's security?



About the Survey

Arctic Wolf recently conducted a study on "The State of Mid-Market Cybersecurity: 2017" in partnership with Vanson Bourne. The study revealed major gaps between the perception and reality of cybersecurity challenges. The survey found that mid-market companies had very high confidence in their cybersecurity defenses, but struggled to effectively defend against malicious activity that has become more sophisticated, targeted and severe.

The survey spoke with 200 cybersecurity IT decision makers from mid-market enterprises with 500–3000 employees across financial, healthcare, manufacturing, and IT service verticals. The data revealed a cybersecurity dissonance among mid-market enterprises, highlighting the disparity between what IT professionals believe versus the reality of their actual security posture.

About Arctic Wolf

Arctic Wolf Networks provides SOC-as-a-service that is redefining the economics of security. AWN CyberSOC is anchored by Concierge Security Engineers and includes 24x7 monitoring, custom alerting and incident investigation and response. There is no hardware or software to purchase, and the end-to-end service includes a proprietary cloud-based SIEM, threat intelligence subscriptions and all the expertise and tools required.

©2017 Arctic Wolf Networks, Inc. All rights reserved. Arctic Wolf Networks, AWN and the Arctic Wolf Networks logo are trademarks of Arctic Wolf Networks, Inc. in the United States and/or other jurisdictions. Other names used in this document are for identification purposes only and may be trademarks of their respective owners. (303-117)