

# Cybersecurity Challenges: Perception vs. Reality - blueAPACHE

Canonical: <https://www.blueapache.com/blog/cybersecurity-challenges-perception-vs-reality>

## Details:

Historical article: 29 March 2017. Research findings and market forecasts below describe the evidence discussed at publication.

New research from Vanson Bourne on the state of mid-market cybersecurity reveals major gaps between perception and reality of cybersecurity challenges. While mid-market enterprises expressed confidence in their cybersecurity defences, in reality, they struggled to defend against malicious activity that has become more sophisticated, targeted and severe. IT decision makers of mid-market organisations in the US said that they were confident their organisation's perimeter and endpoint security products can combat all cybersecurity threats. 90 percent of them also have dedicated IT staff focussing on security, further boosting the confidence that their cybersecurity posture is above average or great. The findings revealed a cybersecurity dissonance among mid-market enterprises, highlighting a disparity between perception and reality. Key findings demonstrated that:

IT and security professionals at midmarket companies have a broad set of responsibilities and are seldom dedicated solely to security.

Their expertise tends to be broad, rather than deep, and they do not have the specialized skills or knowledge required to deal with a complex, evolving threat environment.

Many small and mid-market enterprises have a false sense of security arising from the belief that their size makes them less attractive targets to cyber threats such as hackers, viruses, malware, and cybersecurity breaches. But in reality, almost two-thirds of all targeted attacks hit small and medium size businesses. Typically, small business security is easier to bypass, staff less educated on hacking and social engineering, and the overall risk is much lower. Small companies are increasingly targeted as a backdoor into companies with more robust systems. The disparity was also reinforced by 50 percent of respondents indicating that in the absence of dedicated personnel for day-to-day security operations, security alerts were investigated by IT/security staff when they had time. 77 percent of security alerts are investigated after more than one hour – a dangerous practice since every passing minute makes a security breach harder to contain and recover from.

## ***Comprehensive cybersecurity strategy***

Mid-market enterprises face the same cybersecurity issues as large enterprises with only a fraction of the budget and less-skilled personnel. Almost 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. The security needs of modern businesses have grown beyond their ability to cope efficiently. To combat the ever changing threat landscape, many organisations today outsource at least part of their security management whether that be through anti-virus software or firewalls. SECurity as a Service (SECaaS) is a growing market that is set to be worth \$US8.52b by 2020 . The 'as-a-service' model can mitigate the need for capital investment and dedicated specialist resources, offer easy scalability and agility and in many cases, be a more cost effective solution than managing your security requirements in-house. If you have concerns about your security posture, or would like to learn more about SECaaS, contact our team .

***What research does the blueAPACHE article 'Cybersecurity Challenges: Perception vs. Reality' discuss?***

We discuss new research from Vanson Bourne on the state of mid-market cybersecurity, which reveals major gaps between the perception and reality of cybersecurity challenges.

***What is the main disparity revealed by the Vanson Bourne research?***

The research found a cybersecurity dissonance among mid-market enterprises: while IT decision makers in the US expressed confidence that their organisation's perimeter and endpoint security products could combat all cybersecurity threats, in reality they struggled to defend against malicious activity that has become more sophisticated, targeted and severe.

***What percentage of mid-market organisations had dedicated IT staff focused on security, according to the research?***

90 percent of mid-market organisations had dedicated IT staff focussing on security, which boosted their confidence that their cybersecurity posture was above average or great.

***Why do IT and security professionals at midmarket companies struggle with complex threats?***

According to the findings, IT and security professionals at midmarket companies have a broad set of responsibilities and are seldom dedicated solely to security. Their expertise tends to be broad rather than deep, so they lack the specialized skills or knowledge required to deal with a complex, evolving threat environment.

***Do small and mid-market businesses face fewer cyber attacks because of their size?***

No. Many small and mid-market enterprises have a false sense of security believing their size makes them less attractive targets, but almost two-thirds of all targeted attacks actually hit small and medium size businesses. Small business security is typically easier to bypass, staff are less educated on hacking and social engineering, and overall risk controls are much lower, making small companies increasingly targeted as a backdoor into companies with more robust systems.

***How quickly are security alerts typically investigated at mid-market enterprises, and why is this a concern?***

50 percent of respondents indicated that in the absence of dedicated personnel for day-to-day security operations, security alerts were investigated by IT/security staff only when they had time. 77 percent of security alerts are investigated after more than one hour, which is a dangerous practice since every passing minute makes a security breach harder to contain and recover from.

***What challenge do mid-market enterprises face regarding cybersecurity complexity?***

Mid-market enterprises face the same cybersecurity issues as large enterprises but with only a fraction of the budget and less-skilled personnel. Almost 50 percent of respondents said that security is so complex they don't know where to start to improve their organization's security posture.

***What is SECaaS and how might it help mid-market enterprises?***

The 2017 article describes Security as a Service (SECaaS) and cites a forecast of US\$8.52 billion by 2020. It presents outsourcing as a way to access specialist resources and potentially reduce capital requirements; costs and benefits depend on the agreed service. The market figure is a historical forecast.

***What human and operational factors does the article identify?***

The 2017 article discusses staff with broad responsibilities, limited specialist security expertise and delays in investigating alerts. It argues for a comprehensive security strategy that addresses people and operations as well as technology.