2022

ESET SMB Digital Security Sentiment Report

CYBER RISKS DRIVING SMBs TO ENTERPRISE SOLUTIONS

Digital Security

Progress. Protected.

SCALING SECURITY:

Will SMBs bet on detection and response to get over the next hump in their security journey?

Michal Jankech
Vice President of SMB and MSP Segment

"In business, trouble often come in threes ... or even fours. Think of the Bermuda Triangle, Cerberus ... or the Four Horsemen of the Apocalypse. Whichever you subscribe to, if you are managing digital security at a small to mid-sized business, it is no surprise if trouble comes in the following triad: lack of head count, shortcomings in staff security maturity, and little understanding of one's own security liabilities and tech. These are issues that track to budget and resources. And that pesky fourth problem? Major business impacts vectoring from social, political, and economic conditions."

SCALING SECURITY:

Prior to the COVID-19 pandemic, the tech, retail, telecoms, and even the IT security sectors seemed to hum along, growing well even if not predictably. Beneath that growth, digitalization was moving along quietly. New forms of commerce, communication, services, and products had taken root, but little seemed to show digitalization's full scale and promise. COVID-19 hit the replay button on digitalization. A rush followed to increase productivity and streamline processes, all while a vast army of employees figured out how to work remotely via cloud-based collaboration platforms from Zoom to Microsoft Teams – the no longer quiet work of digitalization became revitalized.

IT budgets ebbed and swelled, transforming how we work, trade, and shop. In parallel, the business case to get serious about protection seemed to trigger a new trend among small and medium-sized businesses (SMBs) to consider both cloud office security and even the more advanced detection and response technology. Certainly, the years from 2020 to 2022 supplied plenty of motivation – consider the Kaseya, Microsoft Exchange, and Emotet attacks, as well as the many web-based attacks, that joined existing concerns around ransomware.

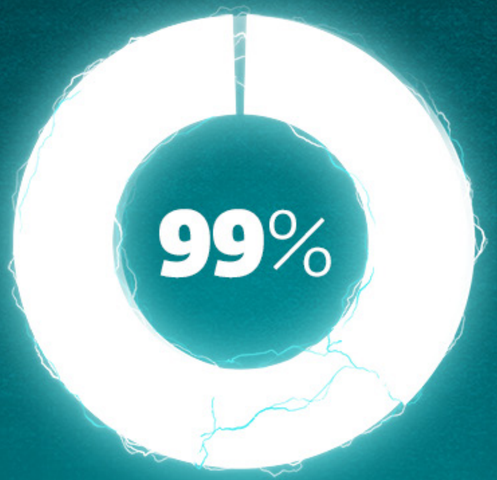
SCALING SECURITY:

Current times have complicated matters further, even beyond the notorious hiring crunch, the chip shortage, and the Great Resignation – they have brought the war in Ukraine to global headlines, with European correspondents citing it as an additional vector for cyberattacks. Front and center in the reporting are threats aimed at business disruption as much as the achievement of nation-state goals.

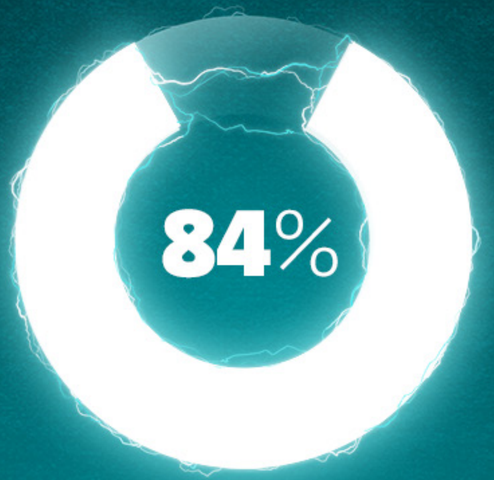
While all businesses face these and a diversity of other security challenges, by and large, SMBs must try to address them from the position of an underdog. This might be seen as reflecting the expected agile and entrepreneurial spirit of an SMB, yet glimpses of the volatile post-COVID-19 economy have increased the need for digital security that is fit for purpose and is scalable.

The 2022 SMB Cybersecurity Survey explores the sentiment of SMBs at this juncture of human resources, technical maturity, and financial stress. Let's review how these events and security developments have reshaped the cybersecurity sentiment we discovered in our survey of SMBs in 2022.

SMBs ARE THE BACKBONE OF THE GLOBAL ECONOMY



of all companies in Europe and North America are SMBs



of SMBs **believe in tech advancements** enabling their growth

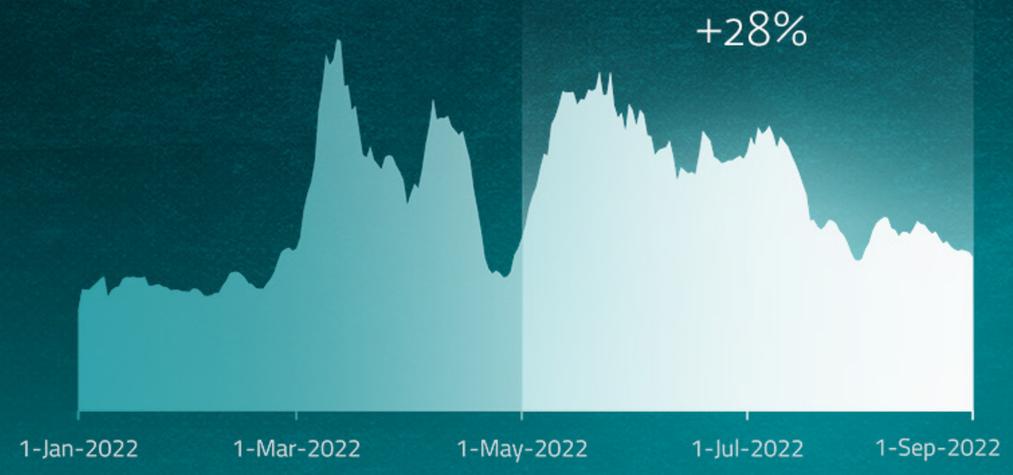
SMBs FACE CHALLENGES PROTECTING THEIR BUSINESSES AS REPORTED IN ESET's LATEST THREAT REPORTS

20% increase in threat detections

of SMBs believe that **cyber warfare is a very real threat** that can impact everyone

SMBs ENCOUNTER A RISE IN WEB AND EMAIL THREATS

Some of the most notorious attack vectors for malware delivery are the web and email. SMBs can prioritize future security efforts to protect their business collaboration tools and applications.



28% increase in web threats

66% increase in Outlook login phishing forms sent via email

CYBERSECURITY SENTIMENT AMONG SMBs

SMBs see many cybersecurity risks and threats but lack confidence in their capability to handle it all. The greatest fear centers around employees encountering malware especially via web-based attacks, although ransomware attacks and third-party security issues are close runners-up.

Top cybersecurity concerns in the next 12 months

CYBERSECURITY SENTIMENT AMONG SMBs

What is fueling these concerns? It might be surprising that SMBs see the lack of cyber awareness among their employees as the leading cause. This is even ahead of such factors as knock-on effects from the war in Ukraine and continuing remote work arrangements post COVID-19. Both of these have triggered an increase in cybersecurity investment at many SMBs – does this indicate that "cybersecurity has already been taken care of" and thus perceived as less important to cyber awareness?

TOP 5 factors increasing the risk of a cyberattack according to SMBs:

43%
Lack of employee **cyber awareness**

37%
Nation-state attacks due to conflict in Ukraine

34%
Vulnerabilities in the **partner / supplier ecosystem**

32%
Continued hybrid or **home working**

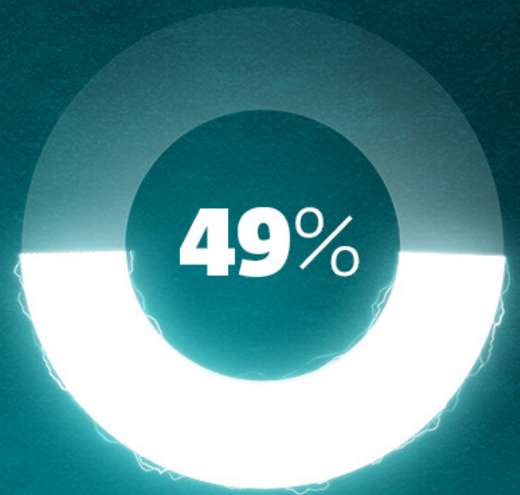
31%
Use of **Remote Desktop Protocol**

CYBERSECURITY SENTIMENT AMONG SMBs

In any case, SMBs see there is more to do. The key challenges right now are keeping up with the latest cybersecurity threats and the security technology to counter them. But overcoming these challenges requires budget – a challenge of its own.

How will businesses prioritize their budget with the economic shifts following COVID-19 and an ongoing war in Europe? Perhaps you are familiar with the proverb that the squeaky wheel gets the grease.

Cyber risk is like a squeaky wheel. Even if you don't want to invest in improved cyberdefenses, an undesired spate of cyberattacks could disrupt your budget plans.

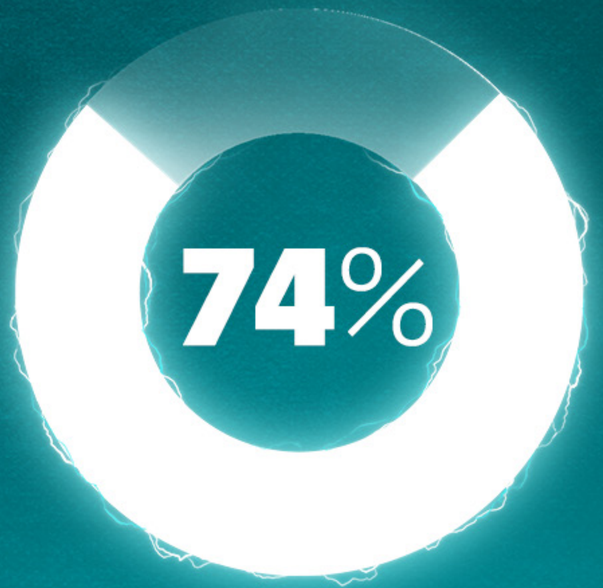


Budget limitations / lack of investment in cybersecurity are among the top three cybersecurity challenges within SMBs' IT departments

SMBs ALSO FEEL MORE VULNERABLE THAN ENTERPRISES...

And if, among the gamut of businesses, SMBs typically believe that their size makes them more vulnerable to cyberattacks than enterprises, that means they hear the squeaky wheel of cyber risk louder.

74% of SMBs believe that businesses of their size are more vulnerable to cyberattacks than enterprises.



SMBs ALSO FEEL MORE VULNERABLE THAN ENTERPRISES...

In particular, SMBs see the highest risks in incidents that lead to the loss of data or grave financial impacts. This assessment of risk seems well justified. In the past year, two-thirds of SMBs experienced a data security incident that, in most cases, took up to three months to investigate, costing SMBs significantly. Organizations' total estimated costs after suffering a breach were at a mean of nearly €220,000 – no small sum to shrug off.

SMBs top concerns over the business implications of a cyberattack

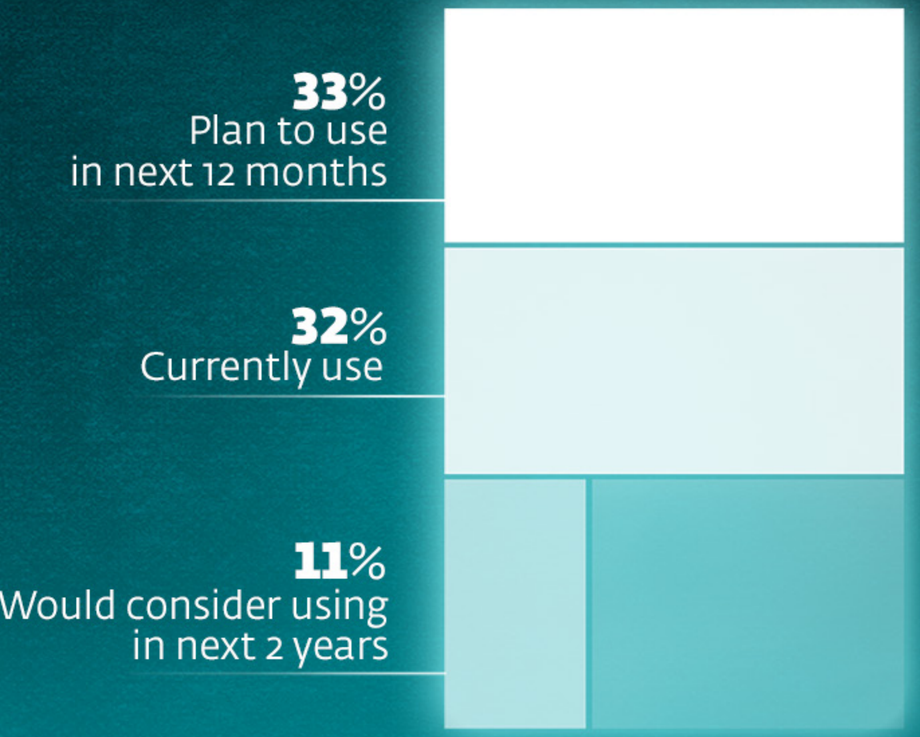
1% Have no concerns

A GROWING HUNGER?

The typical response following such incidents is to invest in training for the IT team, which is no surprise considering that the low level of employee cyber awareness is the principal driver of SMBs' concerns. But many SMBs also respond by conducting an audit or purchasing new cybersecurity tools.

What is shocking is the huge appetite for detection and response tools. These are traditionally used only by enterprises to gain deep visibility into their networks and to determine the root cause of cyber incidents. Having such a capability at an SMB would directly address the challenge of confronting the latest cybersecurity threats with an innovative enterprise-grade tool.

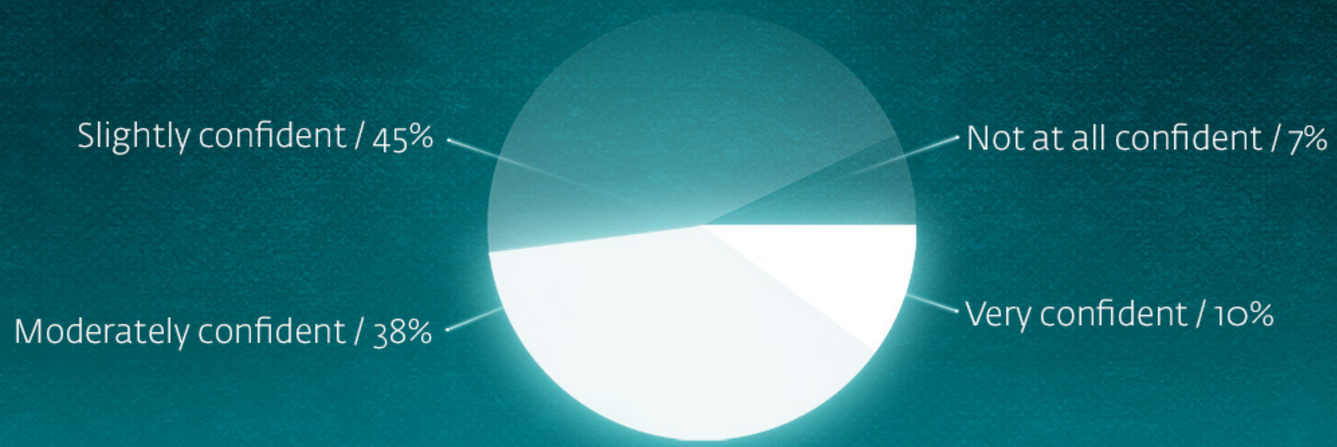
Usage of EDR / XDR / MDR solutions



A GROWING HUNGER?

Unsurprisingly, less than half of SMBs expressed moderate to high confidence in their cyber resilience. This reflects concerns over internal cybersecurity knowledge, access to third-party experts, and poor incident response times among other issues.

Overall confidence in cyber resilience for the next 12 months remains low



Only **48%** of SMBs claimed to be moderately / very confident in their cyber resilience

A GROWING HUNGER?

However, when asked about complex IT security processes like threat forensics, 71% projected high confidence while only 32% of respondents indicated use of endpoint detection and response products. This contrast suggests either overconfidence or the need for improved understanding of what the journey to detection and response provides.

SMBs feel most confident in the following areas:

32%
Secure in their IT team's cybersecurity **knowledge**

30%
Speed with which they can identify, isolate, and respond to a threat

27%
Threat **forensics** capability

A GROWING HUNGER?

It's almost a chicken-and-egg scenario. SMBs recognize the value of threat forensics and indeed think they are able to leverage detection and response. At the same time, actual use of these tools by SMBs is relatively low and requires a sufficiently high level of security maturity by IT teams and a commitment to invest that many SMBs simply haven't shown.

Ultimately, the benchmarking provided by the ESET 2022 SMB Cybersecurity Survey reveals the need for an effective cybersecurity strategy, one that can close gaps and deliver improved cyber resilience. When this journey includes intelligent and scaled use of endpoint detection and response, your business can raise its confidence and return focus to core competencies, growth, and innovation. We hope the report has prompted many important questions and has helped you better determine your appetite for the journey.

ESET partnered with the independent UK-based research company Insight Avenue to conduct the survey for the ESET 2022 SMB Digital Security Sentiment Report by targeting 1,212 IT security decision-makers in the UK, the US, Canada, France, Germany, Spain, Italy, Poland, Sweden, the Czech Republic, the Netherlands, Denmark, Norway, and Finland. The respondents represent businesses ranging in size from 25 to 500 employees and with varying IT security maturity and budgets.

Digital Security
Progress. Protected.

For media inquiries, please contact
your local PR representative.